



Rocket® z/Assurance™ for Mainframe Security

Continuous assurance that your
IBM Z® security is proven, compliant
and modernization ready.



Contents

- 3** Introduction
- 4** Mainframe risk now has enterprise-wide impact
- 5** From security controls to risk assurance
- 6** What is Rocket z/Assurance?
- 7** Rocket z/Assurance Solutions overview
- 8** Why do organizations choose Rocket z/Assurance?
- 9** Risk questions Rocket z/Assurance helps answer
- 10** Getting started
- 11** Talk to a Rocket mainframe security expert

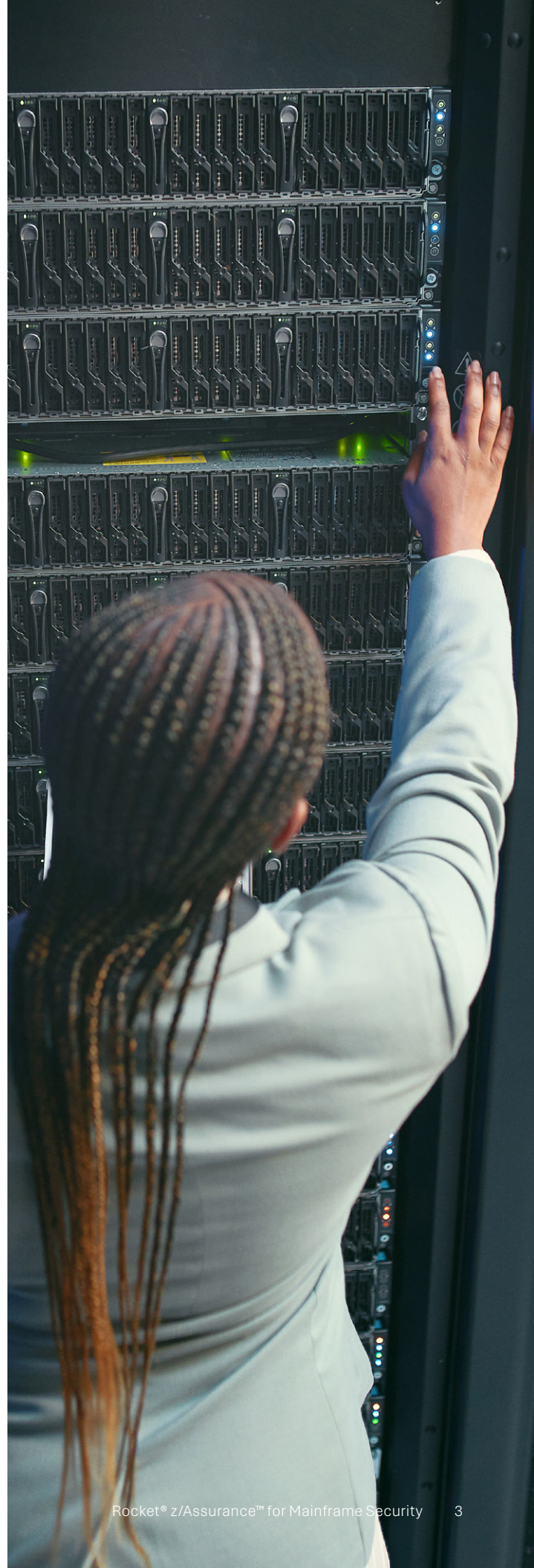


Introduction

Your IBM Z environment runs the business: high-value transactions, regulated data, customer trust, and operations that cannot afford disruption. But as threats accelerate, regulations expand, and modernization opens new pathways into critical systems, security controls alone are no longer enough.

Rocket z/Assurance for Mainframe Security (Rocket z/Assurance) helps you continuously identify, validate, prioritize, and demonstrate that IBM Z risk is under control. It unifies mainframe-specific risk discovery, control validation and remediation prioritization, and executive reporting to help organizations continuously assess and reduce IBM Z exposure. By bringing software, services, and deep mainframe expertise together, Rocket z/Assurance helps security, compliance, and technology leaders demonstrate that critical mainframe systems are protected, compliant, and ready to modernize securely.

Unlike point security tools that focus on isolated controls, Rocket z/Assurance delivers continuous risk assurance for IBM Z by connecting vulnerabilities, controls, patch status, compliance posture, and executive reporting into a single framework.



Mainframe risk now has enterprise-wide impact

IBM Z remains central to the business, yet many organizations lack the same level of continuous visibility, governance, and evidence for IBM Z that they apply across distributed, cloud, and hybrid environments. This can create blind spots around critical data, control effectiveness, remediation progress, and business risk.

01

Security gaps are harder to quantify

Hidden vulnerabilities, configuration drift, patch gaps, and emerging threats can leave exploitable exposure inside mission-critical environments.

04

Modernization introduces new challenges

AI, APIs, open source, and hybrid integration can create new exposure if governance and control validation fail to keep pace.

02

Compliance expectations are growing

DORA, PCI DSS, cyber-resilience mandates, and audit requirements increasingly demand evidence that controls are effective, not simply documented.

05

Board and regulatory scrutiny is increasing

Leaders need defensible answers about residual risk, control effectiveness, remediation progress, and business impact.

03

Operational resilience is under pressure

Ransomware, integrity vulnerabilities, and modernization complexity raise the potential for disruption to critical services.

The question is no longer,

“Do we have security tools?”

It's now,

“Can we prove our mainframe risk is known, managed, and continuously reduced?”



From security controls to risk assurance

Security controls are essential. They protect systems and data through access controls, encryption, monitoring, authentication, vulnerability management, patching, and incident response. But controls alone do not answer the questions that risk leaders, auditors, regulators, and boards are asking.

Questions being asked

01

Which IBM Z risks are real, exploitable, and business-relevant?

02

Which controls are working, and where are they drifting?

03

Which patches are missing, and how long has exposure existed?

04

Which findings require immediate remediation?

05

Can we produce audit-ready evidence without a manual scramble?

06

Can we modernize without increasing residual risk?

Rocket z/Assurance provides the validation layer that connects technical security activity to enterprise risk outcomes through compliance assessments, vulnerability analysis, security audits, patch assurance, cyber resilience validation, and continuous monitoring. It helps organizations move from assumed protection to continuous, evidence-backed assurance.



What is Rocket z/Assurance?

Rocket z/Assurance is Rocket Software's integrated portfolio for managing IBM Z risk, compliance, vulnerabilities, operational resilience, and cyber assurance. Its products and services work together within a unified framework for continuous mainframe risk assurance. Together, these capabilities help security, risk, and IT teams protect critical systems, prove critical systems are secure, compliant, and modernization-ready.

Protect

Continuously strengthen security posture across critical IBM Z environments.

01

Prove

Demonstrate compliance, control effectiveness, and audit readiness.

02

Remediate

Prioritize vulnerabilities and patch risk with platform-specific precision.

03

Modernize Securely

Adopt AI, hybrid integration, and modernization initiatives with confidence.

04



Rocket z/Assurance Solutions overview

SOLUTIONS

Rocket® z/Assure® Vulnerability Analysis Program (VAP)



- Identifies code-level vulnerabilities and integrity exposures that traditional configuration scans may miss, helping teams reduce exploitable mainframe risk.

NEW

Rocket® z/Assure® Compliance



- Automates security policy adherence and control validation to reduce audit scramble and strengthen defensible compliance evidence.

NEW

Rocket® z/Assure® Patch



- Provides visibility into missing security patches and patch exposure, helping organizations evidence current protection and reduce known vulnerability risk.

NEW

Rocket® z/Assure® Quantum



- Enables visibility into cryptographic exposure across IBM Z, helping security teams reduce future risk and prepare for quantum readiness.

NEW

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



- Provides continuous monitoring of IBM Z environments for exploit conditions and emerging exposures, helping organizations stay ahead of security risks.

COMING
2026

Agentic AI



- Accelerates analysis, remediation guidance, and prioritization through natural-language interactions.

Services



- Security Assessments (RACF®, Db2®, and IBM® CICS® sub-system reviews by Rocket experts, mainframe penetration testing, security conversions (from TSS or ACF2 to RACF), and 24/7 Rocket mainframe security expertise).



Why do organizations choose Rocket z/Assurance?

01

Continuous assurance

Rocket z/Assurance gives you confidence that your security controls are effective and your compliance requirements are met. Real-time risk visibility and 24/7 mainframe security expertise keep your systems resilient and make audit and board conversations easier to support.

02

Precision expertise

Benefit from direct access to Rocket's in-house IBM Z security experts, delivering trusted guidance that helps you focus on real exposures, not false positives.

03

Secure modernization

Adopt AI, open source, and hybrid architectures while maintaining strong security, governance, and compliance at every step, protecting your most critical asset, the mainframe, at the core.

Business outcomes

Rocket z/Assurance helps organizations achieve measurable security, compliance, resilience, and modernization outcomes across IBM Z.



Reduce enterprise risk:

Identify and prioritize exploitable IBM Z vulnerabilities before they become incidents, audit findings, or business disruptions.



Demonstrate continuous compliance readiness:

Continuously validate controls and produce clearer evidence for regulatory and audit requirements.



Reduce operational disruption risk:

Strengthen the security, compliance, recoverability, and change readiness of mission-critical systems.



Accelerate secure modernization:

Support innovation while maintaining trust, governance, and risk discipline across IBM Z.



Speed executive decision-making:

Translate IBM Z technical findings into business risk language that executives, auditors, regulators, and boards can understand.



Reduce complexity:

Bring software, services, assessments, and mainframe expertise together through a single trusted partner and assurance portfolio.



Risk questions Rocket z/Assurance helps answer

For CISOs

Can I defend the organization's
IBM Z® risk posture with
current, credible evidence?

01

For Risk and Compliance Leaders

Can we prove control effectiveness
and audit readiness without a
manual evidence scramble?

02

For Mainframe Security and Platform Leaders

Can we identify, prioritize, and remediate the
mainframe risks that matter most?

03

For CIOs and Modernization Leaders

Can we modernize critical systems without weakening
governance, resilience, or compliance?

04



Getting started

Wherever you are on your IBM Z risk journey, Rocket z/Assurance provides a practical starting point based on your most urgent business need:

01

If audit or regulatory pressure is increasing

Start with compliance validation and control evidence.

02

If IBM Z visibility is limited

Begin with a security assessment, and executive risk reporting.

03

If patching and vulnerability prioritization are difficult

Assess exposure with z/Assure VAP (identifies code-level and integrity exposures), z/Assure Patch (provides visibility into missing security patches), and z/Assure CVM (monitors emerging exposure as the environment changes).

04

If modernization is underway

Build assurance into AI, API, open-source, and hybrid initiatives from the start.

05

If quantum readiness is on the roadmap

Start with cryptographic inventory and risk analysis through z/Assure Quantum.

The bottom line

Security implements controls.

Assurance proves risk is being managed.

Rocket z/Assurance helps organizations continuously reduce IBM Z risk, validate compliance, strengthen resilience, and modernize with confidence, backed by Rocket Software's deep mainframe security expertise.



Talk to a Rocket mainframe security expert

Ready to understand, prioritize, and prove your IBM Z risk posture? Connect with a Rocket expert about how Rocket zAssurance can help you move from assumed protection to continuous, defensible risk assurance.

Talk 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.



Modernization.
Without Disruption.™

Visit RocketSoftware.com

©2026 Rocket Software, Inc. or its affiliates.

Rocket and the Rocket Software logos are registered trademarks of Rocket Software, Inc. Other product and company names may be trademarks™ or registered® trademarks of Rocket Software or its affiliates or their respective owners. Use of third-party trademarks does not imply any affiliation with, endorsement by, or association with Rocket Software.

© IBM Z, z/OS, z/VM, CICS, RACF and Db2 are trademarks of International Business Machines Corporation.

MAR-18877_Broch_vAssuranceSolution_V3

