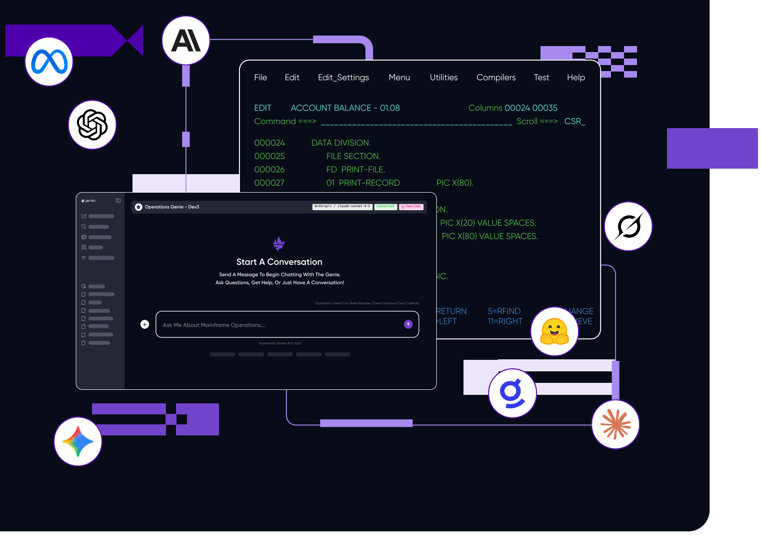
geniez

Geniez GenAI Framework

Security & Vulnerability Assurance



```
EDIT     ACCOUNT BALANCE - 01.08                    Columns 00024 00035
Command ===> ________________________________________ Scroll ===> CSR_
000024      DATA DIVISION.
000025        FILE SECTION.
000026        FD  PRINT-FILE.
000027        01  PRINT-RECORD                PIC X(80).
                                              PIC X(20) VALUE SPACES.
                                              PIC X(80) VALUE SPACES.
```

Start A Conversation

Send A Message To Begin Chatting With The Genie. Ask Questions, Get Help, Or Just Have A Conversation!

Ask Me About Mainframe Operations...

The Geniez GenAI Framework is engineered with a security-by-design philosophy that aligns with the highest standards of enterprise mainframe environments. Its architecture deliberately minimises risk, reduces operational complexity, and enables straightforward security validation. This translates into a solution that is robust, controlled, and trusted without introducing unnecessary exposure.

1. Authentication and Access Control via RACF[1]

Security governance for the framework is fully integrated with RACF[1]:

- All user, service, and operational access is centrally authenticated and authorised through RACF.
- Activities are strictly role-based and fully auditable using native mainframe logging.
- Existing security, risk, and compliance processes extend seamlessly to the framework.

What this means for clients: Proven, trusted and well-understood controls with complete transparency and auditability. No need to change or adopt new security models.

2. Fundamentally reduced attack surface

Through patented technology, the framework is designed to operate with minimal system-level exposure:

- No requirement for APF authorisation.
- No requirement for z/OS UNIX superuser or UID=0 access
- No elevation of system privileges.
- Execution remains within tightly controlled user-space environments.

What this means for clients: A materially smaller attack surface and lower systemic risk compared to solutions that rely on privileged execution.

[1] or Security product of your choice, ACF2 and Top Secret also supported

3. Secure by isolation. No external connectivity required

The framework is intentionally isolated from external networks:

- No external firewall openings to the mainframe are required.
- No internet access is ever needed during development or production use.
- All processing remains securely within the client's internal environment.

What this means for clients: Elimination of common network-based threat vectors and strong protection against data leakage or external intrusion.

4. Continuous secure development and vulnerability management

Security is embedded throughout the development lifecycle:

- Secure coding and design best practices are applied as standard.
- Regular CVE and vulnerability scanning is performed across all components.
- Identified issues are proactively assessed and remediated to prevent downstream risk.

What this means for clients: Confidence that known vulnerabilities are actively managed and addressed before they become operational concerns.

Summary

From an executive and risk-management perspective, the Geniez GenAI Framework delivers:

- Strong, centralised security control through RACF.
- Minimal attack surface with no reliance on privileged system access.
- A closed, firewall-friendly network posture with zero internet dependency.
- Ongoing vulnerability management aligned with industry best practices.

The result: an AI framework that is not only innovative and powerful, but also secure, predictable, and enterprise-ready.

Contact us to learn more
or schedule a live demo at

contact@geniez.ai