

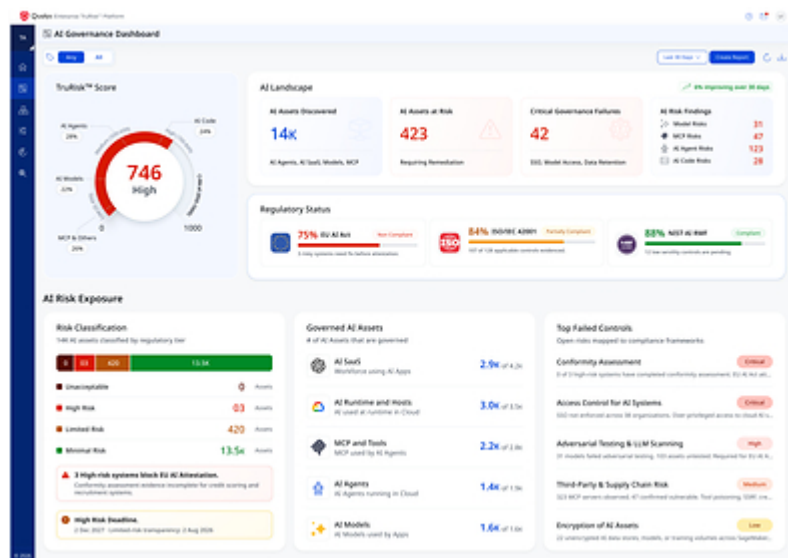


Qualys Expands AI Security with Stronger Governance to Keep Fast Moving AI Adoption Under Control

July 29, 2026

New capabilities in TotalAI enable CISOs to reduce shadow AI, flag abnormal model behavior, and prove controls are working across development and runtime

FOSTER CITY, Calif., July 29, 2026 /PRNewswire/ -- [Qualys, Inc.](#) (NASDAQ: QLYS), a leading provider of cloud-based IT, security and compliance solutions, today announced new capabilities in TotalAI, built on the Qualys Enterprise TruRisk Platform, to empower organizations to discover, test, monitor, and govern enterprise AI risk from design to production. TotalAI provides enterprise CISOs with robust AI governance and risk management capabilities that satisfy new policy requirements around safe AI use in the U.S. and EU.



Enterprise AI adoption has outrun the controls built to govern it. Organizations are layering models, AI agents, and Model Context Protocol (MCP) servers onto security programs never designed for them, while attackers weaponize the same AI tools to move faster than defenders can track. Moreover, no other single point tool answers the questions security leaders face daily: Where is AI running? Which models can leak data or be manipulated? What are AI agents connected to? And can we prove our controls are working? TotalAI answers all four — with the same TruRisk score security teams already use for vulnerabilities, cloud, and containers.

"AI is outrunning the controls built to govern it, and security teams can no longer treat that risk as a separate list to be scanned and closed," said Grace Trinidad, Research Director at IDC. "The industry is moving beyond simply counting vulnerabilities toward continuously minimizing the exploitable surface, what is actually reachable and can be made to do harm, and AI is turning that shift from good practice to a requirement. Organizations that fold AI risk into continuous exposure management, spanning discovery, assessment, runtime visibility, and governance, will be the organizations positioned to adopt AI securely and at scale."

Qualys TotalAI provides enterprises with end-to-end AI security:

- **Gain total visibility into AI use** — Discover shadow AI, cloud AI services, AI agents, models, MCP servers, AI containers, and browser-based AI, so teams know where AI runs across the enterprise and who owns the risk.
- **Govern agentic AI, models and integrations end to end** — See and control the tool calls AI agents make over MCP, so an agent's reach can be contained if needed. Kernel-level (eBPF) instrumentation reveals what AI workloads execute on servers, delivering visibility that scanners and logs can't provide.
- **Prove governance is working** — Give security, engineering, and governance, risk, and compliance (GRC) teams audit-ready evidence of what AI exists, the severity and impact of any issues, and a TruRisk-based prioritization plan of what to fix first.
- **Shift AI security left** — Find AI vulnerabilities, misconfigurations, and exposed secrets earlier, in code and pipelines. Test models for prompt injection, jailbreaks, and unsafe output before they reach production.
- **Go beyond posture to adversarial testing** — TotalAI red-teams both LLMs (prompt injection, jailbreaks) and MCP servers (tool poisoning, SSRF, rug-pull), mapped to the OWASP LLM & MCP Top 10 and the EU AI Act. While most tools govern MCP access, TotalAI scans the MCP server itself.

"With every modern enterprise leveraging AI, the question is changing from 'Is my AI secure?' to 'Can I prove it to my board and regulators?'" said

Sumedh Thakar, president and CEO of Qualys. "TotalAI gives enterprises a single, unified way to assess, govern, and secure AI risk continuously — not through periodic snapshots, but with the real-time clarity and discipline Qualys is known for."

Availability

TotalAI is generally available. To learn more, visit qualys.com/free-trial-new/totalai or visit our booth #2333 at Black Hat USA 2026.

Additional Resources

- Read our blog post, ["Operationalize AI Governance Across Shadow GenAI, MCP, and Agentic Workloads with Qualys TotalAI"](#)
- [Book a meeting](#) with us at Black Hat USA 2026
- Request a demo at qualys.com/free-trial-new/totalai
- Register for the webinar, ["You Are Securing AI. Can You Prove Your AI Is Secure?"](#)
- Follow Qualys on [LinkedIn](#), [Instagram](#) and [X](#)

About Qualys

[Qualys, Inc.](#) (NASDAQ: [QLYS](#)) is a leading provider of cloud-based security, compliance and IT solutions with more than 10,000 subscription customers worldwide, including a majority of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and automate their security and compliance solutions onto a single platform for greater agility, better business outcomes, and substantial cost savings.

The Qualys Enterprise TruRisk Platform leverages a single agent to continuously deliver critical security intelligence while enabling enterprises to automate the full spectrum of vulnerability detection, compliance, and protection for IT systems, workloads and web applications across on premises, endpoints, servers, public and private clouds, containers, and mobile devices. Founded in 1999 as one of the first SaaS security companies, Qualys has strategic partnerships and seamlessly integrates its vulnerability management capabilities into security offerings from cloud service providers, including Oracle Cloud Infrastructure, Amazon Web Services, the Google Cloud Platform and Microsoft Azure, along with a number of leading managed service providers and global consulting organizations. For more information, please visit <http://www.qualys.com>.

Qualys, Qualys VMDR®, Qualys TruRisk and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.

Media Contact:

Rachel Yap Winship

Qualys

Media@Qualys.com



 View original content to download multimedia: <https://www.prnewswire.com/news-releases/qualys-expands-ai-security-with-stronger-governance-to-keep-fast-moving-ai-adoption-under-control-302837084.html>

SOURCE Qualys, Inc.