CLOUDFLARE

KURZDARSTELLUNG

Cloudflare AI Security Suite

Sichern Sie KI-Interaktionen durch Datenkontrolle und Risikomanagement während Ihres gesamten KI-Lebenszyklus.

KI sicher skalieren

KI-Risiken erfordern moderne Sicherheit

Ihre Teams nutzen KI, um Innovationen schneller voranzutreiben, aber dies führt zu kritischen Sicherheitsrisiken. Die alte Vorgehensweise, KI zu blockieren oder komplexe Einzellösungen hinzuzufügen, ist zum Scheitern verurteilt, da sie Innovationen unterdrückt und die Realität ignoriert:

- **85 % der Mitarbeitenden** nutzen KI-Tools, bevor die IT-Abteilung sie überprüfen kann.[1]
- **93 % geben zu,** dass sie Unternehmensdaten ohne Genehmigung in KI-Systeme eingeben.[2]
- **63 % der von einem Datenverstoß betroffenen** Unternehmen haben keine KI-Governance-Richtlinien.[1]

Lernen Sie, wie Sie Ihre Teams stärken und die Produktivitätsvorteile der KI nutzen können, während Sie gleichzeitig die Sicherheit und Kontrolle gewährleisten, die Ihr Unternehmen benötigt.

Eine einheitliche Plattform zur Sicherung von agentenbasierter und generativer KI

Cloudflare stellt eine umfassende Plattform bereit, mit der Ihre Organisation KI sicher und effektiv einsetzen kann. Sicherheitsverantwortliche erhalten Werkzeuge zur Risikosteuerung, IT-Teams werden produktiver, und Plattformingenieure können sicher entwickeln – damit alle gemeinsam sicher innovieren können.

Erste Schritte mit der Cloudflare AI Security Suite

Die Cloudflare AI Security Suite wird auf einer einheitlichen Plattform bereitgestellt, um die Nutzung von KI-Tools am Arbeitsplatz und öffentlich zugängliche Anwendungen zu sichern. Entdecken Sie Schatten-KI, schützen Sie Modelle vor Missbrauch, sichern Sie den Agentenzugriff und verhindern Sie die Datenoffenlegung in Prompts – damit Ihr Unternehmen sicher und effizient mit verbesserter Transparenz und stärkerer Kontrolle innovieren kann.

Transparenz ausweiten

über KI-Anwendungen, API-Endpunkte und KI-Agenten-Verbindungen hinweg.

Risiken abwehren

mit Leitplanken, Statuskontrolle und Echtzeit-Bedrohungsabwehr.

Daten schützen

mit Prompt-Schutzmaßnahmen und Nutzungskontrollen für Mitarbeitende und KI-Agenten.

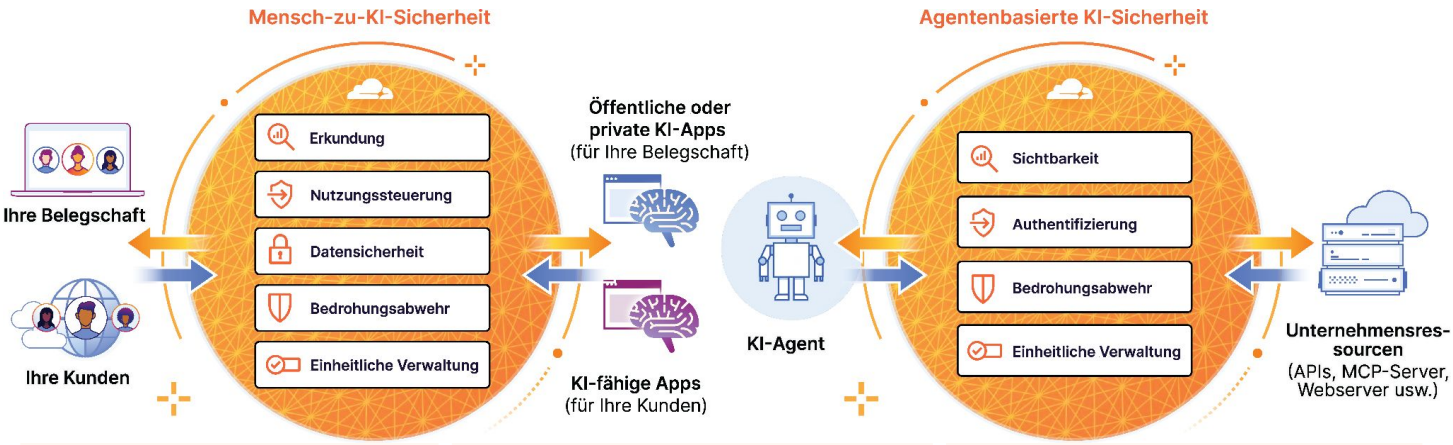
Sicherheit ist ein integraler Bestandteil
der KI-Entwicklung auf Cloudflare.

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

REV:PMM-OCT2025

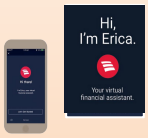
Sichere generative und agentenbasierte KI-Kommunikation mit der Cloudflare AI Security Suite

Schützen Sie die gesamte KI-Kommunikation, indem Sie die Daten kontrollieren, die Ihre Mitarbeitenden in generativer KI verwenden, und die Sicherheitsrisiken, die von autonomen Agenten ausgehen, verwalten.



- **Ihre Belegschaft:** Angestellte, Auftragnehmer, Entwickler usw.
- **Ihre Kunden:** Besucher Ihrer Websites und Apps

- **Generative KI-Anwendungen:** Eigenständig oder eingebettet
  Gemini, Claude, ChatGPT, Copilot
- **KI-gestützte Apps** Beispiel: Erica, der KI-Chatbot der Bank of America



- **APIs** und **MCP-Server** für jede Anwendung.
- **Webserver** für Inferenz und Retrieval-Augmented Generation (RAG)

Google Workspace

Beschleunigen Sie die KI-Einführung mit integrierter Sicherheit über den gesamten KI-Lebenszyklus hinweg

Die KI-Nutzung durch Mitarbeitende sichern

Implementieren Sie KI-Nutzungskontrollen und Verwaltung der KI-Sicherheitsmaßnahmen (AI Security Posture Management, AI-SPM), um Risiken zu minimieren und Daten zu schützen.

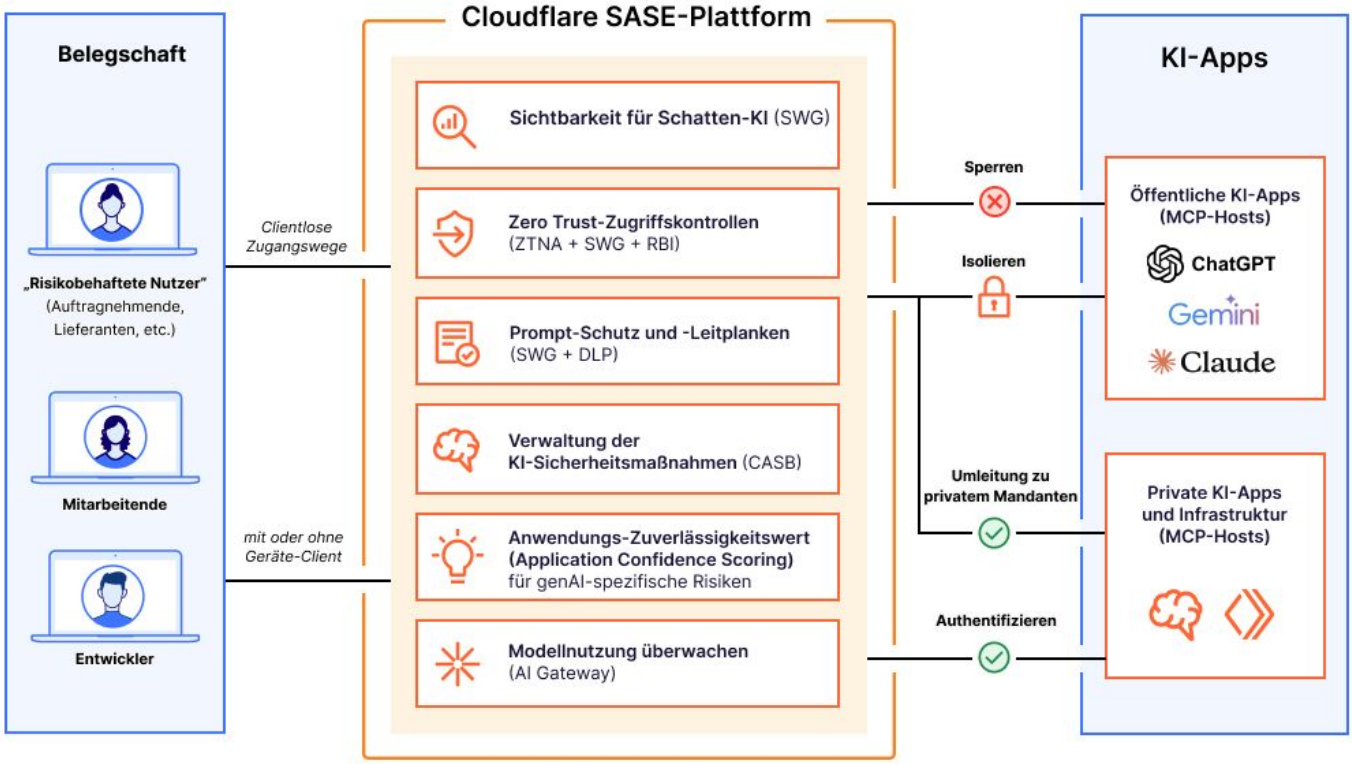
KI-gestützte Anwendungen schützen

Schützen Sie Ihre KI-Anwendungen und APIs in Echtzeit vor Prompt Injection und Datenlecks.

KI sicher entwickeln

Ermöglichen Sie Entwicklern, KI-Anwendungen mit integrierter Beobachtbarkeit, Rate Limiting und Inline-KI-Schutzmaßnahmen zu sichern.

Sichere Nutzung von KI-Anwendungen und -Workloads durch Mitarbeitende mit der SASE-Plattform von Cloudflare



SSE zum Schutz der Mensch-KI-Kommunikation

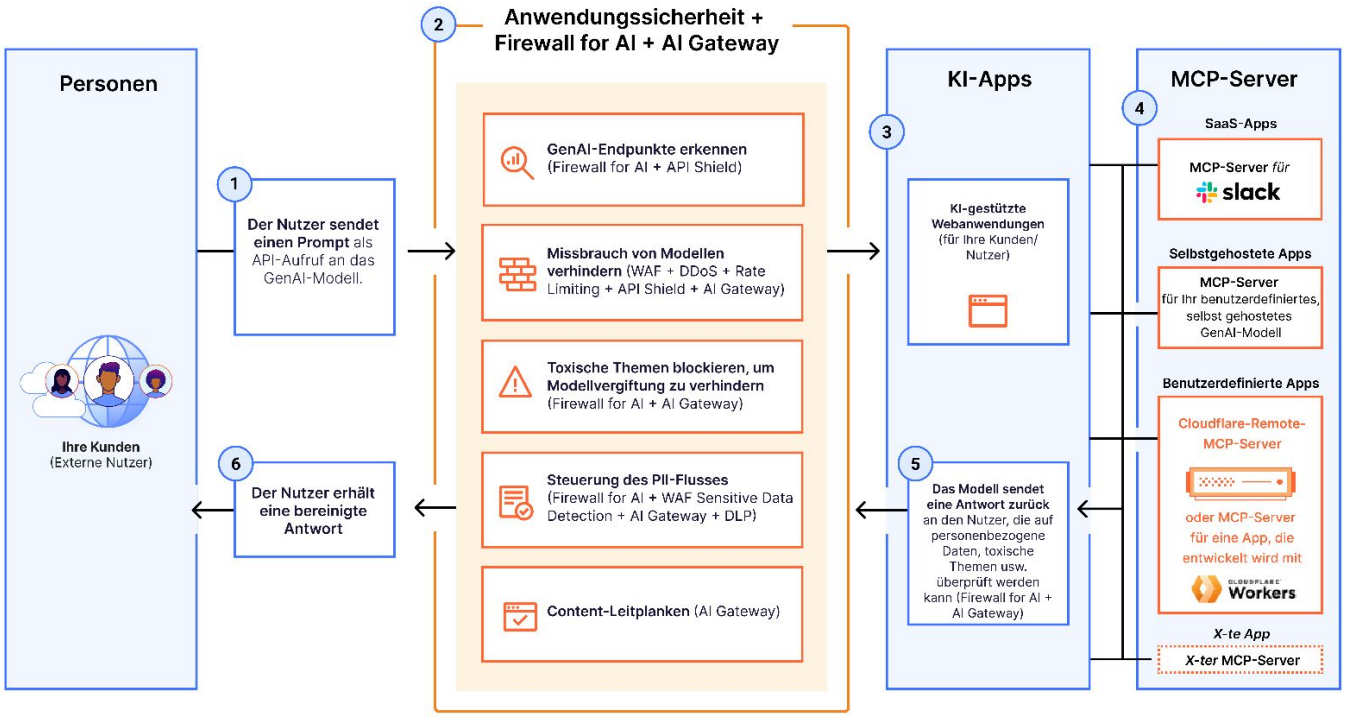
- **Sichtbarkeit:** Entdecken und analysieren Sie die Schatten-KI-Nutzung durch Inline-Traffic-Überprüfung. Bewerten Sie die von diesen KI-Anwendungen ausgehenden Risiken mit transparenter Evaluierung.
- **Zugriffskontrollen:** Benutzerverbindungen blockieren, isolieren, umleiten oder zulassen. Setzen Sie identitätsbasierte Zero-Trust-Regeln pro App durch.
- **Promptschutz und -Leitplanken**: Erkennen und Blockieren von Benutzerprompts basierend auf der Intention (z. B. Jailbreak-Versuche, Code-Missbrauch, PII-Anfragen).
- **Datensicherheit:** Verhindern Sie die Offenlegung sensibler Daten durch KI-gestützte Data Loss Prevention (DLP)-Erkennungen für persönlich identifizierbare Informationen, Quellcode und mehr.
- **Verwaltung des KI-Sicherheitsstatus:** Integrieren Sie GenAI-Tools über eine API, um mit unserem Cloud Access Security Broker (CASB) nach Fehlkonfigurationen zu scannen. Jetzt verfügbar für ChatGPT, Claude, und Google Gemini.

MCP-Serverportale zum Schutz der KI-zu-Ressourcen-Kommunikation

- **Sichtbarkeit:** Aggregieren Sie alle Model Context Protocol (MCP)-Anfrageprotokolle für Überprüfung und Analyse. Überprüfen und genehmigen Sie jeden MCP-Server, bevor Sie ihn zum Portal hinzufügen.
- **Authentifizierung:** Authentifizieren Sie den Benutzerzugriff auf das Portal basierend auf der Identität. Beschränken Sie den Zugriff auf MCP-Server basierend auf dem Prinzip der Vergabe minimaler Zugriffsberechtigungen.
- **Verbindungen:** Verbinden Sie alle zugänglichen MCP-Server mit einer einzigen URL, anstatt jeden MCP-Server einzeln zu konfigurieren.
- **Einheitliche Verwaltung:** Erzwingen Sie für Ihre KI-Verbindungen die gleichen detaillierten Zugriffsrichtlinien wie für Ihre menschlichen Nutzer.

Hinweis: MCP-Serverportale unterstützen jeden MCP-Server, einschließlich (aber nicht beschränkt auf) Remote-MCP-Server, die Sie auf Cloudflare erstellen oder bereitstellen. Diese Funktion ist als Zero Trust-Netzwerkzugang (ZTNA)-Steuerung verfügbar.

Schützen Sie KI-gestützte Apps und Workloads mit der modellunabhängigen Inline-Sicherheit von Clodflare



Schützen Sie öffentlich zugängliche KI mit Anwendungssicherheit und Firewall for AI

- **GenAI-Endpunkte erkennen:** Erkennen Sie automatisch alle KI-Modelle und APIs auf Ihren Websites.
- **KI-Modelle vor Missbrauch schützen:** Verwenden Sie unsere speziell entwickelte Firewall for AI, um Prompt-Injection, Modellvergiftung, übermäßige Nutzung und andere Bedrohungen zu blockieren, die herkömmliche Sicherheitsmaßnahmen umgehen können.
- **PII-Fluss steuern:** Scannen Sie Benutzer-Prompts und Modellantworten, um die Offenlegung sensibler Daten zu verhindern und die Einhaltung der Vorschriften zu gewährleisten.
- **Inhaltliche Leitplanken:** Blockieren Sie unsichere oder schädliche Prompts mithilfe integrierter Modelle wie Llama Guard. Erstellen Sie benutzerdefinierte WAF-Regeln, um verdächtige KI-Interaktionen einfach zu blockieren oder zu protokollieren.

Schützen Sie die KI, die Sie mit der Entwicklerplattform und dem AI Gateway erstellen

- **Einheitliche KI-Steuerungsebene:** Verwalten Sie alle Ihre KI-Anwendungen über ein einziges Dashboard. Leiten Sie Anfragen weiter, zwischenspeichern Sie Antworten, kontrollieren Sie Kosten und überwachen Sie die Performance.
- **Anmeldedaten an der Edge schützen:** API-Schlüssel und -Geheimnisse sicher an der Edge speichern, um clientseitige Gefährdung zu verhindern und die Schlüsselrotation zwischen Anbietern zu vereinfachen.
- **Sicherheitsleitplanken für Inhalte durchsetzen:** Automatische Identifizierung und Blockierung / Unkenntlichmachung von schädlichen Inhalten und PII in Prompts und Antworten.

Cloudflare ist der einzige Anbieter, der sowohl Ihre öffentlichen als auch privaten KI-Umgebungen sichert

Implementieren Sie die richtigen Leitplanken, um KI zuverlässig einzuführen und sicherzustellen, dass die Sicherheit Ihre Innovation beschleunigt und nicht behindert.

- **Einheitlicher KI-Ökosystemschutz:** Komplexe Sicherheitsstacks erhöhen das Risiko. Nutzen Sie eine Plattform, um Daten zu schützen und die Einhaltung der Vorschriften während des gesamten KI-Lebenszyklus sicherzustellen.
- **Zukunftssichere globale Architektur:** Verhindern Sie schon heute die Herausforderungen von morgen mit einem Post-Quantum-sicheren Netzwerk, das für jedes Datenverkehrsvolumen skalierbar ist, sich kontinuierlich an neue Bedrohungen anpasst und für neue Anwendungsfälle programmierbar ist.
- **KI-gestützte Sicherheit:** Unsere KI-gestützten Abwehrmechanismen prüfen Prompts und Antworten auf Bedrohungen in Echtzeit.
- **Bewährte KI-Führerschaft:** Entwickeln Sie mit Zuversicht auf einer Plattform, der 80 % der 50 führenden GenAI-Unternehmen vertrauen.
- **Modellunabhängige Bereitstellung:** Sicherheitskontrollen funktionieren für alle KI-Modelle in Ihrer Umgebung und bieten einen einheitlichen Ansatz zur Steuerung von KI-Bereitstellungen.

Das sagen unsere Kunden

indeed

Die weltweite Stellenbörse Nr. 1
Kundenreferenz lesen

Identifiziert & kontrolliert Schatten-KI

Parallel zum Projekt zur VPN-Abschaffung

APPLIED

Versicherungstech-nologie
Kundenreferenz lesen

Isoliert öffentliche GenAI-Tools wie ChatGPT

um das Kopieren und Einfügen von sensiblen Daten zu verhindern

KI-gestütztes SaaS-Unternehmen

Schützt PII

indem verhindert wird, dass Kunden sensible Informationen an öffentlich zugängliche GenAI-Endpunkte übermitteln

Cyndx

KI-gesteuertes Fintech

95 % reduzierte Inferenzkosten

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

Möchten Sie Ihre Anforderungen an die KI-Sicherheit besprechen?

Fachkundige Beratung einholen

1. 2025 Manage Engine-Studie: Quelle
2. IBM, Cost of a Data Breach Report 2025: Quelle

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