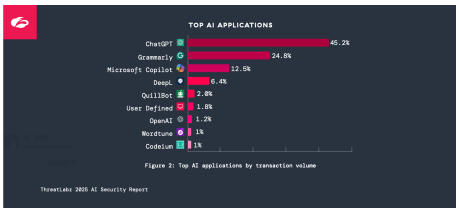
New Zscaler AI Security Report Reveals an Over 3,000% Surge in Enterprise Use of AI/ML Tools

March 20, 2025

Annual ThreatLabz Report Reveals 36x More AI/ML Transactions in World's Largest Security Cloud, Stressing the Need for Zero Trust Everywhere to Enable Secure GenAI Adoption and Stop AI-Powered Threats

ThreatLabz 2025 AI Security Report



Top AI Applications

- **ChatGPT** is the most popular AI/ML application, accounting for nearly half of all AI/ML transactions (45.2%) and is also the most-blocked AI application, followed by Grammarly, and Microsoft Copilot as the second and third most-blocked applications, respectively
- **Agentic AI** and open-source model **DeepSeek** are creating new opportunities for threat actors to weaponize AI and automate and scale their attack
- The top five countries generating the most AI/ML transactions are the **United States, India, United Kingdom, Germany, and Japan**
- The **Finance & Insurance and Manufacturing** industries generate the most AI/ML traffic, with 28.4% and 21.6% share of all AI/ML transactions in the Zscaler cloud, respectively, followed by Services (18.5%), Technology (10.1%), Healthcare (9.6%), and Government (4.2%)

SAN JOSE, Calif., March 20, 2025 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today released the ThreatLabz 2025 AI Security Report, based on insights from more than 536 billion AI transactions processed between February 2024 to December 2024 in the Zscaler Zero Trust Exchange™platform, the largest in-line security cloud, which discovered real-world threat scenarios ranging from AI-enhanced phishing to fake AI platforms. This report also explores recent developments in areas that will undoubtedly influence AI in 2025 and beyond, including agentic AI, the emergence of DeepSeek, and the evolving regulatory landscape.

The report reveals a 3,000+% year-over-year growth in enterprise use of AI/ML tools, highlighting the rapid adoption of AI technologies across industries to unlock new levels of productivity, efficiency, and innovation. Enterprises are sending significant volumes of data to AI tools, totaling 3,624 TB, underscoring the extent to which these technologies are integrated into operations. However, this surge in adoption also brings heightened security concerns. Enterprises blocked 59.9% of all AI/ML transactions, signaling enterprise awareness around the potential risks associated with AI/ML tools, including data leakage, unauthorized access, and compliance violations. Threat actors are also increasingly leveraging AI to amplify the sophistication, speed, and impact of attacks—forcing enterprises to rethink their security strategies.

"As AI transforms industries, it also creates new and unforeseen security challenges," said Deepen Desai, Chief Security Officer at Zscaler. "Data is the gold for AI innovation, but it must be handled securely. The Zscaler Zero Trust Exchange platform, powered by AI with over 500 trillion daily signals, provides real-time insights into threats, data, and access patterns—ensuring organizations can harness AI's transformative capabilities while mitigating its risks. Zero Trust Everywhere is the key to staying ahead in the rapidly evolving threat landscape as cybercriminals look to leverage AI in scaling their attacks."

Key Insights from the ThreatLabz 2025 AI Security Report

ChatGPT Dominates AI/ML Transactions, But Security Concerns Remain
ChatGPT emerged as the most widely used AI/ML application, driving 45.2% of identified global AI/ML transactions in the Zscaler Zero Trust Exchange. However, it was also the most-blocked tool due to enterprises' growing concerns over sensitive data exposure and unsanctioned use. Other most-blocked applications include Grammarly, Microsoft Copilot, QuillBot, and Wordtune, showing broad usage patterns for AI-enhanced content creation and productivity improvements.

"We had no visibility into ChatGPT. Zscaler was our key solution initially to help us understand who was going to it and what they were uploading."
—Jason Koler, CISO, Eaton Corporation See the video case study

DeepSeek and Agentic AI: Innovation Meets Escalating Threats
AI is amplifying cyber risks, with usage of agentic AI and China's open-source DeepSeek enabling threat actors to scale attacks. So far in 2025, we've seen DeepSeek challenge American giants like OpenAI, Anthropic, and Meta, disrupting AI development with strong performance, open access, and low costs. However, such advancements also introduce significant security risks.

Geographies Leading AI Adoption: US and India
The United States and India generated the highest AI/ML transaction volumes, representing the global shift toward AI-driven innovation. However, these changes aren't occurring in a vacuum, and organizations in these and other geographies are grappling with increasing challenges like stringent compliance requirements, high implementation costs, and shortage of skilled talent.

Finance & Insurance Lead Enterprise AI Traffic by Industry
The Finance & Insurance sector accounted for 28.4% of all enterprise AI/ML activity, reflecting its widespread adoption, and indicative of the critical functions supported by the industry, such as fraud detection, risk modeling, and customer service automation. Manufacturing was second, accounting for 21.6% of transactions, likely driven by innovations in supply chain optimization and robotics automation. Additional sectors, including Services (18.5%), Technology (10.1%), and Healthcare (9.6%), are also increasing their reliance on AI, while each industry also faces unique security and

regulatory challenges posing new risks and possibly impacting the overall rate of adoption.

The Zscaler AI Advantage
Built on a true zero trust architecture, Zscaler delivers Zero Trust Everywhere, securing user, workload, IoT/OT communication using business policies, not network policies. Zscaler mitigates AI-powered threats by hiding applications and IP addresses from attackers, inspecting all traffic for threats, and ensuring users access only authorized applications—never full networks. This approach minimizes the attack surface, prevents lateral movement, and stops threats before they can cause harm. Zscaler protects its users against today's most sophisticated AI-driven threats by implementing the following:

- **Zero Trust Foundation:** Minimize the external attack surface through continuous verification and least-privilege access.
- **Real-time AI Insights:** Employ predictive and generative AI to deliver actionable insights that enhance security operations and digital performance.
- **Data Classification:** Leverage AI-driven classification to seamlessly detect and safeguard sensitive data across Zscaler's Data Fabric.
- **Threat Protection**: Block AI-enhanced threats through continuous monitoring and response powered by the Zscaler Zero Trust Exchange.
- **App Segmentation:** Restrict lateral movement and reduce the internal attack surface with AI-driven, automatic app segmentation.
- **Breach Prediction:** Harness the power of Zscaler Breach Predictor that combines the power of generative AI and multi-dimensional predictive models.
- **Cyber Risk Assessments:** Leverages AI-generated security reports to continuously optimize your zero trust implementation.

Download the Full ThreatLabz 2025 AI Security Report
Download the full version of the 2025 AI Security Report here for more information about real-world threat scenarios, AI predictions, insights into AI regulations, and AI best practices.

Methodology
Analysis of 536.5 billion total AI and ML transactions in the Zscaler cloud from February 2024 to December 2024. The Zscaler global security cloud processes over 500 trillion daily signals and blocks 9 billion threats and policy violations per day, delivering over 250,000 daily security updates.

About ThreatLabz
ThreatLabz is the security research arm of Zscaler. This world-class team is responsible for hunting new threats and ensuring that the thousands of organizations using the global Zscaler platform are always protected. In addition to malware research and behavioral analysis, team members are involved in the research and development of new prototype modules for advanced threat protection on the Zscaler platform, and regularly conduct internal security audits to ensure that Zscaler products and infrastructure meet security compliance standards. ThreatLabz regularly publishes in-depth analyses of new and emerging threats on its portal, research.zscaler.com.

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 SASE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform.

Media Contact
Natalia Wodecki
press@zscaler.com

A photo accompanying this announcement is available at https://www.globenewswire.com/NewsRoom/AttachmentNg/9c2bf5d3-5720-4db8-bf1f-a9675f48840e