Sichere GenAI-Einführung mit Zero Trust:

Sichere Nutzung öffentlicher GenAI-Anwendungen

WHITEPAPER

Inhaltsverzeichnis

Einführung

Generative KI (GenAI) verändert die Arbeitsweise von Behörden und erschließt ihnen neuartige Möglichkeiten, die Produktivität zu steigern, Prozesse zu rationalisieren und ihren Bürgern besser zu dienen. Um jedoch das transformative Potenzial von GenAI zu nutzen und gleichzeitig die damit verbundenen Risiken zu mindern, müssen Behörden Zero-Trust-Prinzipien umsetzen. Dieses Paradigma stellt sicher, dass keiner Entität — weder Mensch noch Maschine — standardmäßig vertraut wird, und gewährleistet so kontinuierliche Transparenz und strenge Überprüfung bei allen Interaktionen.

Dieses Whitepaper ist das erste in der Reihe „Sichere GenAI-Einführung mit Zero Trust“. Dabei handelt es sich um eine umfassende Strategie, die Behörden dabei unterstützen soll, sich sicher in der GenAI-Landschaft zurechtzufinden. Die Serie umfasst drei Phasen:

- Phase 1, die in diesem Dokument beschrieben wird, konzentriert sich auf die Sicherung öffentlicher GenAI-Anwendungen, um Risiken wie Datenverluste und nicht genehmigte KI-Nutzung („Schatten-KI“) zu bewältigen.

- In Phase 2 wird die Nutzung von Agentic-AI-Tools untersucht, um die Produktivität der Mitarbeiter sicher zu steigern.

- In Phase 3 liegt der Schwerpunkt auf der sicheren Bereitstellung von GenAI-Systemen für Bürgerservices und der Gewährleistung, dass Regierungssysteme und -daten geschützt bleiben.

Jede Phase betont einen proaktiven, mehrschichtigen Ansatz, der Innovation mit robuster Governance und Sicherheit in Einklang bringt.

Sichere Nutzung öffentlicher GenAI-Anwendungen

Überblick

Behörden sind sich zunehmend des transformativen Potenzials der Generativen KI (GenAI) für ihre Geschäftstätigkeit und die Dienstleistungen, die sie den Bürgern anbieten, bewusst. Diese Technologie eröffnet einen Weg zu erheblichen Produktivitätssteigerungen und zur Weiterentwicklung von Bürgerservices durch vielfältige Anwendungen. Diese reichen vom Verständnis der öffentlichen Meinung und der Bereitstellung KI-gestützter Chatbots für den Bürger- und IT-Support bis hin zur Erleichterung der Sprachübersetzung und Automatisierung interner Prozesse. Dazu zählt das Verfassen von Stellenbeschreibungen, die Zusammenfassung von Besprechungen und die Erstellung öffentlicher Ankündigungen.

Frühanwender unter den Behörden können bereits Verbesserungen bei der Mitarbeitererfahrung und -zufriedenheit feststellen. Die Verfügbarkeit öffentlich zugänglicher Large Language Models (LLMs) wie ChatGPT hat im gesamten öffentlichen Sektor zu Experimenten geführt, da Behörden versuchen, die Möglichkeiten der KI zu verstehen und zu nutzen. Dieses breite Interesse unterstreicht die Möglichkeiten zur Verbesserung der Effizienz und der Servicebereitstellung durch die Integration dieser zukunftsfähigen KI-Tools.

Die Integration von GenAI, insbesondere über öffentliche LLMs und Modelle von Drittanbietern, bringt jedoch erhebliche Sicherheitsherausforderungen mit sich. Durch die unbefugte Verwendung von KI-Tools („Schatten-KI“) können vertrauliche Bürgerdaten, Geschäftsunterlagen oder urheberrechtlich geschützte Inhalte offengelegt werden. Das Risiko wird in Arbeitsabläufen mit Retrieval Augmented Generation (RAG) oder Model Content Protocol (MCP) und KI-Agents noch verstärkt. Dadurch können vertrauliche Daten gefährdet werden und es können Risiken für die innere Sicherheit entstehen, da staatlich geförderte Akteure oder böswillige Organisationen diese Schwachstellen möglicherweise für Spionage, Sabotage oder die Störung kritischer Infrastrukturen ausnutzen. Darüber hinaus stellt GenAI eine breite Angriffsfläche dar, die mit herkömmlichen Sicherheitsmaßnahmen nicht effektiv bewältigt werden kann. Diese beruhen häufig auf restriktiven binären Kontrollen oder bieten keine umfassende Transparenz über verschiedene Umgebungen.

Um das Potenzial von GenAI voll auszuschöpfen, sollten Behörden einen Zero-Trust-Ansatz mit robuster Sicherheit, Transparenz und Benutzerfreundlichkeit verfolgen. Die folgenden Schritte skizzieren einen Prozess, den Behörden durchführen können, um GenAI zu nutzen und gleichzeitig proaktiv die Risiken von Datenverlusten zu mindern und eine unnötige Belastung der Sicherheitsverantwortlichen zu verhindern:

1. Etablierung von KI-Governance-Frameworks und -Richtlinien
2. Enge Integration von User Experience und Schulungen
3. Auswahl der richtigen Architektur unter Berücksichtigung von Sicherheitskriterien
4. Implementierung von Datenschutzstrategien bereits in der Anfangsphase
5. Ganzheitlicher mehrschichtiger Schutzansatz

Im Folgenden werden diese Schritte im Detail erläutert.

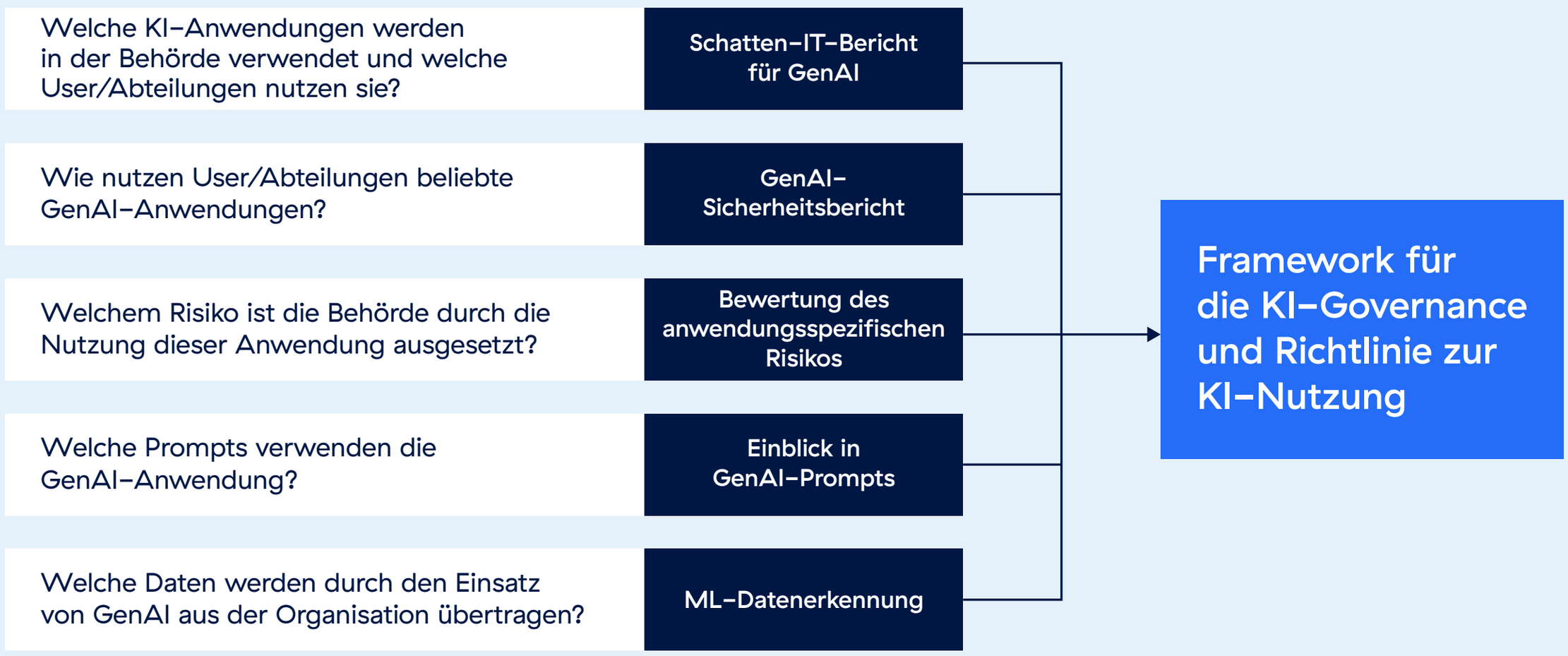
1. Etablierung von KI-Governance-Frameworks und -Richtlinien

Um die Vorteile von GenAI voll auszuschöpfen, müssen Behörden robuste Sicherheitsmaßnahmen implementieren, die Risiken direkt angehen, ohne die Produktivität der User zu beeinträchtigen. In diesem Abschnitt wird untersucht, wie Behörden einen Zero-Trust-Ansatz für GenAI-Anwendungen übernehmen und gleichzeitig sicherstellen können, dass Sicherheitskontrollen die nahtlose User Experience nicht beeinträchtigen.

Die Entwicklung von KI-Governance-Frameworks und -Richtlinien ist eine unverzichtbare Voraussetzung für die sichere Nutzung von GenAI-Anwendungen bei staatlichen Behörden. Dies beinhaltet häufig die Einrichtung einer speziellen Taskforce oder eines Leitungsgremiums zur Überwachung der Entwicklung und Umsetzung von Richtlinien. Als Vorbild kann hier etwa die Alabama GenAI Task Force mit ihrem kollaborativen, funktionsübergreifenden Teamansatz dienen. Zur Steuerung ihrer Maßnahmen sollten die Behörden außerdem etablierte Zero-Trust-Frameworks wie das Zero-Trust-Reifegradmodell von CISA und NIST 800-207 sowie KI-spezifische Sicherheits-Frameworks wie das NIST AI Risk Management Framework (AI RMF) oder TRISM von Gartner nutzen. Durch die Einrichtung einer fokussierten Taskforce und die Nutzung dieser bewährten Frameworks können Behörden die sichere Integration von GenAI-Technologien abteilungsübergreifend beschleunigen.

Um diesen Prozess zu unterstützen, bietet Zscaler Einblicke, die Behörden dabei unterstützen, die KI-Nutzung in ihren Umgebungen zu verfolgen, potenzielle Risiken im Zusammenhang mit GenAI-Anwendungen einzuschätzen und Fälle von Datenverlusten rechtzeitig zu identifizieren. In den Reports von Zscaler finden Behörden wertvolle Hinweise, wie sich wichtige Daten zur aktuellen Verwendung von GenAI-Tools abrufen lassen.

Datenpunkte (bereitgestellt von Zscaler) unterstützen die Erstellung eines KI-Governance-Frameworks und einer KI-Nutzungsrichtlinie



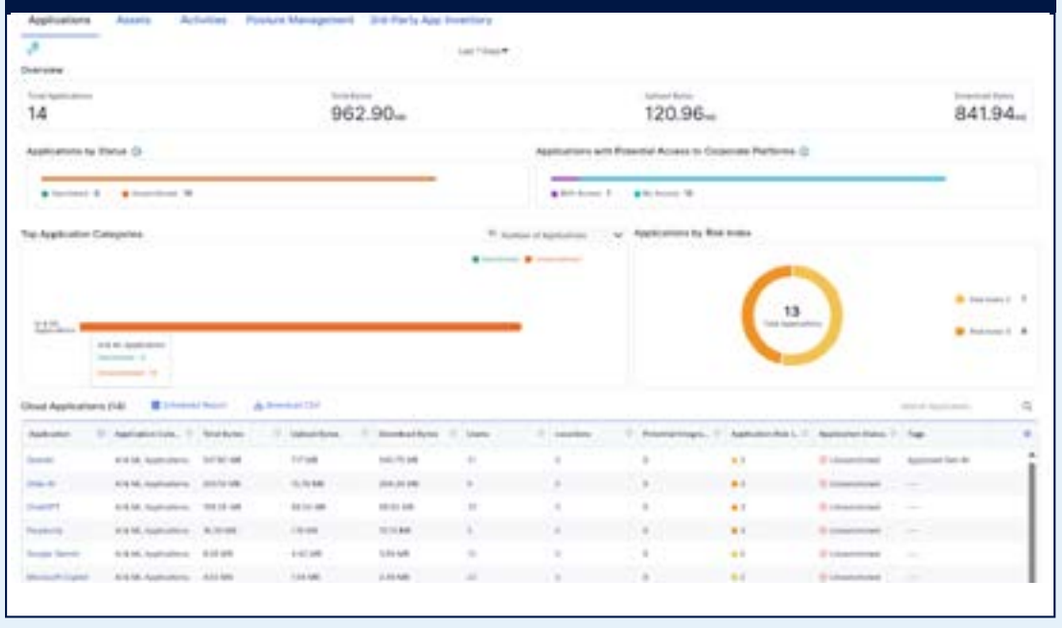
Aktuelle KI-Nutzung verstehen

Das Verständnis der aktuellen KI-Nutzung ist ein wichtiger Schritt bei der Erstellung von Governance-Frameworks. Durch die Analyse der verwendeten GenAI-Anwendungen, ihrer Anwendungsweise und der damit verbundenen Risikofaktoren können Behörden ermitteln, wo der dringendste Handlungsbedarf besteht. Dieser datengesteuerte Ansatz stellt sicher, dass das Framework relevant und umsetzbar bleibt und darauf zugeschnitten ist, die einzigartigen Herausforderungen und Chancen der betreffenden Behörde effektiv zu bewältigen.

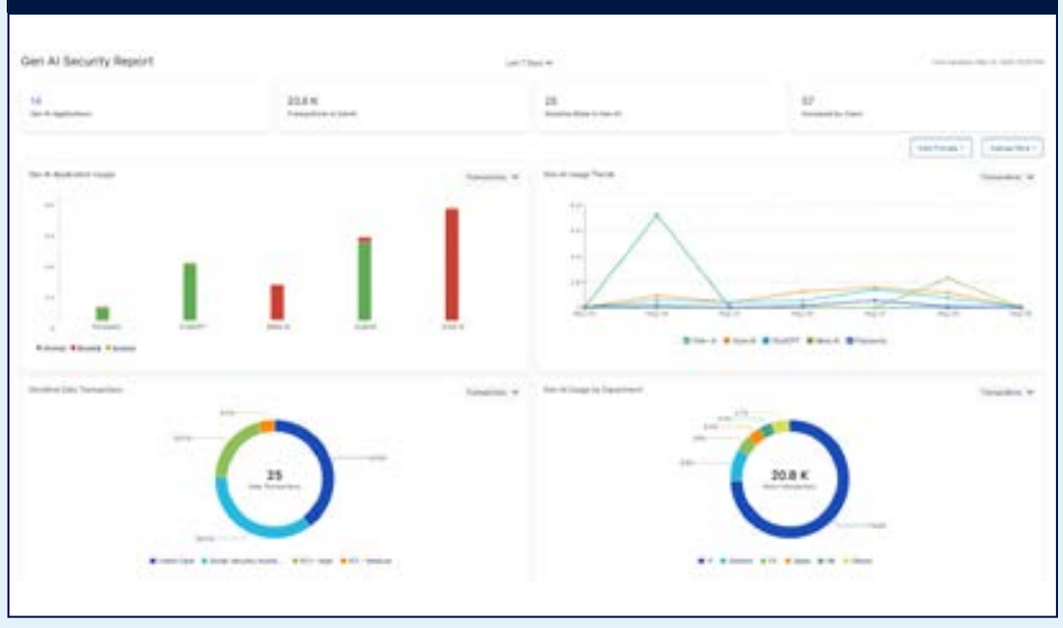
Zscaler stellt detaillierte Berichte zur KI-Nutzung bereit, die Aufschluss darüber geben, welche GenAI-Anwendungen in den verschiedenen Behörden verwendet werden und in welchem Umfang sie genutzt werden. Diese Erkenntnisse können weiter segmentiert werden, um Nutzungsmuster innerhalb bestimmter Abteilungen oder Unterbehörden aufzuzeigen, damit Behörden einen klaren Überblick über ihre KI-Nutzung erhalten.

Einblicke in die Nutzung von Schatten-KI

Erkennen von Schatten-IT für GenAI

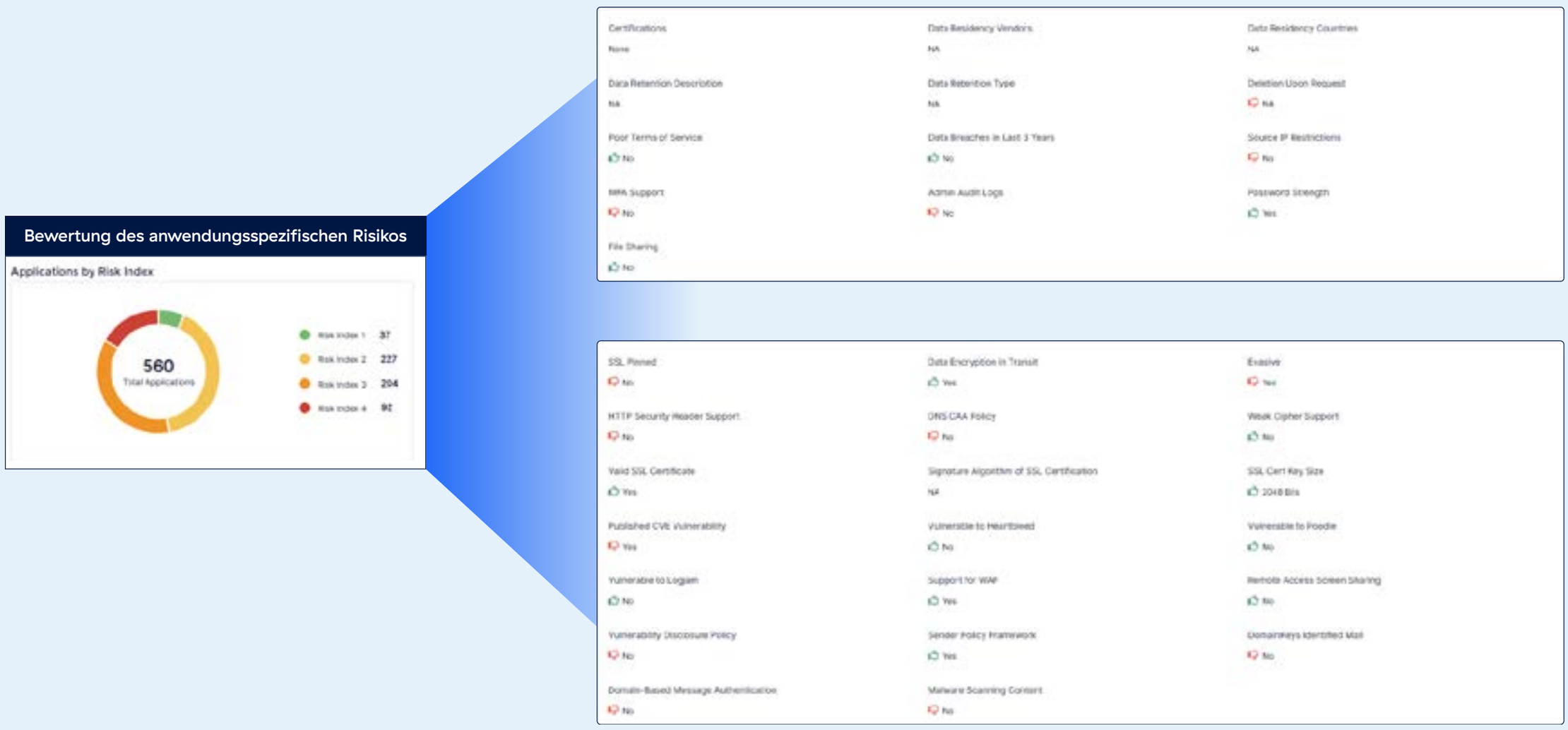


GenAI-Sicherheitsbericht



Durch diese Transparenz können die Behörden die mit diesen Anwendungen verbundenen Risikofaktoren genauer untersuchen. Das ThreatLabz-Team von Zscaler bewertet diese Risiken in Abstimmung mit Bedrohungsinformationen von Drittanbietern und weist ihnen aggregierte Bewertungen von 1 bis 5 zu, wodurch Entscheidungsträgern die Risikobewertung erleichtert wird. Behörden haben außerdem die Flexibilität, diese Bewertungen an ihre individuellen Prioritäten und Anforderungen anzupassen. Risikobewertungen können Schlüsselfaktoren wie Sicherheitslücken oder Probleme bei der Einhaltung gesetzlicher Vorschriften einbeziehen, sodass Entscheidungsträger ihre Ressourcen auf die Bereiche konzentrieren können, die für ihren jeweiligen Auftrag und ihre Sicherheitsanforderungen besonders relevant sind. Im folgenden Bericht werden einige Beispiele für Risikofaktoren wie Sicherheitslücken oder die Nichteinhaltung von Vorschriften aufgeführt, die es den Entscheidungsträgern der Behörde ermöglichen, die Bereiche zu priorisieren, die für die jeweilige Agentur wichtig sind.

Risiken im Zusammenhang mit der Nutzung von Schatten-KI

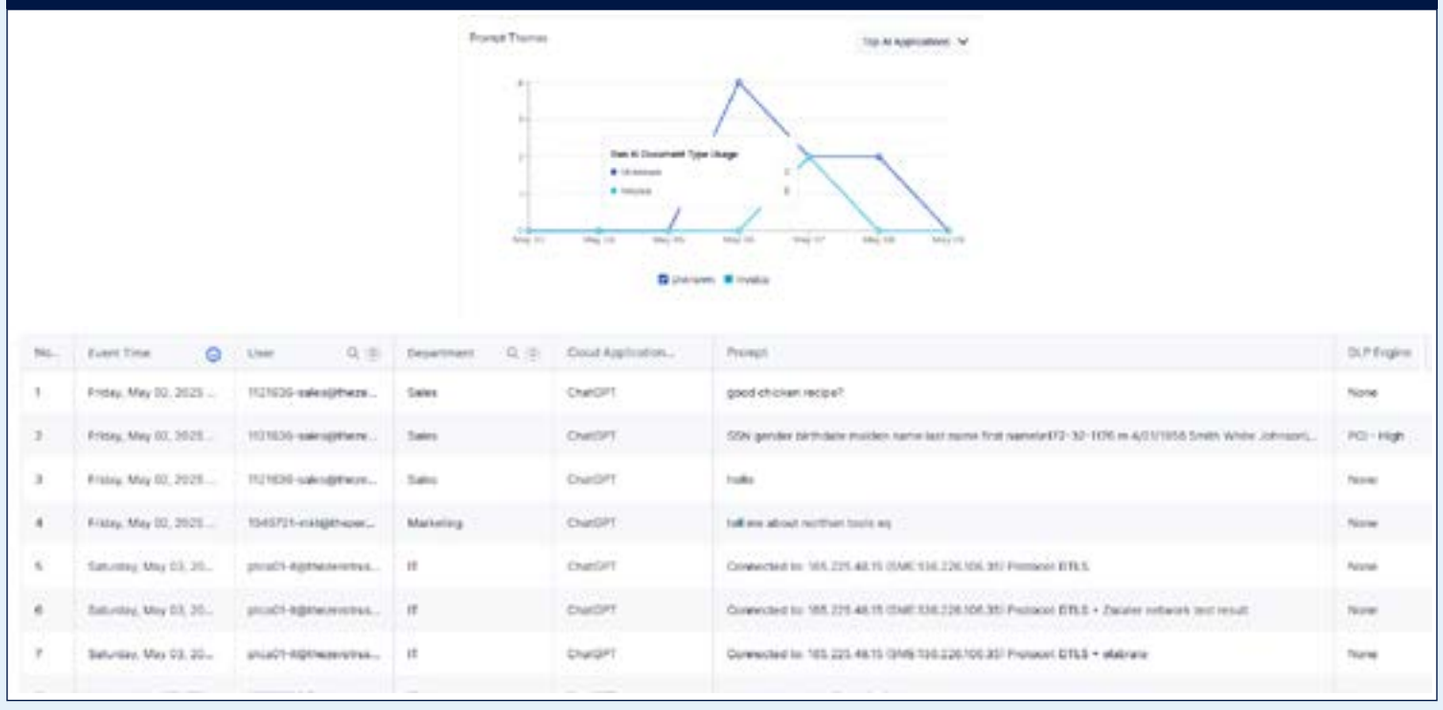


Detaillierte Einblicke in User-Interaktionen mit GenAI-Anwendungen

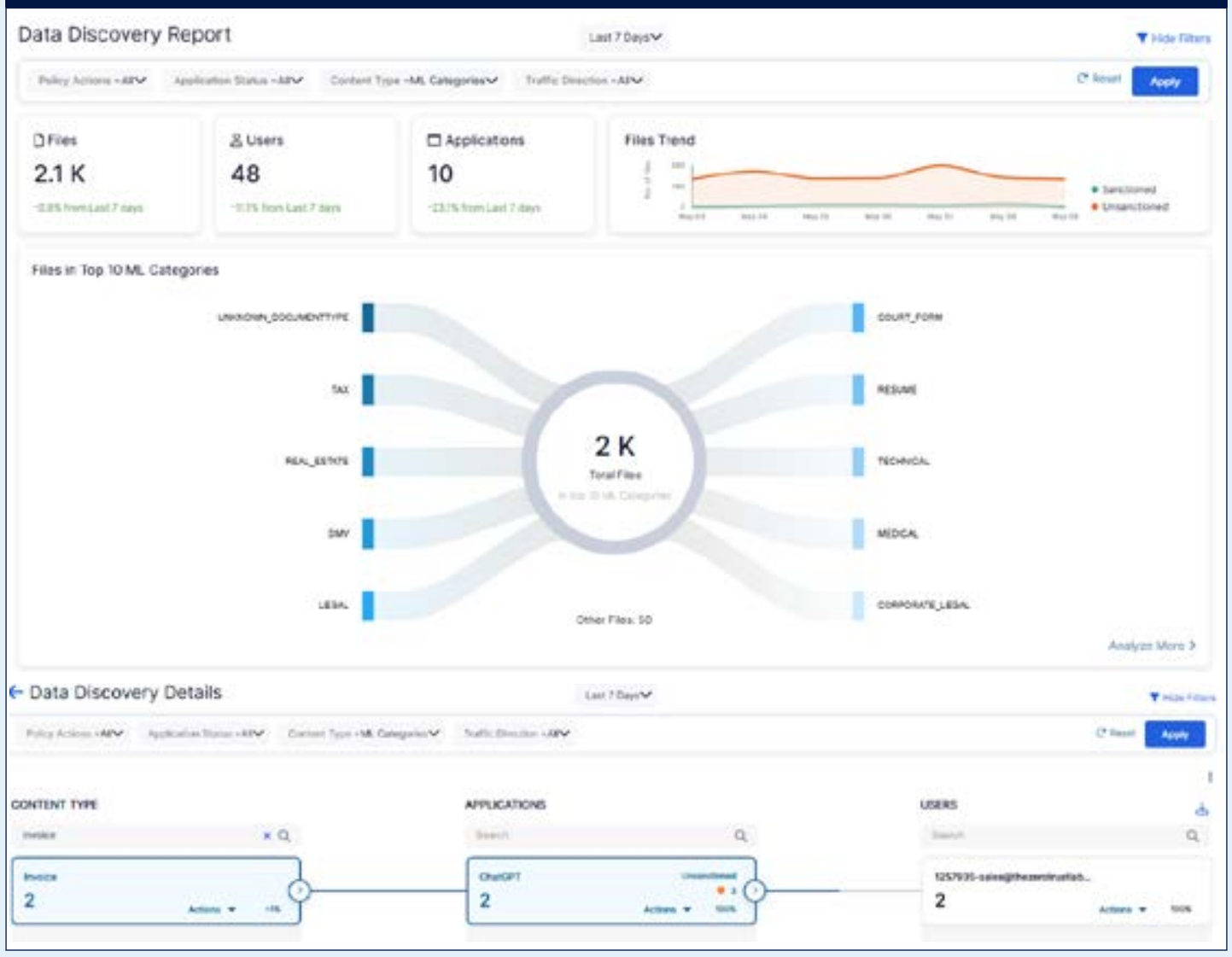
Über die Transparenz auf Anwendungsebene hinaus liefert die Zscaler-Lösung detaillierte Einblicke in sämtliche Transaktionen, Prompts und User-Interaktionen innerhalb von GenAI-Anwendungen. Dazu gehören detaillierte Daten zu den Eingaben der User, nicht nur über Dateiübertragungen, sondern auch über Methoden wie Tastatureingaben, Zwischenablageaktivitäten und andere unterstützte Eingaben. Diese Erkenntnisse sind für Behörden von unschätzbarem Wert, da sie ihnen helfen, die Art der freigegebenen Daten besser zu verstehen, Sicherheitsrichtlinien zu präzisieren und die Einhaltung von Governance-Standards sicherzustellen. Darüber hinaus ist dieser Grad an Transparenz für Auditzwecke unerlässlich und kann zur umfassenden Nachverfolgung und Analyse nahtlos in das SIEM der Behörde exportiert werden.

Bericht über aktuelle Datenübertragungen außerhalb der Behörde

Einblick in GenAI-Prompts



ML-Datenerkennung



Transparenz über unerkannte Datenübertragungen

Zscaler verbessert die Transparenz zusätzlich durch Erkennen von Daten, von denen die Behörden möglicherweise nicht wissen, dass sie über GenAI-Anwendungen nach außen übertragen werden. Der KI/ML-gestützte Report von Zscaler geht über die herkömmlichen DLP-Regeln hinaus und erkennt und klassifiziert proaktiv vertrauliche Daten, die an öffentliche GenAI-Tools übertragen werden. Auf diese Weise können Dateneigentümer und Sicherheitsadministratoren unbekannte oder unerkannte Datenverluste lokalisieren und beheben, bevor sie zu kritischen Problemen werden.

Diese umfassende Datentransparenz ermöglicht es den Behörden, Hochrisikodaten, die öffentlichen LLMs zugänglich gemacht werden könnten, proaktiv zu identifizieren. Darüber hinaus hilft es dabei, die Eigentümerschaft vertraulicher Informationen festzulegen oder zu präzisieren, Nutzungsrichtlinien zu entwickeln und maßgeschneiderte Richtlinien zum Schutz wichtiger Datensätze zu implementieren.

Durch die Kombination von Erkenntnissen zu Usern, Anwendungen, Anwendungsrisiken, Prompts und Datenmustern unterstützt Zscaler die Erstellung spezifischer Richtlinien und Verfahren, die mit den Unternehmenszielen übereinstimmen. Diese Erkenntnisse unterstützen die Ressourcenzuweisung und helfen bei der Definition von Rollen und Verantwortlichkeiten innerhalb des Zero-Trust-Governance-Frameworks. Dadurch können Behörden einen zukunftsorientierten Ansatz verfolgen, der Innovation mit der Definition einer umfassenden Strategie zur Risikominderung in Einklang bringt.

2. Enge Integration von User Experience und Schulungen

User Experience und Schulung spielen eine zentrale Rolle für die sichere und erfolgreiche Einführung von generativer KI (GenAI) in staatlichen Behörden. Um eine reibungslose Einführung zu gewährleisten, ist es wichtig, dass Sicherheitsmaßnahmen und Benutzerschulungen so konzipiert sind, dass die User weiterhin produktiv arbeiten und gleichzeitig ein starker Schutz gewährleistet ist. Die Einführung eines weiteren Tools oder einer weiteren Anwendung sollte nach Möglichkeit vermieden werden. Darüber hinaus müssen wirksame Sicherheitskontrollen mit kontinuierlicher Benutzerschulung einhergehen, um ihre Wirkung zu maximieren. Plattformen sollten sich nahtlos in bestehende Arbeitsabläufe und Kanäle integrieren lassen und gleichzeitig Mechanismen für User-Interaktionen und Feedback beinhalten. Dies kann Behörden dabei unterstützen, die GenAI-Nutzung an Frameworks wie dem NIST AI Risk Management Framework (AI RMF) auszurichten.

Im Folgenden werden einige wichtige Plattformfunktionen erläutert, die diesen Ansatz unterstützen:

Nahtloser GenAI-Zugriff

Der Einsatz von GenAI-Tools dient primär dazu, User von Routineaufgaben zu entlasten und ihnen zu ermöglichen, sich auf solche Arbeiten zu konzentrieren, bei denen menschliches Urteilsvermögen erforderlich ist. Sicherheitsmaßnahmen für GenAI dürfen die Arbeitsabläufe der User nicht beeinträchtigen. Zscaler erleichtert dies, indem es die Notwendigkeit zusätzlicher Software oder verwalteter Browser überflüssig macht. Als Beispiel:

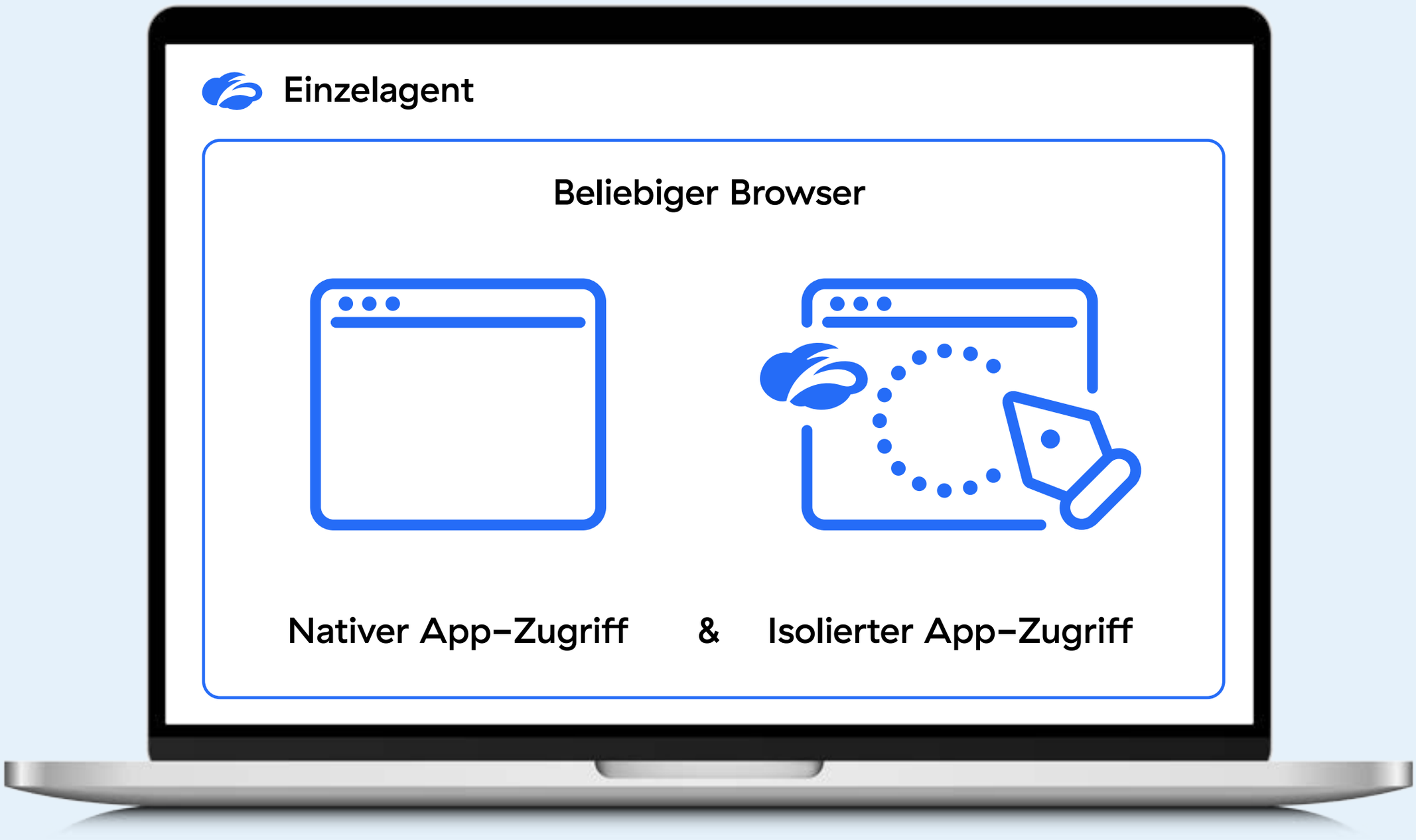
- **Zscaler Single Agent** Derselbe Zscaler-Agent, der den sicheren Zugriff auf öffentliche und private Anwendungen gewährleistet, verwaltet auch die GenAI-Kontrollen und ermöglicht einen nahtlosen Zugriff ohne Einführung zusätzlicher Tools.

- **Sicherer Zugriff ohne Agents**
  User können ihren nativen Browser und ihren vorhandenen Workflow verwenden, um auf gesicherte GenAI-Anwendungen zuzugreifen, ohne dass ein Agent erforderlich ist.

- **Flexible Sicherheitskontrollen:** Anstatt Unternehmen bei der KI-Nutzung nur die Entscheidung zwischen „Zulassen oder Blockieren“ zu ermöglichen, bietet Zscaler eine cloudbasierte Browser-Isolation. Diese Funktion leitet User, die auf GenAI-Anwendungen zugreifen, in eine isolierte Browserumgebung um, die in der Zscaler-Cloud gehostet wird. So wird Usern das Arbeiten mit einer nativen Browser-Oberfläche ermöglicht. Gleichzeitig kann das Unternehmen erweiterte Sicherheitsmaßnahmen wie das Verhindern von Zwischenablageaktivitäten, Drucken oder Datei-Uploads anwenden. Dieses Design stellt sicher, dass Sicherheitsrichtlinien ohne Beeinträchtigung der User Experience durchgesetzt werden. Die Verwaltung erfolgt über eine einheitliche Plattform und einen einzigen Zscaler-Agent, um die Administration zu vereinfachen.

Diese Kontrollen können mit minimalen Auswirkungen auf die vorhandene Infrastruktur oder die Endgeräte bereitgestellt werden. So können Behörden Sicherheitsrichtlinien implementieren und gleichzeitig eine nahtlose User Experience gewährleisten und den Verwaltungsaufwand auf ein Minimum beschränken.

Universal Agent zur Unterstützung von nativem und isoliertem Zugriff

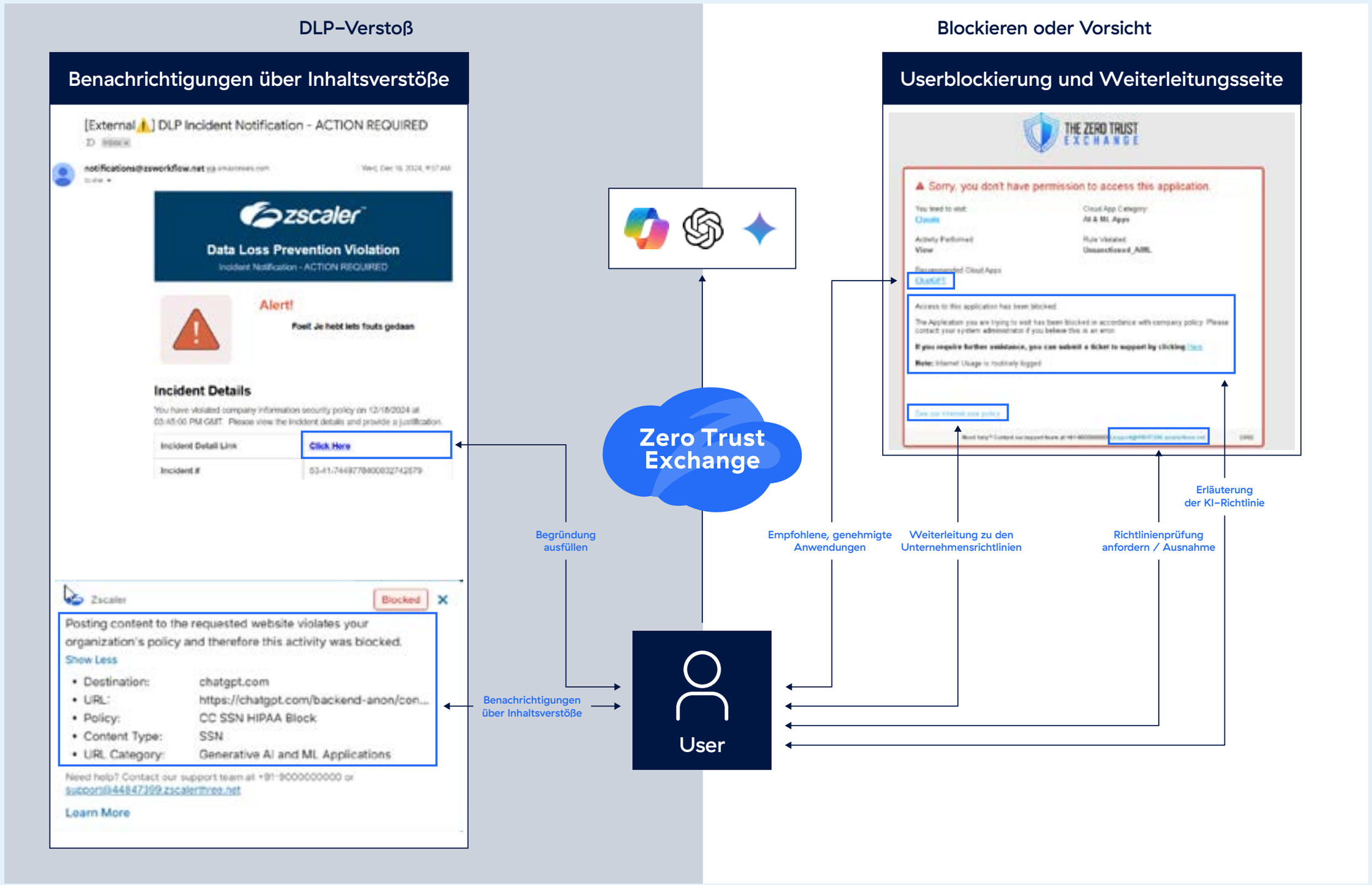


Integrierte User-Schulung und Feedback

Angesichts der rasanten Entwicklung von GenAI ist eine kontinuierliche Aufklärung über die sichere Nutzung und potenzielle Verstöße unerlässlich. Die Schulung sollte regelmäßig und fortlaufend erfolgen und direkt in die nativen Arbeitsabläufe und Tools der User integriert werden. Zscaler unterstützt dies durch dynamische Benachrichtigungen. Wenn eine Ressource blockiert, isoliert oder wegen Inhaltsverstößen gekennzeichnet wird, erhalten User unternehmensspezifische Warnmeldungen. Wenn beispielsweise eine nicht genehmigte GenAI-Anwendung blockiert wird, schlägt Zscaler genehmigte Alternativen vor und hilft so, das User-Verhalten umzulenken und gleichzeitig die Produktivität aufrechtzuerhalten. Zur Verhinderung von Verstößen gegen Richtlinien zur Datennutzung lässt sich Zscaler mit bekannten Tools wie E-Mail und Slack integrieren. So können User in den Tools, die sie bereits verwenden, einfacher Begründungen liefern oder maßgeschneidertes Feedback erhalten.

Durch die Integration von Benutzerschulungen in Sicherheits-Workflows können Behörden eine solide Governance-Grundlage für GenAI-Anwendungen schaffen. Dieser Ansatz stellt nicht nur sicher, dass die User verstehen, wie sie sicher mit der Technologie interagieren. Darüber hinaus trägt er auch dazu bei, einen skalierbaren Rahmen für den Umgang mit GenAI-bezogenen Vorfällen und die Präzisierung der KI-Nutzungsrichtlinien im gesamten Unternehmen zu schaffen.

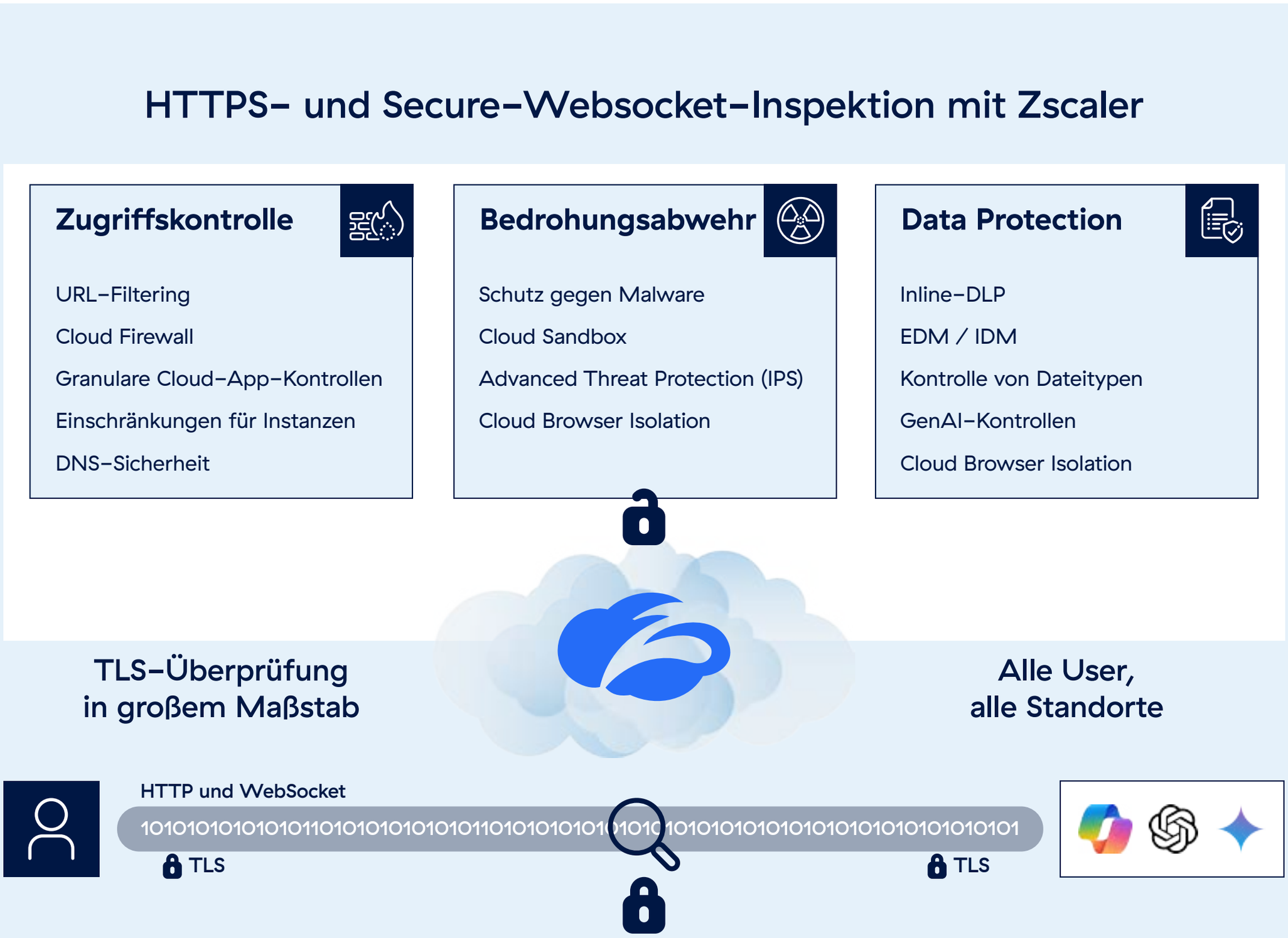
User-Schulung und Feedback mit Zscaler



3. Auswahl der richtigen Architektur unter Berücksichtigung von Sicherheitskriterien

Da sich die Angriffsfläche mit der zunehmenden Verbreitung von KI-Tools vergrößert, ist es von entscheidender Bedeutung, eine Plattform zu wählen, die nicht nur vor KI-basierten Bedrohungen schützt. Daneben muss sie auch die sichere Nutzung von GenAI-Anwendungen ermöglichen, die auf einer Zero-Trust-Architektur und mit FedRAMP-Autorisierung basieren. Zscaler stellt eine umfassende Lösung bereit, die Sicherheit, Benutzerfreundlichkeit und Compliance für Behörden kombiniert, die GenAI einführen.

Behörden können die sicheren GenAI-Funktionen von Zscaler mit minimalen Änderungen an ihrer vorhandenen Infrastruktur nutzen. Der Traffic kann entweder über die Zscaler-App, die mit den wichtigsten Betriebssystemen wie Windows, Mac, iOS, Android und Linux kompatibel ist, über ein Zweigstellengerät oder einfach über einen Browser für die Bereitstellung ohne Agents an die Plattform weitergeleitet werden. Nach der Verbindung stellt Zscaler sicher, dass User authentifiziert und autorisiert sind, bevor sie auf Ressourcen im Internet zugreifen, einschließlich GenAI-Anwendungen. Zscaler fungiert als Proxy und überprüft alle mit GenAI-Anwendungen eingerichteten TLS-Sitzungen. So erhalten Behörden vollständige Transparenz und detaillierte Kontrolle darüber, wie ihre User mit diesen Tools interagieren. Diese Architektur gewährt tiefe Einblicke in die Nutzung von GenAI-Anwendungen durch die User zu gewähren. Zudem stellt sie Behörden mehrere branchenführende Kontrollen zum Schutz ihrer Daten bereit.



Erkennung und Verwaltung von GenAI-Anwendungen automatisieren

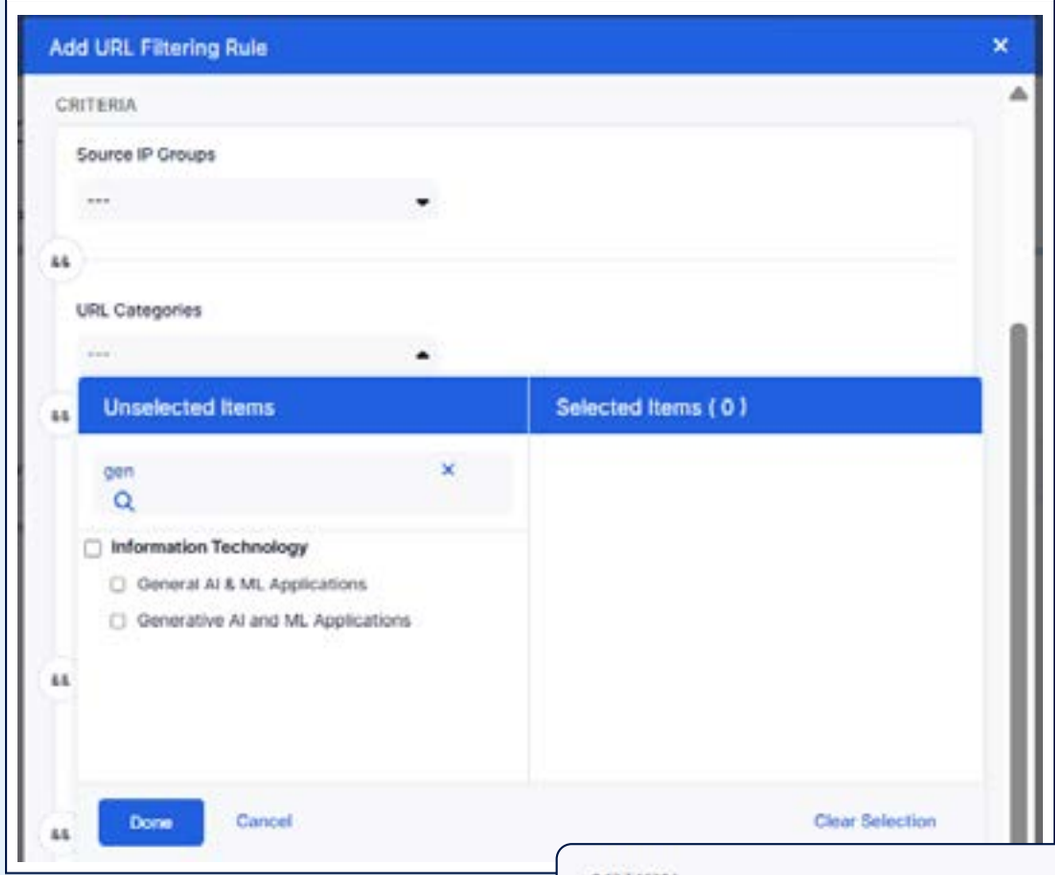
Mit der TLS-Inspektion erhalten Behörden Zugriff auf die gesamte Palette der Funktionen von Zscaler, einschließlich der detaillierten Kontrolle über GenAI- und Machine-Learning-Anwendungen. Ein entscheidender Vorteil liegt in der Kategorisierung von KI/ML-Anwendungen, die durch das ThreatLabz-Team von Zscaler kuratiert wird. Diese Kategorisierung umfasst eine breite Palette von KI-Anwendungen, darunter beliebte Tools wie ChatGPT, Gemini, MetiAI, Claude und andere.

Mithilfe dieser Kategorien können Behörden Richtlinien durchsetzen, um unbekannte oder ungeprüfte GenAI-Anwendungen standardmäßig zu blockieren und so sicherzustellen, dass nur genehmigte Tools zugänglich sind. Neue Anwendungen werden automatisch zu diesen Kategorien hinzugefügt, wodurch den Behörden der Aufwand für die manuelle Erkennung und Bereitstellung entsprechender Updates erspart bleibt. Darüber hinaus haben Behörden die Flexibilität, diese Liste durch Hinzufügen benutzerdefinierter Domänen zu erweitern oder anzupassen, um sie besser an ihre spezifischen Anforderungen anzupassen. Zscaler stellt auch spezielle Kategorien wie „Allgemeine KI/ML-Anwendungen“ und „Generative KI-/ML-Anwendungen“ bereit.

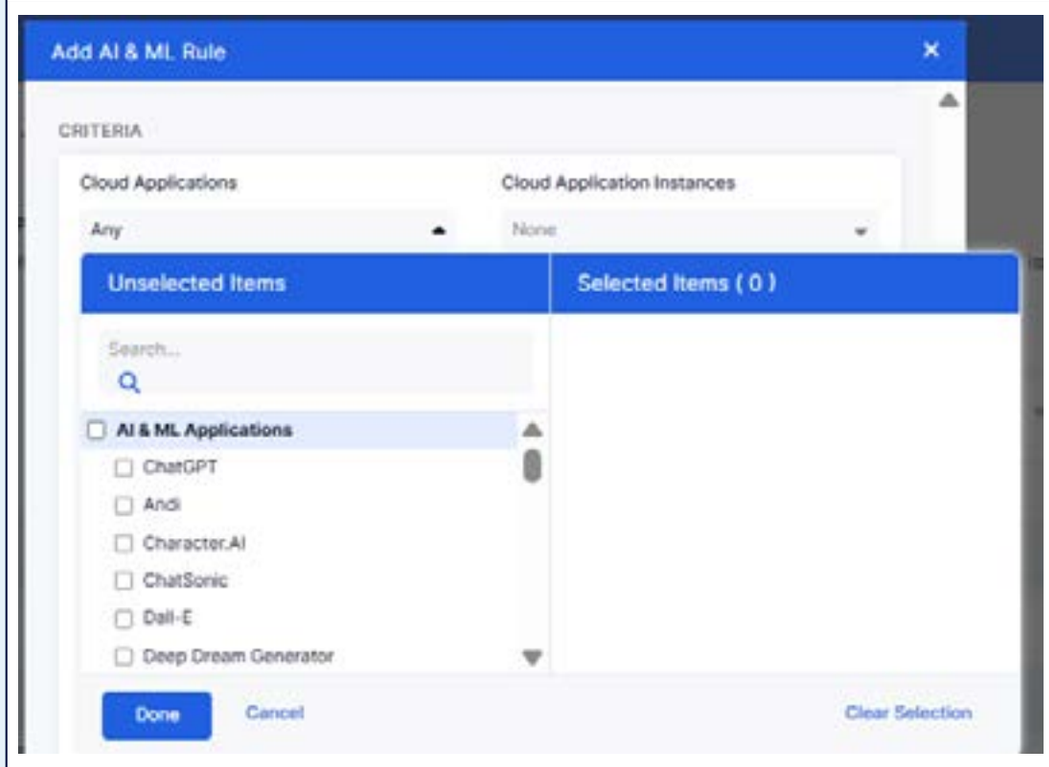
In Kombination mit der Liste „KI-Cloud-Anwendungen“ wird dadurch eine umfassende Abdeckung gewährleistet, um die Sicherheitsrisiken zu reduzieren, die von GenAI-Anwendungen ausgehen. Dieser mehrschichtige Ansatz unterstützt Behörden in dem Bemühen, den Zugriff auf Hunderte von Anwendungen, die jede Woche entwickelt und veröffentlicht werden, effektiv zu verwalten.

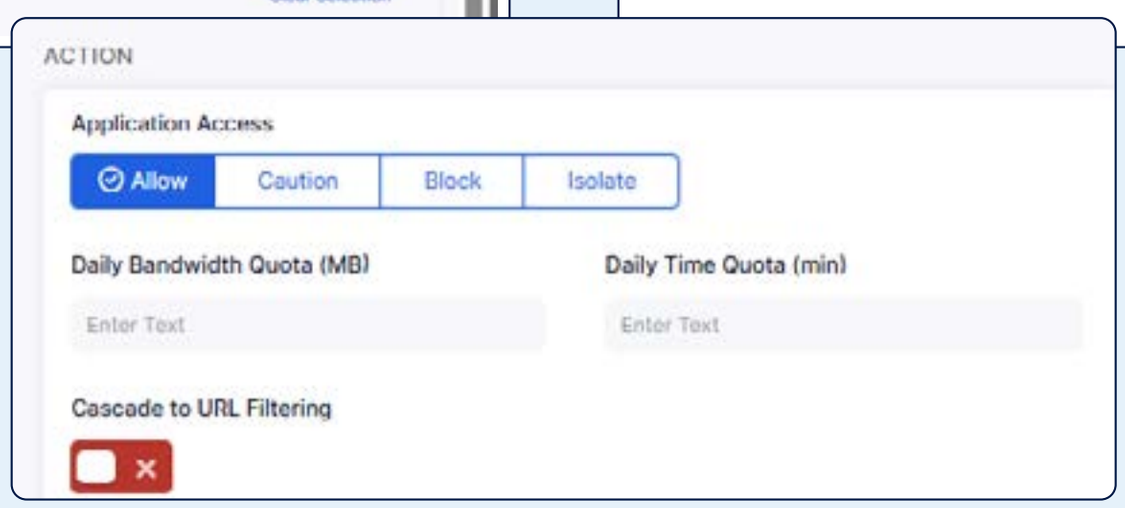
Umfassende und spezifische Kategorien zur Erfassung von KI-Anwendungen

URL-Kategorien für Wide Net



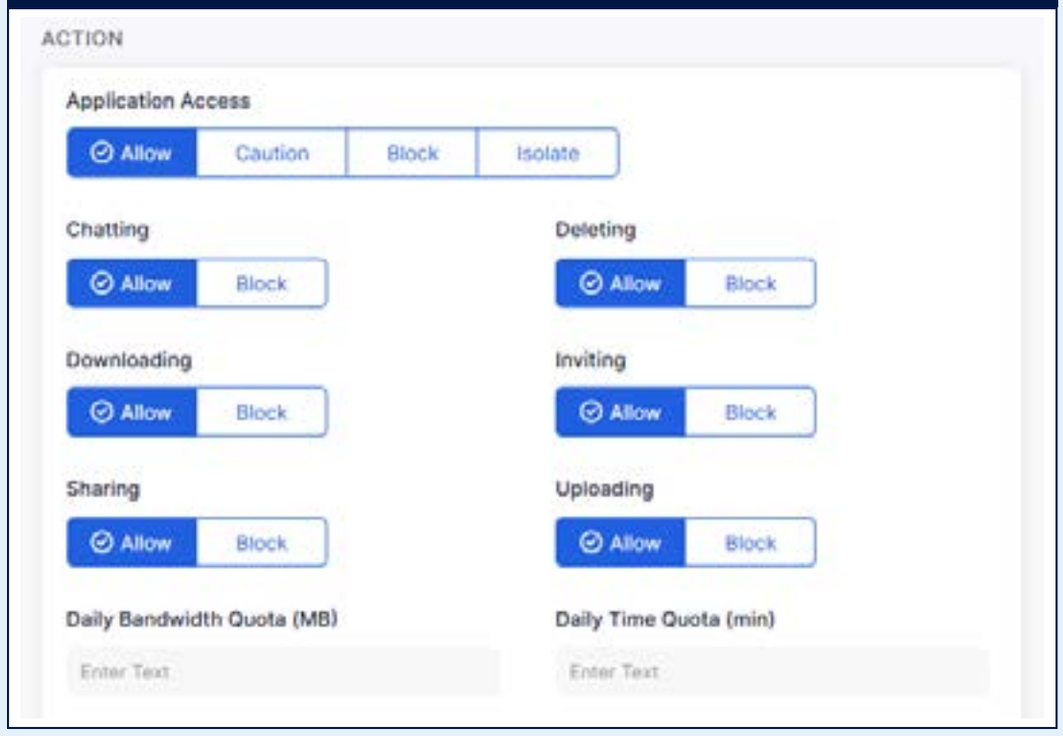
GenAI-Anwendung für granulare Steuerung



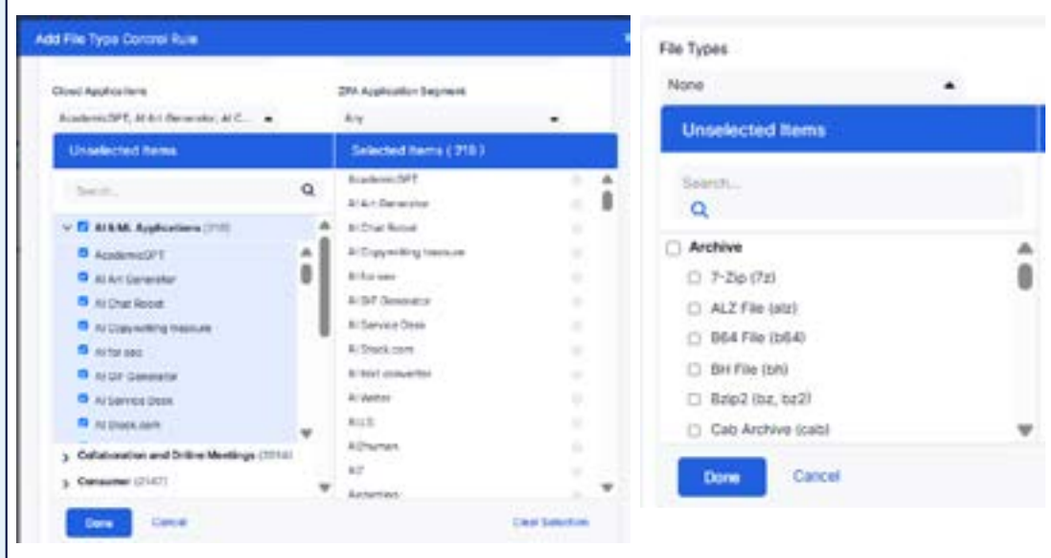


Granulare Kontrollen für SaaS-, Web- und KI-Anwendungen

GenAI-Anwendung Granulare Kontrollen



GenAI-Anwendung Dateiupload-Kontrollen



Genehmigte Apps über die SaaS-Anwendungssicherheitskontrolle zulassen

Zscaler verwaltet nicht nur eine umfassende Liste von KI-Anwendungen, sondern stellt auch granulare Kontrollen für die Interaktionen der User mit GenAI-Anwendungen bereit. Diese Kontrollen sind sehr benutzerfreundlich, leistungsstark und werden über eine einzige Plattform bereitgestellt. Die linke Seite des Bildes zeigt einige Beispiele für granulare Kontrollen, die ggf. im Rahmen einer ChatGPT-Sicherheitsrichtlinie angewendet werden können, wie etwa das Zulassen von Chats, aber das Blockieren von Datei-Uploads oder das Einschränken der Chat-Freigabe. Behörden können diese abteilungsweit oder sogar auf der Ebene einzelner User durchsetzen. Diese granularen Kontrollen können noch weiter präzisiert werden, indem die Dateitypen eingeschränkt werden, die User in GenAI-Anwendungen hochladen dürfen, wie rechts gezeigt. Diese Dateikontrolle kann auch die Einschränkung des Uploads verschlüsselter Dokumente umfassen.

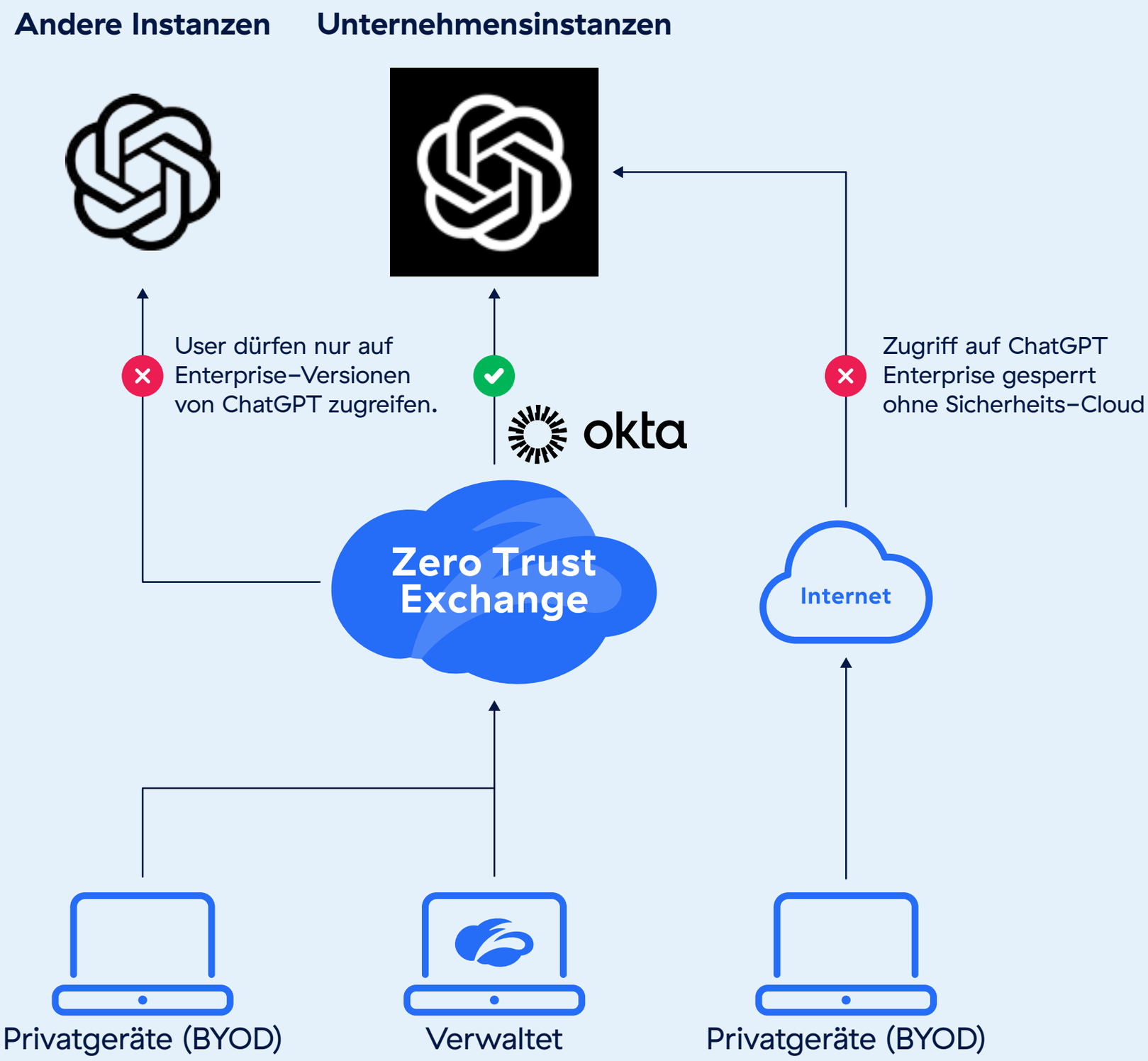
Zugriff auf Unternehmensinstanzen von GenAI-Anwendungen beschränken

Um eine bessere Sicherheit und Kontrolle zu gewährleisten, sollten Behörden unbedingt die Verwendung von Enterprise-Versionen der GenAI-Anwendungen in Erwägung ziehen. Enterprise-Versionen wie ChatGPT Enterprise geben Behörden die volle Kontrolle über ihre Geschäftsdaten und Konversationen, ohne dass die Unternehmensdaten zum Modelltraining beitragen. Diese Lösungen sind SOC2-konform und gewährleisten Verschlüsselung sowohl während der Übertragung als auch im Ruhezustand. Darüber hinaus vereinfachen sie die Userverwaltung mit Funktionen wie teambasiertem Zugriff, Domänenüberprüfung, Single Sign-On (SSO) und Nutzungseinblicken und ermöglichen so eine sichere Bereitstellung im großen Maßstab.

Enterprise-Instanzen von GenAI-Anwendungen sollten mit SSO gekoppelt werden, um die Sicherheit zu maximieren und Behörden mehr Transparenz und Kontrolle über die Anwendungsnutzung zu bieten. Mit SSO können Behörden Richtlinien durchsetzen, die den Zugriff auf andere Versionen von GenAI-Anwendungen blockieren. Beispielsweise stellt die Mandantenkontrolle von Zscaler für ChatGPT sicher, dass nur auf genehmigte Mandanten zugegriffen werden kann, während andere automatisch eingeschränkt werden. Darüber hinaus können Behörden mithilfe von Whitelists Kontrollen auf der Ebene des Identity and Access Management (IAM) einrichten, um sicherzustellen, dass GenAI ausschließlich in Enterprise-Versionen verwendet wird. Zusätzlich lässt sich dadurch gewährleisten, dass der Zugriff über sichere Umgebungen wie die Cloud-Plattform von Zscaler erfolgt. Um den sicheren Zugriff noch weiter zu erweitern, können Enterprise-GenAI-Instanzen mithilfe des BYOD-Zugriffs ohne Agents von Zscaler auch auf nicht verwalteten oder BYOD-Geräten zur Verfügung gestellt werden.

Ein einfacher „Alles zulassen oder alles blockieren"-Ansatz ist in der heutigen GenAI-Landschaft nicht ausreichend. Behörden müssen eine mehrschichtige Sicherheitsstrategie mit granularen Kontrollen einführen, die auf verschiedene Anwendungsinteraktionen zugeschnitten sind. Die Konsolidierung dieser Funktionen in einer einheitlichen Plattform optimiert nicht nur die Bereitstellung, sondern vereinfacht auch die Einhaltung der Kernprinzipien von Zero Trust und gewährleistet den Zugriff nach dem Prinzip der minimalen Rechtevergabe, kontinuierliche Transparenz und umfassenden Schutz für sämtliche GenAI-Interaktionen.

Zugriffskontrolle für genehmigte Instanzen von KI-Anwendungen



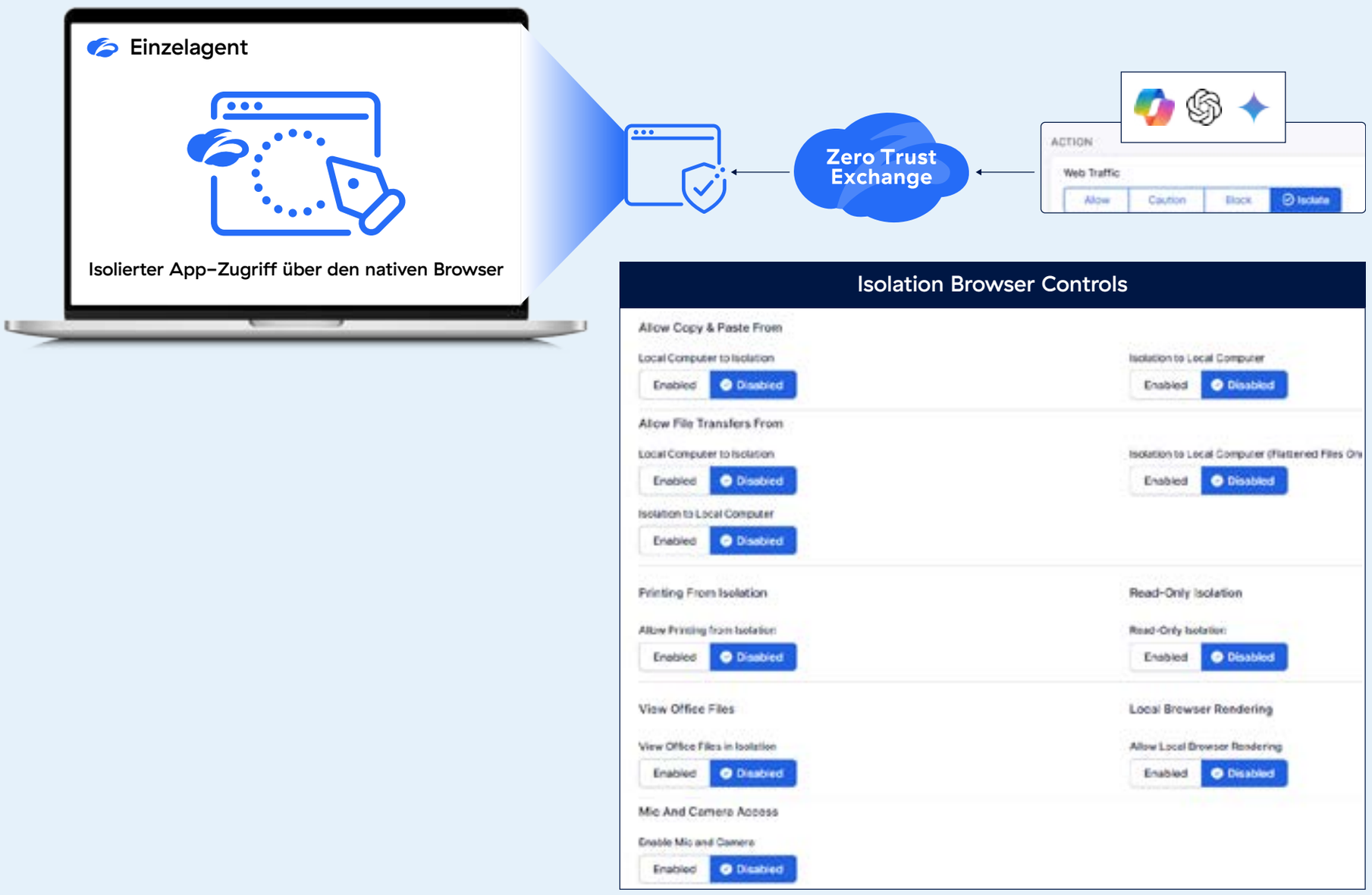
Risiko durch nicht genehmigte GenAI-Anwendungen reduzieren

Wenn Zugriff auf nicht genehmigte GenAI-Anwendungen erforderlich ist (Anwendungen ohne Unternehmenslizenzen und Single Sign-On (SSO)), sollten diese GenAI-Anwendungen als Hochrisiko-Anwendungen behandelt werden. In solche Anwendungen hochgeladene Daten können zum Trainieren der GenAI-Modelle verwendet werden, wodurch möglicherweise vertrauliche Informationen preisgegeben werden. Um diesem erhöhten Risiko zu begegnen, müssen die Behörden zusätzliche Sicherheitskontrollebenen implementieren, um eine strengere Überwachung der Dateninteraktionen zu gewährleisten.

Zscaler bietet mit dem Zero Trust Browser eine effektive Lösung zur Bewältigung dieses Risikos. Mit diesem Tool können Behörden sicheren Zugriff auf nicht genehmigte GenAI-Anwendungen mit erweiterten Kontrollmechanismen bereitstellen, beispielsweise durch die Einschränkung von Aktionen wie Dateiübertragungen, Drucken und Verwendung der Zwischenablage. Darüber hinaus verhindert der Zero Trust Browser, dass GenAI-Anwendungen Code direkt im Browser des Users ausführen. Stattdessen werden Interaktionen auf isolierten Seiten gerendert. Dies trägt zum Schutz vor Fingerprinting, Cookie-Tracking durch Drittanbieter und anderen Sicherheitslücken bei. Gleichzeitig wird Usern ermöglicht, weiterhin den gewohnten von der Behörde bereitgestellten Browser zu verwenden.

Dieser Ansatz kann auf zwei Arten implementiert werden: mit dem Zscaler Unified Agent oder mithilfe eines Modells ohne Agents. Für behördeneigene Geräte wird eine agentbasierte Bereitstellung empfohlen, um sicherzustellen, dass der gesamte Traffic über die Durchsetzungsplattform von Zscaler geleitet wird. In Situationen, in denen kein Agent installiert werden kann, bietet die Option ohne Agents von Zscaler eine sichere Alternative, die einen kontrollierten Zugriff auf GenAI-Anwendungen gewährleistet, ohne die Sicherheit zu beeinträchtigen.

Granulare Kontrollen zur Sicherung isolierter KI-Anwendungen bei gleichzeitiger Berücksichtigung der User Experience



4. Implementierung von Datenschutzstrategien bereits in der Anfangsphase

Wird bei der Einführung von GenAI nicht von Beginn an ein starker Datenschutz implementiert, kann dies zu Datenverlusten, Verstößen gegen Datenschutzbestimmungen und einem Vertrauensverlust der Öffentlichkeit führen. Letztlich wird dadurch der erfolgreiche Einsatz dieser Tools untergraben. Der dialogorientierte und benutzerfreundliche Charakter öffentlicher GenAI-Anwendungen erhöht das Risiko, dass User versehentlich vertrauliche Behördendaten preisgeben. Einfache Aktionen wie das Kopieren und Einfügen von Informationen oder das Hochladen von Dateien können ohne sorgfältige Überwachung zur Offenlegung vertraulicher Daten führen. Dies unterstreicht, warum die Einbindung robuster Datenschutzmaßnahmen ein zentraler Bestandteil jeder öffentlichen GenAI-Einführungsstrategie für staatliche und lokale Behörden sein sollte.

Mit den erweiterten DLP-Funktionen (Data Loss Prevention) von Zscaler können Behörden diese Risiken direkt angehen. Die DLP-Lösung von Zscaler für GenAI wurde entwickelt, um vertrauliche Informationen von Anfang an zu schützen. Sie erkennt und blockiert die Weitergabe vertraulicher Daten — sei es durch einen Prompt, einen Datei-Upload oder Missbrauch —, bevor diese öffentliche GenAI-Modelle erreichen können. Dieser proaktive Ansatz stellt sicher, dass Behörden bei der GenAI-Nutzung vertrauliche Informationen schützen und die Einhaltung von Vorschriften gewährleisten können.

Einführung von DLP beschleunigen

Der Einstieg in den Datenschutz kann für viele Unternehmen eine Herausforderung darstellen. Das gilt erst recht, wenn es darum geht, einerseits den Zugriff auf GenAI-Tools zu gewähren und andererseits starke Schutzmaßnahmen zu implementieren. Zscaler begegnet dieser Herausforderung, indem wir eine optimierte Plattform zur Unterstützung schlanker Teams bereitstellen und eine schnelle Einführung von GenAI mit effektiven Datenschutzkontrollen ermöglichen. Dieser Ansatz stellt sicher, dass Behörden ihr Sicherheitsframework effizient für verschiedene Abteilungen und Benutzergruppen skalieren können.

Für Behörden, die bereits Inline-Regeln für andere Internetziele anwenden, ist die Ausweitung dieser Richtlinien auf GenAI-Anwendungen unkompliziert. Zscaler integriert außerdem vorhandene DLP-Engines und Wörterbücher, die für andere Kanäle verwendet werden, direkt in die KI/ML-Anwendungen, wodurch Redundanzen reduziert und die Bereitstellung beschleunigt wird. Wenn eine Behörde bei Null anfängt, bietet Zscaler vordefinierte Wörterbücher, die mit nur wenigen Klicks auf GenAI-Anwendungen angewendet werden können, um den Verlust vertraulicher Daten zu verhindern. Zusätzlich können bekannte Dokumente oder Datensätze geschützt werden durch EDM/IDM-Funktionen. Durch Tagging von Microsoft Information Protection (MIP) können verschlüsselte oder klassifizierte Daten zusätzlich vor Offenlegung geschützt werden.

Um die Richtlinien weiter zu präzisieren, identifizieren die Machine-Learning-Erkennungsfunktionen von Zscaler bisher unbekannte vertrauliche Informationen und Datenübertragungen in GenAI-Anwendungen. Dadurch können Behörden ihre Schutzstrategie kontinuierlich weiterentwickeln. Durch Feinabstimmung vorhandener Wörterbücher oder die Erstellung benutzerdefinierter Erkennungsregeln mithilfe von regulären Ausdrücken oder Schlüsselwörtern können Behörden die bereitgestellten Ressourcen an ihre jeweiligen Anforderungen anpassen. Zscaler lässt sich auch in Datensicherungslösungen wie Rubrik integrieren und vereinfacht so die Datenidentifizierung und den Datenschutz.

Beschleunigte DLP-Implementierung mit Zscaler

Implementierungstag 0

Behördenspezifische Daten mit EDM und IDM

Vorgefertigte Wörterbücher, die von Behörden verwendet werden sollten

- ABA-Bankleitzahlen,
- Unternehmensfinanzierungsdokument,
- Unternehmensrechtsdokument,
- Gerichtsdokument,
- Zugangsdaten und Geschäftsgeheimnisse,
- Kreditkarten,
- Krankheitsinformationen,
- Führerschein (USA),
- Informationen zu Medikamenten,
- Finanzberichte,
- Einwanderungsdokument,
- Versicherungsdokument,
- Rechnungsdokument,
- Rechtsdokument,
- medizinisches Dokument,
- medizinische Informationen,
- Immobiliendokument,
- Sozialversicherungsnummern (USA),
- Steuerdokument,
- Steueridentifikationsnummer (USA),
- Dokument der Verkehrsbehörde,
- Informationen zu Behandlungen

MIP / AP-Etiketten

Kontinuierliche Überwachung und Transparenz

Unbekannte Datenübertragungen und Apps identifizieren

Daten, die bei Vorfällen erfasst wurden

User-Eingaben und Feedback

Präzisieren und Optimieren | Nach Bedarf

Benutzerdefinierten Wörterbuch-Regex erstellen / Stichwort

Schlüsselwörter (ein oder mehrere Wörter) und Nähe

EDM + IDM auf Datensicherungslösungen erweitern

Durch die Durchsetzung von Richtlinien in Echtzeit und detaillierte Transparenz können IT-Verantwortliche vertrauliche Daten ohne zusätzliche Komplexität oder manuelle Überwachung sichern. Dieser optimierte Ansatz erleichtert die sichere und schnelle Einführung von GenAI-Tools und nutzt deren Produktivitätsvorteile. Zugleich wird die Einhaltung von Vorschriften und das Vertrauen der Öffentlichkeit im Einklang mit dem Zero-Trust-Prinzip „Niemals vertrauen, immer überprüfen“ gewährleistet.

DLP-Governance vereinfachen

Eine häufige Herausforderung bei der Implementierung von Data Loss Prevention (DLP), insbesondere in großen Behörden oder Shared-Services-Organisationen, ist die Menge an Vorfällen, die SOC-Verantwortliche und Dateneigentümer bewältigen müssen. Dazu gehört etwa die Kommunikation mit Mitarbeitern, die einen Vorfall ausgelöst haben, die Intensivierung von Benutzerschulungen, die Bearbeitung von Ausnahmen oder auch die Pflege von Prüfpfaden. Ohne ein effizientes System kann dies schnell zu Überlastung führen.

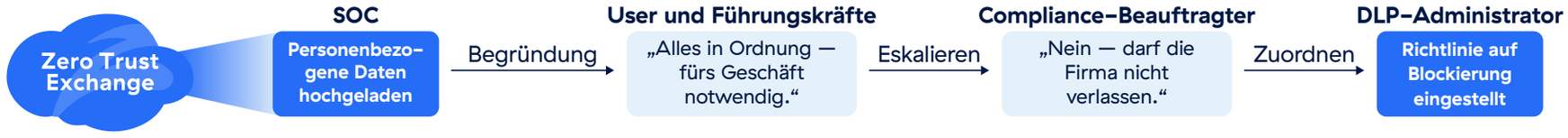
Die Workflow-Automatisierung vereinfacht diesen Prozess, indem sie eine zentrale Lösung für die Verwaltung von GenAI-bezogenen Datenschutzvorfällen bereitstellt. Sie stellt eine vollständige Ansicht aller Vorfälle an einem Ort bereit, einschließlich der Metadaten und Details der spezifischen Aktionen oder Daten, die den Verstoß ausgelöst haben. Diese Zentralisierung ermöglicht es Administratoren, Vorfälle schnell zu überprüfen, zu priorisieren und ggf. zu beheben.

Ein Hauptmerkmal der Workflow-Automatisierung ist die Möglichkeit, Vorfälle anhand gemeinsamer Merkmale zu gruppieren und Prioritäten zuzuweisen. Diese Gruppen können dann bestimmten Administratoren zur gezielten Behebung zugewiesen werden. Automatisierung spielt hier eine wichtige Rolle, indem sie Workflows ermöglicht, die die betroffenen Endbenutzer benachrichtigen oder schulen, Begründungen anfordern oder Probleme zur Genehmigung an Abteilungsleiter oder Dateneigentümer weiterleiten. Automatisierte Workflows können außerdem Maßnahmen zur Behebung von Vorfällen ohne manuelles Eingreifen auslösen.

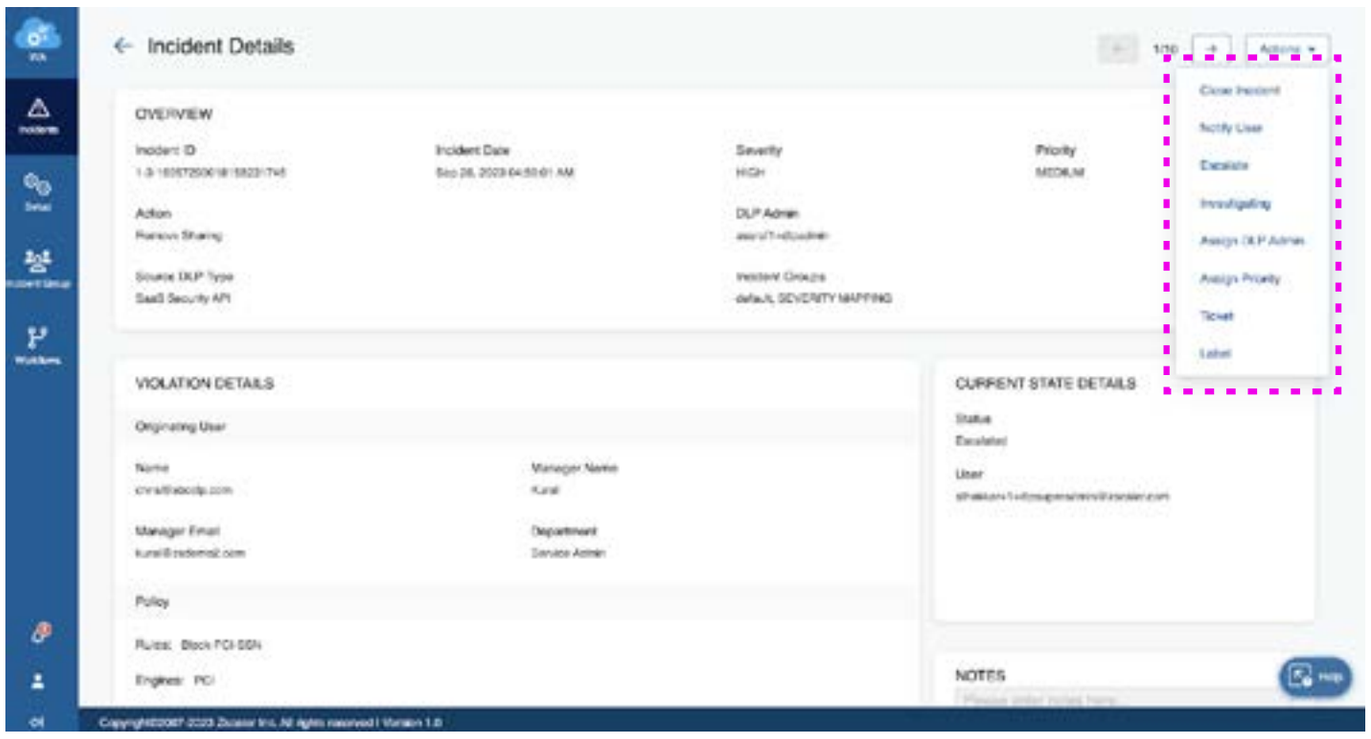
Durch die Nutzung der Workflow-Automatisierung in DLP können Behörden die Lösungszeiten erheblich verkürzen, die Betriebsbelastung des SOC verringern und umsetzbare Erkenntnisse zu Risikobereichen gewinnen. Diese Erkenntnisse können wiederum dazu beitragen, Richtlinien weiter zu präzisieren oder Schulungsprogramme zu verbessern. So wird sichergestellt, dass die User besser für einen sicheren Betrieb gerüstet sind, und zugleich die Wahrscheinlichkeit künftiger Vorfälle verringert.

Vorfallmanagement: Fallmanagement und User-Coaching optimieren

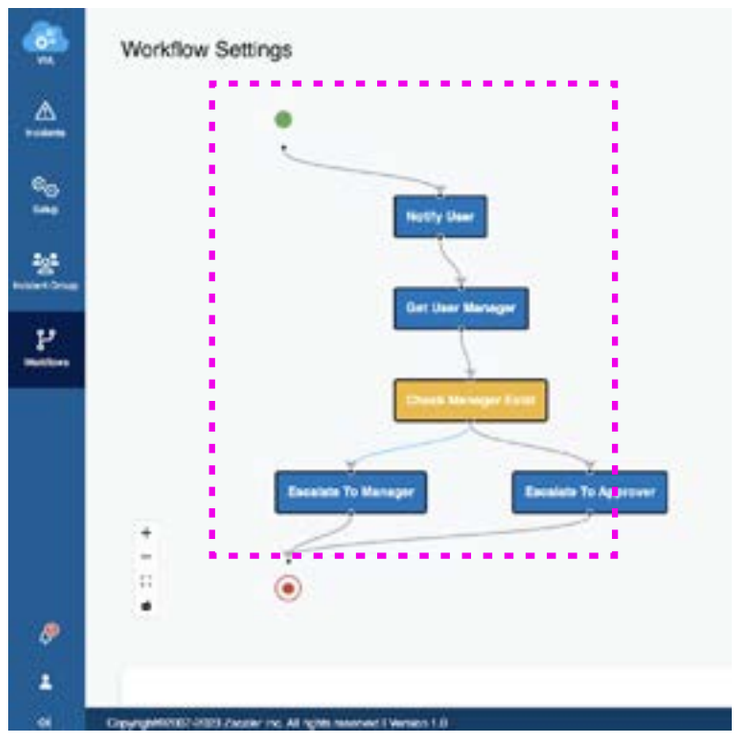
Workflow-Automatisierung
Analyse von Vorfällen, Unterstützung von User-Coaching



Einfache Verwaltung, Zuweisung und Eskalation von Vorfällen



Routinen für Arbeitsabläufe definieren



5. Ganzheitlicher mehrschichtiger Ansatz

Behörden auf staatlicher und kommunaler Ebene können mit generativer KI (GenAI) Effizienzgewinne erschließen und ihr Serviceangebot verbessern. Dabei ist jedoch eine sichere Vorgehensweise unerlässlich. Angesichts der Tausenden verfügbaren GenAI-Tools und der damit verbundenen Risiken wie Datenverluste und unbefugte Nutzung benötigen Behörden eine klare Strategie, die der Sicherheit Priorität einräumt, Zero-Trust-Prinzipien integriert und dennoch Produktivität ermöglicht. Ein mehrschichtiger Ansatz vereinfacht diesen Prozess, indem Anwendungen nach Risiko gruppiert, maßgeschneiderte Sicherheitskontrollen angewendet und das Vorfallmanagement automatisiert werden, um den Druck auf die IT-Teams zu verringern. Diese Strategie hilft Behörden dabei, vertrauliche Daten zu schützen, Abläufe zu optimieren und Usern die sichere Nutzung von GenAI-Anwendungen zu ermöglichen.

Mehrschichtige Kontrollen implementieren

In diesem Abschnitt untersuchen wir, wie Behörden die verschiedenen Elemente einer sicheren GenAI-Einführung mithilfe eines mehrschichtigen Ansatzes zusammenführen können.
Da es bereits Tausende von GenAI-Tools gibt und jede Woche neue hinzukommen, kann die Verwaltung von Richtlinien und Vorfällen ohne eine gut durchdachte Strategie schnell zur Überforderung werden.

Ein mehrschichtiger Ansatz vereinfacht diesen Prozess, indem er den Zugriff organisiert und Datenkontrollen implementiert, die dem jeweiligen Risikoniveau entsprechen. Diese Methode verringert nicht nur den Arbeitsaufwand für Sicherheitsadministratoren, sondern minimiert auch das Risiko von Datenverlusten erheblich und reduziert die Anzahl der Vorfälle, mit denen sich IT- und Sicherheitsverantwortliche befassen müssen. Durch diesen strukturierten Ansatz können Behörden die Leistungsfähigkeit von GenAI sicher und effektiv nutzen und gleichzeitig ihre Betriebseffizienz aufrechterhalten.

Wie bereits erwähnt, bieten Tools wie Shadow IT App Discovery, GenAI Discovery Reports und GenAI Prompt Visibility wertvolle Einblicke. Diese unterstützen die Weiterentwicklung von KI-Richtlinien und die Anpassung von Sicherheitskontrollen an veränderte Anforderungen. Diese Erkenntnisse bilden die Grundlage für einen praktischen, mehrschichtigen Ansatz zur Verwaltung von GenAI-Anwendungen.

Zur Umsetzung dieses Ansatzes empfiehlt es sich, GenAI-Anwendungen in drei Kategorien einzuteilen: Hochrisiko, Mittelrisiko und Niedrigrisiko. Anwendungen mit hohem Risiko sollten vollständig blockiert werden, um eine unnötige Gefährdung durch Sicherheitslücken zu vermeiden. Auf Anwendungen mit mittlerem Risiko kann mit erhöhten Sicherheitskontrollen zugegriffen werden, beispielsweise durch Browserisolierung und strengere Datenschutzmaßnahmen. Für Anwendungen mit geringem Risiko kann der native Zugriff gestattet werden, allerdings mit Einschränkungen bezüglich der spezifischen Inhalte oder Aktionen, die User ausführen können.

Mehrschichtiger Ansatz zur Sicherung von KI-Anwendungen

Diese Struktur unterstützt die Umsetzung eines Zero-Trust-Ansatzes für GenAI bei Behörden. Bei diesem Modell werden unbekannte, neu veröffentlichte oder nicht genehmigte Anwendungen standardmäßig blockiert. Weniger riskante Anwendungen werden durch zusätzliche Sicherheitsebenen isoliert, während User beim Zugriff auf vollständig genehmigte Anwendungen von einer nahtlosen User Experience mit maßgeschneiderten Sicherheitsvorkehrungen profitieren. Um die Implementierung und Verwaltung zu vereinfachen, können Behörden Tools wie benutzerdefinierte Anwendungsbezeichnungen und Risikoprofile verwenden. Diese ermöglichen es Sicherheitsverantwortlichen, voreingestellte Richtlinien zu definieren, die basierend auf dem ihnen zugewiesenen Risiko automatisch auf Anwendungen angewendet werden. Durch die Kennzeichnung einer Anwendung werden die entsprechenden Richtlinien durchgesetzt, wodurch der Verwaltungsaufwand minimiert und gleichzeitig eine robuste Kontrolle aufrechterhalten wird.

Workflows zur Vorfallsreaktion automatisieren

Eine weitere wichtige Ebene, die berücksichtigt werden muss, ist das Vorfallmanagement. Für Behörden ist es von entscheidender Bedeutung, die Anzahl der Vorfälle zu reduzieren, die das Security Operations Center (SOC) oder Datenadministratoren manuell bearbeiten müssen. Verstöße mittlerer und geringer Schwere sollten beispielsweise zu Prüfzwecken protokolliert und automatisch geschlossen werden, ohne dass ein nennenswerter manueller Eingriff erforderlich ist. Da es sich dabei jedoch immer noch um Verstöße gegen die Richtlinien handelt, sollten die Benutzer benachrichtigt und aufgefordert werden, ihr Verhalten zu begründen. Dieser Schritt ist für die Intensivierung der Benutzerschulung und die Förderung der Verantwortlichkeit von unschätzbarem Wert.

Mit Zscaler können Behörden mithilfe von Inhaltsüberprüfungsrichtlinien für GenAI den Schweregrad von Verstößen definieren, die dann an Tools zur Workflow-Automatisierung weitergeleitet werden. Mit dieser Funktion können Administratoren Workflows entwerfen, die auf den Schweregrad des jeweiligen Vorfalls zugeschnitten sind. Attribute wie Schweregrad und weitere Merkmale können verwendet werden, um Vorfälle in Gruppen zu kategorisieren, und diese Gruppen können an automatisierte Arbeitsabläufe gebunden werden. Dieser Ansatz vereinfacht die Bearbeitung von Vorfällen und stellt sicher, dass Verstöße angemessen behandelt werden. Gleichzeitig wird die Belastung der SOC-Verantwortlichen erheblich verringert.

Schlussgedanken

Behörden müssen bei der Nutzung generativer KI-Anwendungen (GenAI) eine Vorreiterrolle einnehmen, um Abläufe zu transformieren, Mitarbeitern mehr Handlungsfreiheit zu geben und ihr Serviceangebot für die Bürger zu verbessern. Die Einführung muss jedoch durch eine Zero-Trust-Architektur untermauert werden. Indem sie sicherstellen, dass jeder User, jedes Gerät und jede Interaktion überprüft, überwacht und kontrolliert wird — unabhängig von Standort und Anwendung —, können Behörden GenAI-Initiativen mit starkem Datenschutz, klarer Governance und optimierten Anwendererfahrungen im Mittelpunkt ihrer Strategie sicher absichern.

Zscaler ermöglicht Behörden, die Produktivitätsvorteile von GenAI mit einem sicheren, mehrschichtigen Ansatz zu nutzen, der die Governance vereinfacht, die Bereitstellung opzimiert und robuste Sicherheit in jede Interaktion einbettet. Durch die Einrichtung von KI-Governance-Frameworks, die Automatisierung der Erkennung und Verwaltung von GenAI-Anwendungen, die Kontrolle der Nutzung von GenAI-Anwendungsinstanzen und die Implementierung erweiterter DLP-Funktionen können Behörden Risiken drastisch reduzieren und ihre Einführungsstrategien mit minimaler Belastung der IT- und Sicherheitsteams skalieren.

Da sich die GenAI-Landschaft ständig weiterentwickelt, wird empfohlen, bei der Einführung einen strategischen, schrittweisen Ansatz zu verfolgen. Beginnen Sie mit der Sicherung des Zugriffs auf öffentliche GenAI-Anwendungen. Erschließen Sie auf sichere Weise eine höhere Produktivität mit Agentic AI (zukünftiges Dokument). Abschließend werden wir untersuchen, wie die GenAI-Funktionen sicher auf bürgerorientierte Leistungen ausgeweitet werden können, um sicherzustellen, dass die Systeme bei jedem Schritt sicher bleiben. Mit Zscaler können Behörden diese Phasen sicher umsetzen, Innovationen beschleunigen und gleichzeitig die höchsten Standards für Datensicherheit und Compliance einhalten.

Bitte wenden Sie sich an Ihren zuständigen Ansprechpartner oder kontaktieren Sie uns, um einen Workshop zu planen.

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

zscaler™

Zero Trust Everywhere