

Zscaler GenAI Security Gov

GenAI Security Benefits

Find Shadow AI

See all GenAI apps in use with granular insights across users, departments, and sensitive data

Understand Input Prompts

See all prompts users send to AI apps, to better understand how they are used in your environment

Isolate AI sessions

Stop data loss by placing AI sessions in a secure isolated browser that enables blocking of cut, paste, and download

Enforce DLP Controls

Stop sensitive data headed to GenAI and with powerful inline DLP classification and blocking

Empowering Your Organization to Innovate Safely with Generative AI

Generative AI tools boost productivity and innovation. However, they also introduce the risk of exposing sensitive company data through AI interactions. Employees may inadvertently share confidential information in prompts, turning generative AI applications into potential security vulnerabilities.

Zscaler Generative AI Security provides organizations with the confidence to leverage AI tools while ensuring robust security and data protection. Our comprehensive platform delivers unmatched visibility, protection, and remediation for all AI-related transactions, empowering organizations to embrace innovation without compromising security.

Use Cases

Control AI Data Risks

Enable safe and productive use of AI applications without the loss of sensitive data

Learn AI Usage Trends

With in-depth prompt level visibility, understand how users are interacting with AI applications

Coach Users on Safe AI Use

Pair with Zscaler Workflow Automation to coach users on incident violations and GenAI best practices

GenAI data risks



Internal source code



Confidential content



Sensitive analysis

Inspect and block Data

GenAI Security
Get prompt visibility

DLP Inspection
Block sensitive data



Control access

Cloud App Control
Block app or warn user

Browser Isolation
Isolate app and data

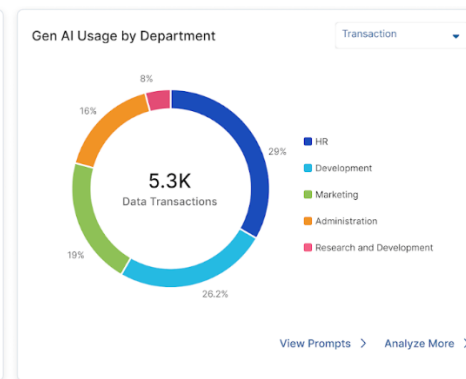
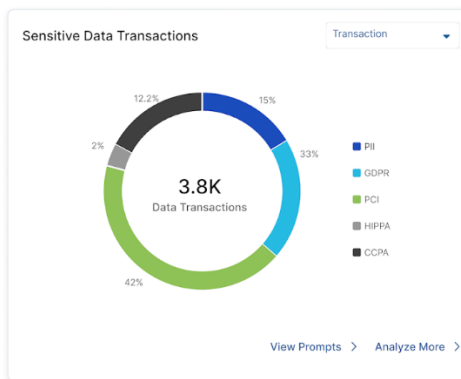
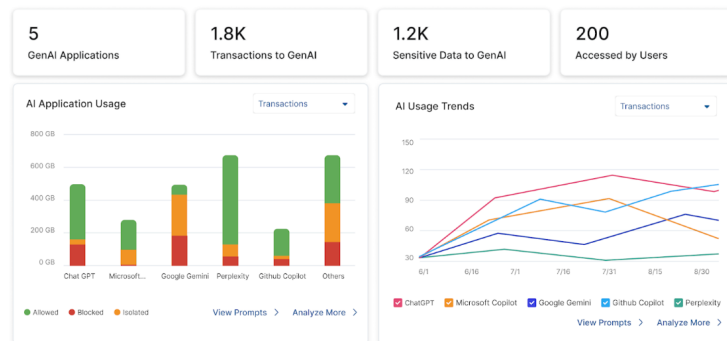
In-depth Visibility and Control

Get complete visibility of all AI activities along with a complete log of each user input prompt

Generative AI Security Report

Last 1 day

Time Updated: May 16, 2023 12:01 PM



Prompts							
Department = All Application = All Access Type = All Time Frame = Today							
Search							
User	Department	Application	Prompt	DLP Engine	Location	Date	
david.b@zscal...	R&D	Microsoft Co...	Define addition function def addition(number1, number2): result = number1 + number2 print("Addition result:", result)	Source Code	Pune	Nov 23, 2023;	
john@infosys...	Customer Supp...	Google Gemini	Please create a customer response email to his request to bill his credit card #	-	Bangalore	Nov 23, 2023;	
jessy@sales..	Billing	ChatGPT	Please create an email for customer John Smith with his invoice details provided below	PII	San Jose	Nov 23, 2023;	
john@gmail...	Sales	Google Gemini	Please create a customer response email to his request to bill his credit card #	PCI	Bangalore	Nov 23, 2023;	