Financial Services Remains the Most AI-Driven Sector

AT-A-GLANCE

Key Findings from ThreatLabz 2026 AI Security Report

Artificial intelligence is no longer emerging technology or a discrete toolset. It is always-on infrastructure, processing data, supporting decision-making, and accelerating operations. In 2025, Zscaler ThreatLabz analyzed 989.3 billion AI/ML transactions across the Zscaler Zero Trust Exchange™, providing a clear view into how organizations are using and restricting AI at scale. The financial services industry sits at the center of this shift.

For the second consecutive year, the Finance & Insurance industry accounted for the largest share of enterprise AI traffic, representing 23.3% of all AI/ML traffic globally, with 230 billion transactions in 2025 alone. This places financial institutions at the forefront of both AI adoption and AI risk exposure.

230 billion transactions: AI at operational scale

Finance & Insurance generated nearly 40 billion more AI/ML transactions than the next closest industry, reinforcing its position as the most active sector for enterprise AI usage.

Much of this activity comes from widely used productivity applications. ThreatLabz analysis identified Grammarly, ChatGPT, and Microsoft Copilot as the most-used AI applications across financial organizations. Their adoption reflects how AI fits naturally into environments where operations depend on large volumes of data and continuous analysis.

This is why AI has already become part of core financial workflows. Common use cases include summarizing research and financial analysis; drafting and reviewing compliance documentation; and fraud detection and anomaly investigation.

As AI expands across these workflows that influence risk, compliance, and operational outcomes, it also brings new requirements for control.

39% of blocked transactions tied to Finance & Insurance

Finance & Insurance also accounted for the largest share of blocked AI/ML transactions of any industry in the Zscaler cloud. In total, the sector comprised 39.1% of all blocked AI/ML activity, reminding us of what is at risk, including:

- Sensitivity of customer financial data
- Regulatory obligations (SOX, GLBA, regional financial regulations, etc.)
- Insider risk and potential data exfiltration
- Inconsistent or evolving data loss prevention (DLP) enforcement

The scale of blocked activity and associated risks point to a structural shift: AI is already reshaping the financial services attack surface.

AI is now part of the financial services attack surface

For financial institutions, AI is no longer adjacent to core systems; it is part of the attack surface and must be secured accordingly.

- More financial workflows involve direct interactions with AI applications such as ChatGPT and Microsoft Copilot
- More enterprise applications include often “hidden” embedded AI capabilities that connect to financial data and internal platforms
- More operational processes rely on AI-generated outputs to support business and risk decisions

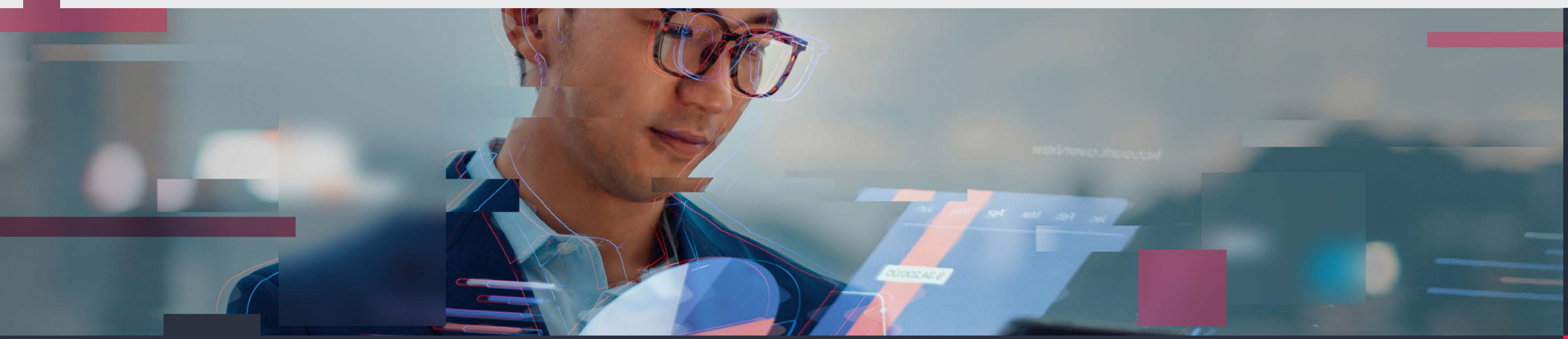
This expanding AI footprint increases the potential for unintentional data leakage through AI prompts and responses, introduces unmanaged or unsanctioned AI usage, and creates new pathways for AI-powered threat actors. Defending the AI attack surface requires a new approach to security built for the AI age.

The AI security imperative for financial services

The financial services industry must secure AI systems, applications, and interactions with the same rigor as other critical infrastructure, ensuring full visibility, consistent policy enforcement, and real-time protections. Zscaler’s unified platform for AI security helps financial institutions safeguard the entire enterprise AI lifecycle:

Discover AI and risk: Identify, map, and gain complete visibility into your entire AI ecosystem, from shadow AI to risky applications, models, and pipelines.
Harden AI systems: Protect models and reduce exposure to prompt injection, data leakage, and misuse by applying runtime protections and guardrails to critical AI systems.
Secure access to AI: Enforce the safe, compliant, and responsible use of AI applications with least-privileged access and inline data protection policies.
Simplify AI governance: Maintain compliance and accountability with continuous oversight across your AI deployments and usage.

Zscaler brings together automated red teaming, dynamic risk assessment, and advanced guardrails to continuously validate controls, minimize AI-driven risk, and enable secure, compliant AI adoption at enterprise scale.



Learn more about the AI adoption trends, AI-powered threats, and security guidance for financial institutions in the full report.

Download now

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world’s largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

**Act Fast.
Stay Secure.**