Rocket software

What Mythos Misses: Mainframe Risk in the AI Era

AI has exposed how vulnerabilities can be discovered, not how they are mitigated.

The myth that puts you at risk

The mainframe isn't an isolated fortress anymore.

Every API, cloud connection, and integration widens your attack surface and opens new pathways for attackers to reach your most critical systems through trusted channels.

Open-source intelligence leaves blind spots

Tools like Mythos surface ecosystem threats. That's valuable, but it's not enough.

Open-source intelligence can't see inside the places where today's most serious enterprise mainframe risk live. Relying on it alone leaves gaps that both attackers and auditors will find.

AI has collapsed the time to exploit

What once took months now takes minutes.

AI scans legacy source code, finds weak spots, and weaponizes them at machine speed—no mainframe expertise required. Attackers can automate credential testing, privilege escalation, configuration analysis, and behavioral testing all at once.

91%

91% of mainframe organizations have faced a breach or compromise in the past five years.

What Mythos can't see

Here's what open-source scanning leaves uncovered:

- **Assembled mainframe binaries:** Code-level vulnerabilities that exist in compiled programs, not source files.
- **Closed-source proprietary software:** Third-party components that open-source tools can't inspect or analyze.
- **Production runtime behavior:** Active exploitation conditions only visible when systems are live.
- **Race conditions and TOCTOU vulnerabilities:** Time-of-check/time-of-use defects that surface only during live operation.
- **Escalation of Authority from policy drift:** Configuration drift in ESMs like RACF®, ACF2, and Top Secret that silently widens access.
- **Memory-related defects:** Use-after-memory-free and related vulnerabilities that static analysis routinely misses.
- **Dormant and over-privileged accounts:** Insider threat vectors that AI-driven attackers actively exploit.
- **Connected-system and API blind spots:** Downstream integrations and event streams that can carry threats directly to the mainframe.
- **Middleware and compiler vulnerabilities:** Obscure flaws in components that bridge open and closed environments.

Every mainframe risk assessment using Rocket® z/Assure® VAP **uncovers high-severity findings. Not rare exceptions — routine results.**

Privileged access is a critical gap

A single compromised credential can unravel your entire security posture.

AI-powered attackers excel at exploiting dormant or privileged accounts and running credential stuffing at scale. Without automated access reviews and anomaly detection across RACF, CA ACF2, and CA Top Secret, you're leaving the door open, and you may not know it until it's too late.

Visibility and integrity must be continuous

Point-in-time snapshots won't keep pace with modern threats.

You need live integrity monitoring across code, configuration, and active runtime, and you need it covering every layer, from your mainframe core to the APIs and cloud platforms connected to it. Without it, attackers can disable forensic logging and erase the evidence your teams rely on.

Audit evidence should be automatic

Auditors expect proof, not promises.

Automate continuous evidence collection to stay ready for DORA, PCI DSS, SOX, and GDPR, without the manual scramble. Modern regulators expect you to demonstrate that controls are actively working, not just in place on paper.

Quantum readiness starts now

Attackers already use "harvest now, decrypt later."

The sensitive data you protect today could be exposed when quantum computing matures. Inventory your cryptography, assess your key management practices, and pilot quantum-safe algorithms for your highest-risk data. A phased rollout is possible. No rip-and-replace required.

See what Mythos can't
Bring it all together. Prove control to your auditors with confidence.

True mainframe resilience demands layered controls: open-source insight combined with code-level, configuration, and runtime visibility — across the mainframe and every system connected to it.

Speak with an expert

Visit rocketsoftware.com

Rocket software

MAR-18501_IG_VAPWhatMythosMisses_V3