AKAMAI-PRODUKTBESCHREIBUNG

Firewall for AI

Akamai Firewall for AI ist eine speziell entwickelte Sicherheitslösung, die KI-basierte Anwendungen, LLMs (Large Language Model, großes Sprachmodell) und KI-basierte APIs vor aufkommenden Cyberbedrohungen schützt. Durch die Sicherung eingehender KI-Abfragen und ausgehender KI-Antworten schließt die Firewall Sicherheitslücken, die durch generative KI-Technologien entstehen.

Dank Echtzeiterkennung, richtlinienbasierter Durchsetzung und adaptiven Sicherheitsmaßnahmen schützt diese Firewall vor Prompt-Injections, Lecks sensible Daten, ausnutzbaren Schwachstellen und KI-spezifischen Denial-of-Service-Angriffen (DoS).

Firewall for AI lässt sich nahtlos in Edge-, Cloud-, Hybrid- und On-Premise-Umgebungen integrieren und gewährleistet konsistente Sicherheit, Governance und Compliance bei gleichbleibender Performance.

KI-spezifischer Bedrohungsschutz

Firewall for AI bietet umfassende Sicherheit für KI-gesteuerte Anwendungen, indem KI-spezifische Schwachstellen identifiziert und abgemildert werden, die von herkömmlichen Sicherheitstools nicht behoben werden.

- **Prompt-Injection-Abwehr** – schützt vor Angreifern, die KI-Modelle durch betrügerische Eingaben manipulieren.
- **DLP (Data Loss Prevention, Schutz vor Datenverlust)** – erkennt und blockiert sensible Datenlecks in KI-generierten Antworten und schützt vor dem Empfang vertraulicher Daten in den Anfragen.
- **Filterung toxischer und schädlicher Inhalte** – kennzeichnet Äußerungen, Fehlinformationen und anstößige Inhalte vor der Ausgabe.
- **Sicherheit der KI vor Angreifern** – schützt vor Remote-Code-Ausführung, Modell-Backdoors und Data Poisoning.
- **Denial-of-Service-Abwehr** – wehrt KI-gesteuerte DoS-Angriffe ab, indem übermäßige Abfrageauslastung und Modellüberlastung kontrolliert werden.

Vorteile für Ihr Unternehmen

Einheitliche KI-Sicherheitsstrategie
Standardisierte KI-Sicherheit über Edge-, Cloud-, Hybrid- und On-Premise-Systeme hinweg

Automatisierte Erkennung von KI-Bedrohungen
KI-spezifische Schutzmaßnahmen ohne manuelle Regelabstimmung

Nahtlose WAAP-Integration
Erweitert den Schutz von Webanwendungen und APIs (WAAP) um KI-Abwehrmechanismen

Verhindert den Missbrauch von KI und rechtliche Risiken
Blockiert Datenlecks, IP-Diebstahl und gesetzliche Verstöße

Einfachere KI-Sicherheit
Interne Techniker müssen Sicherheitsrichtlinien nicht manuell durchsetzen

Multicloud-Flexibilität
Schützt KI-Workloads in verschiedenen Umgebungen

KI-Schutz auf Unternehmensebene
Unterstützt von der globalen Threat Intelligence von Akamai

Flexible Bereitstellungsoptionen

Firewall for AI bietet mehrere Bereitstellungsmodelle, die auf verschiedene KI-Architekturen und Cloudumgebungen zugeschnitten sind.

Bereitstellungsmodell	Beschreibung
Akamai-Edge-Integration	Schützt KI-Anwendungen inline an der Akamai-Edge durch Sicherheitsdurchsetzung mit geringer Latenz.
REST API	Scannt KI-Eingaben und -Ausgaben über API-basierte Risikoerkennung und -Bewertung.
Reverse-Proxy-Bereitstellung (Roadmap-Funktion)	Leitet den KI-Traffic über den sicheren Proxy von Akamai zur gründlichen Überprüfung und Filterung weiter.

Diese Flexibilität ermöglicht es Unternehmen, LLMs überall bereitzustellen, einschließlich Multicloud-, Hybrid- und On-Premise-Umgebungen.

So funktioniert es

KI-Trafficanalyse

Die Firewall überwacht und analysiert KI-Interaktionen und überprüft eingehende Nutzer-Prompts und KI-generierte Ausgaben, um potenzielle Bedrohungen zu erkennen, bevor sie das Modell oder den Endnutzer erreichen. Durch die Analyse des KI-Zyklus von Anfrage und Antwort verhindert die Firewall effektiv Sicherheitsrisiken, während die Anwendungsperformance erhalten bleibt.

Risikobewertung und adaptive Bedrohungsreaktion

Interaktionen mit KI werden anhand mehrerer Sicherheitsindikatoren bewertet, einschließlich der Prompt-Injections, der Offenlegung sensibler Daten und der Ausnutzung von Schwachstellen.

Maßnahmen zur Durchsetzung der Sicherheit

Firewall for AI setzt drei kritische Sicherheitsmaßnahmen basierend auf der Risikobewertung und der Risikobereitschaft des Kunden durch:

- **Überwachen:** Protokolliert erkannte Bedrohungen zur Analyse, ohne KI-Abfragen oder -Antworten zu stören.
- **Ändern:** Passt KI-generierte Ausgaben inline an, entfernt oder ändert unsichere Inhalte und hält gleichzeitig einen natürlicher Gesprächsfluss aufrecht.
- **Ablehnen:** Verhindert, dass Eingaben mit hohem Risiko das KI-Modell erreichen und dass unsichere Antworten an Nutzer zurückgegeben werden.

Vertrauen in Bezug auf Compliance und Governance

Firewall for AI kann Sie dabei unterstützen, Sicherheits- und Compliance-Standards zu erfüllen. Da KI-gesteuerte Anwendungen neue regulatorische Herausforderungen mit sich bringen, ist die Überwachung des Datenschutzes, der Modellintegrität und der Sicherheitsrisiken von entscheidender Bedeutung.

Ausrichtung an Rechtsvorschriften

Die Firewall kann Unternehmen dabei unterstützen, Datenschutz- und Sicherheitsrichtlinien einzuhalten. Durch die Durchsetzung KI-spezifischer Sicherheitsrichtlinien können Unternehmen Risiken im Zusammenhang mit Datenschutzvorschriften, ethischer KI-Nutzung und Corporate-Governance-Vorgaben mindern.

Sicherheitsanalysen und Protokollierung

Firewall for AI bietet detaillierte Prüfprotokolle und Echtzeit-Sicherheitsanalysen, sodass Sicherheitsteams Einblick in KI-Sicherheitsereignisse erhalten. Durch die Überwachung von Abfragemustern, Bedrohungsindikatoren und Reaktionsverhalten können Unternehmen Anomalien proaktiv erkennen, Richtlinienkontrollen durchsetzen und Compliance-Berichte erstellen.

KI-Schutz auf Unternehmensebene

Die Firewall wird von der globalen Threat Intelligence von Akamai gestützt und passt sich kontinuierlich an neue KI-Sicherheitsbedrohungen an. Durch die Nutzung von Echtzeit-Dateneinblicken aus KI-Sicherheitsforschung und Bedrohungsmodellierung können Unternehmen eine resiliente Sicherheitslage beibehalten und gleichzeitig sicherstellen, dass ihre KI-Anwendungen sicher und verantwortungsvoll funktionieren.

Sprechen Sie mit einem Experten, um mehr zu erfahren.