Qualys Advances Enterprise TruRisk Platform to De-Risk Generative AI and LLM Usage from Security and Compliance Challenges

August 5, 2024

New solution, Qualys TotalAI, enables holistic discovery and vulnerability assessment of AI workloads to detect data leaks, injection issues and model theft

FOSTER CITY, Calif., Aug. 5, 2024 /PRNewswire/ -- Qualys, Inc. (NASDAQ: QLYS), a leading provider of disruptive cloud-based IT, security and compliance solutions announced it is expanding its portfolio with Qualys TotalAI, designed to address the growing challenges and risks associated with securing generative AI and large language model (LLM) applications. The solution will be showcased at Black Hat 2024 (booth #1320).

As organizations increasingly integrate AI and LLMs into their products and solutions, they face an expanded attack surface and heightened cyber risks. Traditional cybersecurity practices are proving insufficient to address these new challenges. The need to discover unknown or unapproved LLMs or AI models, known as shadow models, significantly increases exposure to threats, including model theft and data leaks from existing CVEs or misconfigurations. Additionally, there is a rising risk of accidental data loss, compliance issues, and reputational damage due to inappropriate content and AI hallucinations generated by these models. These concerns highlight the urgent need for robust security solutions in the evolving AI landscape.

Qualys TotalAI harnesses the powerful features the Qualys platform is known for to empower organizations in confidently adopting AI technologies. It expands Qualys' renowned asset visibility, vulnerability detection, and remediation capabilities to generative AI and adds LLM scanning. The solution specifically addresses the OWASP Top 10 most critical risks for LLM applications: prompt injection, sensitive information disclosure, and model theft. With Qualys TotalAI, organizations can securely leverage the benefits of AI while upholding rigorous security standards.

"As the global adoption of AI and large language models (LLMs) accelerates, outpacing governance and safety measures, it's crucial for organizations to implement robust protections," said Philip Bues, senior research manager at IDC. "Qualys TotalAI is focused on providing businesses with the tools they need to confidently secure their AI investments, offering comprehensive visibility and defense against emerging cyber threats."

Qualys TotalAI will allow organizations to:

- **Discover All AI Workloads**: Discover, inventory, and classify all AI and LLM assets, including GPUs, software, packages, and models, in production and development while correlating their exposure with the attack surface.
- **Prevent Model Theft**: Extend the power of TruRisk to assess, prioritize and remediate AI software vulnerabilities with 650+ AI-specific detections, correlated with threat feeds and asset exposures, to prevent the risk of model and data theft.
- **Secure AI Infrastructure:** Leverage comprehensive remediation capabilities to exceed security requirements, align with SLAs, and meet business needs. Proactively mitigate potential threats to ensure seamless operations and a strong AI and LLM security posture.
- **Detect Sensitive Data Disclosure:** Assess LLMs for critical attack exposures like prompt injection, sensitive information disclosure, and model theft per the OWASP Top 10 for LLMs. This will ensure confidence in AI risk management and make models audit and compliance ready.

"We're only beginning to scratch the surface of AI and LLM's potential for driving value for enterprises. At the same time, we need to secure this burgeoning journey, so it doesn't add new risk to the business," said Sumedh Thakar, president and CEO of Qualys. "At Qualys, we are committed to helping our customers stay ahead of emerging cybersecurity risk, and with Qualys TotalAI, enterprises can focus on growth and innovation, knowing they will stay protected from the most critical AI threats."

Availability
Qualys TotalAI will be available in Q4 of 2024. Sign up for early access to Qualys TotalAI and a custom Qualys TotalAI Risk Insights Report, providing

visibility into your AI and LLM risk.

Additional Resources

- Read our blog post, "De-risk Generative AI: Enterprise TruRisk Platform Advances to Secure AI and LLM Workloads"
- Sign up for the Qualys TotalAI Risk Insights Report and early access to 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.

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-advances-enterprise-trurisk-platform-to-de-risk-generative-ai-and-llm-usage-from-security-and-compliance-challenges-302213960.html

SOURCE Qualys, Inc.