# Qualys updates TotalAI platform to enhance security across AI lifecycle



Qualys, a prominent cybersecurity company, has announced substantial updates to its TotalAI platform, aimed at enhancing security for organisations throughout the entire AI lifecycle—from development to deployment. These updates come amid rapidly increasing AI adoption in businesses, which often exceeds the pace at which appropriate security controls are implemented.

The enhancements to TotalAI are designed to confront growing concerns among cybersecurity professionals about the risks posed by generative AI technologies. A recent study cited by Qualys revealed that 72% of Chief Information Security Officers (CISOs) worry that generative AI solutions could potentially lead to security breaches within their organisations.

Tyler Shields, Principal Analyst at Enterprise Strategy Group, emphasised the necessity of integrating security into AI operations. Speaking to SecurityBrief Australia, Shields said, "As AI becomes a core component of business innovation, security can no longer be an afterthought. Qualys TotalAI ensures that only trusted, vetted models are deployed into production, enabling both agility and assurance across organisations' AI usage. This security helps organisations achieve their innovation goals while managing their risk."

Among the new capabilities in the updated TotalAI platform is automated prioritisation of AI security threats, achieved by mapping findings to real-world adversarial tactics listed in MITRE ATLAS and prioritising them through the TruRisk scoring system. This allows teams spanning security, IT, and machine learning operations (MLOps) to concentrate efforts on the most critical risks affecting their AI deployments.

Additionally, the platform now includes an on-premises internal large language model (LLM) scanner designed to integrate security testing at every stage—development, staging, and deployment—within existing continuous integration and continuous delivery (CI/CD) workflows. This feature ensures that AI models are protected behind corporate firewalls and prevent exposure to external threats at any point during the model lifecycle.

TotalAI’s threat detection capabilities have expanded to cover 40 distinct attack scenarios. These include advanced jailbreak techniques, prompt injections, manipulations, multilingual exploits, and bias amplification. The platform can simulate adversarial attacks to bolster model resilience against exploitation attempts aimed at manipulating AI outputs or circumventing safeguards.

A particular focus has been placed on defending against cross-modal exploits, which involve malicious inputs hidden within images, audio, or video files designed to influence LLM outputs. By enhancing multimodal detection, the platform addresses vulnerabilities arising from the integration of diverse data types into AI systems.

Sumedh Thakar, President and CEO of Qualys, spoke about the challenges encountered as AI becomes embedded in business operations. "AI is reshaping how businesses operate, but with that innovation comes new and complex risks," he said in an interview with SecurityBrief Australia. Thakar added, "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."

Qualys emphasises that TotalAI goes beyond traditional infrastructure security assessments by directly testing AI models for a variety of vulnerabilities and threats pertinent to contemporary AI environments. The platform is positioned as a comprehensive tool designed to address the realities of AI risk in an evolving threat landscape.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.qualys.com/company/newsroom/news-releases/usa/qualys-advances-enterprise-trurisk-platform-to-de-risk-generative-ai-and-llm/> - This Qualys press release details the launch of Qualys TotalAI, a solution designed to address security and compliance challenges associated with generative AI and large language model (LLM) applications, aiming to secure AI workloads and prevent model theft.
2. <https://www.itp.net/acn/cybersecurity/enhancing-ai-security-qualys-launches-totalai-to-tackle-emerging-cyber-threats> - An article from ITP.net discussing the introduction of Qualys TotalAI, highlighting its capabilities in discovering, inventorying, and classifying AI and LLM assets, as well as its focus on preventing model and data theft.
3. <https://www.tahawultech.com/news/qualys-announces-the-launch-of-qualys-totalai/> - This piece from TahawulTech.com covers the announcement of Qualys TotalAI, emphasizing its features such as assessing LLMs for critical attack exposures like prompt injection and sensitive information disclosure.
4. <https://www.qualys.com/company/newsroom/news-releases/usa/qualys-advances-enterprise-trurisk-platform-to-de-risk-generative-ai-and-llm/> - The Qualys press release also mentions the integration of TruRisk scoring system in TotalAI, which maps findings to real-world adversarial tactics listed in MITRE ATLAS, allowing teams to focus on the most critical risks affecting their AI deployments.
5. <https://www.itp.net/acn/cybersecurity/enhancing-ai-security-qualys-launches-totalai-to-tackle-emerging-cyber-threats> - The ITP.net article highlights Sumedh Thakar's statement on the challenges encountered as AI becomes embedded in business operations, emphasizing the need for robust security measures to manage new and complex risks.
6. <https://www.qualys.com/company/newsroom/news-releases/usa/qualys-advances-enterprise-trurisk-platform-to-de-risk-generative-ai-and-llm/> - The Qualys press release also mentions the expansion of TotalAI's threat detection capabilities to cover 40 distinct attack scenarios, including advanced jailbreak techniques, prompt injections, manipulations, multilingual exploits, and bias amplification.
7. <https://news.google.com/rss/articles/CBMipgFBVV95cUxOT2FBSjh6cGREcG1TWTQ5TlpnTzJnSE9xZmVyeWVLQmxCYVZhTVAtc0ZvWmp6MWFmV3VFRV91RmJVdVhPWWlwWFc1YmNfRHNsVVZUZGprZERjdGJVTWF2SFBndUZrX1Y5S3llR2RDVTZkQjV4cHB6NnZkeUt5UjdqRVFXNS1od0d0YzZaN01TVUVXQlFkWWx5ZElZaTlZNFNRVTFGOF93?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data