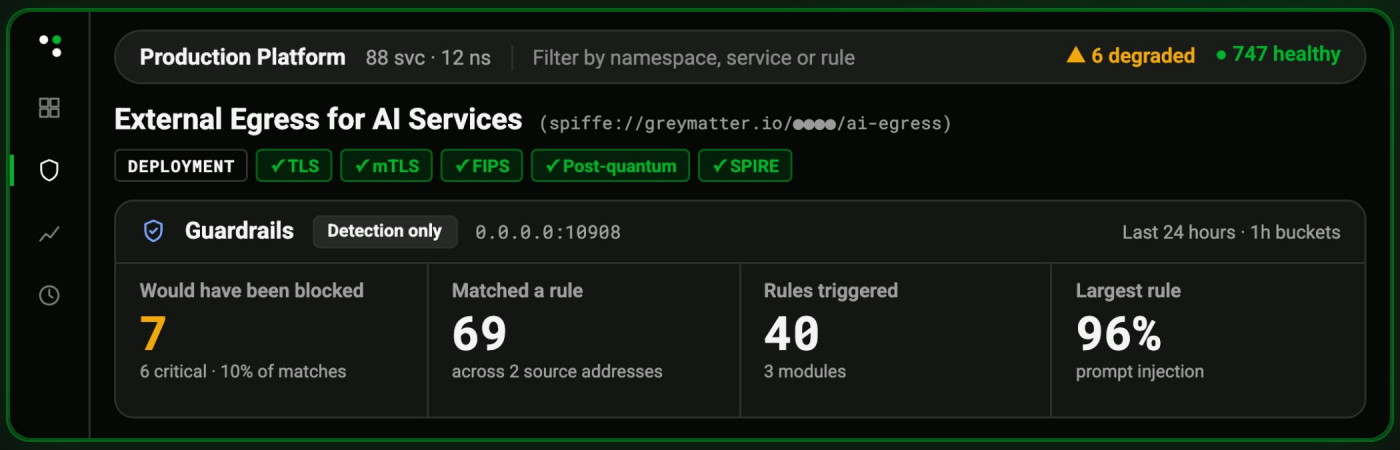
See every call. Inspect every prompt. Prove every control.

Greymatter.io builds AI Guardrails, data loss prevention, and a native WAF into each enforcement point. It fingerprints each credential, so a replayed token stands out.



App Guard on a live AI service: guardrails, DLP, and WAF, detected before you enforce.

AI AND WEB SECURITY

Inspection for AI and web traffic.

AI Guardrails covers the OWASP LLM Top 10 and MCP. DLP flags personal, health, and classified data. A native WAF runs the OWASP Core Rule Set 4+.

FORENSICS

A forensic audit, step by step.

Trace any request or person across 30 days, with identity at each step.

LEAST PRIVILEGE

Learned access, enforced.

Learned callers become the allowlist. Revoked CAC and PIV cards never connect, and certificate status checks stay fresh.

POST-QUANTUM

Cryptography you can prove.

FIPS 140-3 validated (CMVP #5191) and post-quantum encryption are on by default, and measured service by service.

BY THE NUMBERS

12	controls in one Stoplight score
3-in-1	OWASP LLM Top 10, DLP, and an OWASP CRS 4+ WAF
0	credentials written to logs or records

NEXT STEP

Questions, demos, and lab access

Chris Holmes, CEO · chris.holmes@greymatter.io

Speak with a Greymatter.io Expert