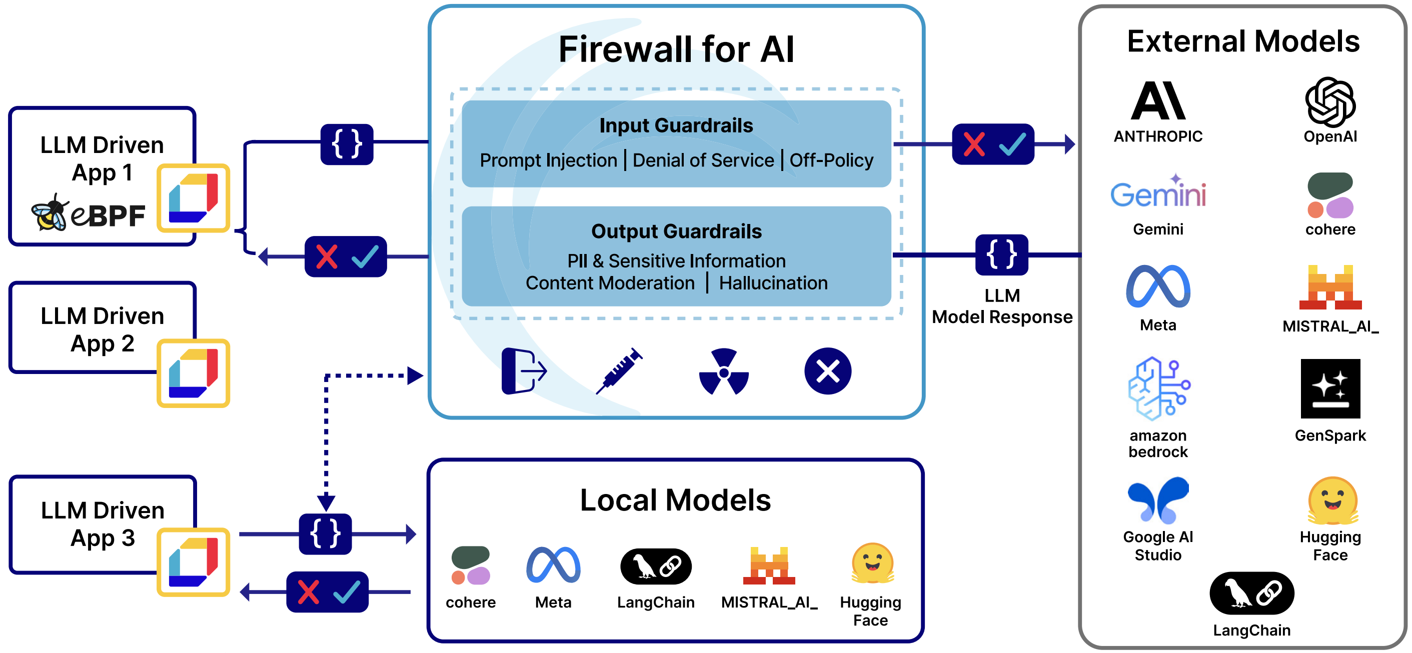
SOLUTION BRIEF

Securing AI From Container to Edge with Aqua Security and Akamai

Aqua and Akamai are partnering to create a holistic solution that protects AI applications across the enterprise. From AI discovery and governance to prompt validation and AI workload protection, this joint solution natively secures AI applications inside and outside the organization without requiring code changes or intrusive SDKs.

AI applications come in many shapes and sizes, but they all have one thing in common: they talk to their AI models in the same manner. The Aqua Enforcer protects AI applications by running embedded in the workloads themselves. By running in the AI workload, Aqua can oversee every model interaction and actively protect it. Integrating with the Akamai Firewall for AI Applications enables Aqua rapid AI prompt and output analysis. In addition, Akamai Firewall for AI adds protection for AI interactions outside of the local environment. With these capabilities working together, customers can govern and protect their vital AI applications inside and outside the organization, while taking advantage of the expansive opportunities AI models offer the business.

Discover and mitigate malicious inputs and toxic outputs holistically from the container to the edge with Akamai and Aqua.



Zero code changes required

Akamai Firewall for AI monitors and detects attack vectors for LLM models and modifies risky outputs in real-time. It protects against prompt injection, sensitive data leaks, and toxic output, among other capabilities. These Akamai protections help support explainability, compliance, and enhance financial control to ensure the AI applications meet ROI targets. In addition, Akamai Firewall for AI provides WAAP integration and leverages the Akamai security platform for a seamless integration with Edge, Cloud, and Hybrid or on-prem environments.

Building on these capabilities, Aqua adds eBPF-based runtime protection for AI workloads, delivering deep visibility and control at the container level, the critical juncture through which all AI application activity flows. By operating at this level, Aqua can observe process-level behavior, including inbound and outbound network traffic, file system access, and runtime events associated with AI components like model inference, prompt handling, and orchestration logic.

Key capabilities of the joint solution

AI and Agentic Model Discovery and Inspection

Detect and inspect AI services, models and interactions in the environment, whether they are local, managed services or SaaS platforms and monitor ingress and egress traffic.

Prompt Defense

Protect against attackers manipulating AI models through deceptive inputs, and flag hate speech, misinformation, and offensive content before delivery.

AI Workload Protection

Prevent workload compromise in real time with runtime detection and response to stop remote code execution, model tampering, suspicious model backdoors, and data poisoning attacks.

Model-Aware Behavior Profiling

Track behaviors specific to AI workloads, detect deviations from expected patterns.

Data Loss Prevention (DLP)

Detect and block sensitive data leaks in AI prompts and AI-generated responses.

Frictionless Deployment

Deploy without SDKs or infrastructure changes with minimal impact on existing AI applications.

Inspect Only Valid Traffic

When integrated inline with the Akamai security platform, to block attacks like Layer 7 DDoS and botnets attacks are blocked before they reach the AI application, reducing the volume and cost of AI protection.

Aqua Security is the pioneer in securing containerized cloud native applications. The Aqua Platform, a Cloud Native Application Protection Platform (CNAPP), enables organizations to secure every cloud native application everywhere, from code commit to runtime. With enterprise scale that doesn't slow development pipelines, Aqua secures your future in the cloud. Founded in 2015, Aqua is headquartered in Boston, MA and Ramat Gan, IL protecting over 500 of the world's largest enterprises. For more information, visit https://www.aquasec.com

Schedule a demo ›