CLOUDFLARE

LÖSUNGSÜBERSICHT

Sichere Nutzung von generativer und agentenbasierter KI durch die Belegschaft

Ermöglichen Sie Ihren Teams die sichere Nutzung beliebiger KI-Tools mit Schutzmaßnahmen, die von der SASE-Plattform von Cloudflare durchgesetzt werden.

Kontrolle zurückgewinnen, Produktivität steigern

Die übereilte Einführung von KI hinterlässt eine Spur wachsender Risiken, einschließlich Datenlecks, Verstöße gegen Vorschriften und einer sich ausweitenden Angriffsfläche. KI vollständig zu blockieren, opfert nur Ihren Wettbewerbsvorteil, und das Experimentieren mit Einzellösungen erhöht die Komplexität.

Cloudflare schützt die KI-Nutzung Ihres Unternehmens, indem es die Transparenz erweitert, Risiken mindert und Daten in KI-Umgebungen ganzheitlich schützt:

- **Entdecken Sie Schatten-KI** und verwalten Sie Richtlinien für alle genehmigten und nicht genehmigten KI-Tools.
- **Stärken Sie die KI-Governance** durch identitätsbasierte Zugriffskontrollen und Statusverwaltung.
- **Stoppen Sie Datenverlust** durch Blockieren sensibler Informationen in Benutzer-Prompts, Erzwingen thematischer Leitplanken und Scannen von KI-Tools auf Fehlkonfigurationen.

Erweitern Sie Cloudflare, um KI sicher zu nutzen, unabhängig davon, ob Ihre KI-Strategie die Nutzung auf bestimmte Anwendungen beschränkt oder das Experimentieren mit einer größeren Vielfalt an Tools vorsieht.

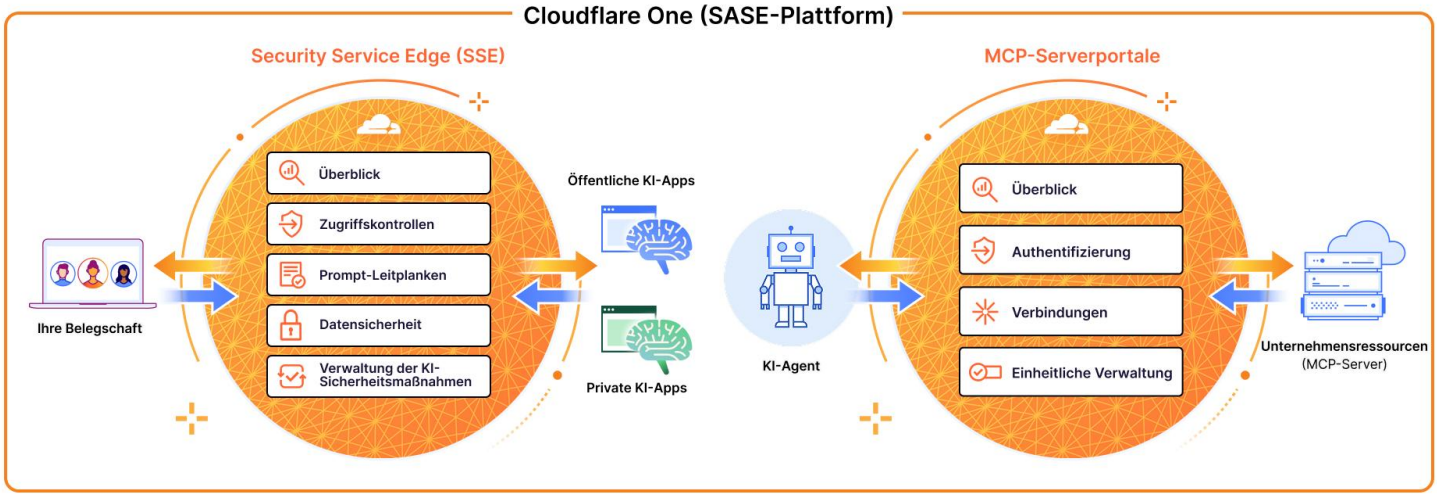
Warum SASE zur Sicherung der KI-Nutzung durch Mitarbeitende?

Die Secure Access Service Edge (SASE)-Plattform von Cloudflare befindet sich zwischen Ihren Mitarbeitenden und KI-Tools. Dies macht SASE zu einem idealen Ausgangspunkt für viele, um KI sicher zu nutzen.

Ob Mitarbeitende mit ChatGPT chatten oder KI-Agenten Informationen über Unternehmensressourcen sammeln: Die SASE-Plattform von Cloudflare setzt einheitliche Sicherheitskontrollen durch.

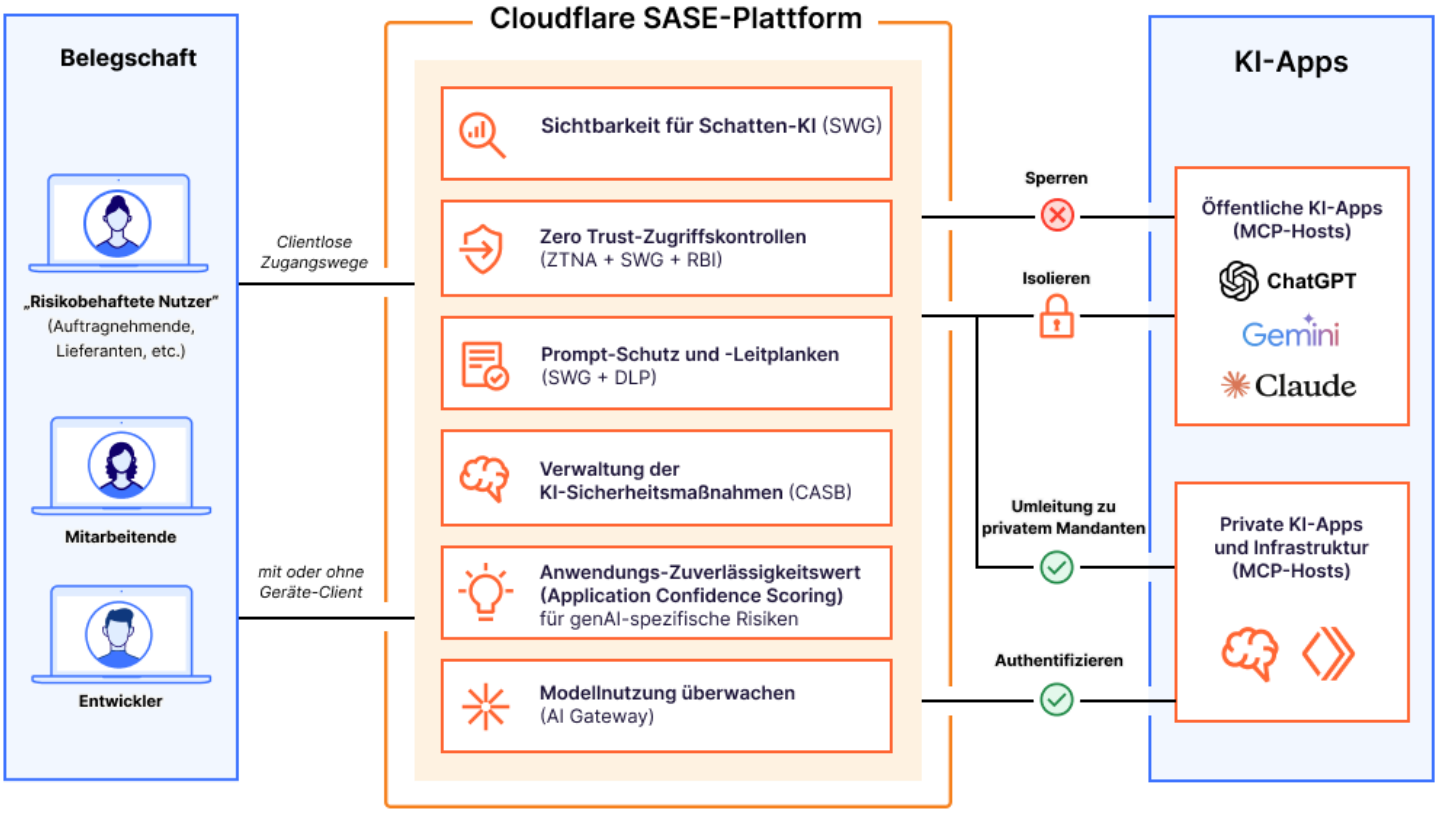
Sichere generative und agentenbasierte KI-Kommunikation

Die SASE-Plattform von Cloudflare bietet ein einheitliches Dashboard und eine zentrale Steuerungsebene zur Verwaltung von Mensch-KI- und Maschine-Maschine-Interaktionen im gesamten Unternehmen.



Im Gegensatz zu anderen SASE-Anbietern unterstützt Cloudflare auch die Verbindung und den Schutz von öffentlich zugänglichen, KI-gestützten Anwendungen und Workloads (wie dem KI-Chatbot oder den Empfehlungs-Engines Ihrer Website).

Schützen Sie die Benutzerkommunikation mit generativen KI-Anwendungen
mit KI-Nutzungskontrollen auf der SASE-Plattform von Cloudflare



- **Sichtbarkeit:** Entdecken und analysieren Sie die Nutzung von Schatten-KI durch Inline-Traffic-Überprüfung. Bewerten Sie die von diesen KI-Anwendungen ausgehenden Risiken mit transparenter Bewertung.
- **Zugriffskontrollen:** Blockieren, Isolieren, Umleiten oder Zulassen von Benutzerverbindungen. Erzwingen Sie identitätsbasierte Zero-Trust-Regeln pro App.
- **Prompt-Schutz und -Leitplanken:** Erkennen und blockieren Sie Benutzerprompts basierend auf der Absicht (z. B. Jailbreak-Versuche, Code-Missbrauch, PII-Anfragen).
- **Datensicherheit:** Verhindern Sie die Offenlegung sensibler Daten mit KI-gestützten Data Loss Prevention (DLP)-Erkennungen für PII, Quellcode und mehr.
- **KI-Sicherheitsstatusverwaltung:** Integrieren Sie GenAI-Tools über eine API (jetzt verfügbar für ChatGPT, Claude, Google Gemini), um mit unserem Cloud Access Security Broker (CASB) nach Fehlkonfigurationen zu suchen.

Ergebnisse für Kunden

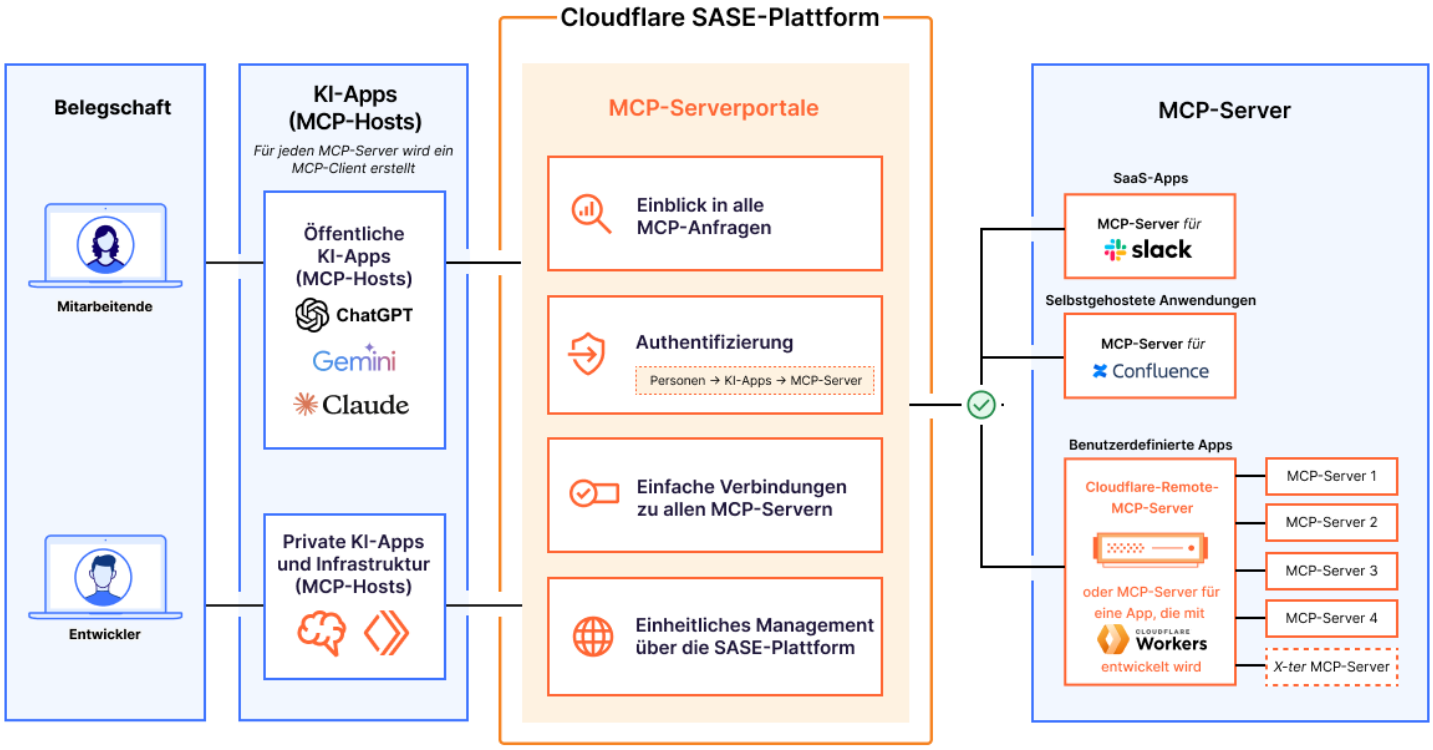
indeed
Die weltweite Stellenbörse Nr. 1

Identifizieren und kontrollieren Sie Schatten-KI
parallel zum Projekt zur VPN-Ablösung

APPLIED
Versicherungs-technologie

Isolieren Sie öffentliche GenAI-Tools wie ChatGPT,
um das Kopieren und Einfügen sensibler Daten zu unterbinden

Sichere agentenbasierte KI-Kommunikation (KI-zu-Ressource)
mit MCP-Serverportalen auf der SASE-Plattform von Cloudflare



- **Transparenz:** Alle MCP-Anforderungsprotokolle für Audits und Analysen zusammenfassen. 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 minimalen Zugriffsberechtigungen.
- **Verbindungen:** Verbinden Sie alle zugänglichen MCP-Server über eine einzige URL, anstatt jeden MCP-Server einzeln zu konfigurieren.
- **Einheitliche Verwaltung:** Erzwingen Sie für KI-Verbindungen die gleichen fein abgestimmten Zugriffsrichtlinien wie für menschliche Nutzer.
- **Tools pro Portal anpassen:** Wählen Sie die spezifischen Tools und Prompts aus, die für jeden Benutzer verfügbar sind.

Hinweis: Die MCP-Serverportale von Cloudflare unterstützen jeden MCP-Server, einschließlich (aber nicht beschränkt auf) jeden Remote-MCP-Server, der auf Cloudflare erstellt oder bereitgestellt wurde. Diese Funktion ist als Zero-Trust-Netzwerkzugriffskontrolle (ZTNA) verfügbar.

Erfahren Sie mehr über unsere Vision in diesem Blog.

Sind Sie bereit herauszufinden, wie Cloudflare Ihre KI-Nutzung sichern kann?

Für Workshop anmelden

