Beschleunigen Sie die KI-Einführung mit integrierter Sicherheit

KI hält Einzug, während klassische Sicherheitsmethoden ins Hintertreffen geraten

98 %

der Unternehmen haben nicht genehmigte Apps, einschließlich Schatten-KI. Diese blinden Flecken bergen das Risiko von Compliance-Verstößen und der Offenlegung von Daten.[1]

50 %

Erfolgsrate von Prompt-Injection-Angriffen, die wichtigste Sicherheitsbedrohung in den OWASP Top 10 für LLM-Anwendungen.[2]

97 %

der Unternehmen, die mit KI-bezogenen Sicherheitsvorfällen konfrontiert waren, verfügten nicht über angemessene KI-Zugriffskontrollen.[3]

93 %

der Angestellten geben zu, ohne Genehmigung Informationen in KI-Tools eingegeben zu haben.[4]

Sichern Sie den KI-Lebenszyklus mit Cloudflare

über generative und agentenbasierte KI hinweg

Mensch-zu-KI-Sicherheit

Ihre Belegschaft

Ihre Kunden

- Erkennung
- Nutzungskontrollen
- Datensicherheit
- Bedrohungsabwehr
- Einheitliche Verwaltung

Öffentliche oder private KI-Anwendungen (für Ihre Belegschaft)

KI-fähige Apps (für Ihre Kunden)

Agentenbasierte KI-Sicherheit

KI-Agent

- Überblick
- Authentifizierung
- Bedrohungsabwehr
- Einheitliche Verwaltung

Firmenressourcen (APIs, MCP-Server, Webserver usw.)

Mehr Transparenz
über KI-Apps, API-Endpunkte und KI-Agenten- und MCP-Verbindungen hinweg

Risiken verwalten
mit Leitplanken, Sicherheitskontrolle und Echtzeit-Bedrohungsabwehr

Daten schützen
mit Prompt-Schutz und Zugriffskontrollen für Mitarbeitende und KI-Agenten

Sicherheit ist integriert

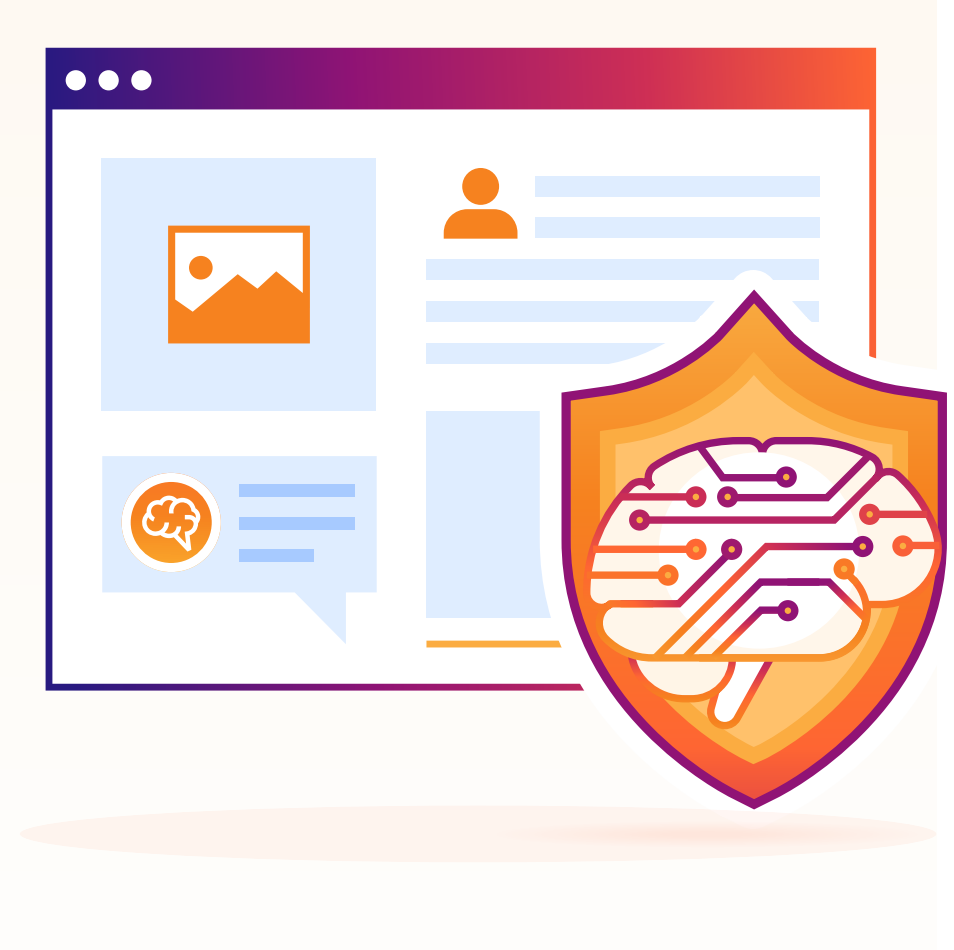
bei der Entwicklung von KI auf Cloudflare

Sichere GenAI-Nutzung durch Mitarbeitende

- Erkennen Sie Schatten-KI
- Bewerten Sie die Risiken von KI-Apps
- Verwalten Sie den Status der KI-App
- Schränken Sie die Eingabe sensibler Daten ein
- Setzen Sie Leitplanken in Prompts und Antworten durch

KI-fähige Anwendungen und Workloads schützen

- Entdecken Sie Schatten-KI-Endpunkte
- Schützen Sie KI-Modelle und Trainingsdaten vor Missbrauch
- Verhindern Sie, dass personenbezogene Daten in Prompts und Antworten offengelegt werden
- Erzwingen Sie die Moderation von Inhalten



Die Produktentwicklung schützen

- Erstellen Sie MCP-Server mit integrierter Authentifizierung/Autorisierung
- Protokollieren und beschränken Sie Anfragen/Antworten von KI-Modellen, Token-Verwendung und Kosten
- Verhindern Sie Service-Unterbrechungen mit Fallback-Modellen und Rate Limiting

Cloudflare macht den Unterschied

Umfassender Schutz des KI-Lebenszyklus

Eine einzige Plattform zur Absicherung der Kommunikation zwischen Mensch und KI und zwischen KI und Ressource – von der Entwicklung bis zur Bereitstellung.

Inline-KI-Sicherheit in Echtzeit

Sichern Sie KI-Prompts und -Antworten in Echtzeit mit Kontrollen, die öffentliche und private KI-Umgebungen abdecken.

Zukunftssichere globale KI-Architektur

Nutzen Sie unser globales Netzwerk für eine einheitliche Edge-Durchsetzung mit dem Umfang und der Performance, die KI erfordert.

Modellunabhängige Bereitstellung

Sicherheitskontrollen funktionieren für alle KI-Modelle in Ihrer Umgebung und bieten einen einheitlichen Ansatz zur Steuerung der KI-Implementierung.

Kundenreferenzen

indeed

Die weltweite Stellenbörse Nr. 1

Identifiziert und steuert Schatten-KI

parallel zum Projekt zur Modernisierung des Remote-Zugriffs

KI-fähiges SaaS-Unternehmen

Schützt PII

indem Kunden daran gehindert werden, sensible Informationen an öffentlich zugängliche GenAI-Endpunkte zu übermitteln

Cyndx

KI-gesteuertes Fintech

Reduziert Inferenzkosten um 95 %

durch den Einsatz von Cloudflare zur Zwischenspeicherung und Ausführung von Antworten von KI-Modellanbietern

Entdecken Sie, wie Cloudflare Ihre KI-Einführung sichern kann

Anwendungsfälle entdecken

---

1. Varonis, „2025 State of Data Security".
2. Liu, S., Wang, Z., Chen, Y., Deng, G., Liu, Y., & Liu, Y. (2024). Automatic and Universal Prompt Injection Attacks against Large Language Models.
3. IBM, 2025 Cost of a Data Breach
4. ManageEngine, The Shadow AI Surge in Enterprises

+49 89 2555 2276 | enterprise@cloudflare.com | www.cloudflare.com/de-de/

REV:BDES-8274.2025OCT13