

Entdecken Sie, wie die Belegschaft Schatten-KI und -IT nutzt

Erhöhen Sie die Transparenz über nicht genehmigte KI- und SaaS-Tools mit der Traffic-Überprüfung von Cloudflare

Unsichtbares aufdecken

Schatten-IT ist kein neues Problem, aber die schnelle Einführung nicht genehmigter KI-Tools treibt eine moderne Krise voran:

- **20 %** aller Unternehmen haben im Jahr 2025 einen Datenverstoß aufgrund von Sicherheitsvorfällen mit Schatten-KI verzeichnet¹
- **85 %** der IT-Führungskräfte sagen, dass Mitarbeitende KI-Tools zu nutzen beginnen, bevor die IT-Abteilung sie bewerten kann²

Mit Cloudflare erhalten Unternehmen wieder mehr Übersicht bei der Verwaltung dieser wachsenden Angriffsfläche:

- **App-Status überprüfen:** [Kategorisieren](#) Sie KI- und SaaS-Apps als genehmigt, nicht genehmigt oder noch in Prüfung
- **Durchsetzung von Richtlinien nach App-Status:** Zulassen, blockieren, isolieren, DLP-Erkennung auf Interaktionen anwenden, Datei-Uploads einschränken und [mehr](#)
- **App-Nutzung analysieren:** [Überwachen Sie aggregierte Trends](#) und führen Sie detaillierte Untersuchungen durch
- **Bewertung der Anwendungsrisiken:** Die Vertrauenswürdigkeit der Anwendungen wird anhand von [Zuverlässigkeitswerten für Anwendungen ermittelt](#)



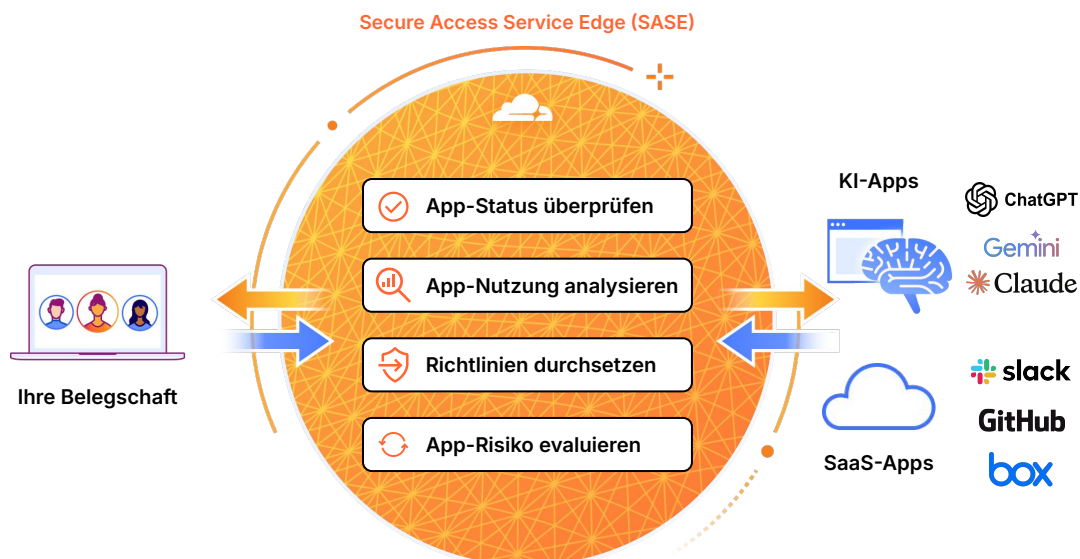
Einzigartige Risiken von Schatten-KI

Schatten-KI unterscheidet sich von traditioneller Schatten-IT. Während SaaS-Anwendungen hauptsächlich Dateien speichern oder freigeben, lernen KI-Tools aus allen Eingaben von Mitarbeitenden.

Das bedeutet, dass sensibles geistiges Eigentum, Kundendaten oder Quellcode unwiderruflich für das Training von Modellen absorbiert werden können, ohne dass eine Entfernung möglich ist.

So funktioniert's

Die SASE-Plattform von Cloudflare sitzt inline zwischen Ihrer Belegschaft und Ihren Ressourcen, um Transparenz und Kontrolle zu vereinen.



Zusätzlich können Sie [den CASB von Cloudflare über API integrieren](#), um nach Fehlkonfigurationen, Nutzeraktivitäten und sensiblen Daten zu suchen. Verwalten Sie die Sicherheitslage für KI-Anwendungen ([ChatGPT](#), [Claude](#), [Google Gemini](#)) und andere SaaS-Anwendungen. Verwenden Sie CASB [zusammen mit Ihrem Identitätsanbieter](#), um zu sehen, wann sich Benutzer bei nicht genehmigten Drittanbieter-Anwendungen authentifizieren.

Beispiel-Dashboards

Filtern Sie diese allgemeine Übersicht über die App-Nutzung nach:

- Anwendung und Anwendungstyp
- Genehmigungsstatus
- Mittels ZTNA geschützt
- Anzahl der Nutzer

Für weitere Informationen können Sie auf den Namen einer KI-Anwendung klicken, um bestimmte Nutzer oder Gruppen, die darauf zugreifen, ihre Nutzungsfrequenz, ihren Standort und die Menge der übertragenen Daten anzuzeigen.

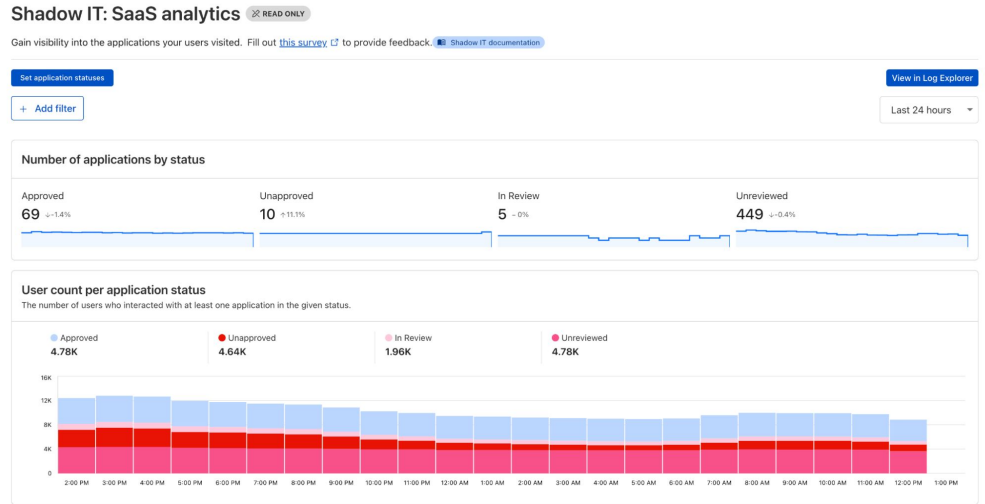


Abbildung 1: Analytics-Dashboard für Schatten-IT

Applications Showing 1-20 of 533

Action ▲

- Unreviewed (4 selected)
- In review (4 selected)
- Unapproved (4 selected)
- Approved (4 selected)

Application	Category	Status	Users
Platform (Do Not Inspect)	Public Cloud	UNREVIEWED	4770
	Productivity	UNREVIEWED	4762
	File Sharing	UNREVIEWED	4750
<input type="checkbox"/> Google Search	Search Engines	UNREVIEWED	4729
<input type="checkbox"/> Gmail	Email	APPROVED	4708
<input type="checkbox"/> Google Play Store	File Sharing	UNREVIEWED	4707
<input type="checkbox"/> Google Chat	Collaboration & Online Meetings	APPROVED	4679
<input type="checkbox"/> Pinterest	Social Networking	UNAPPROVED	4638
<input type="checkbox"/> Google Calendar	Collaboration & Online Meetings	APPROVED	4574
<input checked="" type="checkbox"/> DigiCert	Productivity	UNREVIEWED	4553
<input type="checkbox"/> Google Meet	Collaboration & Online Meetings	APPROVED	4508
<input checked="" type="checkbox"/> Google Workspace	Productivity	UNREVIEWED	4346

Apps organisieren und Zugriffsrichtlinien auf Grundlage des Genehmigungsstatus festlegen:

- Befugt (genehmigt)
- Unbefugt (nicht genehmigt)
- Wird überprüft
- Unüberprüft

Sie wünschen weitere technische Unterstützung? Erfahren Sie in [diesem Lernpfad](#), wie Sie Richtlinien erstellen können.

Abbildung 2: Anwendungsstatus markieren

Wollen Sie mehr darüber erfahren, wie Sie Ihre KI-Strategie sicher gestalten?

Weitere Anwendungsfälle ansehen

Für Workshop anmelden

1. IBM, Cost of a Data Breach Report 2025: [Quelle](#)
2. 2025 Manage Engine-Studie: [Quelle](#)