FEATURE SHEET

Securing GenAI Applications From Code to Cloud

Tracing security threats from runtime to code creation in LLM-powered applications

Key Benefits

- **Secure LLM-powered application code**
  Securing applications' code according to OWASP Top 10 for LLMs guidelines, enables the early identification and remediation of potential security vulnerabilities that may arise from LLM components
- **Trace issues from cloud to the code**
  Identify and fix vulnerabilities by tracing the precise code that introduces risks, ensuring quick reinforcement of defenses against LLM-related cyber threats
- **Prove compliance**
  Ensure ongoing compliance with current regulations and prepare for future laws around LLM use.
- **Identify attacks on LLM-powered applications**
  Detect and prevent attacks instigated through LLM manipulation, ensuring business continuity by establishing necessary boundaries
- **Keep bad out**
  Configure assurance policies to detect and prevent the misuse of LLM components within code, ensuring that all integrations comply with security standards
- **Innovate with confidence**
  Secure both current and future LLM-powered applications with a unified solution that allows innovation without compromising security.

With the increasing adoption of Large Language Models (LLMs), commonly referred to as Generative AI, from providers like OpenAI and others, organizations are looking to elevate their offerings by developing LLM-powered applications. These applications aim to provide customers numerous benefits, including personalized experiences and innovative methods for querying data to gain comprehensive insights.

The use of LLM-powered applications introduces new security risks, necessitating a different development approach that includes stringent security requirements. These requirements are outlined in the OWASP Top 10 for LLMs, which details key security challenges and how to address them.

Aqua enables the detection and mitigation of these security risks during the application development process, ensuring the creation of secure LLM-powered applications. By monitoring compliance with the OWASP Top 10 for LLMs, Aqua ensures that applications are built according to industry standards, allowing organizations to innovate without compromising security.

How it works

1. With Aqua you can scan your code to identify LLM risks according to OWASP Top 10 for LLMs

2. Aqua allows you to connect runtime incidents to LLM malicious behavior and pinpoint to the code where the malicious behavior originated

3. Aqua enables the configuration of assurance policies designed to prevent the introduction of risks associated with Large Language Models (LLMs)

Aqua Security enables organizations to build LLM-powered applications with security incorporated from the first line of code all the way through to their deployment as cloud workloads allowing to trace runtime LLM-related issues identified in the workload back to the specific segments of code.

Aqua Security sees and stops attacks across the entire cloud native application lifecycle in a single, integrated platform. From software supply chain security for developers to cloud security and runtime protection for security teams, Aqua helps customers reduce risk while building the future of their businesses.

The Aqua Platform is the industry's most comprehensive Cloud Native Application Protection Platform (CNAPP). Founded in 2015, Aqua is headquartered in Boston, MA and Ramat Gan, IL with Fortune 1000 customers in over 40 countries. For more information, visit https://www.aquasec.com

Schedule a demo ›