Zscaler 2026 AI Threat Report: 91% Year-over-Year Surge in AI Activity Creates Growing Oversight Gap for Global Enterprises

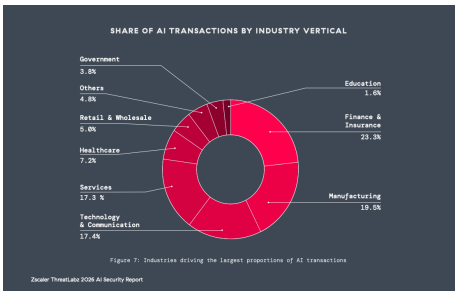
January 27, 2026

Rapid AI adoption creates a critical security gap between innovation and security, requiring organizations to adopt an AI security platform built on Zero Trust

News Highlights

- AI adoption is accelerating faster than enterprise oversight. Despite 200% AI usage growth in key sectors, many organizations still lack a basic inventory of AI models and embedded AI features, elevating AI governance to a board-level priority.
- Enterprise AI systems are vulnerable at machine speed. Zscaler experts found most enterprise AI systems could be compromised in just 16 minutes, with critical flaws uncovered in 100% of systems analyzed.
- AI capabilities are proliferating rapidly across the enterprise. The number of applications driving AI/ML transactions quadrupled year-over-year to more than 3,400, increasing complexity and reducing centralized visibility.
- AI is becoming a high-volume conduit for sensitive enterprise data. Data transfers to AI/ML applications surged 93%, totaling more than 18,000 terabytes which paints an expanding target on AI platforms for cybercriminals across the globe.

2026 ThreatLabz AI Security Report



Transactions by industry vertical

SAN JOSE, Calif., Jan. 27, 2026 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today released the findings of the ThreatLabz 2026 AI Security Report, warning that enterprises are unprepared for the next wave of AI-driven cyber risk, even as AI becomes embedded in business operations. Based on an analysis of nearly one trillion AI/ML transactions across the Zscaler Zero Trust Exchange™ platform between January and December of 2025, the research shows that enterprises are reaching a tipping point where AI has transitioned from a productivity tool to a primary vector for autonomous, machine-speed conflict. The report analyzes AI and ML traffic together because enterprise AI systems rely on machine learning models to operate at scale.

"AI is no longer just a productivity tool but a primary vector for autonomous, machine-speed attacks by both crimeware and nation-state," said Deepen Desai, EVP Cybersecurity at Zscaler. "In the age of Agentic AI, an intrusion can move from discovery to lateral movement to data theft in minutes, rendering traditional defenses obsolete. To win this race, organizations must fight AI with AI by deploying an intelligent Zero Trust architecture that shuts down the potential paths for the attackers of all kinds."

AI in the Enterprise: Emerging Trends and Security Issues from the 2026 Report

AI Adoption is Outpacing Oversight

AI usage now spans every business function, yet in many sectors, adoption is scaling faster than the C-suite can manage. Finance & Insurance remains the most AI-driven sector by volume, accounting for 23% of all AI/ML traffic, while the Technology and Education sectors recorded explosive year-over-year growth in transactions — 202% and 184%, respectively. Despite this, Zscaler research reveals a critical gap: many organizations still lack a basic inventory of active AI models and embedded features, leaving them unaware of exactly where sensitive data is exposed.

As Agentic AI Looms, 100% of Enterprise AI Systems Found Vulnerable to Breach at Machine Speed

While AI security discussions often focus on hypothetical future threats, Zscaler's red team testing revealed a more immediate reality: when enterprise AI systems are tested under real adversarial conditions, they break almost immediately. In controlled scans, critical vulnerabilities surfaced in minutes, not hours. The median time to first critical failure was just 16 minutes, with 90% of systems compromised in under 90 minutes. In the most extreme case, the defense was bypassed in a single second.

As more evidence of AI-driven attacks by cybercriminals and nation-state espionage groups is uncovered, ThreatLabz warns autonomous and semi-autonomous "agentic" AI will increasingly automate cyberattacks, with AI agents assuming responsibility for reconnaissance, exploitation, and lateral movement. Defenders must assume that attacks can scale and adapt at machine speed, not human speed.

AI Usage Surges 4x, Fueling New Enterprise Supply Chain Vulnerabilities

ThreatLabz found AI/ML activity increased 91% year-over-year across an ecosystem of more than 3,400 applications. This rapid adoption has left many organizations with no clear map of the AI models interacting with their data or the supply chains behind them. ThreatLabz warns that this AI supply chain is now a primary target, as weaknesses in common model files allow attackers to move laterally into core business systems.

Unmanaged Embedded AI Creates Critical Data Exposure Risks

An enormous volume of activity is happening on "standalone AI" such as ChatGPT, which logged 115 billion transactions in 2025 and Codeium, which logged 42 billion transactions. “Embedded AI,” AI capabilities built directly into everyday enterprise SaaS applications and platforms, have become one of the fastest growing sources of unmanaged risk. Because these features are often active by default and escape detection by legacy security filters, they create a back door for sensitive corporate data to flow into AI models without oversight. Among all platforms analyzed, Atlassian was a leading source of embedded AI activity, reflecting widespread use of AI-powered features within its core platforms, such as Jira and Confluence.

18,000 TB of Data Poured into AI: A New Target for Machine-Speed Attacks

In 2025, enterprise data transfers to AI/ML applications surged to 18,033 terabytes (TB)—a 93% year-over-year increase and roughly equivalent to 3.6 billion digital photos. The massive influx has transformed tools like Grammarly (3,615 TB) and ChatGPT (2,021 TB) into the world’s most concentrated repositories of corporate intelligence.

The scale of this risk is quantified by 410 million Data Loss Prevention (DLP) policy violations tied to ChatGPT alone, including attempts to share Social Security numbers, source code, and medical records. These findings signal that AI governance has transitioned from a policy discussion to an immediate operational necessity. ThreatLabz warns that as these repositories grow, they are becoming high-priority targets for cyber espionage.

Modernize AI security with Zero Trust

Legacy firewalls and VPNs fail in dynamic AI environments, creating visibility gaps and security blind spots. Zscaler replaces this complexity with AI-native security, providing the real-time visibility and guardrails needed to innovate safely.

The Zscaler Zero Trust Exchange helps organizations stay ahead of AI-powered threats by:

- **Eliminating Attack Surfaces**: Enforce continuous verification and least-privileged access.
- **Blocking AI Threats**: Inspect all traffic, including encrypted data, to stop threats in real time.
- **Protecting Data Everywhere**: Automatically discover and classify sensitive data across all environments.
- **Neutralizing Lateral Movement**: Use AI-powered segmentation to contain attackers.
- **Optimizing Responses**: Leverage predictive AI to accelerate security operations and posture management.

Master the new rules of AI security and download the full report

Rapidly accelerating AI adoption demands a new approach to protection. To stay ahead of evolving risks, download the full ThreatLabz 2026 AI Security Report for comprehensive threat analysis and actionable best practices.

Follow Zscaler on LinkedIn, X, and Instagram.

Research Methodology

The report draws on an analysis of 989.3 billion AI/ML transactions generated by ~9K organizations across the Zscaler Zero Trust Exchange™ from January 2025–December 2025, providing a grounded view into how AI is actually being used (and restricted) across global environments.

About Zscaler
Zscaler (NASDAQ: ZS) is a pioneer and global leader in zero trust security. The world’s largest businesses, critical infrastructure organizations, and government agencies rely on Zscaler to secure users, branches, applications, data & devices, and to accelerate digital transformation initiatives. Distributed across 160+ data centers globally, the Zscaler Zero Trust Exchange™ platform combined with advanced AI combats billions of cyber threats and policy violations every day and unlocks productivity gains for modern enterprises by reducing costs and complexity.

Media Contact
Nick Gonzalez, Director of Global Public Relations, press@zscaler.com

A photo accompanying this announcement is available at https://www.globenewswire.com/NewsRoom/AttachmentNg/f6075799-2667-4962-9e31-b5a6d3a18410