Rocket® software

Modernizing for Compliance, Risk, Security, and Identity Governance

From blind spots to provable control

Executive intro

Your mainframe is the **mission-critical operating system** that keeps an organization's most essential financial and operational systems running — securely, reliably, with data integrity and without interruption. It provides the data to the business's most critical operations: z/OS® supports core revenue, payment, settlement, and regulatory systems. An integrity failure can directly threaten business continuity, customer trust, and financial stability.

For years, leaders assumed it was safe simply because it was surrounded by a moat called a firewall. In today's hybrid environment, that assumption no longer holds.

The mainframe now connects to cloud analytics, modern APIs, and open systems, which expands the attack surface. At the same time, AI has collapsed the time it takes to find and exploit vulnerabilities, even for attackers without deep mainframe expertise. CIOs and risk leaders tell us they're being asked to do more than define a single security framework. They need to prove control, integrity, resilience, and audit readiness across cloud, open systems, and the mainframe alike. This brief lays out how executives are thinking about this priority, and how Rocket® Software helps you strengthen security and risk mitigation without disrupting the systems that run your business.

Who it's for

This brief is written for CIOs, CISOs, CROs, and senior risk leaders at large multi-national organizations, especially in highly regulated industries such as banking, insurance, defense and healthcare. If you're accountable for security governance, regulatory compliance, and defensible oversight across a hybrid estate, this is for you.

The top challenges leaders face

The "isolated mainframe" myth.
The idea that the mainframe is a sealed fortress is now a dangerous assumption. As you offload data, connect to cloud, and integrate APIs, the green screen is no longer the only attack surface.

AI-accelerated threats.
Advanced models can analyze decades of obscure source code, correlate patterns, and uncover exploitable conditions in minutes rather than months. Vulnerabilities can be weaponized at machine speed.

Visibility gaps where risk lives.
Open-source and AI-based tools like Mythos have surfaced valuable risk signals, but they can't see inside assembled, proprietary mainframe code, closed-source vendor software, or runtime behavior in production, exactly where many highly critical risks hide.

Privileged access and identity risk.
A single compromised credential can unravel your posture. Dormant accounts, overly broad permissions, and policy drift across RACF, CA ACF2, and CA Top Secret create openings that attackers will exploit at scale.

Proving control, not just claiming it.
Regulators and auditors increasingly want evidence, not intentions. Without visibility into what's actually occurring in production, governance becomes hard to enforce and even harder to prove.

Top priorities leaders are setting

- Treat the mainframe as integral to enterprise security strategy, not separate from it.
- Move from theoretical risk to provable control with continuous, defensible evidence.
- Extend vulnerability management into assembled code and runtime behavior, not just source and dependencies.
- Tighten identity governance: enforce least-privilege, clean up dormant IDs, and strengthen MFA.
- Stay ahead of mandates like DORA, GDPR, PCI DSS, and SOX with audit-ready reporting.
- Strengthen recovery readiness so the business can withstand disruption and demonstrate resilience.

How Rocket Assurance helps: the solution

Rocket Software partners with you to modernize security in place, meeting you wherever you are on your journey. The goal is straightforward: turn blind spots into reportable controls, without disrupting operations.

01 **See where impactful risk actually lives.** Rocket® z/Assure® VAP provides precise, actionable insight into vulnerabilities that reside in assembled code and production environments, with a false-positive rate of just 0.08%, the most precise vulnerability scanning technology on the market. Every assessment Rocket has run has uncovered vulnerabilities, a clear signal that no environment is risk-free.

02 **Operationalize risk reduction.** Rocket helps teams move from theoretical risk to practical action: prioritizing what needs fixing, tracking progress, automating patch validation, and governing posture over time. Rocket® Security Patch Auditor verifies that required security patches for known vulnerabilities are correctly identified and installed across mainframe environments.

03 **Support audit-ready compliance.** Pre-configured compliance reporting and continuous evidence collection help your risk and assurance teams demonstrate control to auditors and regulators across frameworks like DORA, GDPR, PCI DSS, and SOX. Rocket® Continuous Vulnerability Monitor ensures real-time monitoring of production mainframe systems to identify indicators of configuration-based vulnerabilities.

04 **Strengthen identity governance and secure access.** Rocket supports tighter access reviews, least-privilege enforcement, and secure host access (such as Rocket® Secure Host Access) that integrates with your identity and access management, helping you close the gaps attacker's target.

05 **Improve recovery readiness.** Rocket® Rapid Data Recovery can address ransomware and recover specific datasets in hours rather than days, supporting demanding recovery targets and resilience requirements.

Why this approach works

Modernizing in place protects the reliability you already trust while extending modern security, monitoring, and recovery into the platform. You don't have to choose between resilience and progress. Your modernization journey today builds the foundation for protecting the data your business depends on tomorrow. The evidence underscores the urgency: more than 91% of mainframe organizations have experienced a security compromise in the past five years, yet only 28% of IT leaders feel extremely confident in their response to mainframe vulnerabilities.

Decision-maker takeaway:
This approach reduces enterprise risk, supports compliance, and gives you defensible evidence of control, directly supporting the oversight you're accountable for.

Requirements and considerations

- Inventory your mainframe attack surface, including cloud connections, APIs, and offloaded data.
- Catalog your cryptographic landscape so you can plan for emerging risks, including quantum, without rip-and-replace.
- Map current privileged accounts and identity controls before tightening least-privilege.
- Define the evidence your auditors and regulators expect, then automate its collection.

Next step

See how Rocket Software can help you move from blind spots to provable control, without disrupting the systems your business depends on. Schedule a working session with our team to map your compliance, risk, and security priorities to a practical, low-risk plan.

Talk to an expert

Compliance, risk, and security checklist

Use this as a quick readiness check for security modernization:

- We treat the mainframe as part of our enterprise security strategy, not a separate silo.
- Vulnerability scanning covers compiled code and runtime behavior, not just source.
- Patch validation, reporting, and audit trails are automated.
- Privileged access is reviewed regularly, with dormant accounts removed.
- Least-privilege and MFA are enforced across RACF, ACF2, and Top Secret.
- Compliance reporting maps to DORA, GDPR, PCI DSS, and SOX.
- Continuous evidence collection supports audit and assurance teams.
- Recovery can target specific datasets quickly, including ransomware scenarios.
- Our cryptographic landscape is cataloged with a phased plan for quantum-safe readiness.
- Risk is operationalized: prioritized, tracked, and governed over time.

Rocket® software

Modernization. **Without Disruption.**™

Visit RocketSoftware.com

MAR-18415_Broch_MFRiskAndCompliance_V3