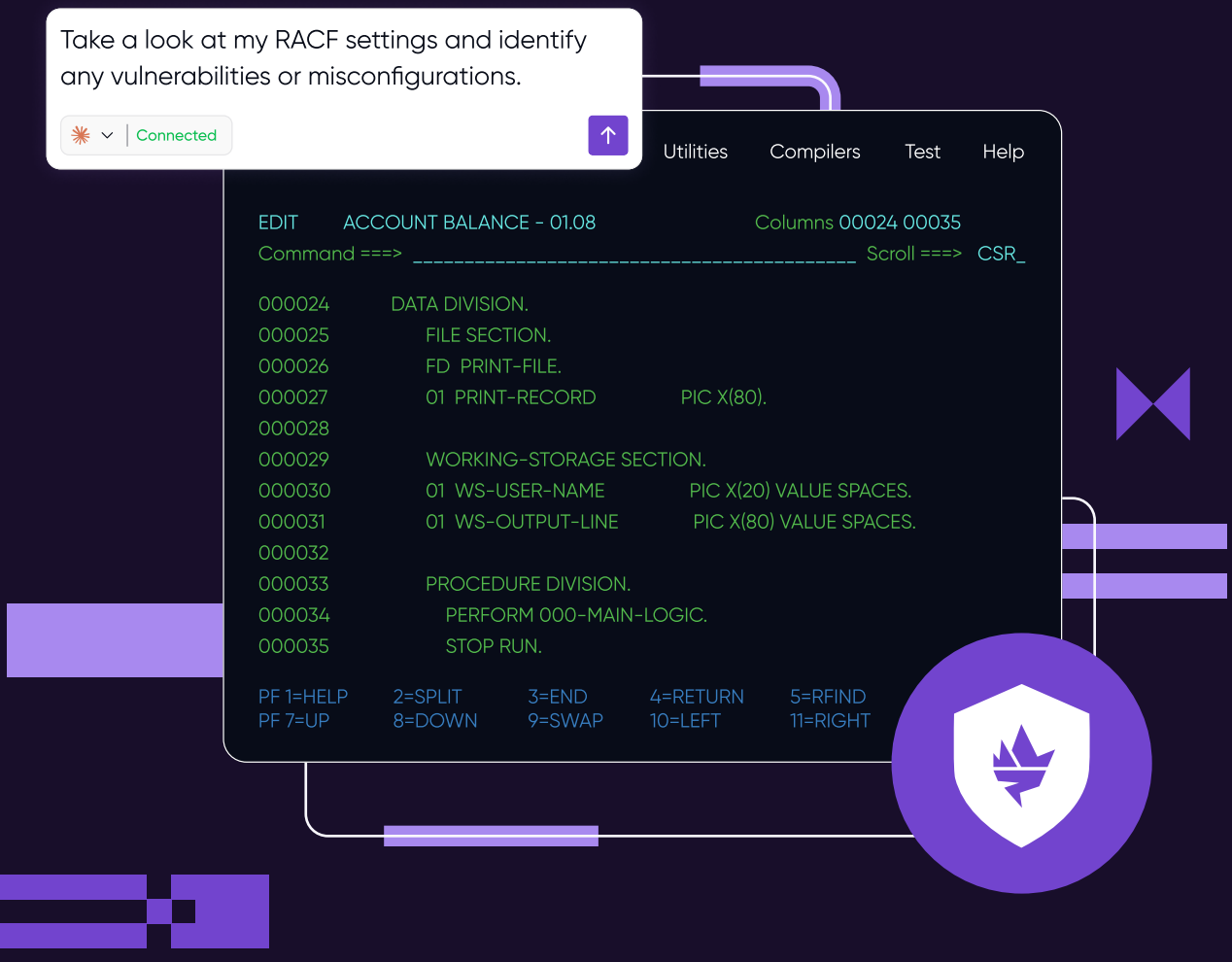
Defending the Mainframe with AI in the Age of AI-Driven Attacks

Leveraging AI Against AI with Geniez and Next-Generation Security Models



geniez

Executive Summary

The rapid evolution of generative AI is fundamentally reshaping the cybersecurity landscape, introducing a new class of threats where attackers are no longer just human actors, but highly capable AI systems. Advanced models such as Mythos and GPT-5.5-cyber demonstrate unprecedented abilities in code analysis, reasoning, and autonomous vulnerability discovery. These capabilities can be leveraged for both defense and large-scale cyberattacks.

While mainframes have historically been considered among the most secure enterprise platforms, their complexity, legacy codebases, and fragmented security tooling create an environment where AI-powered attackers can identify risks that traditional methods often miss. This creates a growing imbalance: attackers can operate at machine scale, while defenders remain constrained by manual processes and periodic reviews.

To address this shift, organizations must adopt an "AI vs. AI" security strategy leveraging advanced AI to defend against AI-driven threats. Geniez AI enables this transformation by bringing AI-native security capabilities directly into the mainframe environment. Its GenAI framework securely connects leading large language models to mainframe data sources, enabling real-time, natural language-driven analysis across configurations, permissions, and code.

Through capabilities such as AI-powered vulnerability detection in COBOL and Assembler, dynamic configuration analysis via the Operations Genie, and specialized Security Subject Matter Genies (SMGs), Geniez provides holistic, cross-domain visibility into mainframe security. This approach allows enterprises to continuously identify vulnerabilities, detect misconfigurations, and uncover complex privilege escalation paths that traditional tools cannot easily detect.

Ultimately, the paper argues that cybersecurity has reached a strategic inflection point. Organizations that continue to rely solely on traditional security tools and approaches risk falling behind, while those that embrace AI-native defenses can achieve faster detection, deeper insights, and continuous validation of their security posture. Geniez AI positions itself as a key enabler of this shift, helping enterprises transform their mainframe from a static system into a dynamically secured, AI-powered environment

Introduction: A New Era of AI-Driven Cyber Capabilities

Recent advancements in generative AI are reshaping the cybersecurity landscape both defensively and offensively.

Initiatives like Anthropic's Project Glasswing highlight how frontier AI systems are being explored for high-impact enterprise and government use cases, including cybersecurity. At the same time, the emergence of powerful models such as Mythos and ChatGPT 5.5-cyber demonstrates a new class of AI capable of sophisticated reasoning, code analysis, and autonomous problem-solving.

While these capabilities unlock enormous defensive potential, they also introduce a critical risk:

The same models can be used to identify, exploit, and automate cyberattacks at scale.

According to Techcrunch, Treasury Secretary Scott Bessent and Fed Chair Jerome Powell called 6 banks: JPMorgan Chase, Goldman Sachs, Citigroup, Wells Fargo,, Bank of America, and Morgan Stanley, to encourage them to look at Mythos and utilize it to check for security vulnerabilities in their code and systems.

This is important because just a month before, Anthropic was defined as a "supply chain risk" by the Department of Defense. This is the first time for a US company being declared supply chain risk and blacklisted from being used by the US government or its suppliers.

Department of Defense CTO Emil Michael on May 1st 2026 said Anthropic is still a supply chain risk, but that Mythos, the company's artificial intelligence model with advanced cyber capabilities, is a "separate national security moment."

The implication is clear:

Organizations are entering an era where attackers are no longer humans with tools but AI systems with reasoning capabilities.

The Risk and Challenge: When the Attacker Is an AI

Mainframes have long been considered among the most secure computing platforms in the enterprise. Their reputation is built on decades of hardened infrastructure, strict access controls, and operational discipline.

However, this perception is increasingly being challenged.

The core issue is not that mainframes are inherently insecure, it's that **the nature of the attacker has fundamentally changed.**

Modern GenAI systems can:

- Analyze massive configuration surfaces instantly
- Correlate permissions, datasets, and execution paths
- Identify non-obvious privilege escalation chains
- Generate exploit strategies across systems

A clear example from the distributed world is the vulnerability discovered by Wiz in GitHub (CVE-2026-3854), where complex interactions led to a critical security issue that traditional approaches had missed.

This illustrates a broader point:

If vulnerabilities can evade human detection in modern systems, AI-powered attackers will find them.

The Mainframe-Specific Challenge

In the mainframe environment, the complexity is even greater:

- Interdependencies between **RACF**, system configurations, and datasets
- Sensitive control points such as **APF, SVC, PPT, and authorized commands**
- Legacy codebases (COBOL, Assembler) with decades of accumulated logic
- Limited tooling for holistic, cross-domain security analysis

Traditional security approaches that include manual reviews, rule-based scanning, and periodic audits are not designed to compete with AI-driven exploration.

This creates an asymmetry:

- Attackers can use AI to explore infinitely
- Defenders are still constrained by human-scale processes

Conclusion

To counter AI-driven threats, organizations must adopt the same paradigm:
You need AI defending your environment because AI is attacking it.

Geniez AI: Bringing AI-Native Security to the Mainframe

Geniez AI addresses this challenge by enabling organizations to apply GenAI capabilities directly to their mainframe environments.

At its core, the Geniez GenAI Framework:

- Connects **any LLM to any mainframe data source**
- Provides **secure, governed, and auditable access**
- Enables **real-time analysis using natural language**
- Extends AI capabilities into traditionally siloed systems

This creates a foundation for **AI-native security operations.**

Securing Code: AI-Powered Vulnerability Detection

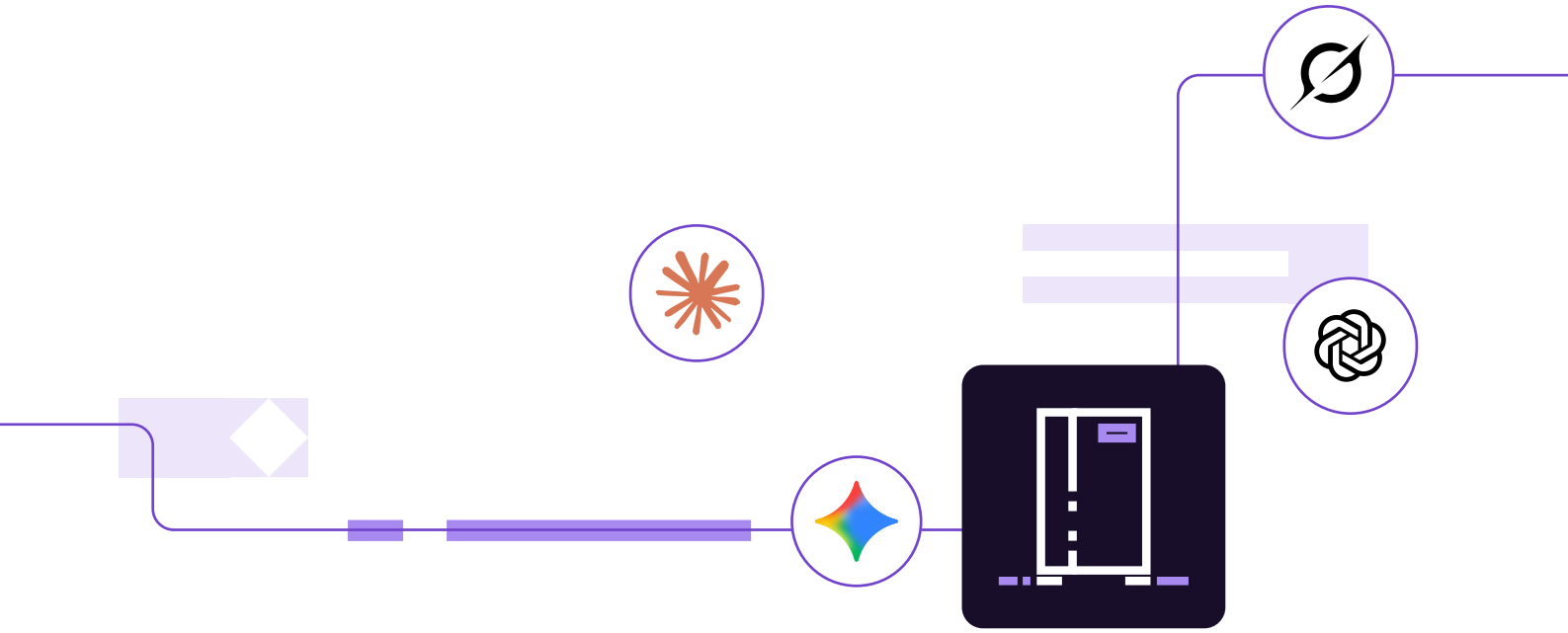
Legacy code represents a major and often under-analyzed risk surface. Mainframe code in COBOL and Assembler has been on the mainframe from its inception. There was no code review or understanding of its code for sometimes decades as the system programmers who have written the code without comments and proper documentation have long retired from the company.

Geniez enables organizations to:

- Connect its framework to tools like Copilot, Claude Code, Amazon Q or other code assistants
- Leverage the latest LLMs like Claude Opus 4.7, GPT 5.5-cyber and others to run **AI-powered scans across COBOL and Assembler programs**
- Detect vulnerabilities, insecure patterns, and logic flaws

This allows teams to:

- Modernize security practices without rewriting applications
- Apply consistent analysis across thousands of programs
- Identify issues that traditional static analysis tools may miss



Securing Configurations with AI: Operations Genie

One of the most critical attack surfaces in the mainframe is configuration.

Geniez enables security teams to use its **Operations Genie AI assistant** to analyze configurations dynamically and holistically.

Example Use Cases

Security teams can ask:

> Take a look at my RACF settings and identify any vulnerabilities or misconfigurations.
>
> Connected

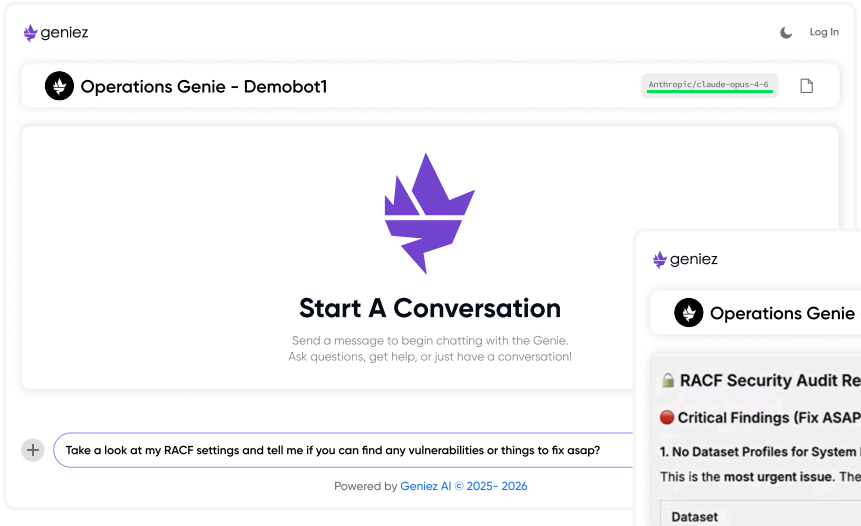
> Analyze SYS1.PARMLIB—especially SVC, APF, PPT, and authorized TSO/E commands—and cross-reference with RACF permissions. Highlight any risks.
>
> Connected

Behind the scenes, the Operations Genie will:

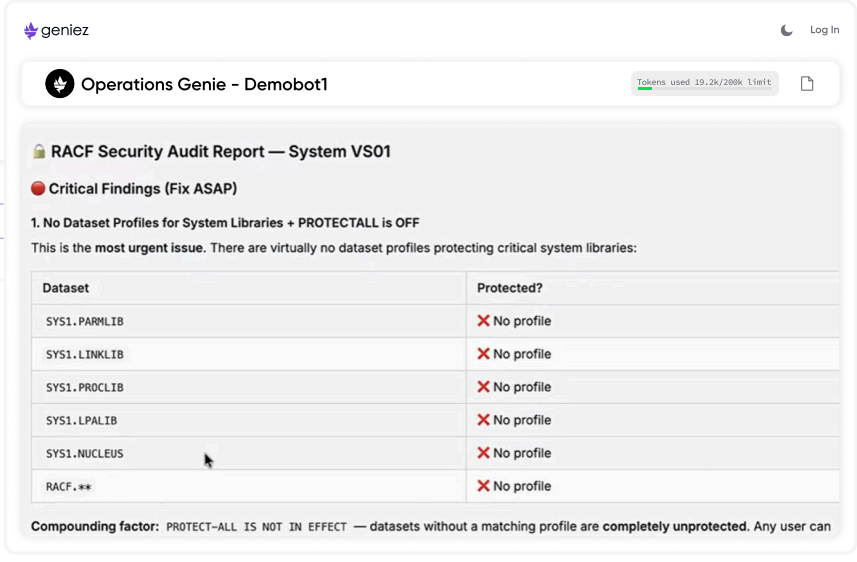
- Correlates configuration data across subsystems
- Maps permission chains and escalation paths
- Identifies inconsistencies and risky patterns
- Surfaces findings in natural language

This transforms security reviews from:

- Static → dynamic
- Manual → automated
- Fragmented → holistic



Operations Genie Screen shot of security prompt



Example of an answer to the previous diagram prompt

Security SMG: Specialized AI for Mainframe Security

Geniez has developed a dedicated Security SMG (Subject Matter Genie) designed specifically for mainframe security use cases.

Capabilities include

Configuration Analysis

RACF settings and permission chains

PARMLIB components (APF, SVC, PPT, LPA, AUTH TSO/E)

Code Vulnerability Scanning

COBOL and Assembler analysis at scale

Audit and Compliance Reviews

Automated security assessments

Anomaly Detection

Based on SMF records (RACF, MVS, TCP/IP)

Cross-Domain Correlation

Linking configurations, permissions, and runtime behavior

This aligns directly with the reality of modern threats:

> Security is no longer about isolated checks—it's about understanding the system as a whole.

The Strategic Shift: AI vs AI

The industry is entering a new equilibrium:

- Attackers are using advanced AI models to find vulnerabilities
- Defenders must deploy equally capable AI systems to detect and prevent them

Mainframes, despite their strength, are not immune to this shift.

Organizations that rely solely on traditional security methods risk falling behind.

Those that adopt AI-native approaches gain:

- Faster detection
- Deeper analysis
- Broader coverage
- Continuous security posture validation

Conclusion

The rise of advanced models like Mythos and initiatives like Project Glasswing signals a turning point in cybersecurity.

The question is no longer whether AI will impact security - it already has.

The real question is:

Will your organization use AI only as a tool, or as a core defense strategy?

Geniez AI enables enterprises to bring GenAI directly into the heart of their most critical systems, the mainframe, turning a traditionally static environment into a dynamically secured one.

Learn More

To learn more about how Geniez AI can help secure your mainframe environment, contact: **contact@geniez.ai**