Rocket® software

Security Confidence Isn't Security Readiness:

What security leaders must do after AI reveals hidden risk in the mainframe

A guide for security and compliance leaders on closing the gap between believing systems are secure and proving they are.

Contents

Executive summary

For years, many organizations operated under a comfortable assumption: their existing controls provided sufficient protection for the mainframe. The platform was proven. The perimeter was familiar. And the risk, most believed, was well understood. Then Mythos changed the conversation.

AI-assisted vulnerability discovery showed that long-standing vulnerabilities can remain hidden for decades before anyone exposes them. But vulnerability discovery is only one piece of a much larger challenge.

New compliance and security research reveals a striking contradiction. Organizations remain highly confident in their security posture (99% believe their approach aligns with best practices), yet they continue to experience audit findings, extensive remediation projects, and significant compliance costs. That gap between confidence and outcomes is the heart of this paper.

The question facing security leaders is no longer whether they can identify vulnerabilities. The harder question is this: Can we continuously manage, monitor, and prove control over risk across the mainframe environment?

This paper explores how your organization can make the shift from vulnerability awareness to security readiness and why that shift now defines defensible mainframe security.

Mythos was a wake-up call, not the whole story

Mythos didn’t create risk. It revealed risk that already existed.

For decades, mainframe security rested quietly on an idea that felt reassuring: the platform was too complex, too specialized, and too obscure for attackers to exploit. Compromising it required deep institutional knowledge, privileged access, and time. That combination felt like protection.

Mythos challenged that thinking directly. By demonstrating how AI-assisted discovery can uncover open-source threats that signal risk to the mainframe ecosystem, it forced a difficult realization at the executive level. The mainframe can no longer be treated as opaque simply because it is specialized. Mythos did not look inside assembled mainframe binaries, closed-source vendor software, or production runtime behavior. It showed that risk signals around the ecosystem can surface faster than many organizations expected, and that those signals deserve a stronger operational response.

Why mythos changed executive perceptions

Boards and risk leaders had long treated the mainframe as a settled matter. Mythos reframed it as an open question. When a discovery method can reveal open-source threats that went unnoticed for years, leaders must ask where similar indicators of risk may exist across the mainframe ecosystem. That's a governance concern, not just a technical one.

How AI has accelerated vulnerability discovery

AI has accelerated how quickly risk signals can be discovered and connected. What once required highly specialized manual analysis can increasingly be surfaced through automated pattern recognition, especially in open-source components and related ecosystem dependencies. The barrier to discovery is falling, and the pace of security response must rise with it.

The end of "security through obscurity"

Obscurity was never a control. It was an assumption. AI has retired that assumption for good. Attackers no longer need decades of mainframe expertise to find exploitable conditions. They can let a model correlate obscure code patterns and surface weaknesses at machine speed.

Why security teams are reevaluating assumptions

The result is a healthy reexamination across the industry. Teams that once trusted point-in-time reviews and perimeter defenses now recognize those measures address only part of the picture. The mainframe ecosystem is part of the modern threat surface, and it deserves the same rigor applied to cloud and distributed systems.

The discovery of a vulnerability is important. But finding risk does not reduce risk. Awareness is a starting point, not a solution.

Why visibility alone doesn't improve security

Many organizations can identify vulnerabilities. Fewer can consistently manage them.

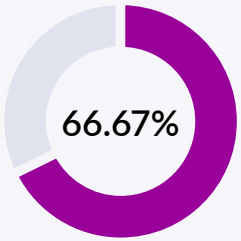
Discovery gets the attention, but it's the easy part. The hard, ongoing work begins after you find the vulnerability: when you have to prioritize it, remediate it, validate the fix, and prove to an auditor that your controls actually work. That's where confidence and readiness part ways.

The difference between visibility and control

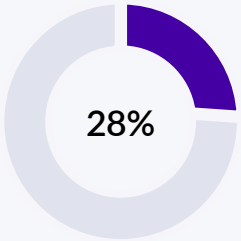
Visibility tells you what exists. Control tells you what you're doing about it, consistently and continuously. A scan that reveals 100 issues has value. But value turns into risk reduction only when you triage those issues, resolve the ones that matter most, and confirm they stay resolved. Visibility without control is a to-do list, not a security program.

Why auditors care about controls, not assumptions

Auditors don't accept confidence as evidence. They want to see that controls exist, function as intended, and produce a verifiable record. "We believe our systems are secure" carries no weight in an audit. "Here is continuous evidence that our controls are working" does. The distinction shapes every audit outcome.



Two-thirds of organizations spent $500,000 or more on user access remediation over the past two years.



28% spent $1 million or more on user access remediation over the past two years.

The growing operational burden of proving compliance

Proving compliance has become a heavy, recurring cost. Remediation consumes teams and time. Privileged access issues alone often require groups of six to 10 employees and 41 to 80 total hours to resolve. Closing a single compliance finding takes four weeks or longer at 73% of organizations. Two-thirds of organizations spent $500,000 or more on user access remediation over the past two years, and 28% spent $1 million or more. These aren't rare events. They're the ongoing tax of reactive security.

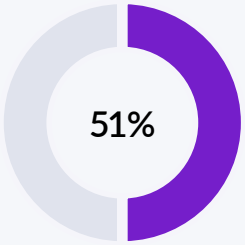
Why reactive security programs struggle

Reactive programs are always a step behind. They respond to findings after auditors surface them, scramble to assemble evidence at review time, and treat security as a series of point-in-time snapshots. In an environment where AI accelerates discovery, that cadence can't keep pace. The gap between "we passed last year's audit" and "we can prove control today" keeps widening.

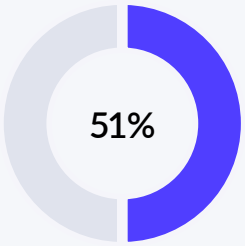
Closing a single compliance finding takes four weeks or longer at 73% of organizations.

Hanover Insight

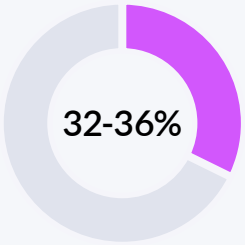
Security confidence remains high. Yet organizations continue to face:



Audit findings: 51% have experienced findings tied to insufficient access logging and monitoring.



Remediation activities: 51% required remediation following an audit. Compliance costs: Two-thirds spent $500,000 or more on access remediation in two years.



Security gaps: Only 32% have implemented single sign-on, and 36% use passwordless or certificate-based authentication.

The challenge isn't discovering vulnerabilities. It's operationalizing security after discovery.

The blind spots AI still doesn't solve

AI can expose risk. It can't replace governance, monitoring, or compliance controls.

AI is a powerful discovery engine. But discovery is where its usefulness ends and your program's discipline begins. Four blind spots remain, and each demands sustained operational capability rather than a one-time revelation. That is where Rocket Assurance fits: as a unified approach to mainframe security, compliance, vulnerability management, and cyber-risk solutions that helps organizations move from security activity to continuous assurance.

Finding a vulnerability is the beginning of a lifecycle, not the end of one. Security leaders need to manage risk continuously across the mainframe's compiled binaries, configurations, and runtime, not just its source code.

The questions security leaders are asking:

- What vulnerabilities exist today?
- Which ones pose the greatest risk?
- Which remain unresolved?

Answering these consistently requires code-based and configuration-based vulnerability management purpose-built for the mainframe. **Rocket® z/Assure® Vulnerability Analysis Program (VAP)** delivers exactly that, looking inside assembled binaries and active runtime where the most serious risks hide. With a false positive rate of just 0.08%, security teams can focus on true threats rather than chasing noise.

Privileged access and identity risk

A single compromised credential can unravel an entire security posture. AI-driven attackers excel at exploiting dormant accounts and orchestrating credential abuse at scale, which makes identity governance a constant priority rather than a periodic review.

The questions security leaders are asking:

- Who has elevated access?
- Should they?
- How is privileged activity monitored?

These questions point directly to the need for strong access governance across RACF, ACF2, and Top Secret, with tight least-privilege enforcement and active monitoring of privileged sessions. Rocket® Secure Host Access (SHA) integrates host access with your enterprise identity and access management (IAM) strategy, including multi-factor authentication (MFA) and single sign-on (SSO), to achieve genuine, phishing-resistant defense in depth. The 2025 Forrester TEI Study found that SHA delivers a 30% improvement in security posture and $921,000 in help desk savings over three years.

Compliance and audit readiness

Regulators expect proof, not promises. Frameworks like DORA, PCI DSS, and NYDFS raise the bar on evidence, and manual, point-in-time snapshots no longer satisfy that expectation.

The questions security leaders are asking:

- Can we prove controls are working?
- Can we provide evidence quickly?
- Are we continuously compliant?

Rocket's Mainframe Security Services include compliance assessments that verify your mainframe security settings align with corporate policy, identify gaps, and provide the foundation for a scalable, auditable risk management program. These services reduce manual effort and give security leaders clear, defensible evidence when regulators come knocking.

Continuous monitoring and change detection

Risk isn't static, and neither is your environment. Configurations drift, code changes, and new integrations expand the attack surface daily. Without continuous monitoring, you can't tell whether your posture is improving or quietly deteriorating.

The questions security leaders are asking:

- What changed yesterday?
- What changed today?
- Is our risk posture improving or deteriorating?

Rocket's integrity assessment services shine a light deep into mainframe code to detect unauthorized change. Combined with VAP's continuous scanning, security teams can catch suspicious activity early, before it escalates and before forensic evidence disappears.

What security-ready organizations do differently

Leading organizations focus on continuous assurance rather than point-in-time assessments.

The organizations pulling ahead share a mindset. They treat security as an ongoing practice of proof, not a periodic exercise in reassurance. Four behaviors set them apart.

01

Continuous vulnerability visibility

They move from annual reviews to ongoing monitoring. Instead of assessing risk once a year and hoping nothing shifts in between, they maintain a live understanding of where vulnerabilities exist and how urgent each one is. Discovery becomes a continuous stream, not a scheduled event.

02

Continuous control validation

They verify that policies remain effective over time. A control that worked at implementation can erode through configuration drift or new integrations. Security-ready organizations test continuously, confirming that their controls still do what they were designed to do today, not just at the last audit.

03

Unified security and compliance operations

They reduce silos between functions. When security, compliance, audit, and mainframe operations work from a shared view of risk, evidence flows naturally and gaps close faster. High-readiness organizations reflect this in their cadence. 57% formally review access controls at least quarterly as part of broader security initiatives. Clear ownership matters too: cybersecurity teams hold primary accountability for mainframe access compliance at 50% of organizations.

04

They replace assumptions with measurable proof. Rather than asserting that systems are secure, they generate auditable evidence that demonstrates it. This shift from belief to proof is what turns high confidence into genuine readiness and satisfies the scrutiny of auditors and regulators alike.

The mainframe security readiness framework

The behaviors above come together in a practical, repeatable model. This framework gives you a structure for moving from confidence to readiness across five reinforcing pillars.

It also reflects the Rocket Assurance brand promise: security and risk management are what organizations do; assurance is the continuous evidence that those efforts are working. Use it to self-assess, identify gaps, and prioritize where to strengthen your program.

Identify Risk

Know where vulnerabilities exist. Maintain continuous, deep visibility into code-based and configuration-based vulnerabilities across the mainframe, including compiled binaries and runtime behavior. Prioritize findings by severity and business impact so your teams focus where risk is greatest.

Control Access

Protect critical systems and data. Enforce least-privilege access, eliminate dormant credentials, and integrate mainframe identity with enterprise identity systems. Strong access governance closes the blind spots that AI-driven attackers work hardest to exploit.

Monitor Continuously

Track changes and emerging threats. Watch code, configuration, and runtime for change as it happens. Continuous monitoring lets you detect suspicious activity early, before it escalates and before forensic evidence disappears.

Prove Compliance

Generate auditable evidence. Automate continuous evidence collection so you can demonstrate control effectiveness across DORA, PCI DSS, NYDFS, and other frameworks. Replace manual, point-in-time snapshots with proof that's always ready.

Respond Faster

Reduce remediation effort and operational friction. Streamline how you triage, remediate, and validate fixes so issues close in days rather than weeks. Faster response lowers both risk exposure and the operational cost of compliance. Rocket's Rapid Data Recovery can respond to ransomware attacks in hours rather than days or weeks, helping organizations meet stringent regulatory recovery windows.

Each pillar strengthens the others. Together, they transform security from a reactive obligation into a continuous, defensible practice.

How rocket assurance helps you build security readiness

Moving from visibility to control requires more than good intentions. It requires the right capabilities working together across the full scope of mainframe security.

Rocket Assurance brings Rocket's mainframe security, compliance, vulnerability management, cyber resilience, and cyber-risk capabilities together under one portfolio so security leaders can demonstrate, validate, and continuously prove that critical mainframe systems are secure, compliant, resilient, and modernization-ready. Here is how Rocket Assurance maps to the outcomes that matter most.

Security goal	Rocket Assurance capability	What it delivers
Vulnerability management	Rocket Assurance: Rocket® z/Assure® VAP	Continuous scanning of compiled binaries and runtime with a 0.08% false positive rate
Access security	Rocket Assurance: Rocket® Secure Host Access	Phishing-resistant, MFA and SSO-integrated host access governance
Compliance and audit readiness	Rocket Assurance: Mainframe Security Services: Compliance Assessment	Alignment verification against corporate policy and regulatory frameworks
Code integrity and change detection	Rocket Assurance: Mainframe Security Services: Integrity Assessment	Deep code inspection to identify unauthorized or suspicious change
Resilience and recovery	Rocket Assurance: Rocket® Rapid Data Recovery	Dataset-level recovery in hours to meet DORA and ransomware response demands
Open-source risk management	Rocket Assurance: Rocket® Open AppDev for Z	Tested, certified open-source tools aligned with NIST CVE updates
Security conversion and governance	Rocket Assurance: Mainframe Security Services: Security Conversion	Seamless migration to IBM® RACF® with improved governance and control
Deployment model	On prem, cloud, hybrid (one solution)	On prem, cloud (separate products)
Emerging assurance capabilities	Future Rocket Assurance offerings	Add Security Patch Auditor, Quantum Safety Analyzer, Continuous Vulnerability Monitor, and Compliance Automation Manager once launch timing and availability are confirmed.

Rocket Assurance capabilities don't operate in isolation. They work together to close the gaps that point-in-time tools miss and give security leaders the continuous, evidence-based assurance that auditors and regulators require. As new Rocket Assurance offerings become generally available, they can be added to this portfolio view to keep the message current without diluting the core assurance story.

AI revealed the blind spot. Security readiness closes it.

The Mythos discovery demonstrated that vulnerabilities can remain hidden far longer than many organizations expected. That lesson matters. But the larger lesson isn't about a single vulnerability, or even a single discovery method.

It's about the difference between believing systems are secure and being able to prove they are.

High confidence is comfortable. It's also, on its own, insufficient. The research is clear: organizations can feel confident and still face audit findings, costly remediation, and persistent gaps. Confidence isn't the problem. Mistaking it for readiness is.

The organizations that will thrive in this new landscape are already making the shift. They're moving beyond vulnerability discovery to establish continuous visibility, continuous control validation, and continuous compliance readiness. They're replacing assumptions with evidence and treating the mainframe as an integral part of enterprise security strategy.

That's the shift from security confidence to security readiness. AI revealed the blind spot. Rocket Assurance is how Rocket helps you close it, with the continuous evidence, validation, and confidence security leaders need to prove their most critical systems are secure, compliant, resilient, and ready for what comes next.

Speak to an expert

About Rocket Software

Rocket Software is the global technology leader in modernization and 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 3,000 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 around the world. Rocket Software is portfolio company of Bain Capital Private Equity.

Rocket® software

Modernization. **Without Disruption.**™

Visit RocketSoftware.com

MAR-18785_eBook_MFSecurityHanover_V2