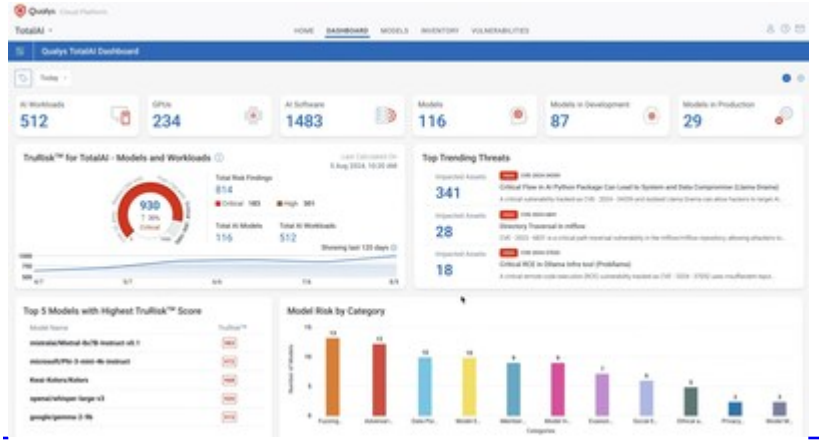
Qualys Expands Platform to Protect Against AI and LLM Model Risk from Development to Deployment

April 29, 2025

New enhancements in TotalAI strengthen AI security capabilities with extended threat coverage, multi–modal protections, and internal LLM scanner

FOSTER CITY, Calif., April 29, 2025 /PRNewswire/ -- Qualys, Inc. (NASDAQ: QLYS), a leading provider of disruptive cloud-based IT, security and compliance solutions, today announced major updates to its TotalAI solution to secure organizations' complete MLOps pipeline from development to deployment. Organizations will now be able to rapidly test their large language models (LLMs), even during their development testing cycles, with stronger protection against more attacks and on-premises scanning powered by an internal LLM scanner.



With the current rush of AI adoption, organizations are moving at an unprecedented pace – often without implementing foundational security controls necessary to manage risk. A recent study revealed 72% of CISOs are concerned generative AI solutions could result in security breaches for their organizations. Enterprises need a better solution to bridge the gap between innovation and secure implementation.

As AI becomes a core component of business innovation, security can no longer be an afterthought," said Tyler Shields, principal analyst at Enterprise Strategy Group. "Qualys TotalAI ensures that only trusted, vetted models are deployed into production, enabling both agility and assurance across organizations' AI usage. This security helps organizations achieve their innovation goals while managing their risk."

Qualys TotalAI is purpose-built for the unique realities of AI risk, going beyond basic infrastructure assessments to directly test models for jailbreak vulnerabilities, bias, sensitive information exposure, and critical risks mapped to the OWASP Top 10 for LLMs. Taking a risk-led approach, TotalAI not only finds AI-specific exposures — it helps teams resolve them faster, protect operational resilience, and maintain brand trust. TotalAI delivers:

- **Automatic Prioritization of AI Security Risks**: Findings are mapped to real-world adversarial tactics with MITRE ATLAS and automatically prioritized through the Qualys TruRisk™ scoring engine, helping security, IT, and MLOps teams zero in on the most business-critical risks.
- **Faster, Safer AI Application Development:** With the new internal on-premises LLM scanner, organization can now incorporate comprehensive security testing of their LLM models during development, staging, and deployment – all without ever exposing models externally. This shift-left approach, incorporating security and testing of AI-powered applications into existing CI/CD workflows, strengthens both agility and security posture, while ensuring sensitive models remain protected behind corporate firewalls.
- **Enhanced Defense Against Emerging AI Threats:** TotalAI now expands to detect 40 different attack scenarios, including advanced jailbreak techniques, prompt injections and manipulations, multilingual exploits, and bias amplification. The expanded scenarios simulate real-world adversarial tactics and strengthen model resilience against exploitation, preventing attackers from manipulating outputs or bypassing safeguards.
- **Protection from Cross-modal Exploits with Multimodal Threat Coverage:** TotalAI's enhanced multimodal detection identifies prompts or perturbations hidden inside images, audio, and video files that are designed to manipulate LLM outputs, helping organizations safeguard against cross-modal exploits.

"AI is reshaping how businesses operate, but with that innovation comes new and complex risks," said Sumedh Thakar, president and CEO of Qualys. "TotalAI delivers the visibility, intelligence, and automation required to stay agile and secure, protecting AI workloads at every stage — from development through deployment. We are proud to lead the way with the industry's most comprehensive solution, helping businesses innovate with confidence, while staying ahead of emerging AI threats."

Availability

Qualys TotalAI is now available. For a 30-day trial, visit qualys.com/forms/totalai or read our blog to learn more.

Additional Resources

- Read our blog post, "Guard Against GenAI and LLM Risks from Development to Deployment with Qualys TotalAI"
- Sign up for a free trial of Qualys TotalAI
- Follow Qualys on LinkedIn and X

About Qualys
Qualys, Inc. (NASDAQ: QLYS) is a leading provider of disruptive 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.

Media Contact:
Rachel Yap Winship
Qualys
Media@Qualys.com

View original content to download multimedia:https://www.prnewswire.com/news-releases/qualys-expands-platform-to-protect-against-ai-and-llm-model-risk-from-development-to-deployment-302440627.html

SOURCE Qualys, Inc.