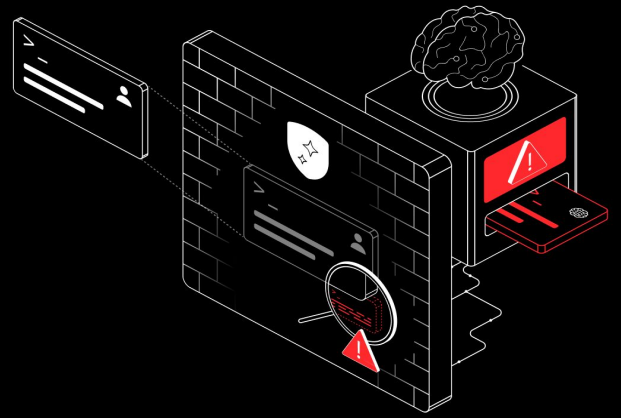


AI Firewall

Unlock your AI innovation with a firewall tailored to attacks targeting models and adjacent technologies. Protect AI applications from natural-language inputs attempting to trigger unintended actions



Automatically mitigate attacks targeting AI threat vectors

- ✓ Deploy with the flip of a switch
- ✓ Mitigate LLM specific threats
- ✓ Gain vendor and model agnostic protection

Proprietary detection & guardrails

- **Highly accurate** AI Firewall leverages an updated deployment of Fastly's proprietary SmartParse detection engine tailored to the AI attack surface.
- **Multi-layered protection** Efficacy is enhanced by our three step approach:
 1. All requests are first inspected by our modified SmartParse detection engine monitoring for LLM-specific threat categories
 2. Requests get guardrails injected into them to sanitize all responses
 3. Responses are validated for refusal responses and leak protection

32%

of organizations
are experiencing AI
prompt-based
attacks

Simple to deploy

- AI Firewall deploys with the flip of a switch within Fastly's AI Runtime Control solution. Every request destined for a model will be seamlessly inspected for threats to mitigate.

Defense in depth

- Reduce unwanted traffic destined for models by pairing AI Firewall with Fastly's Next-Gen WAF, DDoS Protection, Bot Management, and API Security solutions.

Learn more at

<https://www.fastly.com/products/ai-runtime-control>