

# Sicherheit in einer KI-geprägten Zukunft: Zero Trust für Finanzdienstleister

Ein strategischer Ansatz zur Cybersicherheit im Zeitalter der KI

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Lösungsprofil

## Kurzübersicht: Orientierung in unsicheren Zeiten

In einer KI-geprägten Zukunft müssen Finanzdienstleister komplexe Herausforderungen voller verborgener Bedrohungen und Unwägbarkeiten meistern, bei denen jede Interaktion ein Risiko darstellen kann. So wie man in einer gefährlichen und unvorhersehbaren Umgebung äußerste Vorsicht walten lässt, müssen Finanzdienstleiser auch bei der KI-Sicherheit mit größter Wachsamkeit vorgehen. Diese Kurzübersicht skizziert die Maßnahmen, die Finanzdienstleistungsunternehmen ergreifen können, um sich in dieser von KI geprägten Landschaft zu schützen.

Es wird besprochen, wie KI die Bedrohungslandschaft verändert und neue Risiken wie KI-gestützten Betrug und automatisierte Cyberangriffe mit sich bringt. Darüber hinaus werden zentrale Trends und Prognosen aufgezeigt, sodass Organisationen die Folgen von KI antizipieren und strategisch darauf reagieren können.

In diesem risikoreichen Umfeld, in dem man weder internen noch externen Entitäten blind vertrauen kann, ist Zero Trust die beste Verteidigung. In dieser Kurzübersicht erfahren Finanzdienstleistungsunternehmen, wie sie ihre Zero-Trust-Strategie aufbauen und konkrete Maßnahmen für eine sichere und resiliente KI-Zukunft ergreifen können.

## KI und die sich ständig weiterentwickelnde Bedrohungslandschaft

KI verändert die Bedrohungslandschaft rasant und bringt komplexe Risiken mit sich, die herkömmliche Sicherheitsmodelle vor große Herausforderungen stellen. Angriffe haben sich weiterentwickelt und sind in großem Maßstab effektiver geworden, sodass Opfer ihren Betrieb fortsetzen können, während Angreifer mit der Veröffentlichung ihrer Daten drohen. Zwar existieren zahlreiche Megatrends und Vorhersagen rund um KI, doch konzentrieren wir uns auf drei Trends für 2024—2025, die sich besonders rasant weiterentwickeln.

## Drei Trends für 2024—2025, die Sie nicht verpassen dürfen

### Grundlegende KI-Entwicklung

Large Language Models (LLMs) haben die generative KI revolutioniert: Mittlerweile ist diese nicht mehr rein aufgabenorientiert, sondern liefert dynamische, kontextbezogene Lösungen. Aber wie alles in der realen Welt wird sich auch KI kontinuierlich weiterentwickeln. Diese LLMs haben uns in ihren Bann gezogen, sobald sie die kritische „Uncanny Valley"-Schwelle überwunden hatten.

„Uncanny Valley" bezeichnet in diesem Fall das Unbehagen, das Menschen verspüren, wenn KI menschliches Verhalten fast perfekt imitiert, dabei aber noch erkennbar künstlich bleibt.

Generative KI und insbesondere ChatGPT haben die ‚Uncanny Valley'-Schwelle überschritten, als das Tool innerhalb von zwei Monaten 100 Millionen Nutzer erreichte — ein außergewöhnlicher Erfolg. Nun, da diese Schwelle überschritten ist, steht noch mehr bevor, das aus neurologischer Sicht und im Hinblick auf die kognitive Entwicklung potenziell weitreichendere Auswirkungen haben könnte als generative KI allein.

### Ransomware-Angriffe ohne Verschlüsselung

Früher nutzten Ransomware-Angreifer Verschlüsselung, um Daten zu stehlen und Unternehmen zu erpressen: Wer nicht zahlte, konnte seinen Betrieb nicht fortführen.

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Mit der Zeit wurde den Ransomware-Angreifern klar: Wer weniger fordert und den Betrieb der Opfer nicht komplett lahmlegt, erzielt oft höhere Einnahmen. Beispielsweise senken sie das Lösegeld von 10 auf 2 Millionen Dollar, und die Wahrscheinlichkeit, dass Unternehmen zahlen, steigt von 5 % auf 70—80 %. Auf diese Weise wird das Ransomware-Geschäft in großem Maßstab deutlich lukrativer. Hierbei spricht man von Ransomware ohne Verschlüsselung.

Bei Ransomware ohne Verschlüsselung stehlen die Angreifer die Daten, drohen Ihnen, aber in vielen Fällen dürfen Sie den Betrieb weiterführen, weil sie Ihr Geschäft nicht komplett lahmlegen wollen.

Indem der Geschäftsbetrieb nicht gestört wird, können Reputationsschäden geringer ausfallen. Angreifer versuchen manchmal auch, die Opfer davon zu überzeugen, den Vorgang nicht der US-Börsenaufsichtsbehörde (SEC) oder anderen Aufsichtsbehörden zu melden, da der Betrag so gering ist.

### KI-gestützte Ransomware-Angriffe

KI-gestützte Ransomware-Angriffe erhöhen die Erfolgsquote, erleichtern das Eindringen und ermöglichen eine stärkere Automatisierung. In diesem Fall nutzen Angreifer KI, um Cyberangriffe zu automatisieren und deren Komplexität zu erhöhen, wodurch sie schneller, gezielter und schwerer zu erkennen sind.

## Vier Strategien für Finanzdienstleister, um sich im sich wandelnden KI-Umfeld zurechtzufinden

Der Einsatz von KI in Unternehmen nimmt rasant zu, gleichzeitig steigen aber auch die Risiken. Vier strategische Handlungsebenen unterstützen Finanzdienstleister dabei, die Herausforderungen einer sich kontinuierlich entwickelnden KI-Welt zu bewältigen.

**Im Jahr 2024 stieg der Einsatz von KI-/ML-Tools um 594 %, während die Nutzung von ChatGPT um 634 %** zunahm (Zscaler ThreatLabz-Report 2024 zur KI-Sicherheit).

### Richtlinien und ethische Grundsätze

Finanzdienstleistungsunternehmen müssen umfassende Richtlinien entwickeln, die den ethischen Einsatz von KI regeln, die Einhaltung gesetzlicher Vorgaben sicherstellen und das Vertrauen der Kunden stärken. Dazu gehört der Aufbau eines Frameworks, der Datenschutz, Transparenz von Algorithmen und die Verringerung von KI-Bias berücksichtigt und verantwortungsbewusste KI-Praktiken in den Mittelpunkt stellt.

### Kerngeschäft

Welche Auswirkungen hat KI auf das Kerngeschäft? Laut einer Studie der Harvard Business Review zeigen Unternehmen derselben Branche, die KI nutzen, deutlich bessere Leistungen als diejenigen, die darauf verzichten — und der Abstand wächst weiterhin.

Wie also können Sie KI in Ihr Unternehmen integrieren? Werden Sie diese Maßnahmen gemeinsam mit einem Partner umsetzen, oder planen Sie, sie eigenständig durchzuführen? Beabsichtigen Sie, eigene KI-Modelle zu entwickeln und zu betreiben? Planen Sie, sich an der Nutzung größerer KI-Modelle zu beteiligen? Und um welchen konkreten Anwendungsfall handelt es sich?

Organisationen sollten prüfen, wie KI ihre Kernprozesse verbessern kann, etwa durch optimierten Kundenservice, effizientere Abläufe und datengestützte Entscheidungsfindung.

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

Organisationen sollten prüfen, wie KI ihre Kernprozesse verbessern kann, etwa durch optimierten Kundenservice, effizientere Abläufe und datengestützte Entscheidungsfindung. Indem sie die Bereiche identifizieren, in denen KI einen echten Mehrwert bietet, können Finanzdienstleistungsunternehmen Wettbewerbsvorteile schaffen und Innovationen vorantreiben, die mit den strategischen Zielen in Einklang stehen.

## Forschung, Entwicklung und Infrastruktur

Wenn KI-Tools in Unternehmen Einzug halten, stellt sich die Frage: Wie geht man damit um? Durch Investitionen in eine leistungsfähige Infrastruktur, die KI-Funktionen unterstützt — etwa Cloud-Computing, Big-Data-Analysen und Machine Learning — können Organisationen neue Technologien nutzen und Lösungen entwickeln, die den sich wandelnden Bedürfnissen der Kunden gerecht werden.

## Vorteile im Bereich Cybersicherheit

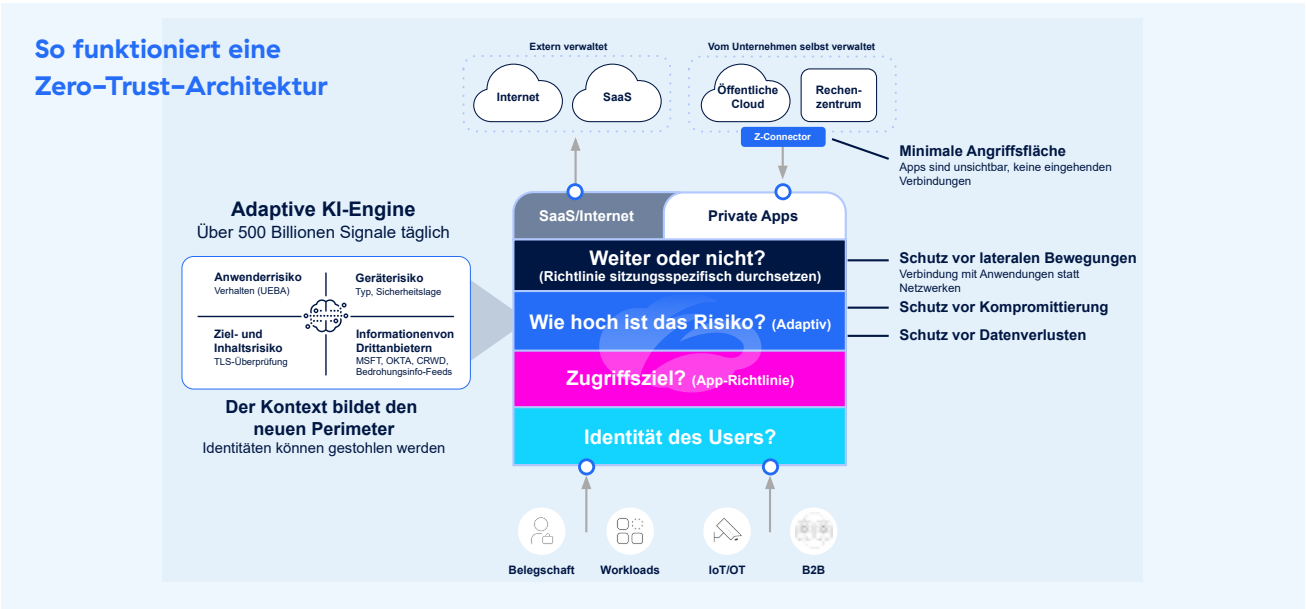
Durch den Einsatz von KI-gestützten Sicherheitslösungen können Finanzinstitute ihre Cybersicherheit verbessern und Bedrohungen in Echtzeit identifizieren und abwehren.

Sie sollten sich fragen: Welche Vorteile bietet KI für die Cybersicherheit? Und welche potenziellen Risiken bestehen? Wie könnte sie gegen Sie eingesetzt werden? Wie können Sie sich darauf vorbereiten? Durch den Einsatz KI-gestützter Sicherheitsmaßnahmen können Organisationen sensible Daten und Ressourcen besser schützen und Resilienz gegenüber komplexen Bedrohungen sicherstellen.

## Die Rolle von Zero Trust bei der Reduzierung von Cyberrisiken

Auch wenn der Einsatz von KI in Unternehmen rapide zunimmt, werden **18,5 %** aller KI-Transaktionen blockiert — ein Anstieg von **577 %**, der auf wachsende Sicherheitsbedenken hinweist (Zscaler ThreatLabz-Report 2024 zur KI-Sicherheit). In diesem riskanten Umfeld, in dem man weder internen noch externen Entitäten blind vertrauen kann, stellt Zero Trust die beste Verteidigung dar.

Zero Trust hilft dabei, sich in einem risikoreichen Umfeld zu orientieren, indem der Ansatz ausschließlich die Zugriffe zulässt, die wirklich erforderlich sind, und auch nur, wenn sie erforderlich sind. Mit einem Zero-Trust-Ansatz, bei dem niemandem automatisch vertraut wird, lässt sich das Cyberrisiko deutlich senken, egal, ob es sich um User, Workloads, Geräte oder Partnerunternehmen handelt:




© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

**1. Bestätigung der Identität: Halt! Um wen handelt es sich?**

a. Wer möchte eine Verbindung herstellen?
b. Welche Attribute liegen vor?
c. Wohin geht die Verbindung?

**2. Kontrolle der Anwendungsrichtlinien: Womit möchte der User eine Verbindung herstellen?**

a. Womit möchte der User eine Verbindung herstellen? In diesem Schritt bewertet Zero Trust Risiken anhand des Kontextes und verhindert so Kompromittierungen und Datenverluste.

**3. Adaptives Kontextrisiko: Worin besteht das Risiko?**

a. Worin besteht das Risiko? Verhindern Sie Kompromittierungen und Datenverluste, indem Sie das User-Risiko, das Geräterisiko, das Ziel, das Inhaltsrisiko und Informationen von Drittanbietern (Okta, CrowdStrike usw.) auswerten.

**4. Durchsetzen von Richtlinien**

a. Verhindern Sie laterale Bewegungen, sodass Verbindungen nur zu Anwendungen, nicht zum Netzwerk hergestellt werden. b. Setzen Sie Richtlinien für SaaS/Internetverbindungen pro Sitzung und pro User durch. c. Private Anwendungen: Minimieren Sie die Angriffsfläche, sodass Anwendungen unsichtbar sind und keine eingehenden Verbindungen hergestellt werden können.

## Der Weg zu Zero Trust

Um Ihr Unternehmen vor der zunehmenden Bedrohung durch KI-gestützte Cyberangriffe zu schützen, ist die Implementierung einer Zero-Trust-Strategie entscheidend. Die Umsetzung einer Zero-Trust-Strategie sollte schrittweise erfolgen, in handhabbare Etappen gegliedert sein und die geschäftlichen Prioritäten sowie Sicherheitsziele berücksichtigen — so lässt sich eine skalierbare und robuste Sicherheitsarchitektur aufbauen.

**1. Schützen Sie Ihre Belegschaft**

a. Phase 1A — keine Netzwerkänderungen
   i. Cyber- und Datenschutz, digitale Erfahrung und Quantifizierung von Risiken
b. Phase 1B — Vereinfachung des Netzwerks
   i. Zero-Trust-Zweigstellen/-Internetcafés, fortschrittliche Cyber- und Datenschutzstrategie und Gewinnung von Geschäftseinblicken

**2. Sichern Sie Workloads ab**

a. Cyber- und Datenschutz für Workloads
b. Zero-Trust-Workload-Networking und -Segmentierung

**3. Externer Zugriff**

a. Zero-Trust-Zugriff auf Drittanbieter-Apps
b. Zero-Trust-Verbindungen zu Websites von Drittanbietern

**4. Schützen Sie Geräte (IoT/OT)**

a. Cyber- und Datenschutz für IoT/OT
b. Zero-Trust-IoT-/OT-Konnektivität

© 2024 Zscaler, Inc. Alle Rechte vorbehalten.

## Fazit

In einem sich schnell wandelnden Umfeld, in dem niemand — weder innerhalb noch außerhalb des Unternehmens — automatisch als vertrauenswürdig erachtet werden kann, bietet Zero Trust den effektivsten Schutz. Da sich Technologie und KI weiterentwickeln und letztendlich gleichzeitig zum Einsatz kommen, stellt eine Zero-Trust-Strategie sicher, dass nur die richtigen User und Prozesse bei Bedarf auf die erforderlichen Ressourcen zugreifen können. So bleibt Ihr Unternehmen resilient und zukunftssicher.

Reduzieren Sie Ihr Cyberrisiko und starten Sie Ihren Weg zu Zero Trust. Mehr erfahren Sie unter zscaler.com/de.

## Über den Autor



Mit mehr als 30 Jahren Erfahrung als Unternehmer, IT-Sicherheitsexperte und Führungskraft bei Firmen wie RSA, Arbor Networks, CA, McAfee und Cybereason widmet sich Sam Curry der Stärkung der Cyberabwehr und der Verwirklichung von Sicherheit in einer vernetzten Welt. Derzeit ist Sam Curry Global VP und CISO bei Zscaler. Nebenbei ist er als Redner aktiv, moderiert den Podcast „On the Hook“, engagiert sich in verschiedenen Gremien und Publikationen und ist Mentor im Bereich IT-Sicherheit. Kontaktieren Sie den Autor auf LinkedIn.

zscaler™ | 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.com/de** oder folgen Sie uns auf Twitter unter **@zscaler**.

© 2024 Zscaler, Inc. Alle Rechte vorbehalten. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ und weitere unter **zscaler.com/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.

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