DESCRIZIONE DEL PRODOTTO AKAMAI

Firewall for AI

Akamai Firewall for AI è una soluzione per la sicurezza appositamente progettata per proteggere applicazioni e API basate sull'AI, oltre ai modelli LLM (Large Language Model), dalle emergenti minacce informatiche. Proteggendo le domande dell'AI in entrata e le relative risposte in uscita, il firewall colma le falle nella sicurezza introdotte dall'AI generativa.

Con funzioni di rilevamento in tempo reale, applicazione delle regole basate su policy e misure di sicurezza adattiva, questo firewall protegge da attacchi di tipo injection dei prompt, tentativi di fuga dei dati sensibili, exploit dannosi e attacchi DoS (Denial-of-Service) sferrati contro l'AI.

Integrandosi perfettamente con l'edge, il cloud, gli ambienti ibridi e on-premise, Firewall for AI garantisce caratteristiche di sicurezza, affidabilità, governance e conformità, preservando, al contempo, un elevato livello di performance.

Una protezione dalle minacce specifica per l'AI

Firewall for AI fornisce una sicurezza completa per le applicazioni basate sull'AI identificando e mitigando le vulnerabilità specifiche dell'AI che i tradizionali strumenti di sicurezza non riescono a gestire.

- **Difesa dagli attacchi di tipo injection dei prompt:** la soluzione protegge dalla manipolazione dei modelli di AI effettuata dai criminali con input dannosi.
- **Prevenzione della perdita di dati (DLP):** rileva e blocca le fughe di dati sensibili nelle risposte generate dall'AI e protegge dalla ricezione di dati sensibili nelle richieste.
- **Filtraggio di contenuti inappropriati e dannosi**: la soluzione segnala la presenza di contenuti di incitamento all'odio, informazioni errate e contenuti offensivi prima di trasmetterli.
- **Protezione dell'AI dai criminali**: la soluzione protegge dall'esecuzione di codice remoto, dalle backdoor dei modelli e dagli attacchi di data poisoning.
- **Mitigazione degli attacchi DoS (Denial-of-Service)**: mitiga gli attacchi DoS basati sull'AI controllando l'eccessivo utilizzo delle query e il sovraccarico dei modelli.

Vantaggi per le aziende

Approccio alla sicurezza dell'AI unificata
Sicurezza dell'AI standardizzata sull'edge, nel cloud, in ambienti ibridi e on-premise

Rilevamento automatizzato delle minacce all'AI
Sistemi di protezione specifici per l'AI senza una modifica manuale delle regole

Perfetta integrazione con le soluzioni WAAP
Estende le funzionalità delle soluzioni WAAP (Web Application and API Protection) con i sistemi di difesa dell'AI

Previene l'uso improprio dell'AI e i rischi legali correlati
Blocca le fughe di dati, il furto dell'IP e le violazioni di normative

Sicurezza dell'AI semplificata
Non sono richiesti tecnici in-house per l'applicazione manuale delle policy di sicurezza

Flessibilità multicloud
Protegge i carichi di lavoro dell'AI in vari ambienti

Efficace protezione dell'AI
Supportato dall'intelligence globale sulle minacce di Akamai

Opzioni di implementazione flessibili

Firewall for AI offre più modelli di implementazione in base ai diversi ambienti cloud e alle varie architetture dell'AI.

Modello di implementazione	Descrizione
Integrazione sull'edge di Akamai	Protegge le applicazioni basate sull'AI in corrispondenza dell'edge di Akamai con un sistema di sicurezza a bassa latenza.
API REST	Esegue la scansione di input e output dell'AI tramite un sistema di rilevamento e classificazione dei rischi basato sulle API.
Implementazione di un proxy inverso (funzionalità di roadmap)	Instrada il traffico dell'AI tramite il proxy sicuro di Akamai per consentire di eseguire approfondite operazioni di ispezione e filtraggio.

Questa flessibilità consente alle organizzazioni di proteggere i modelli LLM implementati ovunque, inclusi ambienti multicloud, ibridi e on-premise.

Come funziona

Analisi del traffico dell'AI

Il firewall monitora e analizza le interazioni dell'AI, esaminando i prompt degli utenti in entrata e gli output generati dall'AI per rilevare le potenziali minacce prima che raggiungano il modello o gli utenti finali. Analizzando il ciclo di domande e risposte dell'AI, il firewall previene in modo efficace i rischi per la sicurezza, preservando, al contempo, l'elevato livello di performance delle applicazioni.

Classificazione dei rischi e risposta adattiva alle minacce

Le interazioni dell'AI vengono valutate sulla base di diversi indicatori relativi alla sicurezza, tra cui attacchi di tipo injection dei prompt, esposizione dei dati sensibili ed exploit dannosi.

Applicazione delle misure di sicurezza

La soluzione Firewall for AI rafforza tre fondamentali misure di sicurezza basate sulla valutazione dei rischi e sulla propensione al rischio dei clienti:

- **Monitoraggio:** le minacce rilevate vengono registrate a scopo di analisi senza interferire con le domande o le risposte dell'AI.
- **Modifica:** gli output generati dall'AI vengono modificati, rimuovendo o alterando i contenuti non sicuri per mantenere un flusso naturale nella conversazione.
- **Rifiuto:** la soluzione impedisce agli input ad alto rischio di raggiungere il modello di AI e previene la ricezione di risposte non sicure da parte degli utenti.

Conformità e governance con la massima tranquillità

La soluzione Firewall for AI può aiutare a soddisfare gli standard di sicurezza e conformità. Le applicazioni basate sull'AI introducono nuovi problemi in termini di normative, pertanto è fondamentale mantenere la supervisione sulla privacy dei dati, sull'integrità dei modelli e sui rischi per la sicurezza.

Allineamento alle normative

Il firewall può aiutare le organizzazioni a conformarsi alle linee guida su privacy, integrità e sicurezza. Applicando le policy di sicurezza specifiche dell'AI, le aziende possono mitigare i rischi relativi alle normative in materia di protezione dei dati, ad un utilizzo etico dell'AI e agli obblighi di governance aziendale.

Analisi e registri di sicurezza

La soluzione Firewall for AI fornisce registri di verifica dettagliati e analisi della sicurezza in tempo reale, offrendo ai team addetti alla sicurezza la necessaria visibilità sugli eventi di sicurezza dell'AI. Monitorando i modelli delle domande, gli indicatori delle minacce e i comportamenti delle risposte, le organizzazioni possono rilevare in modo proattivo le anomalie, applicare i controlli delle policy e generare i rapporti sulla conformità.

Efficace protezione dell'AI

Supportato dall'intelligence globale sulle minacce di Akamai, il firewall si adatta continuamente alle minacce sulla sicurezza dell'AI. Utilizzando le informazioni sui dati in tempo reale ricavati dalle ricerche sulla sicurezza dell'AI e dalla modellazione delle minacce, le organizzazioni possono mantenere un sistema di sicurezza resiliente, garantendo, al contempo, alle loro applicazioni basate sull'AI di operare in modo sicuro e responsabile.

Parlate con un esperto per ulteriori informazioni.