Qualys TotalAI

Enterprise-Ready AI Risk Management and Governance Across the Full Lifecycle.

Discover the Complete AI Attack Surface
Instantly map all AI assets (infra, models, SaaS) for full-stack visibility.

Expose the AI Risks That Matter
Unify posture gaps, access risks, and threat context across your AI stack.

Shift AI Security to the Left
Intercept code flaws and policy violations directly in your CI/CD pipelines.

Expose Hidden AI Supply Chain Risk
Audit open-source models, ML packages, and container dependencies automatically.

Test Models Before Attackers Do
Stress-test LLMs against adversarial attacks and safety failures.

Prove the Agentic Layer Can't Be Abused
Restrict agent permissions and stress-test MCP integrations.

Monitor What AI Actually Does at Runtime
Continuously monitor live AI workloads for anomalous behavior and protocol hijacks.

Govern AI SaaS and Workforce Usage
Enforce AI SaaS compliance and detect data exposure from browser GenAI tools.

Turn Every AI Signal into Prioritized Risk, Enforceable Controls, And Proof of Governance.

Cut through AI risk noise with TruRisk
Correlate security findings into a single TruRisk score to prioritize complex, multi-vector threat paths.

Turn Findings into Guardrails and Fixes
Automatically translate findings into controls, owner-routed tickets, and re-test for verified risk reduction.

Prove AI Governance Is Working
Map technical telemetry for audit-ready compliance and regulations like EU AI Act, NIST, & enterprise policies.

v260828

©2026 Qualys, Inc. All Rights Reserved.