



Generative KI: Sichere Nutzung und weniger Datenrisiken

Zscaler bietet Transparenz und Kontrolle über generative KI und ermöglicht es Unternehmen, die durch KI angestoßenen Innovationen voranzutreiben und gleichzeitig sensible Daten zu schützen.

Risiken und Chancen generativer KI

KI-Tools werden in vielen Unternehmen als neue Möglichkeit wahrgenommen, die Produktivität zu steigern. Sie stellen jedoch ein Risiko für sensible Daten dar, die durch unsachgemäße Nutzung offengelegt werden können. Mit Zscaler können Unternehmen die Nutzung bestimmter KI-Anwendungen auf ihr Unternehmen zuschneiden und gleichzeitig sicherstellen, dass sie vollständigen Data Protection und lückenlose Transparenz bei der Nutzung haben.

Sicherheitsbedenken bei generativer KI

- Wer nutzt KI-Anwendungen?
- Können Sie den gesamten Zugriff bis hin zum User kontrollieren?
- Haben Sie granulare Kontrolle über bestimmte Anwendungen?
- Wie hoch sind die Risiken von KI-Anwendungen?
- Können Sie sensible Daten aus KI-Anwendungen schützen?
- Können Sie KI-Anfragen im gesamten Unternehmen überprüfen?

Kernfunktionen



Risikobasierte KI-Nutzungskontrollen

Erlauben Sie nur die Nutzung geeigneter KI-Anwendungen auf der Grundlage des Risikos — mit granularen Nutzungskontrollen, bis hin zu einzelnen Teams und Usern.



KI-Transparenz Sie erhalten vollen Einblick in alle Prompts und Anfragen in ChatGPT und erfahren, welche Personen im Unternehmen KI nutzen.



Data Protection für KI Durch KI-Anwendungen mit vollständiger DLP können Sie verhindern, dass Daten in KI-Prompts exfiltriert werden.



Unterbindung von riskantem Verhalten

Integrieren Sie zusätzliche Sicherheitsmaßnahmen wie Browser-Isolierung, um das Hochladen und Herunterladen von Daten sowie die Verwendung der Zwischenablage zu verhindern und die Exfiltration großer Mengen potenziell sensibler Daten in Prompts zu verhindern.

Hauptvorteile



Gesteigerte Innovation

Setzen Sie KI ein, um Teams und Innovationen zu fördern.



Anpassung der KI-Nutzung und ihrer Risiken

Reduzieren Sie Risiken und Kosten, indem Sie nur die geeigneten KI-Anwendungen zulassen, die für das Unternehmen wirklich sinnvoll sind.



Lückenlose Transparenz

Mit kontinuierlichem Einblick in die Nutzung und Prompts können Unternehmen KI-Nutzung und -Aktivitäten stets nachvollziehen, kontrollieren und optimieren.



Interner Quellcode



Erstellung vertraulicher Inhalte



Sensible Analyse

Zugriffskontrolle

URL-Filterrichtlinie
Kontrollen für Cloud-Anwendungen
Sicheres Browsen (Isolierung)

Unterbindung von Datenverlusten

Inline-DLP-Überprüfung

Zero Trust Exchange



Generative KI

KI-Transparenz

Details zur Anwendungsnutzung (ZIA)
Richtlinienverstöße (DLP)

SIEM-Logging

Zscaler Nanolog Streaming

Mit Zscaler können Unternehmen alle Sicherheits- und Datenkontrollen für generative KI über eine einheitliche Plattform nutzen.

Neben der Absicherung der KI-Nutzung setzt Zscaler seit Jahren auch auf KI, um IT- und Sicherheitsteams zu positiveren Sicherheitsergebnissen zu verhelfen.



KI-gestützte Segmentierung Nutzen Sie die automatische Anwendungssegmentierung zur Festlegung geeigneter Zero-Trust-Zugriffsrichtlinien, um die interne Angriffsfläche zu minimieren und Sicherheitsrisiken zu senken.



Schneller Data Protection Beschleunigen Sie Ihre Data-Protection-Prozesse mithilfe von ML-basierter automatischer Datenklassifizierung — ganz ohne Konfiguration.



KI-gestützte Ursachenanalyse Ermitteln Sie Ursachen negativer Erfahrungen 180-mal schneller, sodass Probleme zügig behoben werden und User ihre Arbeit umgehend wieder aufnehmen können, während Sie gleichzeitig Ihre IT-Teams entlasten.



KI-gestützte Sandbox-Analyse Die KI bietet zuverlässigen Schutz vor Patient-Zero-Infektionen, da sie bösartige Dateien sofort erkennt und das Eindringen in die Organisation verhindert, bis die Sandbox-Analyse abgeschlossen ist.



Experience your world, secured.™

Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, zuverlässiger und sicherer arbeiten können. Die Zscaler Zero Trust Exchange schützt Tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an beliebigen Standorten vor Cyberangriffen und Datenverlust. Die SSE-basierte Zero Trust Exchange ist in über 150 Rechenzentren auf der ganzen Welt verfügbar und die weltweit größte Inline-Cloud-Sicherheitsplattform. Informieren Sie sich auf [zscaler.de](https://www.zscaler.de) oder folgen Sie uns auf Twitter unter [@zscaler](https://twitter.com/zscaler).

© 2023 Zscaler, Inc. Alle Rechte vorbehalten. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™ und ZPA™ sowie weitere unter [zscaler.de/legal/trademarks](https://www.zscaler.de/legal/trademarks) aufgeführte Marken sind entweder (i) eingetragene Marken bzw. Dienstleistungsmarken oder (ii) Marken bzw. Dienstleistungsmarken von Zscaler, Inc. in den USA und/oder anderen Ländern. Alle anderen Marken sind das Eigentum Ihrer jeweiligen Inhaber.