Zero Trust Security for GenAI Applications on AWS

Challenges

GenAI apps bring benefits and new security challenges

Enterprise organizations view GenAI apps as essential for improved decision making, faster growth, and greater efficiency. But GenAI apps also present significant challenges for IT and security teams.

The Zscaler ThreatLabz 2025 AI Security Report reveals that AI/ML transactions increased by 3,465% year-over-year, and the Finance/Insurance and Manufacturing industries generated the most traffic. However, 60% of all enterprise AI/ML transactions were blocked due to concerns about data leakage, unauthorized access, and compliance violations.

The Zscaler Solution

Proven zero trust platform that secures the use of GenAI

Zscaler provides organizations with visibility and control over user's interactions with GenAI apps, while preventing the exposure of sensitive data. The Zscaler Zero Trust Exchange™ is a cloud-native platform that delivers zero trust security for all users, apps, and workloads from any device and location.

In addition, robust dashboards, prompt and response visibility and powerful data loss controls keep data safe and users productive. Zscaler also eliminates the poor security 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 Security Competency Partner, protecting thousands of AWS customers worldwide.

Granular visibility

Automatically discover GenAI 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 GenAI 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

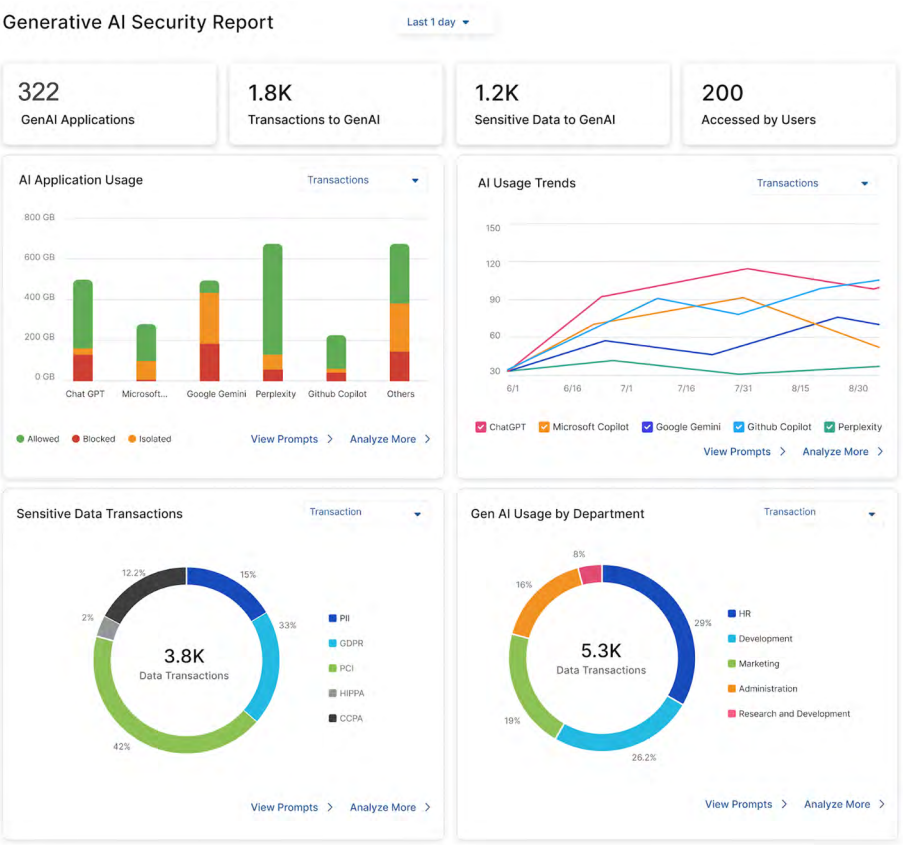
Zscaler AI-SPM monitors AI deployments, training data, configurations, and potential misuse within AI environments to mitigate security and compliance risks.

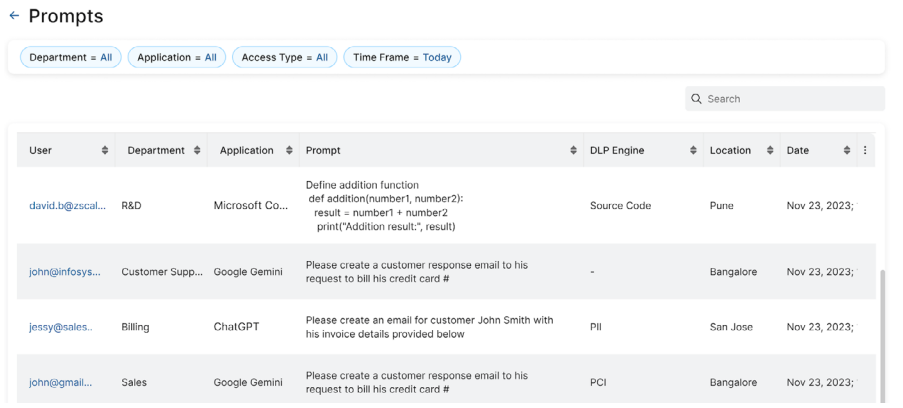
[1]Gartner: Magic Quadrant for Security Service Edge (SSE), May 20, 2025

Zscaler Zero Trust

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

In-depth Visibility and Control





Secure AWS GenAI 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 GenAI, Zscaler AI-SPM, and Zscaler for AWS.

zscaler™ | Experience your world, secured.™

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 160 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline 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