Data Sheet

Generative AI: Secure use while reducing data risks

Zscaler provides visibility and control over generative AI enabling organizations to move forward with innovation sparked by AI, while protecting sensitive data.

The risks and rewards of generative AI

AI tools are emerging as the next frontier of productivity in many organizations. However, they present risks to sensitive data that can be exposed through inappropriate use. With Zscaler, organizations can tailor the use of particular AI applications for their organization while ensuring they have complete data protection and full visibility into usage.

Security Concerns for Generative AI

- Who is using AI Apps?
- Can you control access, down to the user?
- Do you have granular control over specific apps
- What are the risk levels of AI apps
- Can you secure sensitive data from AI Apps
- Can you audit queries to AI across the organization?

Key capabilities

AI risk-based usage controls

Permit use of only appropriate AI applications—based on risk—with granular usage controls, down to individual teams and users.

AI visibility

Understand who is using AI across the organization while gaining full visibility into all prompts and queries in ChatGPT.

Data protection for AI

Prevent potential data leakage via AI applications with full DLP protecting data from being exfiltrated in AI prompts

Prevent risky actions

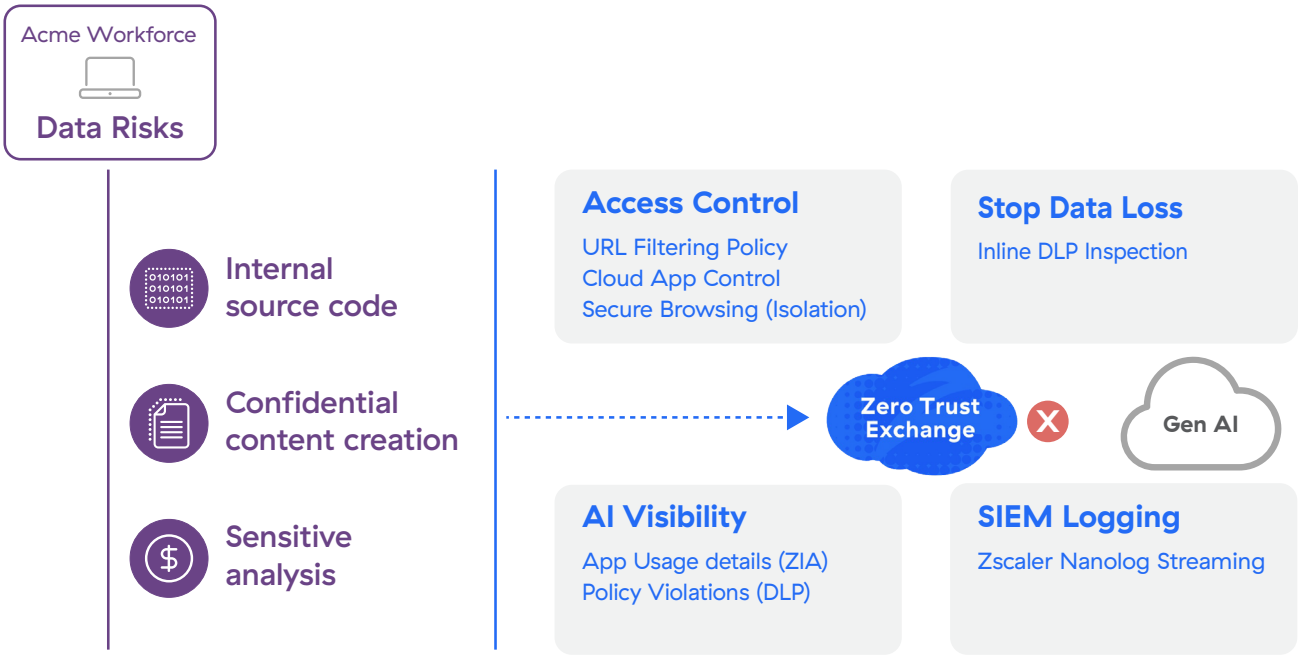
Incorporate additional security measures such as browser isolation to prevent data uploads, downloads, and clipboard use; preventing exfiltration of large amounts of potentially sensitive data in prompts.

Key benefits

Spark innovation with AI
Confidently put AI to use to empower teams and innovation.

Rightsize AI use and its risk
Manage risk and expenses by only allowing the appropriate AI apps that make sense for the organization for less risk and expense.

Ongoing AI insights
With ongoing visibility into usage and prompts, organizations can continuously understand, control, and refine AI use and activity.



With Zscaler, organizations can streamline all Generative AI security and data controls into one unified platform.

In addition to securing the use of AI, Zscaler has also called on AI for years to deliver more positive security outcomes for IT and security teams.

AI-powered segmentation

Minimize internal attack surface with automatically identified application segments to create the right zero trust access policies to reduce security risk.

Fast time to data protection

Protect data immediately with ML-based automatic data classification—with no configuration necessary—to accelerate your data protection programs.

AI-driven root cause analysis

Identify root causes of poor experiences 180 times faster to help users get back to work in seconds, accelerate MTTR, and free up IT from time-consuming troubleshooting and analysis.

AI-driven sandboxing verdicts

Avoid patient 0 infections with AI that instantly knows if a new file is malicious without allowing it into an organization while waiting for a sandbox verdict.

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 150 data centers globally, the SSE-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