Zscaler AI Security auf einen Blick

AUF EINEN BLICK

Vorteile von AI Security

KI-ASSETS + -RISIKEN ENTDECKEN
Entdecken und kartieren Sie Ihr gesamtes KI-Ökosystem — von Schatten-KI und riskanten Anwendungen bis hin zu KI-Modellen und -Pipelines und vielem mehr.

KI-SCHWACHSTELLEN FINDEN
Red Team testet KI-Systeme auf Schwachstellen und Risiken mit kontinuierlichen und automatisierten Tests.

SICHERER KI-ZUGRIFF
Nutzen Sie integrierte KI-Mechanismen, um in Echtzeit eine sichere Nutzung und Schutz vor Bedrohungen und Datenverlusten zu gewährleisten.

VORSCHRIFTSKONFORME KI-NUTZUNG
Verwalten Sie Ihre KI-Infrastruktur und -Implementierungen mithilfe von KI-Frameworks, um die Einhaltung der Risikovorgaben zu gewährleisten.

End-to-End-KI-Sicherheit mit Zscaler

Zscaler bietet KI-gestützte Lösungen, die Unternehmen dabei helfen, die transformative Kraft der KI zu nutzen und gleichzeitig die damit verbundenen Risiken zu bewältigen.

Ganzheitlicher Funktionsumfang von der Erkennung riskanter KI-Nutzung bis hin zur Gewährleistung einer sicheren Entwicklung und dem Schutz vertraulicher Builds durch fortschrittliche Inline-Abwehrmechanismen.

Zscaler erschließt Unternehmen neue Möglichkeiten zur Absicherung von KI-Innovationen. Mit Zscaler können Sie das Potenzial der KI voll ausschöpfen und die Geschäftsentwicklung vorantreiben, ohne sich von Risiken ausbremsen zu lassen.



Warum Zscaler für KI-Sicherheit

KOMPLETTER KI-LEBENSZYKLUS
KI-Sicherheit von der Entdeckung bis zur Implementierung

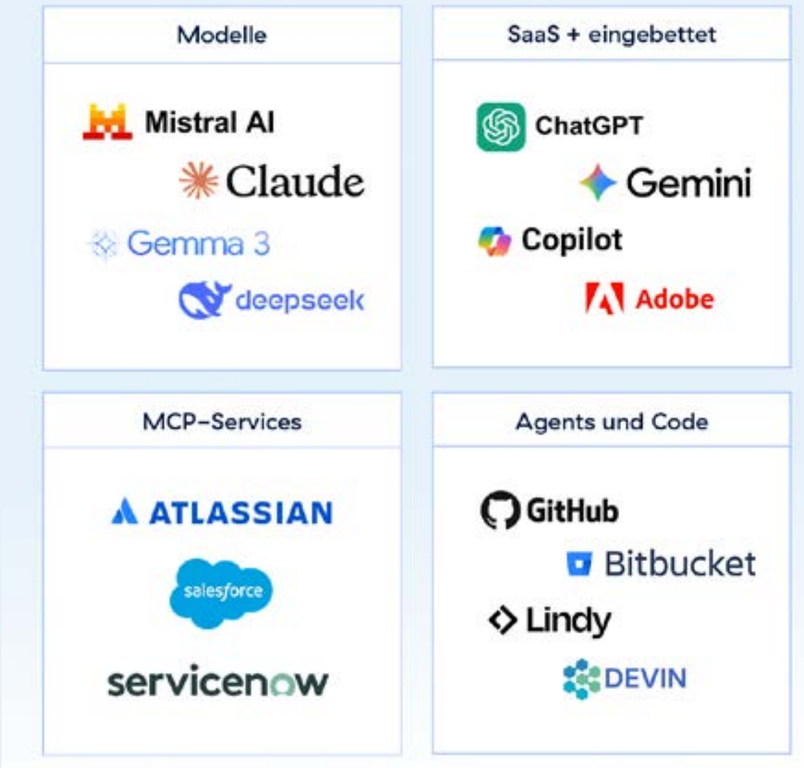
EINHEITLICHE PLATTFORM
Die bewährte Plattform integriert KI-Sicherheit mit Zero Trust.

BEWÄHRTER PARTNER
Expertise in Kundenerfolg und Transformation

Asset Discovery mit KI-gestütztem SPM

Die Erfassung des eigenen KI-Bestands ist angesichts der dynamischen Entwicklung von KI in der Wirtschaft eine Herausforderung. Ohne klare Transparenz hinsichtlich Schatten-KI, Modellen, Service, MCP-Servern und Pipelines haben Unternehmen Schwierigkeiten, Risiken effektiv zu erkennen und entsprechend zu reagieren.

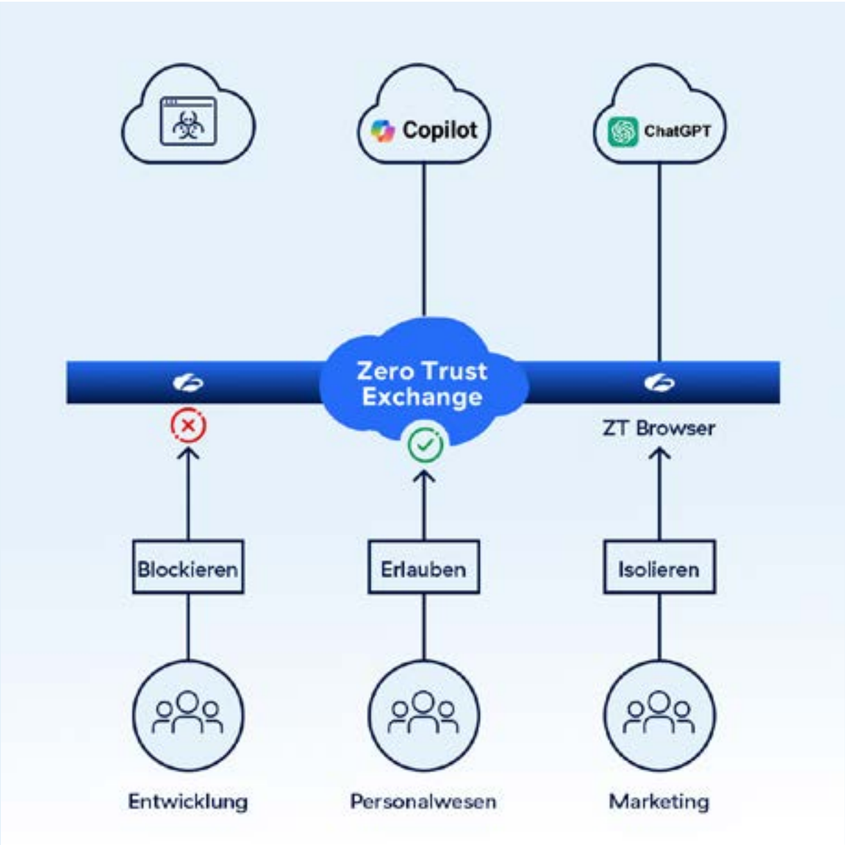
Mit Zscaler AI SPM erhalten Unternehmen einen umfassenden Einblick in ihre KI-Ökosysteme. Es bietet Einblick in Ihre Nutzung von Gen AI-Anwendungen, LLMs, Modellen, MCP-Servern und Pipelines und hilft Ihnen bei der Erkennung riskanter Schwachstellen und Sicherheitslücken, die Ihre Daten und Ihr Geschäft gefährden könnten.



AI Access Security

Die Kontrolle des Zugriffs und die Gewährleistung der Sicherheit von GenAI-Anwendungen in SaaS-Umgebung stellen Unternehmen zunehmend vor Herausforderungen. Da sich Schatten-KI ungehindert ausbreitet und die Risiken von Datenverlusten oder nicht konformer Nutzung zunehmen, benötigen Unternehmen effektive Lösungen, um diesen Bedrohungen zu begegnen.

Mit AI Access Security von Zscaler können Sie die sichere, regelkonforme und verantwortungsvolle Nutzung von KI-Anwendungen durchsetzen. Wenden Sie granulare Zugriffskontrollen an, um festzulegen, welche User oder Apps mit KI-Tools interagieren dürfen. Nutzen Sie DLP-Schutz oder -Isolation, um Datenverluste durch KI-Prompts zu verhindern, und setzen Sie die Inhaltsmoderation durch, um die Einhaltung der unternehmensinternen Richtlinien zur akzeptablen Nutzung sicherzustellen.



©2026 Zscaler, Inc. Alle Rechte vorbehalten.

Testen mit automatisiertem Red Teaming

Das Testen von KI-Systemen auf Schwachstellen ist allzu oft ein komplexer und zeitaufwändiger Prozess. Für Unternehmen ohne dedizierte Red-Team-Ressourcen kann es nahezu unmöglich erscheinen, gründliche Evaluierungen durchzuführen.

Automatic and Continuous Red Teaming von Zscaler begegnet diesen Herausforderungen mit einer innovativen, automatisierten Red-Teaming-Engine. Mit über 25 vordefinierten Tests und der Unterstützung für vollständig kundenspezifische Tests und Datensatz-Uploads ermöglicht SPLX Unternehmen, Testszenarien an ihre spezifischen Domänen, aufsichtsrechtlichen Rahmenbedingungen und Anwendungsfälle anzupassen.



Inline-Schutz mit AI Guard

LLMs haben sich schnell zu einem gefährlichen neuen Einfallstor für Bedrohungen und Datenverlust entwickelt. Ohne eine leistungsstarke Inline-Überprüfung dieser Verbindungen sind Unternehmen anfällig für Datenverluste, kompromittierte KI-Systeme und böswillige Bedrohungen.

Mit Zscaler AI Guard können Unternehmen eine leistungsstarke Inline-Prüfung von KI-Prompts und -Interaktionen durchführen. Die Lösung unterstützt Sie dabei, risikoreiche Bedrohungen wie Prompt-Injections und Jailbreaking zu erkennen, den Verlust vertraulicher Daten zu verhindern und Inhalte zu moderieren, um eine sichere Nutzung und Richtlinien für die akzeptable Nutzung durchzusetzen. Aufbauend auf dem Fachwissen eines vertrauenswürdigen Marktführers im Bereich der Inline-Überprüfung gewährleistet Zscaler einen robusten Schutz für Ihren kritischen KI-Traffic.



©2026 Zscaler, Inc. Alle Rechte vorbehalten.

KI-Governance mit KI-SPM

Die Gewährleistung von Compliance und Governance für KI-Systeme wird zunehmend komplexer, da Unternehmen KI in großem Umfang einsetzen. Ohne eine angemessene Überwachung der Einhaltung von Richtlinien und KI-spezifischen Frameworks riskieren Unternehmen rechtliche, finanzielle und reputationsbezogene Schäden.

Mit dem KI-Governance-Ansatz von Zscaler können Sie die Compliance-Überwachung automatisieren und Berichtsprozesse optimieren.
Die KI-Systeme werden kontinuierlich auf ihre Übereinstimmung mit internen Richtlinien und aufsichtsrechtlichen Standards überwacht, während gleichzeitig die notwendigen Nachweise zur Unterstützung von Audits und zur Erfüllung der Anforderungen bereitgestellt werden. Stellen Sie sicher, dass der Einsatz von KI den Governance-Rahmenbedingungen entspricht, um Ihrem Unternehmen zu helfen, Risiken zu minimieren und die operative Integrität zu wahren.



Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Die Zscaler Zero Trust Exchange™ schützt tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlusten. Als weltweit größte Inline-Cloud-Sicherheitsplattform wird die SASE-basierte Zero Trust Exchange™ in über 150 Rechenzentren auf der ganzen Welt bereitgestellt. Weitere Informationen erhalten Sie auf **zscaler.com/de**. Auf X (ehemals Twitter) finden Sie uns unter **@zscaler**.

© 2026 Zscaler, Inc. Alle Rechte vorbehalten. Zscaler™ sowie weitere unter **zscaler.com/de/legal/trademarks** aufgeführte Marken sind entweder (i) eingetragene Handelsmarken bzw. Dienstleistungsmarken oder (ii) Handelsmarken bzw. Dienstleistungsmarken von Zscaler, Inc. in den USA und/oder anderen Ländern. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber.

+1 408 533 0288 **Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA** **zscaler.com/de**

zscaler™

Zero Trust Everywhere