FICHE PRODUIT AKAMAI

Firewall for AI

Akamai Firewall for AI est une solution de sécurité spécialement conçue pour protéger les applications basées sur l'IA, les grands modèles de langage (LLM) et les API basées sur l'IA contre les cybermenaces émergentes. En sécurisant les requêtes d'IA entrantes et les réponses d'IA sortantes, le pare-feu comble les lacunes en matière de sécurité introduites par l'IA générative.

Grâce à la détection en temps réel, à l'application de règles et à des mesures de sécurité adaptatives, ce pare-feu protège contre les injections rapides, les fuites de données sensibles, les failles de sécurité et les attaques par déni de service (DoS) spécifiques à l'IA.

S'intégrant de manière fluide aux environnements en bordure de l'Internet, aux environnements cloud, hybrides et sur site, Firewall for AI garantit une sécurité, une sûreté, une gouvernance et une conformité cohérentes tout en préservant les performances.

Protection contre les menaces spécifiques à l'IA

Firewall for AI assure une sécurité complète des applications basées sur l'IA en identifiant et en atténuant les vulnérabilités spécifiques à l'IA que les outils de sécurité traditionnels ne parviennent pas à traiter.

- **Défense contre l'injection de prompt** : protège contre les attaquants qui manipulent les modèles d'IA à l'aide de saisies malveillantes.
- **Prévention des pertes de données (DLP)** : détecte et bloque les fuites de données sensibles dans les réponses générées par l'IA et protège contre la réception de données sensibles dans les requêtes.
- **Filtrage du contenu toxique et nuisible** : signale les propos haineux, les informations erronées et les contenus offensants avant leur diffusion.
- **Sécurité contre l'IA malveillante** : protection contre l'exécution de code à distance, les portes dérobées de modèles et les attaques par empoisonnement de données.
- **Atténuation des attaques par déni de service** : atténue les attaques DoS basées sur l'IA en contrôlant l'utilisation excessive des requêtes et la surcharge des modèles.

Avantages pour votre entreprise

Stratégie de sécurité de l'IA unifiée
Sécurité de l'IA standardisée en bordure de l'Internet, dans le cloud, dans les environnements hybrides et sur site

Détection automatisée des menaces liées à l'IA
Protections spécifiques à l'IA sans réglage manuel des règles

Intégration WAAP fluide
Étend la protection des applications Web et des API (WAAP) grâce à des dispositifs de défense basés sur l'IA

Empêche l'utilisation abusive de l'IA et les risques juridiques
Bloque les fuites de données, le vol de propriété intellectuelle et les violations réglementaires

Sécurité de l'IA simplifiée
Ne nécessite pas l'intervention d'ingénieurs internes pour appliquer manuellement les politiques de sécurité

Flexibilité multicloud
Protège les charges de travail d'IA dans tous les environnements

Protection de l'IA de niveau entreprise
S'appuie sur les informations complètes sur les menaces d'Akamai

Options de déploiement flexibles

Firewall for AI offre plusieurs modèles de déploiement adaptés à différentes architectures IA et différents environnements cloud.

Modèle de déploiement	Description
Intégration en bordure de l'Internet Akamai	Protège les applications d'IA en bordure de l'Internet Akamai avec une mise en œuvre de la sécurité à faible latence.
API REST	Analyse les entrées et sorties d'IA via la détection et l'évaluation des risques basées sur une API.
Déploiement de proxy inverse (fonctionnalité de feuille de route)	Achemine le trafic IA via le proxy sécurisé d'Akamai pour une inspection et un filtrage approfondis.

Cette flexibilité permet aux entreprises de sécuriser les LLM déployés partout, y compris dans des environnements multicloud, hybrides et sur site.

Fonctionnement

Analyse du trafic IA

Le pare-feu surveille et analyse les interactions de l'IA, en inspectant les invites utilisateur entrantes et les sorties générées afin de détecter les menaces potentielles avant qu'elles n'atteignent le modèle ou l'utilisateur final. En analysant le cycle de requête-réponse de l'IA, le pare-feu prévient efficacement les risques de sécurité tout en préservant les performances des applications.

Évaluation des risques et réponse adaptative aux menaces

Les interactions de l'IA sont évaluées en fonction de plusieurs indicateurs de sécurité, notamment les injections d'invites, l'exposition de données sensibles et les exploits malveillants.

Mesures de sécurité

Firewall for AI applique trois mesures de sécurité essentielles en fonction de l'évaluation du risque et de l'appétence au risque du client :

- **Surveillance :** enregistre les menaces détectées pour les analyser sans interférer avec les requêtes ou les réponses de l'IA.
- **Modification :** ajuste les résultats générés par l'IA en ligne, en supprimant ou en modifiant les contenus dangereux tout en maintenant un flux de conversation naturel.
- **Refus :** empêche les saisies à haut risque d'atteindre le modèle d'IA et évite le renvoi de réponses dangereuses aux utilisateurs.

Confiance en matière de conformité et de gouvernance

Firewall for AI vous aide à respecter les normes de sécurité et de conformité. Les applications basées sur l'IA posant de nouveaux défis réglementaires, il est essentiel de maintenir une surveillance de la confidentialité des données, de l'intégrité des modèles et des risques de sécurité.

Alignement réglementaire

Le pare-feu permet aux entreprises de se conformer aux directives en matière de protection de la vie privée, de sûreté et de sécurité. En appliquant des politiques de sécurité spécifiques à l'IA, les entreprises peuvent atténuer les risques liés aux réglementations en matière de protection des données, à l'utilisation éthique de l'IA et aux obligations de gouvernance d'entreprise.

Analyse et journalisation de la sécurité

Firewall for AI fournit des journaux d'audit détaillés et des analyses de sécurité en temps réel, offrant aux équipes de sécurité une visibilité sur les événements de sécurité liés à l'IA. La surveillance des modèles de requêtes, des indicateurs de menaces et des comportements de réponse permet aux entreprises de détecter de manière proactive les anomalies, d'appliquer des contrôles de règle et de générer des rapports de conformité.

Protection de l'IA de niveau entreprise

S'appuyant sur les informations complètes sur les menaces d'Akamai, le pare-feu s'adapte en permanence aux nouvelles menaces de sécurité liées à l'IA. En exploitant les informations en temps réel issues de la recherche en matière de sécurité de l'IA et de la modélisation des menaces, les entreprises sont en mesure de maintenir une posture de sécurité résiliente tout en garantissant le fonctionnement sûr et responsable de leurs applications d'IA.

Échangez avec un expert pour en savoir plus.