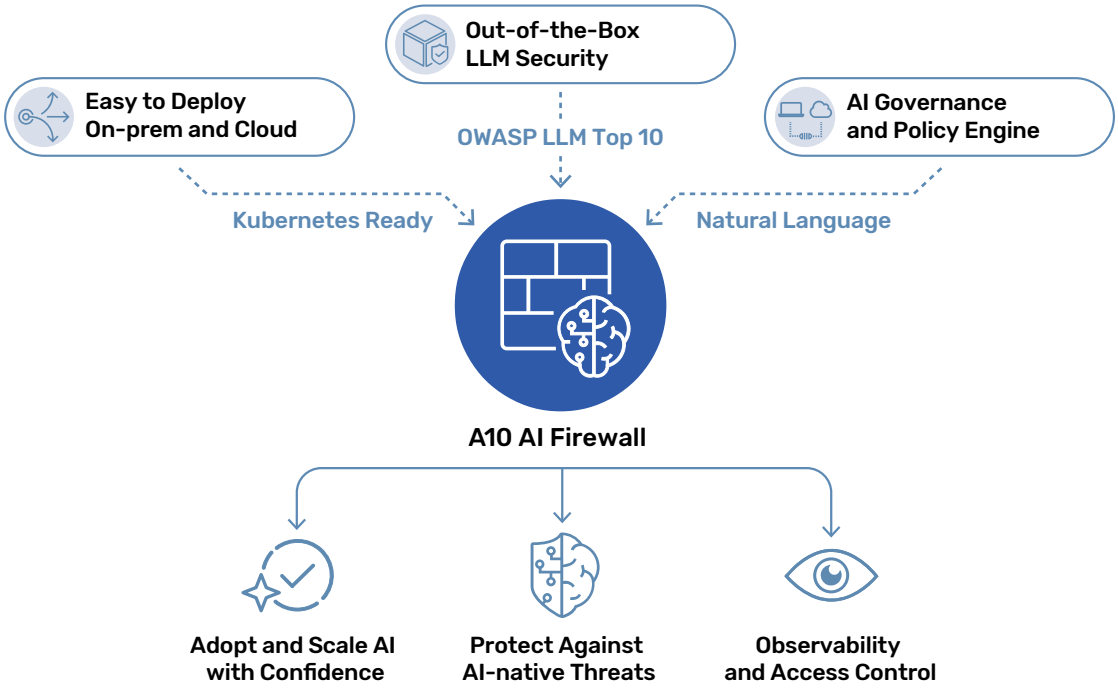
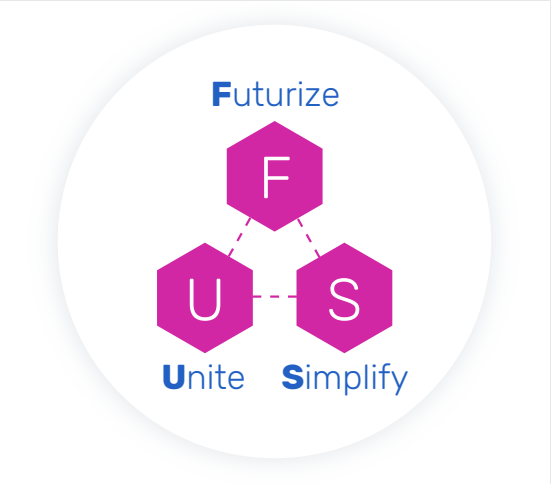
The AI-native Threat Protection and Governance Solution

Guardrails for AI, Wherever it Runs.

AI applications are rapidly becoming foundational to modern business outcomes. However, they introduce a new class of AI-native threats that traditional security tools were never designed to detect. Given the asymmetrical nature of traffic generated by AI-powered applications, the threats are semantic and embedded in the meaning and intent of natural language. As a result, they remain invisible to signature-based and pattern-matching defenses.

A10 AI Firewall is a natural language LLM guardrail system that comes as a Kubernetes-native deployment model. It integrates directly into modern AI application stacks, securing inbound and outbound orchestration traffic at runtime without any complexity or performance trade-offs.





Futurize, Unite, and Simplify (FUS) the Protection of your Application Ecosystem

- **Futurize**: Stay ahead of AI-native threats such as prompt injection, system prompt leakage, tool misuse, and unsafe outputs using semantic inspection designed for LLM-driven applications.
- **Unite**: Unify input inspection, output validation, and policy enforcement into a single runtime control point with one security layer across the entire AI interaction lifecycle.
- **Simplify**: Enterprise-grade AI governance built in, ensuring AI applications comply with enterprise policies, data protection requirements, and frameworks such as OWASP LLM Top 10 with enterprise-grade AI governance built in.

How It Works

Adopt and Scale AI with Confidence: Deploy as a low-latency appliance in the data center or natively in a Kubernetes pod, running on-premises or in the cloud. As AI traffic grows, guardrails scale automatically using elastic GPU acceleration to maintain consistent protection without performance bottlenecks. With long-context inspection, even large document uploads and RAG-based workflows are analyzed for risk. Hitless updates and intelligent session management ensure continuous protection with zero downtime, so your AI applications can scale securely and seamlessly.

Protect Against AI-native Threats: With a dual-layer inspection engine that combines natural language analysis with reasoning-based threat detection to understand both patterns and intent, A10 AI Firewall inspects every AI interaction before it reaches your application and before responses reach users. It blocks prompt injection, system prompt leakage, sensitive data exposure, tool misuse, and unsafe outputs in real time. Protection is mapped directly to the OWASP Top 10 for LLMs, ensuring coverage against AI-native vulnerabilities. Multi-label classification allows a single prompt to be evaluated for multiple risks simultaneously, increasing accuracy while minimizing false positives.

Observability and Access Control: With the A10 AI Firewall, you get security with comprehensive visibility. It can be run in monitoring mode for visibility or blocking mode for active enforcement. Granular policies allow teams to define rules by user group, application, or risk threshold. Detailed audit logs capture who asked what, when, and why a request was blocked, complete with OWASP mapping and reasoning insights. Built-in dashboards and SIEM integrations ensure AI security data aligns with enterprise governance frameworks and compliance requirements.

Ready to protect your AI-powered applications and go full throttle on AI adoption?

Reach out to the A10 team and learn how.

About A10

A10Networks.com

Contact Us

A10Networks.com/contact

Part Number: A10-BR-20125-EN-01 March 2026