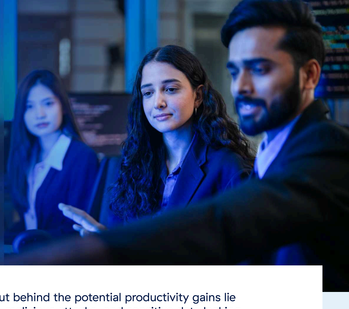


Are you ready to embrace GenAI securely?

Your 7-step checklist

GenAI is reshaping how we all work. But behind the potential productivity gains lie hidden risks, like weak access controls, malicious attacks, and sensitive data leaking into tools.

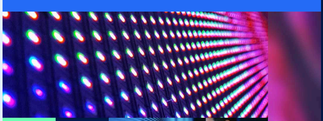
Use this checklist to evaluate whether your organisation is ready to innovate safely with GenAI — or whether it's stealthily increasing your exposure.

01

Do you know who's using GenAI, and for what?

If you can't see what's going on in your AI environment, you can't keep it secure. Ask yourself:

- Do you have visibility of the GenAI tools your teams are accessing?
- Can you see what types of data are being shared or generated?
- Are you able to detect unsanctioned 'shadow' AI apps?



03

Are your policies consistent across all your GenAI tools?

Patchy security policies create loopholes that staff may exploit without realising. Reflect on the following:

- Do you enforce consistent data-sharing rules across all GenAI apps?
- Can you block unsafe actions while permitting safe ones?
- Are your policies adaptable by role, user group, and data type?

05

Can you enforce controls in real time?

AI can quickly expose sensitive data, so speedy rule enforcement is critical. Consider this:

- Can you detect sensitive data before it leaves a device or app?
- Are colleagues alerted in real time when they try something risky?
- Can you stop dangerous actions without stopping legitimate work?

07

Is your approach scalable and future-ready?

AI evolves continually. Your security must keep pace with the latest tools and regulations. Ask yourself:

- Can you add new AI apps without rebuilding policies?
- Do your controls scale across browsers, endpoints, SaaS, internal apps, and APIs?
- Can your AI policies adapt as regulations and frameworks change?

02

Do you understand what data is at risk when using GenAI?

AI models retain prompts. If your colleagues enter sensitive data, it could be permanently exposed. Consider this:

- Do you automatically classify sensitive and regulated data, wherever it lives?
- Can you identify when sensitive data is being sent to public GenAI tools?
- Can your classification system adapt to new content types, such as AI-generated text, summaries or screenshots?

04

Are your security controls balanced and proportionate?

Overly restrictive controls kill productivity and encourage unsafe workarounds. Ask yourself:

- Do you permit low-risk tasks, like writing summaries, drafts, and coding?
- Can you selectively block uploads of sensitive data?
- Can you guide colleagues toward approved AI tools?

06

Do you have a unified view of AI risk?

Good AI governance relies on visibility across your organisation. Reflect on the following:

- Can you identify trends, like which teams are using AI most, and what for?
- Can you report on incidents, policy actions, and high-risk behaviour?
- Can you gain insights to help refine your policies and improve secure usage?

Control AI risk, keep the benefits

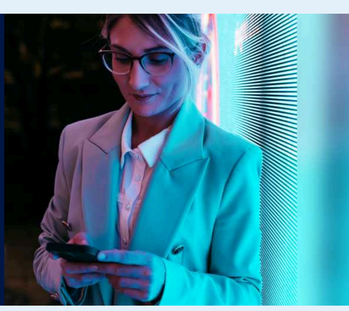
Does your current approach to GenAI let you confidently answer 'yes' to these critical questions? Zscaler's Data Security Platform is here to make sure you can. Gain full visibility with interactive dashboards to track usage and identify trends. Protect sensitive data from exposure with smart prompt blocking. And enforce granular, adaptive policies to empower your teams while ensuring consistent security across all GenAI interactions.

To see how Zscaler helps your organisation secure GenAI data at scale, request a demo now.

Book a demo

For an expert perspective on strategies for securing AI, watch the webinar.

Watch now



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 centres globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on X (Twitter) **@zscaler.**