Zero Trust, Kontrolle, Innovation

Sichere KI-Nutzung: Das Erfolgsrezept von Zscaler



©2026 Zscaler, Inc. Alle Rechte vorbehalten.

WHITEPAPER

Einführung

In der dynamischen digitalen Landschaft von heute erweist sich künstliche Intelligenz (KI) zunehmend als zweischneidiges Schwert. Einerseits erschließt sie Unternehmen transformative Möglichkeiten, andererseits bringt sie beispiellose Komplexität in den Bereichen Sicherheit, Governance und Risikomanagement mit sich. Unternehmen, die KI nutzen, um Innovation, Agilität und Effizienz zu fördern, stehen vor einer zentralen Herausforderung: Wie lässt sich KI so einsetzen, dass vertrauliche Daten geschützt, die Einhaltung von Vorschriften gewährleistet und Vertrauen aufgebaut wird — sowohl intern als auch extern?

Bei Zscaler steht diese Herausforderung im Mittelpunkt unserer IT-Strategie. Als weltweit führender Anbieter von Cloud-Sicherheit verfolgen wir einen proaktiven Ansatz zur Integration von KI in Unternehmensprozesse und gewährleisten dabei gleichzeitig strenge Sorgfalts- und Governance-Maßnahmen. Dieses Engagement unterstreicht nicht nur unsere führende Rolle in der Cybersicherheitsbranche, sondern auch unser Bewusstsein für die entscheidende Bedeutung der KI-Sicherheit für Unternehmen aller Branchen.
In diesem Whitepaper erläutern wir **den Ansatz von Zscaler IT zur sicheren KI-Einführung und diskutieren die grundlegenden Prinzipien, die Unternehmen anwenden müssen, um das Potenzial von KI mit der Notwendigkeit der Minimierung von Risiken in Einklang zu bringen.**

©2026 Zscaler, Inc. Alle Rechte vorbehalten.

Die komplexen Herausforderungen der KI

Die Versprechen der KI gehen naturgemäß mit Risiken einher, denen Unternehmen begegnen müssen, um ihr Potenzial erfolgreich zu nutzen. Von der **Gefahr des Datenverlusts durch Modellkompromittierung bis hin zu den Gefahren von Verzerrungen, Missbrauch oder unregulierten Ergebnissen: Unternehmen begeben sich in ein Minenfeld voller Sicherheits-, Compliance- und Governance-Herausforderungen.** Unternehmen, die KI zur Transformation ihrer Abläufe nutzen wollen, müssen diese Risiken bewältigen, ohne die Innovationskraft zu beeinträchtigen. Die Voraussetzung dafür sind proaktive Strategien und robuste Frameworks für KI-Sicherheit.

Ohne umfassende Schutzmaßnahmen sind Unternehmen erheblichen Risiken ausgesetzt: von der Gefährdung geistigen Eigentums über den Verlust des Kundenvertrauens bis hin zu potenziellen Verstößen gegen gesetzliche Vorschriften. Unternehmen müssen nicht nur die unbefugte Nutzung von KI unterbinden, sondern auch eine strenge Kontrolle von Modellen und Ergebnissen gewährleisten, um Vertrauen und Zuverlässigkeit zu erhalten. Als führendes Unternehmen im Bereich Sicherheitsinnovationen **stellt sich Zscaler IT dieser Verantwortung und hat ein umfassendes KI-Sicherheits- und Governance-Framework entwickelt, das auf Zero-Trust-Prinzipien basiert und globale Standards wie das NIST AI Risk Management Framework einhält.** Unser mehrschichtiger Ansatz begegnet den spezifischen Herausforderungen der KI und stellt sicher, dass vertrauliche Daten geschützt bleiben und die Resilienz des Unternehmens gewährleistet bleibt.

Es steht viel auf dem Spiel, und die Risikominderung im Zeitalter der KI erfordert den Einsatz von Lösungen, die Vertrauen ermöglichen und gleichzeitig die Betriebsabläufe absichern. Nur durch sorgfältige Governance, durchdachte Frameworks und Spitzentechnologie können Unternehmen die Zukunft der KI-Einführung souverän meistern. Bei Zscaler ist der strenge, auf Governance basierende Ansatz zur Sicherung von KI keine optionale Priorität, sondern ein grundlegender, obligatorischer Standard für alle Betriebsabläufe.

Framework und Prozesse für die KI-Governance

Die sichere KI-Nutzung beginnt mit Governance und Prozessen. Unsere KI-Governance orientiert sich an Kernprinzipien und soliden Richtliniendokumenten, darunter die Richtlinie zur Nutzung generativer künstlicher Intelligenz und interne Sorgfaltsstandards. Das grundlegende Ziel unseres Frameworks für die KI-Sicherheit ist der Schutz von Daten (sowohl Kunden- als auch Unternehmensdaten) vor Problemen wie Modelllecks, Halluzinationen und Missbrauch.

Grundlegende KI-Prinzipien und Durchsetzung von Richtlinien

Der Ansatz von Zscaler im Bereich KI basiert auf vier Kernprinzipien: Verantwortlichkeit, Fairness, Transparenz sowie Sicherheit und Compliance.

Unser Dokument zu Sicherheitsstandards für generative KI basiert auf dem NIST AI Risk Management Framework sowie branchenspezifischen Best Practices. Zu den wichtigsten Anforderungen an alle Angestellten und Zeitarbeiter gehören:

©2026 Zscaler, Inc. Alle Rechte vorbehalten.

- **Einschränkung bestimmter öffentlicher GenAI:** Nicht genehmigte KI-Modelle und LLMs sowie Modelle und LLMs aus Hochrisiko-Staaten sind gesperrt. Eingeschränkter Zugriff kann nur über eine Sicherheitsausnahme für spezifische Geschäftsanwendungsfälle, wie Forschung und Entwicklung oder Innovation, gewährt werden.

- **Sichere öffentliche KI:** Die Nutzung öffentlicher KI-Tools muss über genehmigte Sicherheitskontrollen, einschließlich DLP-Richtlinien und AI Guard, erfolgen, um Datenschutz und Governance zu gewährleisten. Diese Maßnahmen dienen der Festlegung klarer Leitlinien und der Überwachung aller Interaktionen mit öffentlicher KI gemäß den Sicherheitsanforderungen von Zscaler.

- **Datenbeschränkungen:** User dürfen in GenAI-Tools keine personenbezogenen Daten (PII) oder wesentliche nicht-öffentliche Informationen (z. B. Übernahmekandidaten, unveröffentlichte Produkt-Roadmaps) eingeben. Die Eingabe von vertraulichen Informationen (z. B. Sicherheitsinformationen/-reports, Technologie und technische Informationen, Kundendaten) ist ebenfalls untersagt.

- **Menschliche Überprüfung erforderlich:** Die Ergebnisse von GenAI-Tools unterliegen einer menschlichen Überprüfung. GenAI-Tools dürfen nicht ohne menschliches Eingreifen oder eine Überprüfung zur automatisierten Entscheidungsfindung eingesetzt werden.

- **Verbote von HR-Tools:** Die Nutzung von KI/ML-Tools zu beschäftigungsbezogenen Zwecken, wie z. B. Einstellungsbeurteilungen, Einstellungsentscheidungen oder die Festlegung von Beschäftigungsbedingungen, ist ohne vorherige Prüfung und Genehmigung der Compliance- bzw. Arbeitsrecht-Beauftragten ausdrücklich untersagt.

Genehmigte interne KI-Plattformen

Zscaler führt eine Liste zugelassener GenAI-Tools, -Plattformen und LLMs. Die Verwendung von KI-Modellen, -Tools oder -Services, die mit sanktionierten oder Hochrisiko-Staaten in Verbindung stehen, einschließlich chinesischer LLMs wie DeepSeek und Qwen, zu Produkt-, Forschungs- und Entwicklungs- sowie unternehmerischen Zwecken ist ausdrücklich untersagt.

Bereich	Genehmigte Plattform/Tool	Sicherheit und Risikominderung
Allgemeine Mitarbeiternutzung	**ZChat** (vom Unternehmen genehmigt und auf einem dedizierten Zscaler-Tenant gehostet). **ChatGPT** und **Gemini** (genehmigte öffentliche Tools).	Erfordert ZPA-basierte Sicherheitsüberprüfungen bzw. ZIA-SSL-Untersuchung, AI Guard und die obligatorische Abmeldung von der Missbrauchsüberwachung durch Drittanbieter.
Engineering/ Produktentwicklung	Microsoft AzureAI, Google Vertex AI, Amazon AWS AI Services, Z-Llama (internes LLM-Gateway).	Erfordert ZIA DLP, einen vom Kunden verwalteten Verschlüsselungsschlüssel (CMEK) für SaaS, ZPA-Konnektivität zu „Crown Jewels"-Systemen (wie Bitbucket) und Ausführung von SAST/SCA Sicherheitstools für generierten Code.
Softwareentwicklung	Zugelassene Tools können Vorschläge/ Snippets für Code in kundenorientierten Produkten oder Code für interne Tests oder Geschäftsanwendungen (z. B. ein Skript zur Automatisierung der Gehaltsabrechnung) generieren.	Der gesamte generierte Code unterliegt den etablierten Standards des Zscaler-Softwareentwicklungszyklus, einschließlich Peer-Review durch menschliche Fachkräfte, Unit-Tests und Bewertung von Sicherheitslücken.

©2026 Zscaler, Inc. Alle Rechte vorbehalten.

Beschaffungsprozess und Due-Diligence-Prüfung von KI-Anbietern:

Vor der Beschaffung von KI-Produkten oder -Services von Drittanbietern haben wir einen strengen internen Genehmigungsprozess vorgeschrieben, an dem die zuständigen Abteilungen für Sicherheit, Datenschutz und Rechtsangelegenheiten beteiligt sind. Dies dient der Minderung von Risiken im Zusammenhang mit der Nutzung von KI-Tools externer Anbieter.

Im ersten Schritt muss der/die Projektverantwortliche sicherstellen, dass eine unterzeichnete Geheimhaltungsvereinbarung mit dem betreffenden Anbieter vorliegt, und ein vollständig ausgefülltes Antragsformular einreichen.

Die interne Sicherheitsprüfung erfordert eine umfassende Dokumentation seitens des Anbieters:

- **Fragebogen zur Lieferantensicherheit (VSQ):** Muss vollständig ausgefüllt werden.
- **SOC 2 Typ 2 Bericht:** Ein gültiger Bericht bzw. ein „Bridge Letter“ für den laufenden Prozess muss vorliegen.
- **Ergebnisse des Penetrationstests:** Muss innerhalb der letzten zwei Jahre erfolgt sein und nachweisen, dass in der Produktionsumgebung keine offenen Schwachstellen der Stufen „Kritisch“ oder „Hoch“ bestehen, oder einen klaren Leitfaden bzw. Zeitplan für deren Behebung enthalten.

Standards für Datensicherheit und Modell-Hosting:

Zscaler bewertet die KI-Architektur und den Datenfluss mithilfe des Five Safes Frameworks zur KI-Risikobewertung und verlangt sichere Datenverwaltungsmaßnahmen (Anonymisierung, Maskierung, Tokenisierung) zum Schutz vertraulicher Daten.

Die Kriterien für die Genehmigung hängen davon ab, wo das KI-Modell gehostet wird und welche Art von Daten verarbeitet werden (öffentlich, eingeschränkt oder vertraulich):

- **Bei von Fremdanbietern gehosteten Modellen (z. B. OpenAI API)** wird für öffentliche oder eingeschränkte Daten der Verzicht des Anbieters auf Datenspeicherung und Missbrauchsüberwachungsprozesse dringend empfohlen. Vertrauliche Daten erfordern, dass der Anbieter die Trennung von Usern und Mandanten gewährleistet, der Fremdanbieterservice ohne Datenspeicherung betrieben wird und sichergestellt wird, dass Mitarbeitende des Fremdanbieters niemals auf vertrauliche Daten von Zscaler zugreifen.
- **Einschränkungen beim Modelltraining:** Kundendaten werden niemals zum Training interner oder externer KI verwendet. Lesen Sie dazu den Beitrag über unser Engagement für verantwortungsvolle KI auf unserer externen Website. Zscaler schreibt vor, dass interne Daten von Zscaler nicht zum Training allgemeiner Modelle von Anbietern verwendet werden dürfen. Falls eingeschränkte oder vertrauliche interne Daten für das Training verwendet werden, müssen diese stark anonymisiert/aggregiert werden und das Modell darf ausschließlich für Zscaler trainiert und verwendet werden. Entscheidend ist, dass Fremdanbieter eines Herstellers ihre Modelle nicht mit Zscaler-Daten trainieren dürfen.

©2026 Zscaler, Inc. Alle Rechte vorbehalten.

Rechtliche und vertragliche Schutzmaßnahmen:

Die Rechtsbeauftragten integrieren Klauseln in Lieferantenverträge, um die Nutzung von Zscaler-Daten stark einzuschränken. Der Standardwortlaut verbietet Anbietern ausdrücklich den Zugriff auf, die Erfassung oder die Verwendung von Zscaler-Daten zu folgenden Zwecken:

- **Training, Bereitstellung oder Optimierung** der KI- oder ML-Modelle des Anbieters oder Dritter.
- **Generieren von Output oder Erbringung von Services** jeglicher Art für eigene Zwecke, verbundene Unternehmen oder Dritte.

Falls ein Anbieter Zscaler-Daten für das Training von KI/ML benötigt,**Ausnahmegenehigung** beantragen. Wird diese genehmigt, werden spezifische Schutzklauseln formuliert, um das Risiko für Zscaler zu begrenzen. Im Falle einer Genehmigung werden spezifische Schutzklauseln formuliert, um das Risiko für Zscaler zu begrenzen. Dazu gehören die Beschränkung der Nutzung auf eine **ausschließlich von Zscaler genutzte Instanz** sowie die Sicherstellung, dass Zscaler alle geistigen Eigentumsrechte an den Zscaler-Daten und allen daraus generierten Ergebnissen besitzt.

KI-Sicherheitsstatus: Zscaler-Produkte in Aktion

Nachdem alle Prozesse im Zusammenhang mit der Governance, der Einrichtung des Frameworks und der Einbindung von Anbietern abgeschlossen sind, ist die Absicherung der KI der nächste entscheidende Schritt. Erreicht wird dies durch Einsatz der eigenen Produkte von Zscaler. Die Tools und Strategien von Zscaler zur Sicherung der KI-Entwicklung konzentrieren sich auf den Schutz vertraulicher Daten, die Gewährleistung des Datenschutzes und die Verhinderung von Missbrauch durch fortschrittliche kontextbezogene Richtlinien und eine zukunftsfähige Zero-Trust-Architektur.

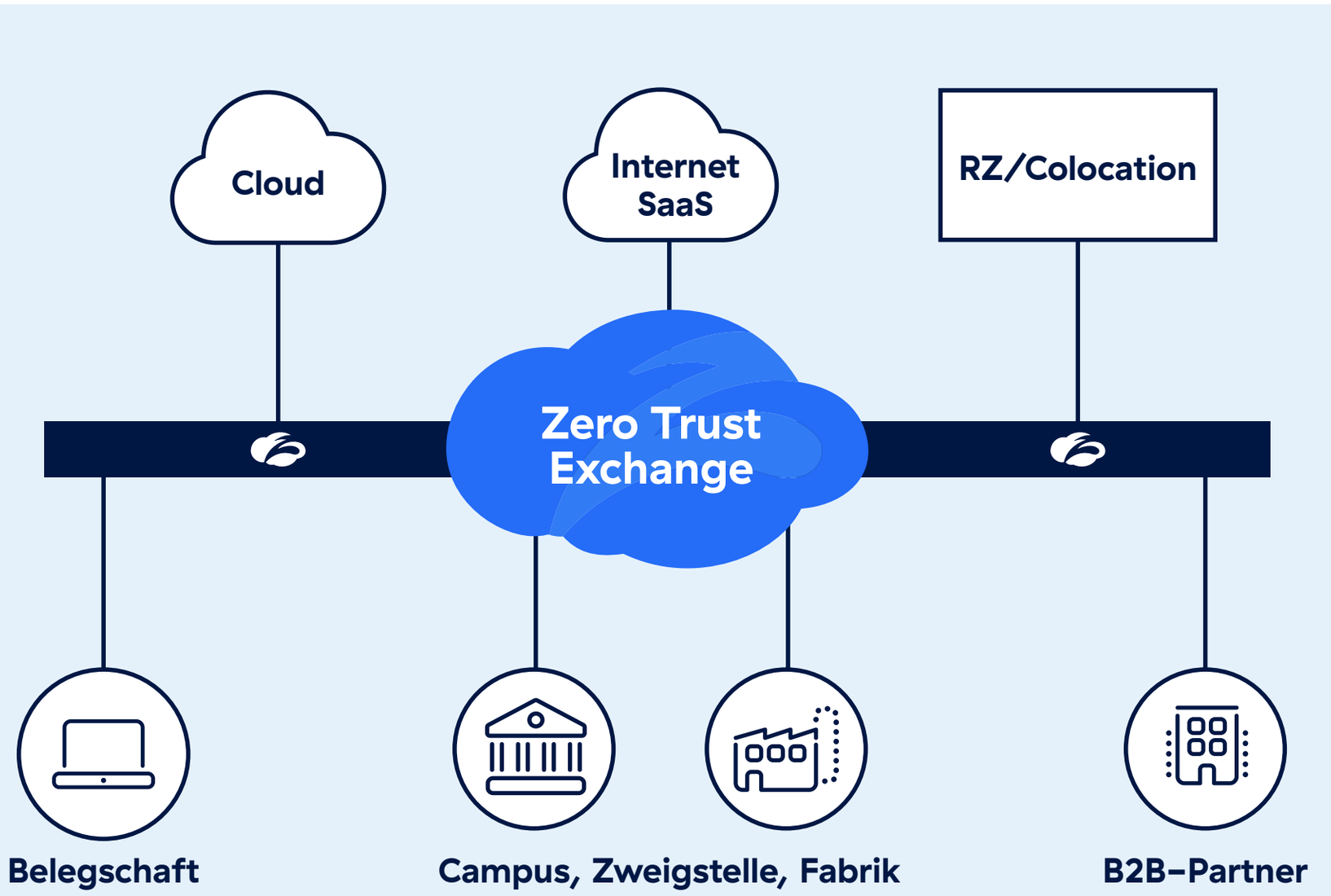

ABB. 1: Die Zscaler-Architektur für Vernetzung und Sicherheit beseitigt Komplexität und Risiko

©2026 Zscaler, Inc. Alle Rechte vorbehalten.

Zero-Trust-Grundlagen und Netzwerksicherheit

Das Sicherheitskonzept von Zscaler basiert auf dem Zero-Trust-Prinzip, wodurch eine sichere Konnektivität und eine strenge Zugriffskontrolle gewährleistet werden.

- **Zscaler Internet Access (ZIA) für Internetsicherheit:** Der gesamte Internettraffic der User wird über ZIA geleitet, wo er vor der Zugriffsgewährung anhand von Richtlinien geprüft wird. Zu den Richtlinien gehören SSL-Inspektion, erweiterte Bedrohungserkennung, Sandboxing und DLP-Richtlinien. Cloud-Umgebungen werden mit Cloud Connectors bereitgestellt, um den ausgehenden Datenverkehr von Cloud-Workloads ins Internet zu sichern.

- **Zscaler Private Access (ZPA) für interne Anwendungen:** Verbindungen zu allen internen Anwendungen werden über ZPA geleitet und erfordern daher Sicherheitsüberprüfungen, bevor der Zugriff gewährt wird. In Cloud-Umgebungen werden Anwendungskonnektoren eingesetzt, die einen nahtlosen und sicheren Zugriff auf privat gehostete Cloud-Anwendungen ermöglichen.

- **Zscaler AI Guard** gewährleistet Laufzeitschutz für KI-Anwendungen, die vom Unternehmen verwaltet werden, und gewährleistet so Sicherheit und Compliance im KI-Betrieb.

- **Zero Trust Branch (ZTB):** Alle Zscaler-Zweigstellen wurden auf ein Café-ähnliches Konnektivitätsmodell umgestellt, wodurch teure Firewalls und Routing-Geräte entfallen. Durch den Einsatz der ZTB-Appliances in den Zweigstellen werden Netzwerksicherheit am Netzwerkrand, SD-WAN und Mikrosegmentierung kombiniert. Alle User, Besucher und IoT-Geräte werden explizit in separate Netzwerke mit jeweils einem User getrennt. Dadurch wird jegliche laterale Bewegung zwischen den Zweigstellen unterbunden.

Sicherung der öffentlichen KI-Nutzung

Öffentliche KI-Plattformen (z. B. ChatGPT, Perplexity, CoPiliot, Grok usw.) sind nützlich, um Arbeitsabläufe zu beschleunigen, komplexe Probleme zu lösen und Daten zu verarbeiten. Allerdings kann ihre Verwendung unbeabsichtigt vertrauliche Daten exponieren, Einfallstore für Schadsoftware schaffen und die Risiken unsicherer Nutzungsszenarien verschärfen. Zscaler begegnet diesen Herausforderungen durch den Einsatz mehrschichtiger Kontrollmechanismen.

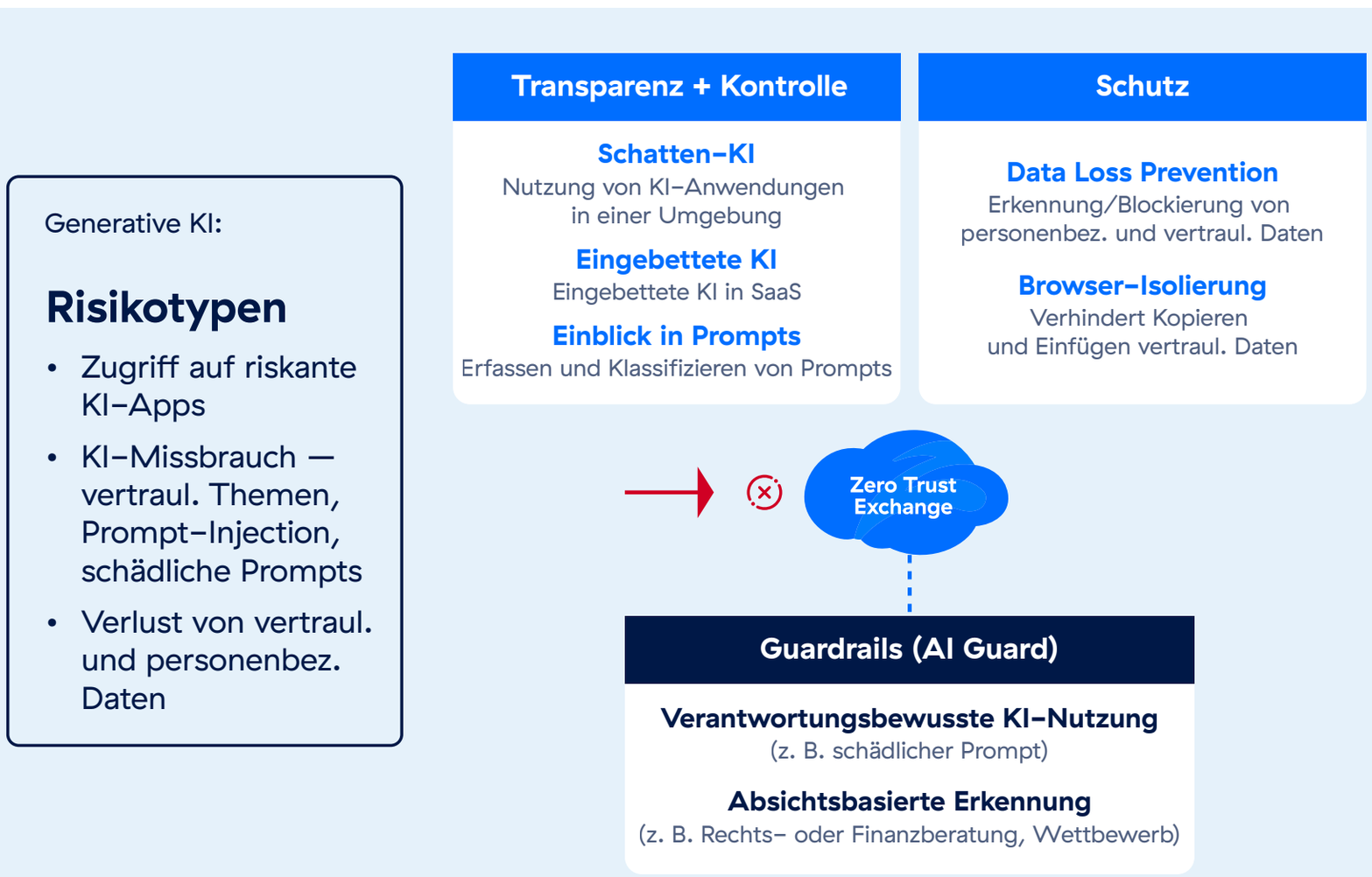

ABB. 2: Zscaler sichert die Nutzung öffentlicher und privater generativer KI

©2026 Zscaler, Inc. Alle Rechte vorbehalten.

- **Blockierung unerwünschter KI-URLs und Schatten-KI-Cloud-Apps** Mithilfe der URL-Filterung und Cloud-Anwendungsrichtlinien von ZIA wird der unbefugte Zugriff auf bestimmte KI-Plattformen und Cloud-Anwendungen blockiert, die für generative KI verwendet werden.

- **Isolierung von KI-/ML-URL-Kategorien zur Einschränkung der Datenweitergabe** Durch die Nutzung der ebenfalls in ZIA integrierten KI-/ML-URL-Kategorisierung gewähren wir Zugriff auf allgemeine KI-/ML-Inhalte, allerdings in einer isolierten Browsersitzung. Der gesamte Traffic zu dieser Kategorie, der nicht ausdrücklich durch die vorstehend erwähnte Richtlinie blockiert wurde, wird an den Zero Trust Browser von Zscaler weitergeleitet. Indem Endusern das Kopieren und Einfügen vertraulicher Daten untersagt wird, lassen sich potenzielle Sicherheitsverletzungen oder der Missbrauch von KI eindämmen, ohne Innovation zu hemmen.

- **Inline-DLP-Prüfung** Überwachung des gesamten Internettraffics einschließlich KI-Interaktionen in Echtzeit, um zu verhindern, dass vertrauliche Daten in laufende Arbeitsabläufe gelangen oder exfiltriert werden.

- **GenAI Security** protokolliert und analysiert den gesamten zulässigen KI-Traffic. Dieser Bericht wird aktiv in ZIA mit Soforterfassung ausgeführt. Er liefert den Sicherheitsbeauftragten und dem CISO detaillierte Berichte zu folgenden Punkten:

  - Welche GenAI-Tools werden verwendet (genehmigt oder blockiert)?
  - Wer nutzt diese Tools?
  - Kategorisierung von Prompts

- **AI Guard für öffentliche KI (LLM Guardrails)** — Prompt- und Response-Guardrails mit AI Guard, die zusätzliche Hürden zur Überprüfung der an zugelassene öffentliche KI-Plattformen gesendeten Anfragen mitsamt ihrer Antworten ermöglichen. Konkret beinhaltet dies:

  - Blockierung der Übermittlung personenbezogener Daten an das LLM.
  - Vermeidung von schädlichen oder unangemessenen Anfragen und Antworten.
  - Blockierung von Prompt-Injection- und Jailbreaking-Versuchen zur Umgehung von Kontrollmechanismen mit kontinuierlicher Aktualisierung, sobald neue KI-spezifische Angriffsvektoren auftauchen.

Diese Schutzmechanismen gewährleisten, dass User verantwortungsvoll mit KI-Tools interagieren, ohne vertrauliche Unternehmensdaten preiszugeben. Außerdem wird der Umfang der vom LLM ausgegebenen Daten eingeschränkt, um den User und das Unternehmen zu schützen.

Einrichtung einer sicheren privaten GenAI-Plattform

Zscaler IT hat eine private generative KI-Plattform entwickelt, auf der alle Mitarbeitenden KI sicher nutzen können. Das Sicherheitsmodell von ZChat basiert auf den Zero-Trust-Prinzipien von Zscaler und nutzt alle KI- und ZPA-Funktionen der Zscaler-Plattform in Kombination mit Okta für Identitätsverwaltung und rollenbasierte Zugriffskontrolle (RBAC). Informationen zu ZChat:

- **Internes Hosting:** Hosting in Zscaler AWS: ZChat wird innerhalb von Amazon Web Services (AWS) gehostet und nutzt die Cloud-native Architektur von Zscaler. Dies ermöglicht eine skalierbare und ausfallsichere Bereitstellung unter Verwendung der integrierten Sicherheitsfunktionen von AWS.

©2026 Zscaler, Inc. Alle Rechte vorbehalten.

- **User-Authentifizierung:** ZChat ist zur Authentifizierung in Okta integriert. Dadurch wird sichergestellt, dass nur berechtigte User — die über Okta bereitgestellt und verwaltet werden — auf ZChat zugreifen können.

- **Rollenbasierte Zugriffskontrolle (RBAC):** Der Zugriff auf ZChat wird durch rollenbasierte Zugriffskontrollen in der Anwendung weiter eingeschränkt. Dadurch wird sichergestellt, dass User nur Zugriff auf die Funktionen und Daten haben, die ihrer jeweiligen Rolle entsprechen.

- **Kommunikation mit der OpenAI von Zscaler auf Azure:** ZChat kommuniziert über sichere Verbindungspfade mit den auf Microsoft Azure gehosteten OpenAI-Services von Zscaler.

- **Zugriffskontrolle über ZPA:** Zscaler Private Access ermöglicht den sicheren Zugriff auf private KI-Anwendungen durch die Segmentierung des Userzugriffs mithilfe softwaredefinierter Perimeter. Dies verhindert laterale Ausbreitung, reduziert die Angriffsfläche und stellt sicher, dass nur authentifizierte und autorisierte User mit datenintensiven KI-Systemen interagieren können.

- **Gerätestatus:** Die Einhaltung der Vorschriften und die vollständige Verwaltung aller Geräte sind zwingend erforderlich, bevor eine Verbindung zu privaten, ZPA-fähigen Unternehmensanwendungen hergestellt werden kann.

- **AI Guard für private KI:** Ähnlich wie bei öffentlicher KI stattet Zscaler private KI-Tools mit Schutzmechanismen aus, die Aktivitäten wie die Weitergabe personenbezogener Daten, unangemessene Nutzung oder Ausnutzung durch schädliche Anweisungen (z. B. Jailbreak-Versuche) verhindern. Durch die Integration dieser Schutzmechanismen in private Unternehmensanwendungen können wir strenge KI-Nutzungsrichtlinien durchsetzen und gleichzeitig das volle Potenzial der KI ausschöpfen.

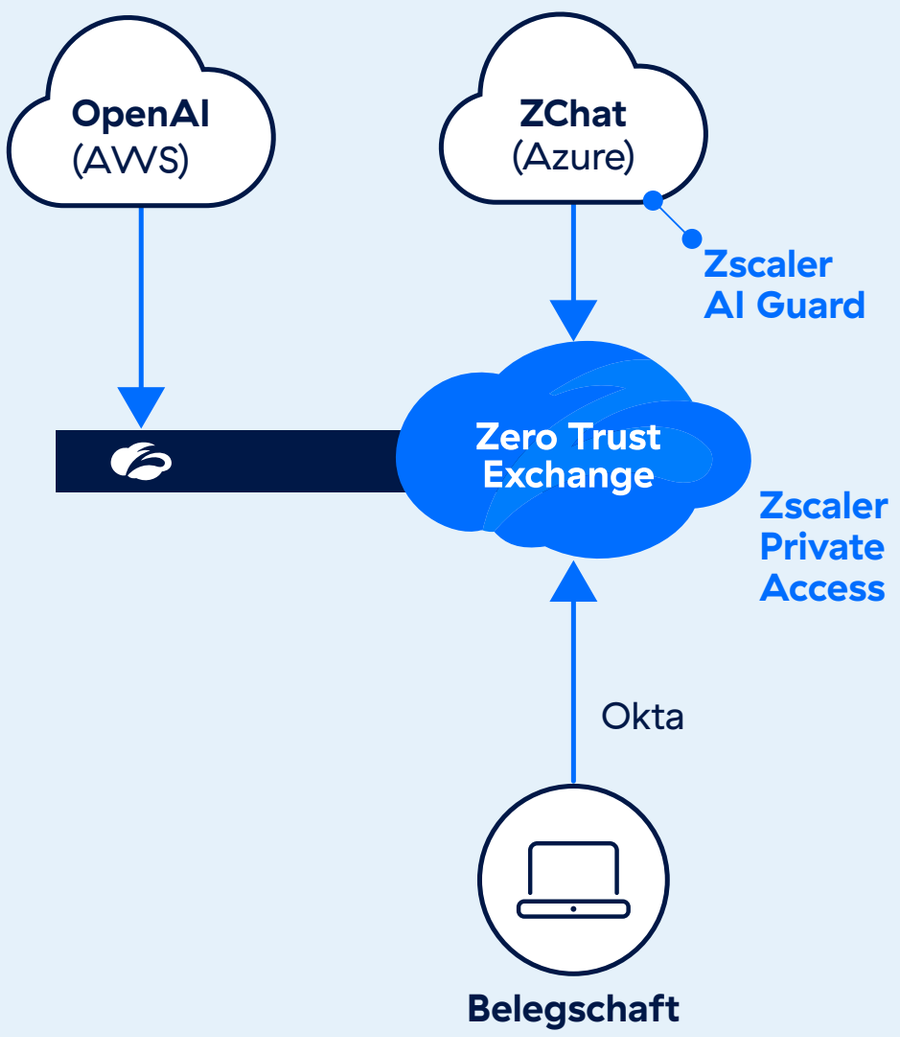

ABB. 3: Zscaler Private Access (ZPA) ermöglicht Mitarbeitenden einen sicheren Zugriff auf die private ZChat-Anwendung (die in AWS ausgeführt wird). ZPA sichert außerdem die Backend-Kommunikation zwischen ZChat und den OpenAI-Services von Zscaler, die in Microsoft Azure gehostet werden. Alle privaten GenAI-Interaktionen (Prompts und Antworten) innerhalb von ZChat werden durch Zscaler AI Guard geschützt.

©2026 Zscaler, Inc. Alle Rechte vorbehalten.

KI gesichert:

Umfassende Schutzmaßnahmen für das Unternehmen

Sicherheitsvorteile

- **Zero-Trust-Architektur:** Zscaler erzwingt das Prinzip der minimalen Rechtevergabe und einen von Grund auf sicheren Zugriff für alle User, Geräte und Anwendungen, wodurch die Angriffsfläche minimiert und eine laterale Ausbreitung in mehreren Umgebungen verhindert wird.

- **Umfassende Governance:** Alle KI-Initiativen unterliegen strengen internen Richtlinien und orientieren sich an Rahmenwerken wie dem NIST AI Risk Management Framework.

- **Robuster Datenschutz:** Vertrauliche Daten (z. B. personenbezogene Daten, Geschäftsgeheimnisse) werden durch strenge Dateneingabe- und -ausgabekontrollen, Inline-DLP und Browserisolation geschützt — so werden unbeabsichtigte Datenabflüsse oder Missbrauch verhindert werden.

- **Kontinuierliche Überwachung der KI-Aktivitäten:** Der Gen AI Security Report bietet detaillierte Überwachungs- und Berichtsfunktionen, die die Echtzeitverfolgung der Tool-Nutzung ermöglichen und die Einhaltung der Nutzungsrichtlinien gewährleisten.

- **Mehrstufige KI-Schutzmechanismen:** Zscaler AI Guard bietet eine sofortige Überwachung und Reaktionsfähigkeit — es blockiert Versuche, vertrauliche Daten weiterzugeben, stoppt Jailbreak-Exploits und verhindert schädliche oder unautorisierte Anfragen sowohl für öffentliche GenAI als auch für interne/private KI.

- **Minderung des Anbieterrisikos:** Alle KI-Tools von Drittanbietern werden einer umfassenden Due-Diligence-Prüfung unterzogen, einschließlich Sicherheitsüberprüfungen, Penetrationstests und vetraglichen/rechtlichen Datenschutzmaßnahmen (z. B. werden keine Daten für externes KI-Training verwendet).

Steigerung der Mitarbeiterproduktivität

- **Sicherer Einsatz von KI:** Zscaler bietet sicheren Zugriff auf private und öffentliche KI-Tools. So können Mitarbeitende KI sicher für Forschung, Programmierung und Workflow-Automatisierung nutzen — und Innovationen ohne Datenrisiko vorantreiben.

- **Schnellere Entscheidungsfindung:** Mitarbeitende können KI nutzen, um Erkenntnisse zu gewinnen, Daten zusammenzufassen und Aufgaben zu automatisieren, da sie wissen, dass Schutzmechanismen und Compliance-Prüfungen vorhanden sind.

- **Beschleunigte Entwicklung:** Entwickler nutzen sichere, vorab genehmigte GenAI- und Code-Vorschlagstools (geschützt durch Code-Reviews und Sicherheitsprüfungen). Dadurch wird der Entwicklungszyklus verkürzt und gleichzeitig hohe Standards eingehalten.

©2026 Zscaler, Inc. Alle Rechte vorbehalten.

Nachweisbarer Geschäftsnutzen

- **Stärkung von Vertrauen und Compliance:** Durch die Ausrichtung an globalen Standards und die proaktive Implementierung von KI-Kontrollen reduziert Zscaler aufsichtsrechtliche Risiken, schafft Vertrauen bei den Kunden und schützt den Ruf des Unternehmens.

- **Reduziertes Cyberrisiko:** Strenge Segmentierung, Trafficprüfung und die Durchsetzung von Richtlinien senken das Risiko von Datenschutzverletzungen, Verstößen gegen Compliance-Vorgaben und Verlusten geistigen Eigentums drastisch — was zu Kosteneinsparungen führt.

- **Mehr Agilität und Innovation:** Die sicheren Frameworks von Zscaler ermöglichen Unternehmen, das Potenzial von KI schnell und sicher zu erkunden, und unterstützen so differenzierte Geschäftsmodelle und eine schnellere Markteinführung neuer Angebote.

- **Branchenführerschaft und Marktdifferenzierung:** Indem Zscaler die Nutzung eigener Produkte fördert und Erfolge transparent dokumentiert, beweist das Unternehmen Führungsstärke im Bereich sicherer KI, gibt Kunden ein Vorbild und stärkt seine Wettbewerbsposition.

Fazit: Vertrauenswürdige KI auf Zero-Trust-Basis im großen Maßstab

Zscaler IT ist ein Beispiel dafür, wie man KI-Innovationen nutzen kann, ohne Kompromisse bei Sicherheit, Datenschutz oder Compliance einzugehen. Durch Implementierung eines umfassenden Governance-Rahmenwerks, die Integration strenger Richtlinien und Nutzung der Leistungsfähigkeit der eigenen Zero Trust Exchange hat sich Zscaler als führendes Unternehmen im Bereich der sicheren KI-Einführung etabliert. Tools wie ZIA mit KI-gestützter Prompt-Erfassung, AI Guard und integrierter DLP gewährleisten, dass die Nutzung von KI nicht nur skalierbar, sondern auch transparent und streng geregelt ist. Dieser Ansatz ermöglicht Zscaler, Cyberbedrohungen abzuwehren, vertrauliche Daten zu schützen und aufsichtsrechtliche Vorgaben zu erfüllen. Gleichzeitig wird dadurch die betriebliche Effizienz gesteigert und Innovation gefördert.

Der Ansatz von Zscaler im Bereich der KI-Sicherheit beweist, dass Unternehmen das transformative Potenzial von KI vertrauensvoll nutzen und gleichzeitig Vertrauen und Resilienz gewährleisten können. Durch die verantwortungsvolle Beschleunigung von Innovationen und die Festlegung von Maßstäben für eine sichere KI-Governance spielt Zscaler weiterhin eine Vorreiterrolle bei der Ermöglichung vertrauenswürdiger KI im Unternehmensmaßstab.

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 **www.zscaler.com/de**. Gerne können Sie uns auch auf X folgen **@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™

Act Fast.
Stay Secure.