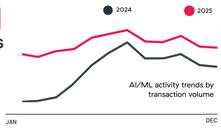
AI at Internet Scale: The Fastest-Growing Attack Surface

Findings from the ThreatLabz 2026 AI Security Report

THE EXPLOSION

Nearly 1 trillion AI/ML transactions analyzed

Enterprises are relying on AI to move faster, automate decisions, and increase productivity.



Analysis period: January–December 2025

AI is no longer emerging. It's dominant.

83% Increase in Transactions

THE SHIFT

AI is embedded across enterprise workflows

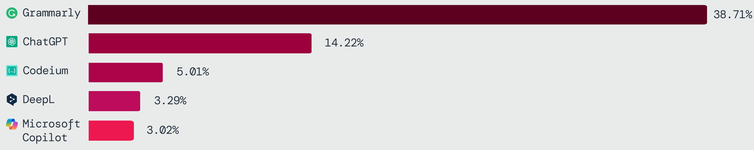
AI has become always-on infrastructure, expanding opportunity and the attack surface at once.

FROM 875 TO 3,500 APPS

Driving AI/ML Transactions

AI adoption is accelerating faster than security controls can adapt. Shadow AI is a major factor behind this shift.

Top 5 applications by traffic share



THE IMPACT

Industries are operationalizing AI at scale

As organizations reap the benefits of AI, reliance increases exposure—and no sector is immune.

Top AI-active industries

- Finance & Insurance
- Healthcare
- Services
- Technology & Communication
- Manufacturing

AI adoption is not isolated to tech.
It's systemic across the global economy.

THE RISK

AI is a new enterprise risk layer

AI platforms process large volumes of sensitive data, making them prime channels for data exfiltration.

18,033 TB

of data sent to AI apps

Equivalent to roughly 3.6 billion digital photos

93% increase year-over-year

AI/ML apps with the most DLP policy violations

- ChatGPT: 410,181,006
- Codeium: 242,263,311
- GitHub Copilot: 31,223,009

Without effective DLP controls, the risk of exposure is immediate and real.

Sensitive data is increasingly at stake:

As AI proliferates, enterprise data moves across more applications, often with limited visibility and inconsistent guardrails.

Common sensitive data detected

- PII
- Source code
- Payment data
- Healthcare records

Systemic vulnerabilities amplify the risk

Inherent weaknesses in AI systems create even more opportunities for exploitation.

25+ enterprise environments tested by Zscaler red teaming experts

220K+ adversarial attack attempts

100% of AI systems had critical vulnerabilities

THE RESPONSE

Enterprises are actively restricting AI use

Organizations are blocking AI traffic to contain risk, but restriction alone is not a security strategy.

39% of AI transactions were blocked

Top blocked applications

1	Grammarly
2	GitHub Copilot
3	ChatGPT
4	Microsoft Copilot
5	QuillBot

High blocking rates reflect concerns around data exposure and privacy.

WHAT MUST CHANGE

AI is reshaping the enterprise. Security must evolve with it

Securing AI demands comprehensive visibility, runtime protections, and a foundation of zero trust.

2026 enterprise AI security requirements

- ☐ Discover and map your full AI footprint and risks
- ☐ Align AI usage to governance and regulatory controls
- ☐ Apply least-privilege access to AI systems
- ☐ Enforce AI guardrails with inline inspection
- ☐ Validate model integrity and supply chain dependencies
- ☐ Continuously test AI systems under adversarial conditions

Read the ThreatLabz 2026 AI Security Report

Explore the full research and analysis, including where AI adoption is accelerating, how AI-enabled threats are evolving, and what it takes to securely embrace AI in the enterprise.

DOWNLOAD THE REPORT