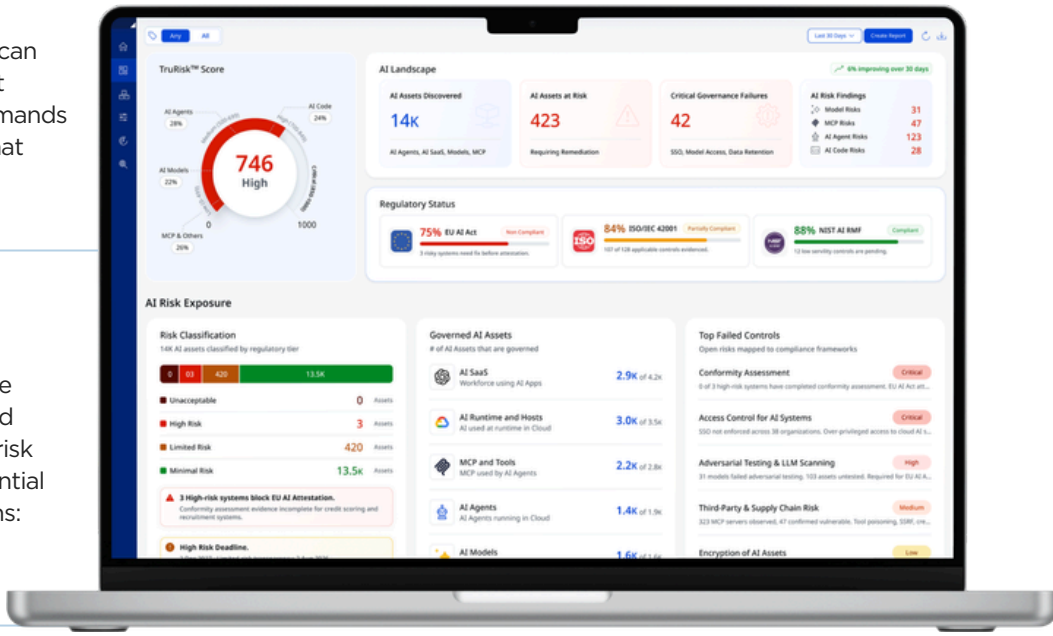
CAN YOU PROVE YOUR AI IS SAFE?

Scale AI Innovation. Stay Secure. Prove Your AI Governance Works.

AI has become enterprise infrastructure, adopted faster than most organisations can secure them. Static policies alone cannot prove AI safety - true AI governance demands continuous technical proof to validate that security controls operate effectively.



Qualys TotalAI

Qualys TotalAI helps organizations move from fragmented AI controls, policies and tools to a complete code-to-runtime AI risk management by consolidating four essential components of AI governance operations: Discover, Assess, Remediate, Report.

960+ AI-specific detections

300+ attack scenarios

55+ posture controls

Discover the AI You Can't See

- Build continuous inventories of sanctioned and shadow AI across hosts, cloud, MCPs, containers, pipelines, and SaaS.
- Map all assets to ownership, operating context, exposure, and risk.
- Leverage Qualys AI fingerprinting across GPUs, models, containers, and MCP servers.

Secure AI Risk at Every Stage

- **Posture & Code**: Uncover misconfigurations, toxic permissions, secrets, and vulnerable dependencies.
- **Behavior**: Test LLMs and MCP servers for prompt injection, jailbreaks, and tool poisoning.
- **Runtime**: Use kernel-level eBPF and SaaS telemetry from browser and connectors to monitor agent execution and data movement.

Remediate AI Risks That Matter Most

- Correlate severity, model behavior, exposure, and runtime evidence to highlight toxic risk combinations.
- Deliver actionable guidance and deployment-ready guardrails directly to responsible owners.
- Retest fixes to record defensible proof of closure.

Report AI Governance with Evidence

- Convert continuous evidence into audit-ready outputs for boards, customers and regulators.
- Document inventory, test failures, prioritized risks, and retest closures.
- Map findings to NIST AI RMF, EU AI Act, OWASP Top 10 for LLMs, and MITRE ATLAS.

FedRAMP Moderate Authorized

TotalAI is FedRAMP Moderate Authorized - deployable today withaudit-ready evidence for NIST AI RMF, NIST SP 800-53, and CMMC 2.0.

Discover your AI footprint. Secure your AI attack surface. Build your AI governance baseline in 30 days.

Try Now

v260721

©2026 Qualys, Inc. All rights reserved.