KI-Nutzung und -Risiken: Finanzdienstleistungsbranche weiterhin Spitzenreiter

AUF EINEN BLICK

Wichtigste Erkenntnisse aus dem ThreatLabz-Bericht zur KI-Sicherheit 2026

Künstliche Intelligenz ist keine neu aufkommende Technologie oder ein eigenständiges Werkzeugset mehr. Sondern sie hat sich als permanent verfügbare Infrastruktur etabliert, die Daten verarbeitet, Entscheidungsprozesse unterstützt und Abläufe beschleunigt. Im Jahr 2025 analysierte Zscaler ThreatLabz 989,3 Milliarden KI/ML-Transaktionen über die Zscaler Zero Trust Exchange™, um einen aussagekräftigen Einblick darüber zu gewinnen, wie Unternehmen KI in großem Umfang einsetzen und einschränken. Die Finanzdienstleistungsbranche ist zentral von diesem Wandel betroffen.

Zum zweiten Mal in Folge machte der Finanz- und Versicherungssektor mit 23,3 %den größten Anteil des weltweit in der Wirtschaft generierten KI-Traffics aus. Allein im Jahr 2025 waren es insgesamt 230 Milliarden Transaktionen. Dies positioniert Finanzinstitute als Spitzenreiter sowohl bei der KI-Nutzung als auch beim damit verbundenen KI-Risiko.

230 Milliarden Transaktionen: KI im operativen Maßstab

Im Finanz- und Versicherungswesen wurden fast 40 Milliarden mehr KI/ML-Transaktionen mehr generiert als in der zweitplatzierten Branche, was seine Position als aktivster Sektor für den Einsatz von KI in Unternehmen stärkt.

Ein Großteil dieser Aktivität geht auf weit verbreitete Produktivitätsanwendungen zurück. Die Analyse von ThreatLabz ergab, dass Grammarly, ChatGPT und Microsoft Copilot die am häufigsten verwendeten KI-Anwendungen in Finanzunternehmen sind. Ihre Verbreitung spiegelt wider, wie sich KI auf natürliche Weise in Umgebungen einfügt, in denen der Betrieb von großen Datenmengen und kontinuierlicher Analyse abhängt.

Aus diesem Grund hat sich KI bereits als Bestandteil zentraler Arbeitsabläufe im Finanzsektor etabliert.. Zu den typischen Anwendungsfällen gehören die Zusammenfassung von Forschungsergebnissen und Finanzanalysen, die Erstellung und Überprüfung von Compliance-Dokumentationen sowie die Betrugserkennung und die Untersuchung von Anomalien.

Mit der zunehmenden Verbreitung von KI in diesen Arbeitsabläufen, die Risiko, Compliance und operative Ergebnisse beeinflussen, entstehen auch neue Anforderungen an die Kontrolle.

39 % der blockierten Transaktionen im Finanz- und Versicherungswesen beobachtet

Auf Finanzen und Versicherungen entfiel ebenfalls der größte Anteil der blockierten KI/ML-Transaktionen in der Zscaler-Cloud. Insgesamt machte der Sektor 39,1 % aller blockierten KI/ML-Transaktionen aus. Daran zeigen sich die spezifischen Risiken:

- Vertraulichkeit der Finanzdaten von Kunden
- Aufsichtsrechtliche Verpflichtungen (SOX, GLBA, regionale Finanzvorschriften usw.)
- Insiderrisiko und potenzielle Datenexfiltrationen
- Inkonsistente Durchsetzung von DLP-Maßnahmen zur Verhinderung von Datenverlusten

Das Ausmaß der blockierten Aktivitäten und der damit verbundenen Risiken deutet auf einen Strukturwandel hin: Künstliche Intelligenz verändert bereits die Angriffsfläche im Finanzdienstleistungssektor.

Den KI-Risiken einen Schritt voraus

Jetzt herunterladen

KI ist mittlerweile Bestandteil der Angriffsfläche im Finanzwesen

Für Finanzinstitute ist KI nicht länger nur ein Randbereich der Kernsysteme; sie ist Bestandteil der Angriffsfläche und muss entsprechend geschützt werden.

- Immer mehr sektorspezifische Arbeitsabläufe beinhalten direkte Interaktionen mit KI-Anwendungen wie ChatGPT und Microsoft Copilot.
- Immer mehr Unternehmensanwendungen beinhalten oft „versteckte“ eingebettete KI- Funktionen, die mit Finanzdaten und internen Plattformen verbunden sind.
- Immer mehr Betriebsabläufe stützen sich auf KI-generierte Outputs, um Geschäfts- und Risikoentscheidungen zu unterstützen.

Diese zunehmende Verbreitung von KI erhöht das Potenzial für unbeabsichtigte Datenlecks durch KI-Prompts und Antworten, führt zu unkontrollierter oder nicht genehmigter KI-Nutzung und schafft neue Wege für KI-gestützte Bedrohungsakteure. Die Verteidigung der Angriffsfläche von KI erfordert einen neuen Sicherheitsansatz, der speziell für das KI-Zeitalter entwickelt wurde.

KI-Sicherheit als Imperativ für Finanzdienstleister

Die Finanzdienstleistungsbranche muss KI-Systeme, -Anwendungen und -Interaktionen mit der gleichen Sorgfalt schützen wie andere kritische Infrastrukturen, um vollständige Transparenz, konsequente Richtliniendurchsetzung und Echtzeitschutz zu gewährleisten. Die ganzheitliche Plattform von Zscaler für KI-Sicherheit unterstützt Finanzinstitute dabei, den gesamten KI-Lebenszyklus im Unternehmen abzusichern.

Entdecken Sie KI und Risiken: Identifizieren, dokumentieren und überwachen Sie Ihr gesamtes KI-Ökosystem — von Schatten-KI bis hin zu risikoreichen Anwendungen, Modellen und Pipelines.
Härten Sie KI-Systeme: Schützen Sie Modelle und reduzieren Sie das Risiko von Prompt Injection, Datenlecks und Missbrauch durch Laufzeitschutz und Sicherheitsvorkehrungen für kritische KI-Systeme.
Sichern Sie den Zugriff auf KI: Gewährleisten Sie die sichere, vorschriftskonforme und verantwortungsvolle Nutzung von KI-Anwendungen durch minimale Zugriffsberechtigungen und integrierte Datenschutzrichtlinien.
Vereinfachen Sie die KI-Governance: Erfüllen Sie Compliance- und Rechenschaftspflichten durch kontinuierliche Überwachung Ihrer KI-Implementierungen und -Nutzung.

Die Zscaler-Plattform kombiniert automatisiertes Red Teaming, dynamische Risikobewertung und fortschrittliche Schutzmechanismen, um Kontrollen kontinuierlich zu validieren, KI-bedingte Risiken zu minimieren und eine sichere, konforme KI-Einführung im Unternehmensmaßstab zu ermöglichen.

Im vollständigen Bericht erfahren Sie mehr über die Trends bei der Einführung von KI, KI-gestützte Bedrohungen und Sicherheitshinweise für Finanzinstitute.

Jetzt herunterladen

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**.

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

zscaler™

**Act Fast.
Stay Secure.**