Organizations rush to use generative AI tools, despite significant security concerns

New All Eyes on Securing GenAI research from Zscaler explores how today's organizations are approaching GenAI tool usage and the security implications this might have.

KEY FINDINGS

Despite significant security concerns, business uptake of GenAI tools is strong

89% of organizations consider GenAI tools to be a **potential security risk**

48% see GenAI tools as more of threat than an opportunity

And yet

95% are using GenAI tools in some guise:

57% allow their use fully

38% are approaching their use with caution

Only **5%** are holding back to see where the technology goes, or have blocked its use entirely

The top five use cases are:

- Data analysis **78%**
- R&D services development **55%**
- Marketing **53%**
- End-user tasks **44%**
- Logistics **41%**

Top concerns included:
The potential loss of sensitive data 43%
A lack of resource to monitor use 43%
And a lack of understanding around the benefits/dangers 41%

Evidence shows that organizations are failing to act on their security concerns

23% of those organizations using GenAI tools **aren't monitoring this usage** at all

33% have yet to implement any additional GenAI-related security measures

— though 31% have this on their roadmaps

The rollout pressure isn't coming from where people might think

Only **5%** of respondents said current interest/usage of GenAI tools stemmed from general employees

59% said usage was being driven by IT teams

21% said business leads were in the driving seat

With the window for regaining control of GenAI security closing, organizations must act now

92% of respondents expect interest in using GenAI tools to increase between **now and the end of the year**

Classifying data is a vital first step to ensuring the secure use of GenAI — as it stands, only **46%** of respondents were confident that all their data has been **classified according to criticality**. A further **44%** have at least **classified some of it.**

Steps to secure GenAI tool use:

1. **Conduct thorough security risk assessments** for GenAI applications to understand and respond to vulnerabilities
2. **Implement a holistic zero trust architecture** to authorize only approved GenAI applications and users
3. **Establish a comprehensive logging system** for tracking all GenAI prompts and responses
4. **Enable zero trust-powered Data Loss Prevention measures** to secure all GenAI activities and prevent data exfiltration

A cloud-based security service like the Zscaler Zero Trust Exchange enables IT teams to keep full logs of tool usage, as well as create and enforce policies around the GenAI sites employees can visit and how they interact.

For more on the Zscaler Zero Trust Exchange and how Zscaler can enable organizations to lean into GenAI with confidence visit:
https://www.zscaler.com/products-and-solutions/securing-generative-ai

METHODOLOGY

In October 2023, Zscaler commissioned Sapio Research to conduct a survey of 901 IT decision makers (ITDMs) across 10 markets (Australia & New Zealand, France, Germany, India, Italy, Netherlands, Singapore, Spain, UK & Ireland, USA). These ITDMs work at companies of 500+ employees, and across industries.

ABOUT ZSCALER

Zscaler (NASDAQ: ZS) accelerates digital transformation so 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.