RESUMO DO PRODUTO DA AKAMAI

Firewall for AI

O Akamai Firewall for AI é uma solução de segurança desenvolvida especificamente para proteger aplicações com tecnologia de IA, LLMs (modelos de linguagem grandes) e APIs orientadas por IA contra ciberameaças emergentes. Ao proteger consultas de IA de entrada e respostas de IA de saída, o firewall elimina as lacunas de segurança resultantes da IA generativa.

Com detecção em tempo real, aplicação baseada em políticas e medidas de segurança adaptáveis, esse firewall protege contra injeções de prompt, vazamentos de dados confidenciais, explorações de adversários e ataques de DoS (negação de serviço) específicos de IA.

Integrando-se perfeitamente a ambientes de edge, nuvem, híbridos e locais, o Firewall for AI garante segurança, proteção, governança e conformidade consistentes, ao mesmo tempo em que preserva o desempenho.

Proteção contra ameaças específicas de IA

O Firewall for AI fornece segurança abrangente para aplicações orientadas por IA, identificando e mitigando vulnerabilidades específicas de IA que as ferramentas de segurança tradicionais não conseguem resolver.

- **Defesa contra injeções de prompt**: protege contra invasores que manipulam modelos de IA por meio de entradas enganosas.
- **DLP (prevenção contra perda de dados)**: detecta e bloqueia vazamentos de dados confidenciais em respostas geradas por IA e protege contra o recebimento de dados confidenciais nas solicitações.
- **Filtragem de conteúdo tóxico e prejudicial**: sinaliza discurso de ódio, informações erradas e conteúdo ofensivo antes da entrega.
- **Segurança de IA contra adversários**: protege contra execução remota de código, backdoors de modelo e ataques de envenenamento de dados.
- **Mitigação de negação de serviço**: mitiga ataques de DoS por IA controlando o uso excessivo de consultas e a sobrecarga de modelos.

Benefícios para a sua empresa

Postura de segurança de IA unificada
Segurança de IA padronizada em ambientes de edge, nuvem, híbridos e locais

Detecção automatizada de ameaças de IA
Proteções específicas de IA sem ajuste manual de regras

Integração perfeita da WAAP
Estende a WAAP (proteção de aplicações web e APIs) com defesas de IA

Evita o uso indevido de IA e riscos legais
Bloqueia vazamentos de dados, roubo de IP e violações regulatórias

Segurança de IA simplificada
Não é necessário que engenheiros internos apliquem manualmente políticas de segurança

Flexibilidade multinuvem
Protege as cargas de trabalho de IA em todos os ambientes

Proteção de IA de nível empresarial
Com a inteligência global da Akamai contra ameaças

Opções flexíveis de implantação

O Firewall for AI oferece vários modelos de implantação adaptados para diferentes arquiteturas de IA e ambientes de nuvem.

Modelo de implantação	Descrição
Integração de edge da Akamai	Protege as aplicações de IA em linha na edge da Akamai com aplicação de segurança de baixa latência.
API REST	Verifica entradas e saídas de IA por meio de detecção e pontuação de riscos com base em APIs.
Implementação de proxy reverso (recurso de roteiro)	Encaminha o tráfego de IA por meio do proxy seguro da Akamai para inspeção e filtragem detalhadas.

Essa flexibilidade permite que as organizações protejam os LLMs implantados em qualquer lugar, incluindo ambientes multinuvem, híbridos e locais.

Como funciona

Análise de tráfego de IA

O firewall monitora e analisa as interações de IA, inspecionando os prompts de entrada do usuário e os resultados gerados por IA para detectar possíveis ameaças antes que elas cheguem ao modelo ou ao usuário final. Ao analisar o ciclo de resposta a consultas da IA, o firewall evita riscos à segurança e preserva o desempenho das aplicações com eficiência.

Pontuação de risco e resposta adaptável a ameaças

As interações de IA são avaliadas com base em vários indicadores de segurança, incluindo injeções de prompt, exposição de dados confidenciais e explorações de adversários.

Ações de aplicação de segurança

O Firewall for AI impõe três medidas de segurança essenciais com base na pontuação de risco e no apetite por risco do cliente:

- **Monitorar:** Registra ameaças detectadas para análise sem interferir nas consultas ou respostas de IA.
- **Modificar:** Ajusta as saídas geradas por IA em linha, removendo ou alterando conteúdo impróprio enquanto mantém um fluxo de conversação natural.
- **Negar:** Impede que entradas de alto risco cheguem ao modelo de IA e impede que respostas impróprias sejam retornadas aos usuários.

Conformidade e confiança na governança

O Firewall for AI pode ajudar no cumprimento dos padrões de segurança e conformidade. À medida que as aplicações orientadas por IA acabam por trazer novos desafios regulatórios, é fundamental manter a supervisão da privacidade de dados, da integridade do modelo e dos riscos de segurança.

Alinhamento regulatório

O firewall pode ajudar as organizações a cumprir as diretrizes de privacidade, segurança e proteção. Ao impor políticas de segurança específicas de IA, as empresas podem mitigar os riscos relacionados a regulamentos de proteção de dados, uso de IA ética e exigências de governança corporativa.

Análise e registro de segurança

O Firewall for AI fornece registros de auditoria detalhados e análises de segurança em tempo real, proporcionando às equipes de segurança visibilidade dos eventos de segurança de IA. Ao monitorar padrões de consulta, indicadores de ameaça e comportamentos de resposta, as organizações podem detectar anomalias, aplicar controles de políticas e gerar relatórios de conformidade de forma proativa.

Proteção de IA de nível empresarial

Com a inteligência global da Akamai contra ameaças, o firewall se adapta continuamente às crescentes ameaças à segurança de IA. Ao utilizar os insights de dados em tempo real da pesquisa de segurança de IA e da modelagem de ameaças, as organizações podem manter uma postura de segurança resiliente e garantir que suas aplicações de IA operem com segurança e responsabilidade.

Fale com um especialista para saber mais.