Zero Trust Security for AI Applications on AWS

Challenges

AI brings benefits along with new access and security challenges

Enterprise organizations view AI apps as essential for improved decision making, faster growth, and greater efficiency. But AI apps, including agentic AI, present significant visibility, access, and security challenges.

The Zscaler ThreatLabz 2026 AI Security Report reveals that enterprise AI/ML transactions increased 91% year-over-year and there are over 3,400 AI apps available. Finance/Insurance and Manufacturing industries generated the most traffic. However, 39% of transactions were blocked due to concerns about data leakage, unauthorized access, and compliance.

The Zscaler Solution

Proven zero trust platform that secures the use of AI everywhere

Zscaler provides organizations with visibility and control over interactions with public and private AI apps, while preventing the exposure of sensitive data. The Zscaler Zero Trust Exchange™ is a cloud-native platform that delivers zero trust access and security for all users, apps, and workloads at any location.

In addition, robust dashboards, prompt and response visibility, and powerful data loss prevention controls keep data safe and users productive. Zscaler also eliminates the poor security, slow performance, and cost / complexity that comes with legacy VPNs and firewalls.

Benefits

Zscaler has been a leader in zero trust[1] for over a decade, and is an AWS AI Competency Partner (Agentic AI Applications category), protecting thousands of AWS customers worldwide.

Granular visibility

Automatically discover AI apps, usage by department, and gain visibility into user prompts and responses. Dashboard includes trends, sensitive data transactions, and more.

Protect sensitive data

AI driven data discovery finds sensitive data across endpoints, inline, and public clouds. Block sensitive data headed to AI apps, identify misconfigurations / vulnerabilities, and remediate risk.

Zero trust access

Manage user access to AI apps and apply consistent policies that allow direct access, block, warn, or allow access using browser isolation to prevent cut, paste, and download.

Secure Amazon Bedrock

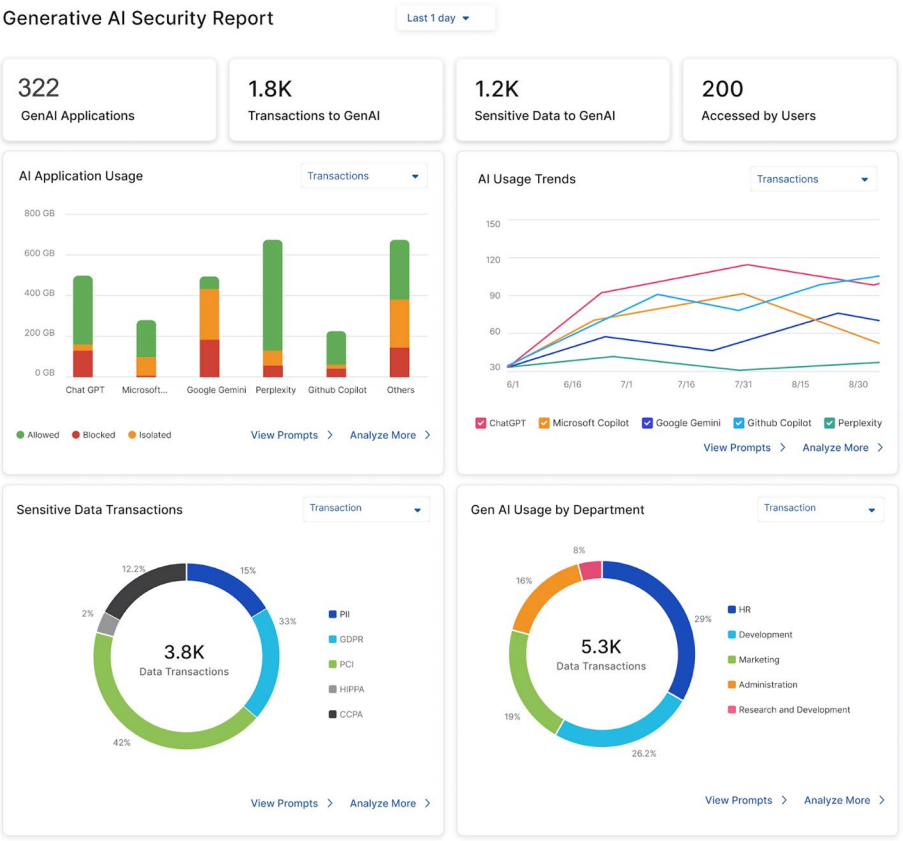
Zscaler AI-SPM monitors AI deployments, training data, configurations, and potential misuse within AI environments to mitigate security and compliance risks.

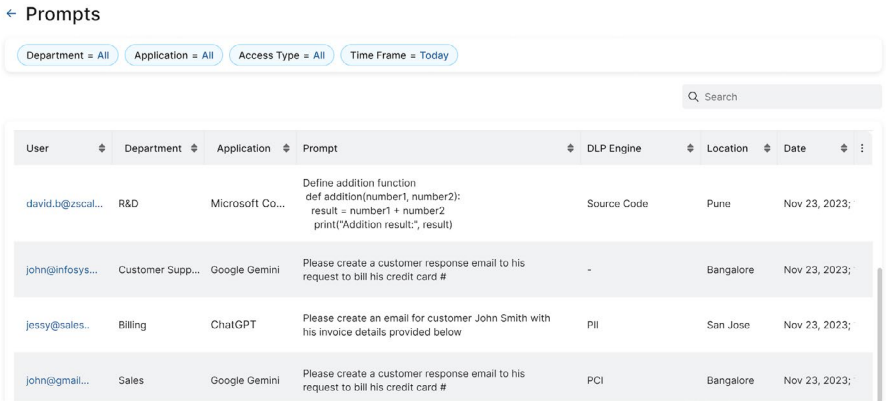
[1]Gartner: Magic Quadrant for Security Service Edge (SSE), May 20, 2025

Zscaler Zero Trust

The Zscaler Zero Trust Exchange is the world's largest inline security cloud. It securely connects users, devices, applications and workloads with over 160 PoPs globally and in most AWS regions.

In-depth Visibility and Control





Secure AWS AI apps

Amazon Bedrock

Amazon SageMaker

Amazon Q

"Zscaler DLP gives the security team a granular view into shadow generative AI application usage, including user input prompts. If AI app usage does not align with corporate policy, it enforces real-time DLP blocking and application isolation."

Debashis Singh
CIO, Persistent

Learn more about Zscaler security for AI, Zscaler AI-SPM, and Zscaler for AWS.

zscaler™ | **Act fast. Stay secure.™**

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. 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