A Lynchpin Media BRAND

CXO priorities

zscaler™

2024 Europe CXO Priorities Report: Key GenAI trends, security challenges and priorities for the C-suite in Europe

Contents

Introduction

In late 2022, the world witnessed the rise of Generative AI (GenAI). The boom peaked with the release of thousands of software infiltrating every sector and penetrating deeply into various facets of business and human life. With simple prompts, organisations were now able to generate text, images, videos or other data using generative models.

However, just as GenAI models ease workflow by learning patterns and structure of input data to achieve more accurate outcomes, it also paves the way for security issues. GenAI models often require access to vast amounts of data to function effectively hence increasing the risk of sensitive business data being exposed or mishandled, leading to breaches of confidentiality.

Amidst the innovation, organisations in Europe are not left out as they equally navigate a web of security challenges. From data privacy concerns to the threat of adversarial attacks and safeguarding AI systems against vulnerabilities, the risk of malicious exploitation is now paramount.

This CXO Priorities survey, in collaboration with Zscaler, aims to build an overview of the current AI-related challenges and priorities faced by organisations in Europe. It explores key GenAI trends, security challenges and priorities for the C-suite in Europe.

Survey overview:

To find out more about the current challenges and priorities around GenAI facing organisations in Europe, we surveyed CIOs, CISOs, CTOs, VPs of Networks and VPs of Security about what factors are driving advanced technology in the face of changing regulations.

This report aims to present an overview of the current evolution of GenAI tools and explore the complexities of managing security risks.

Through this survey we aimed to discover:

- GenAI and current tools and threat landscape
- The role and impact regulations with GenAI
- Priorities and planning ahead

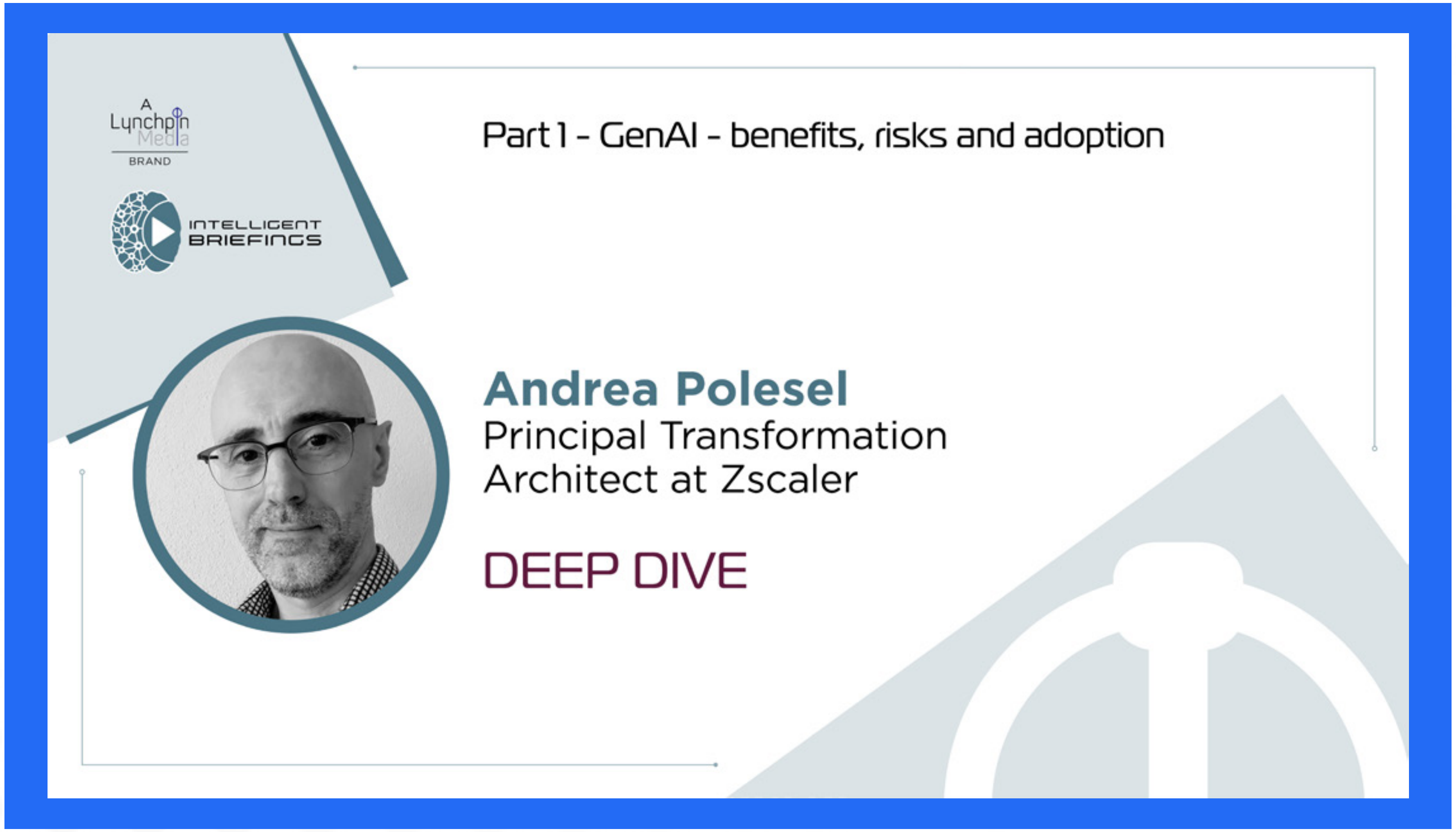
Key findings

- Concerns around loss of sensitive data (23%) and lack of resource to monitor use (21%) are the top reasons why organisations have not adopted GenAI tools like ChatGPT
- The main challenges organisations face when it comes to securing Generative AI applications is lack of awareness of GenAI (22%) and budget constraints (22%)
- The survey reveals a split in awareness regarding the key provisions of the EU Artificial Intelligence Act (AI Act) concerning GenAI. Almost half (48%) confirm they have read or reviewed the key provisions.
- Over half of respondents (57%) are neutral or believe the AI Act doesn't provide sufficient security and guidance for organisations using GenAI technologies
- The survey indicates that 32% of organisations are already looking into the specific requirements of NIS2, highlighting a proactive approach to regulatory compliance
- The survey reveals that a significant portion of organisations are planning to implement security measures specifically designed for Generative AI applications. Nearly half of respondents (49%) plan to do so within the next year, with 22% planning implementation within the next six months and 27% within the next year.
- The manipulation of AI algorithms (26%) is the biggest concern organisations have regarding the security risks of GenAI
- Nearly two fifths (38%) of survey respondents are planning to implement security tools driven by Artificial Intelligence (AI)
- Over two fifths of respondents (41%) believe their organisations are likely to be impacted by the AI Act's regulations on GenAI
- The survey indicates that 41% of respondents believe additional regulations are needed to ensure the safe and secure use of GenAI
- The top two investment areas include strengthening hybrid working security strategies (10%) and investing in GenAI tools (10%)

VIDEO:
Part 1 – GenAI – benefits, risks and adoption

Throughout this video series, we unravel the relationship between Zero Trust and Generative AI with a dedicated episode to each of the key elements. Each segment draws attention to the varying aspects of AI and the tools that can make this technology safer for businesses. We focus on the specifics of Zscaler's approach and how the company plans to adapt its security measures to meet the challenges and opportunities.

CLICK/TAP the thumbnail to play the video . . .



A Lynchpin Media BRAND

INTELLIGENT BRIEFINGS

Part 1 - GenAI - benefits, risks and adoption

Andrea Polesel
Principal Transformation
Architect at Zscaler

DEEP DIVE

Part 1: GenAI and current security landscape

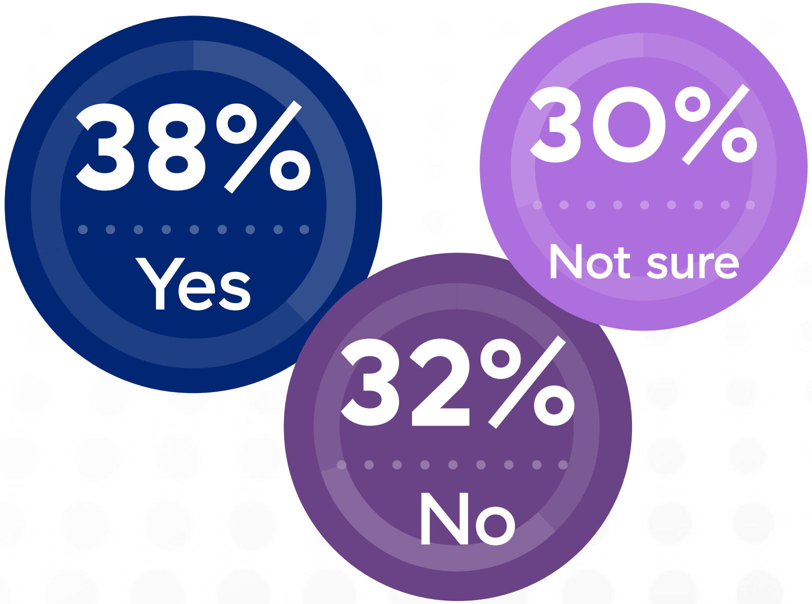
The evolution of GenAI in today's business landscape presents both promise and peril. While GenAI's digital interconnectedness with data offers boundless innovation opportunities, it also exposes vulnerabilities in every system.

From safeguarding personal data to fortifying critical infrastructure, these challenges are inevitable. In this chapter, we asked participants what security tools their organisations are using, their challenges, level of security and what additional security measures their organisation was implementing.

Is your organisation currently using or planning to implement security tools driven by Artificial Intelligence (AI)?

Key insights:

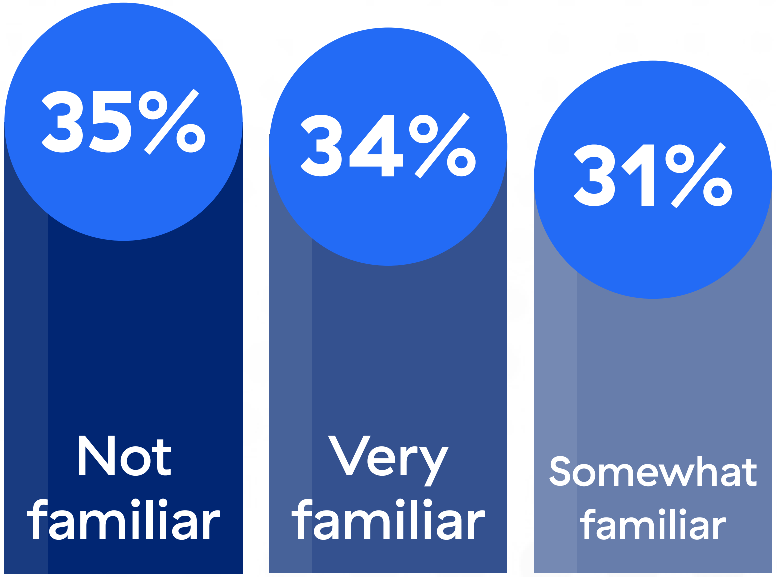
With a spread across responses slightly skewed towards the use or implementation of AI powered security tools, these statistics reflect the current trends and considerations in the adoption of AI for organisational security. AI tools offer significant advantages for protecting against risks and ensuring information safety.



How familiar are you with Generative AI and its potential security risks?

Key insights:

The survey shows a balanced familiarity with Generative AI and its potential security risks, with respondents almost evenly split between being very familiar, somewhat familiar and not familiar. This indicates varied levels of awareness and highlights the need for increased education and adoption of robust security measures to address the risks associated with Generative AI.

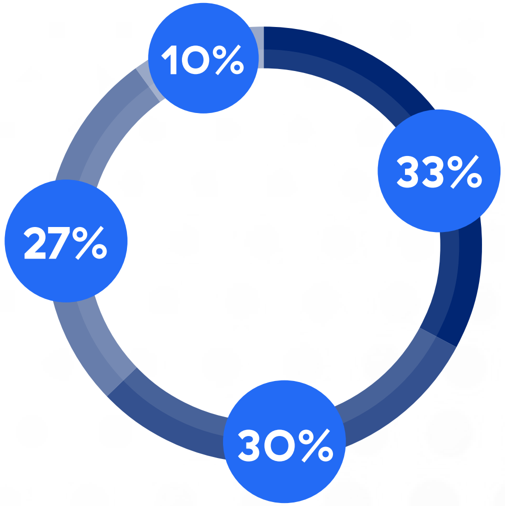


Part 1:
GenAI
and current
security landscape

Which of the following best describes your approach towards GenAI tools at an organisational level (e.g. governed by IT)?

Key insights:

With responses indicating a mix of adoption strategies, organisations are approaching GenAI tools with varying levels of caution. A significant portion are either allowing their use or cautiously evaluating them, reflecting a trend towards careful consideration and integration of GenAI technologies while ensuring security and compliance.



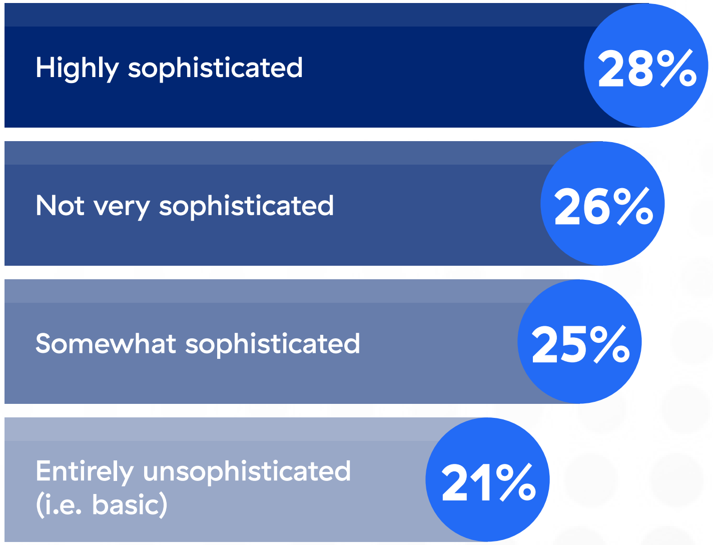
- ● We allow the use of these tools
- ● We're approaching the use of these tools with caution
- ● We're holding back to see where the technology goes
- ● We are blocking the use of these tools
- ⁙ Other – please specify

Part 1:
GenAI
and current
security landscape

How would you rate your organisation's use of GenAI tools in terms of sophistication (based on a corporate usage policy delivered by the IT team)?

Key insights:

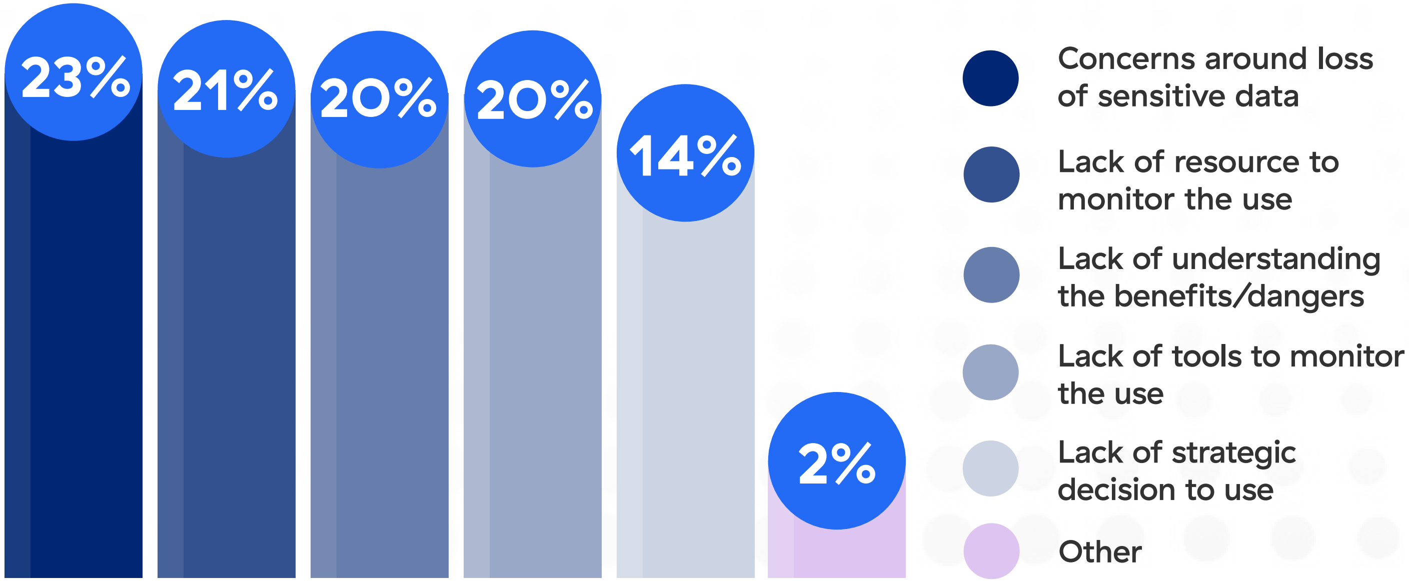
With a spread across responses indicating varied levels of sophistication, these statistics reflect the diverse stages of GenAI tool adoption within organisations. While some exhibit advanced usage guided by IT policies, others are still in the early stages. This suggests ongoing development and refinement in leveraging GenAI capabilities.



What are the main reasons for your organisation not yet using GenAI tools like ChatGPT?

Key insights:

With responses split, these statistics reflect the primary barriers to adopting GenAI tools like ChatGPT. Concerns around data security, insufficient understanding of benefits and risks, and lack of resources and monitoring tools highlight the challenges organisations face in integrating GenAI technologies into their operations.



Part 1:
GenAI
and current
security landscape

What are the main concerns your organisation has regarding the security risks of Generative AI?

Key insights:

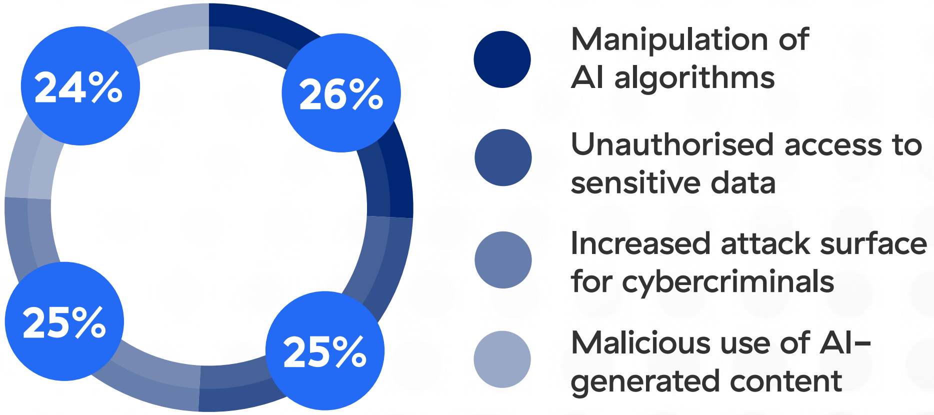
The growing integration of Generative AI into organisational frameworks brings forth several pivotal security concerns. With a quarter of organisations fearing unauthorised access to sensitive data, the sophisticated nature of AI algorithms presents an enhanced risk of data breaches. Generative AI systems, often requiring vast amounts of data for training, can inadvertently expose sensitive information if not adequately secured. This concern demonstrates the necessity for robust data governance and stringent access controls.

At the same time, 24% of organisations are wary of the malicious use of AI-generated content. This threat is multifaceted, encompassing the creation of deepfakes, spear-phishing campaigns and disinformation. The potential for AI to generate convincingly authentic content at scale exacerbates the challenges in distinguishing legitimate communications from fraudulent ones. Therefore, organisations must consider prioritising investment in advanced detection mechanisms and user education to mitigate this risk.

Moreover, the manipulation of AI algorithms, highlighted by over a quarter of respondents, signifies a critical vulnerability. Adversarial attacks, where malicious actors subtly alter inputs to deceive AI systems can have dire consequences, particularly in sectors like finance, healthcare and national security. Ensuring the integrity and robustness of AI models through continuous monitoring and anomaly detection is paramount.

The increased attack surface due to AI adoption, noted by 25% of organisations, reflects the broader cybersecurity landscape's complexity. As AI systems integrate more deeply into operational workflows, they become attractive targets for cybercriminals. This expanded attack surface necessitates a holistic approach to cybersecurity, encompassing AI-specific threat modelling, incident response planning and regular security assessments.

The security risks associated with Generative AI are wide-ranging and demand a comprehensive, proactive approach to safeguard organisational assets and maintain trust in AI-driven innovations.



What are the main challenges your organisation faces in securing Generative AI applications?

Key insights:

Securing Generative AI applications presents a range of challenge for organisations, reflecting broader trends in cybersecurity and AI adoption. A lack of awareness of Generative AI (GenAI) among 22% of respondents signifies a fundamental knowledge gap.

This deficiency hinders effective risk assessment and mitigation strategies, making it imperative for organisations to prioritise education and training initiatives to elevate baseline understanding.

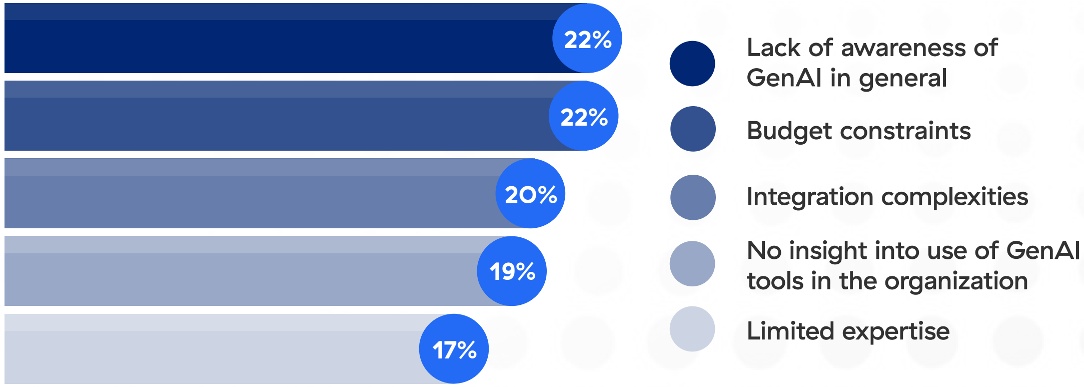
Limited expertise, noted by 17% of respondents underscores the scarcity of skilled professionals adept in both AI and cybersecurity. This talent shortfall can lead to misconfigurations and oversight, increasing vulnerability. Organisations should invest in upskilling their workforce and fostering interdisciplinary collaboration to bridge this gap.

Integration complexities, affecting 20% of organisations, highlight the challenges of seamlessly embedding GenAI into existing systems. These complexities can introduce new vulnerabilities and operational disruptions. A meticulous approach to integration, involving thorough testing and phased deployment, is essential to ensure security and functionality.

Budget constraints, reported by 22%, reflect the broader economic pressures facing many organisations. Allocating sufficient resources to secure GenAI applications is challenging but necessary. Cost-effective solutions, such as leveraging open-source tools and shared resources, can help mitigate budgetary limitations.

Finally, the lack of insight into the use of GenAI tools, identified by 19% of respondents, indicates a significant oversight in governance. Without visibility, organisations cannot effectively monitor or manage risks. Implementing comprehensive auditing and monitoring frameworks is crucial to maintain control and ensure compliance.

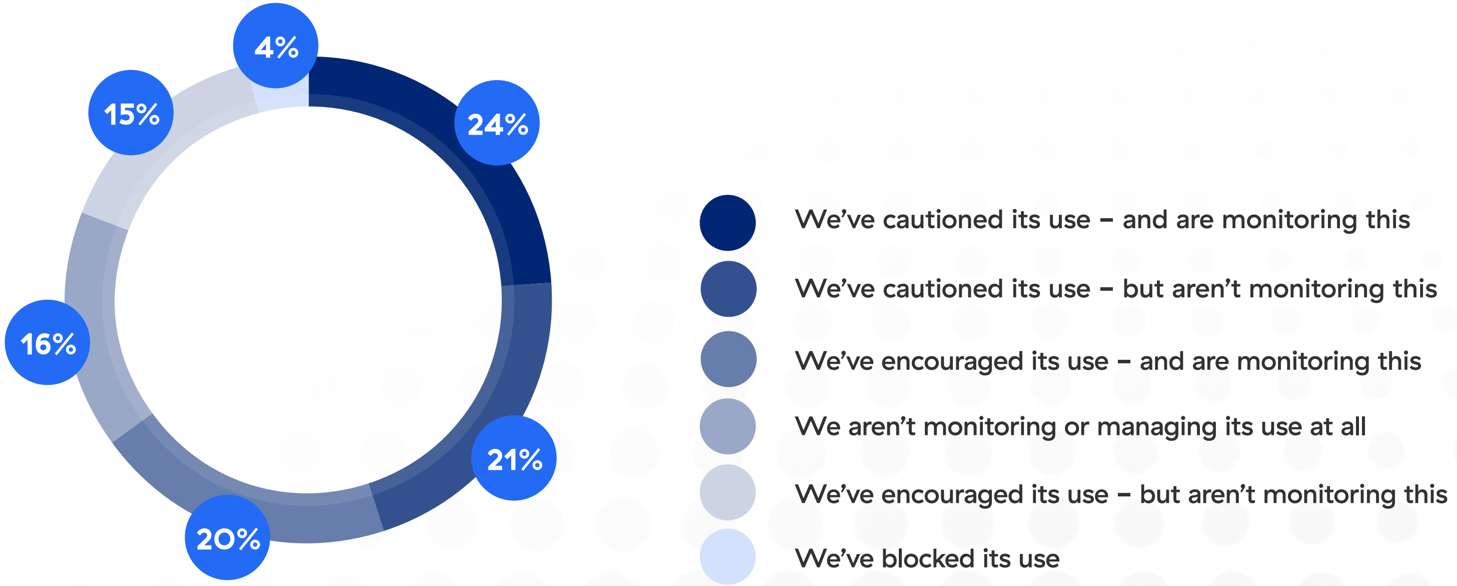
Securing Generative AI applications demands a holistic approach addressing awareness, expertise, integration, budget and visibility. By tackling these challenges, organisations can safeguard their assets and harness the full potential of GenAI technologies.



How are you currently managing employees’ GenAI tool (i.e. ChatGPT) usage within your organisation?

Key insights:

These statistics highlight diverse approaches to managing employees’ use of Gen AI tools like ChatGPT within organisations. Responses vary from blocking usage to encouraging it, with differing levels of monitoring. This variation reflects the ongoing balancing act between leveraging innovative tools and ensuring proper oversight to maintain security and compliance.

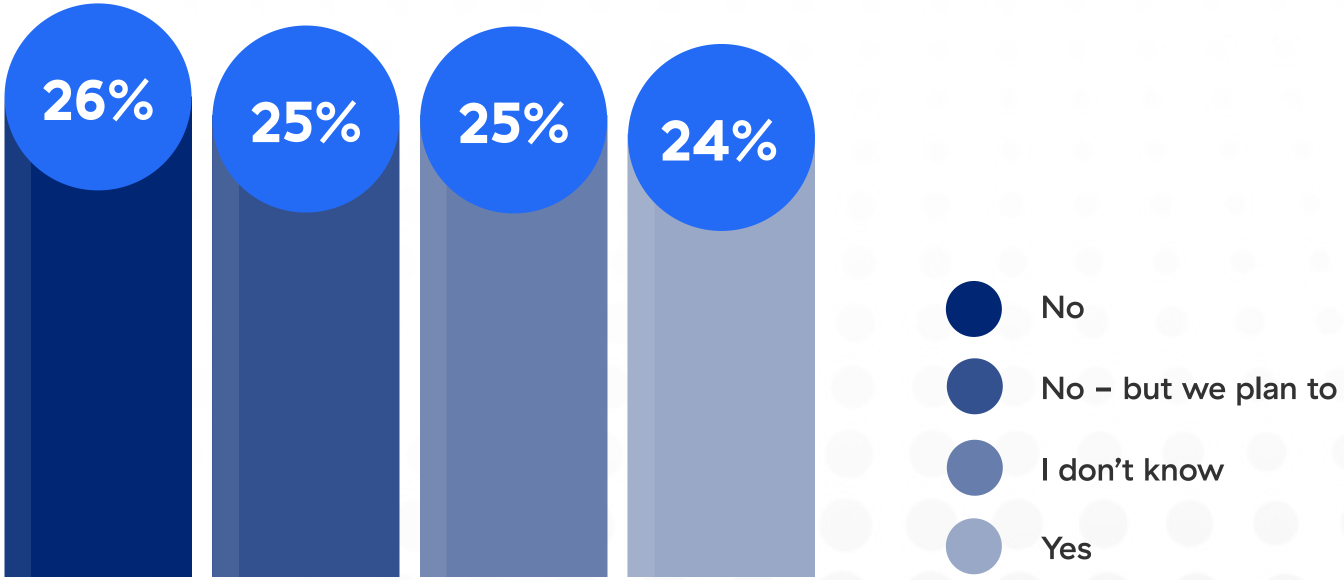


Part 1:
GenAI
and current
security landscape

Have you implemented any additional security measures to protect critical data with GenAI in mind (e.g. DLP, AI monitoring tools, etc.)?

Key insights:

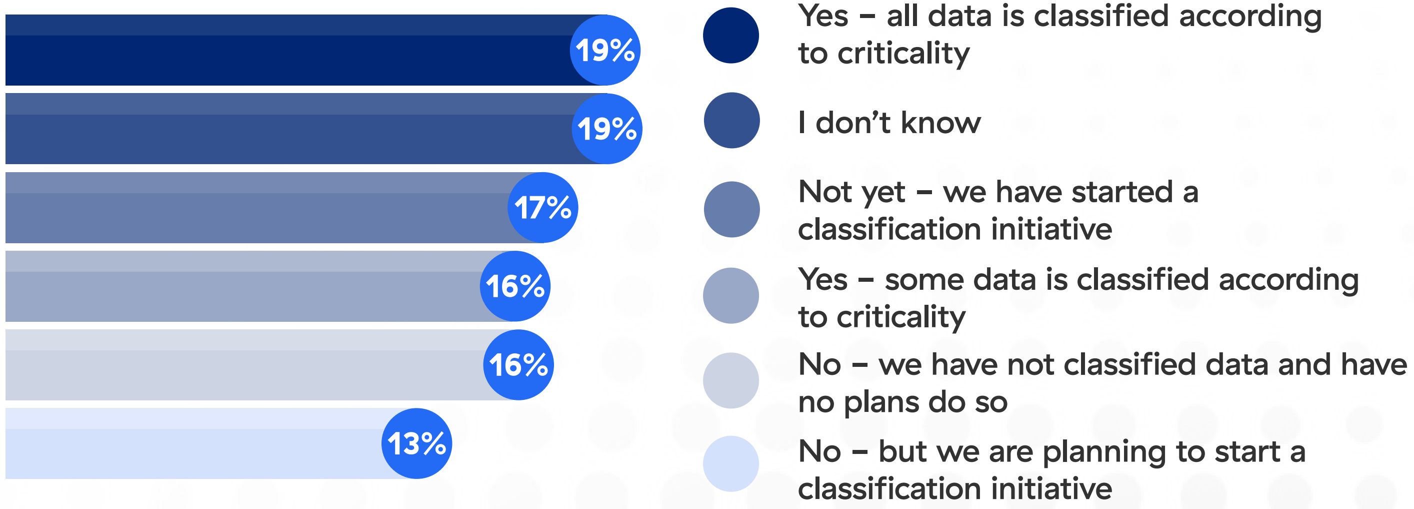
Reflecting varied responses, the data highlights organisations' approaches to implementing additional security measures for GenAI. While 24% have already done so, a quarter plan to, indicating recognition of the importance of safeguarding critical data. However, a significant portion remains undecided or has not taken action, suggesting potential gaps in security readiness.



Has your organisation categorised/classified its data according to criticality (e.g. in the course of a Zero Trust initiative)?

Key insights:

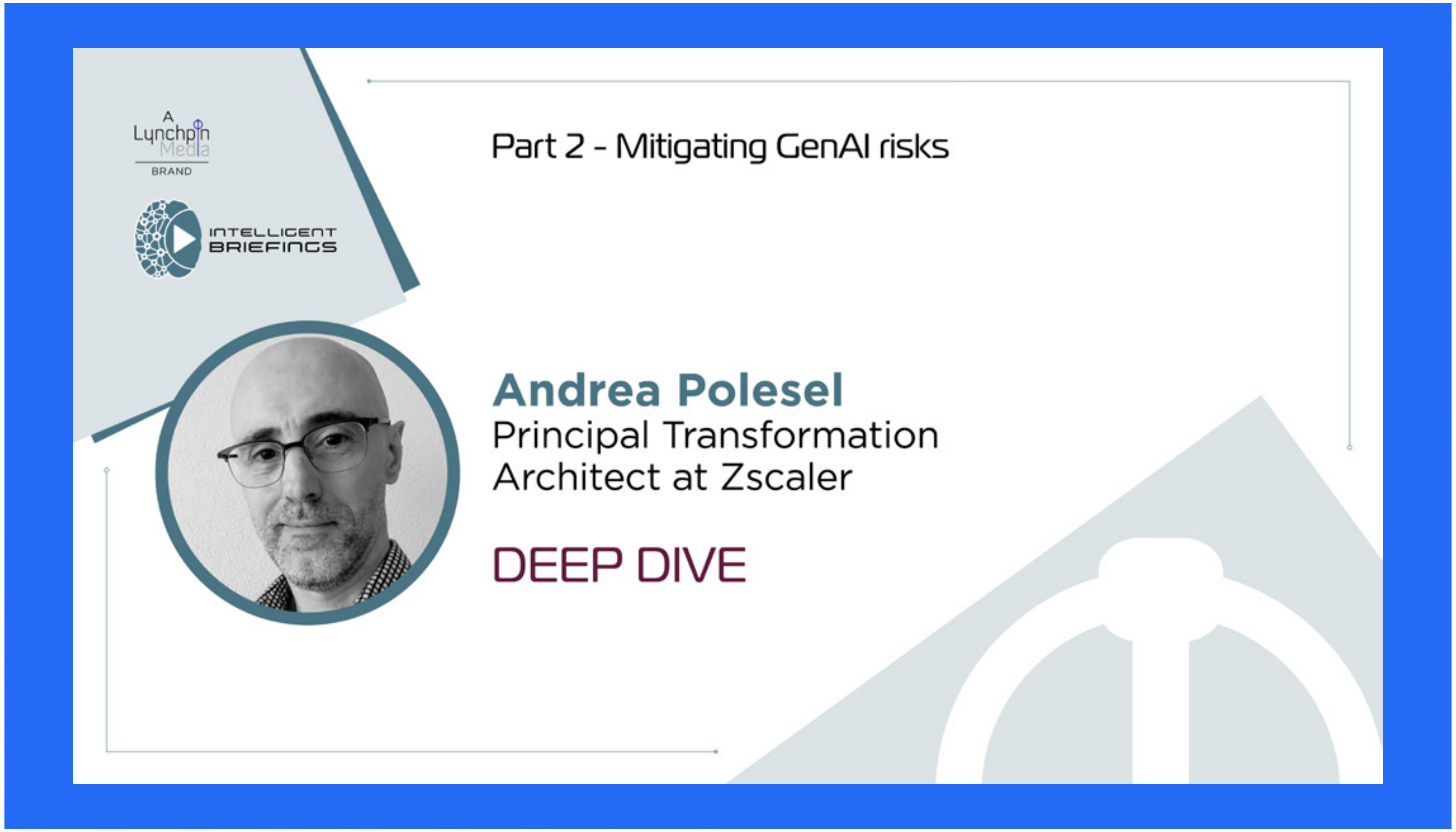
Responses reflect varying degrees of implementation of data classification practices, indicating differing levels of maturity in data management frameworks. This underscores the importance of robust data governance frameworks, especially in the context of Zero Trust initiatives and cybersecurity protocols.



VIDEO:
Part 2 – Mitigating GenAI risks

Throughout this video series, we unravel the relationship between Zero Trust and Generative AI with a dedicated episode to each of the key elements. Each segment draws attention to the varying aspects of AI and the tools that can make this technology safer for businesses. We focus on the specifics of Zscaler's approach and how the company plans to adapt its security measures to meet the challenges and opportunities.

CLICK/TAP the thumbnail to play the video . . .



Part 2 - Mitigating GenAI risks

Andrea Polesel
Principal Transformation Architect at Zscaler

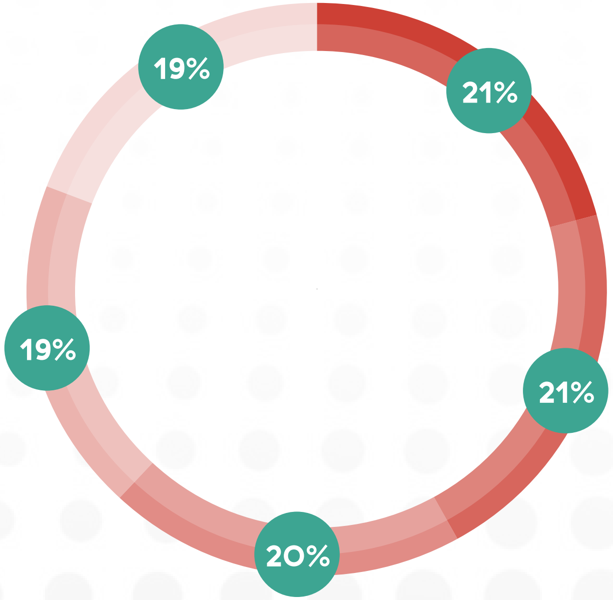
DEEP DIVE

Part 2: Regulations and priorities

● **How do you expect interest in using GenAI tools like ChatGPT to change during the rest of 2024?**

Key insights:

Responses indicate varied outlooks, suggesting uncertainty about the trajectory of GenAI interest. This uncertainty may stem from evolving technological landscapes or shifting organisational priorities, reflecting the dynamic nature of AI adoption in organisations and industries.



● Increase significantly

● Decrease somewhat

● Decrease significantly

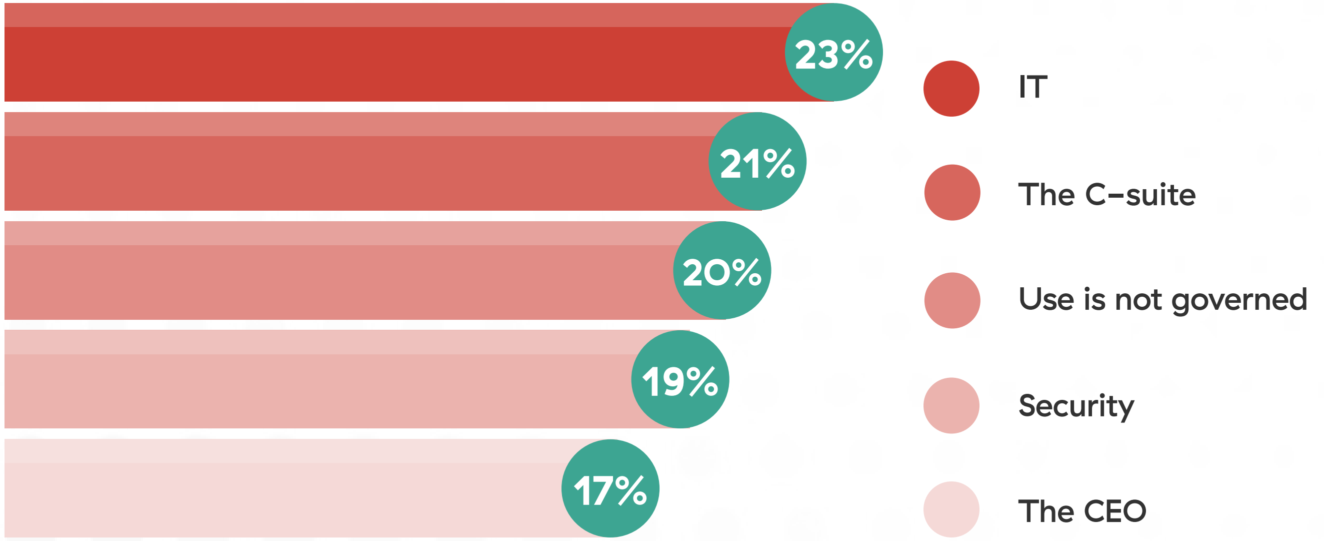
● Increase somewhat

● Neither increase nor decrease

Within your organisation, who primarily owns the decision making process around GenAI tool usage?

Key insights:

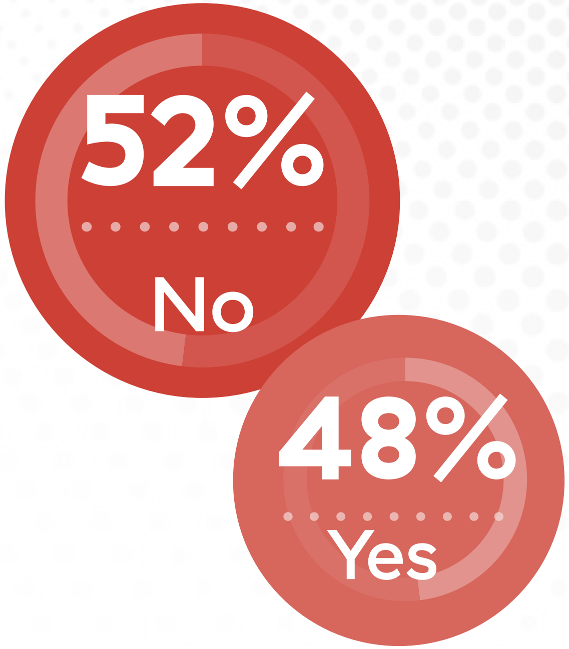
Responses depict a distributed landscape, with various stakeholders, including CEOs, IT and security teams, involved in decision-making. This highlights the collaborative nature of technology adoption and underscores the importance of cross-functional coordination in GenAI implementation strategies.



Have you read or reviewed the key provisions of the EU Artificial Intelligence Act (AI Act) with regards to GenAI?

Key insights:

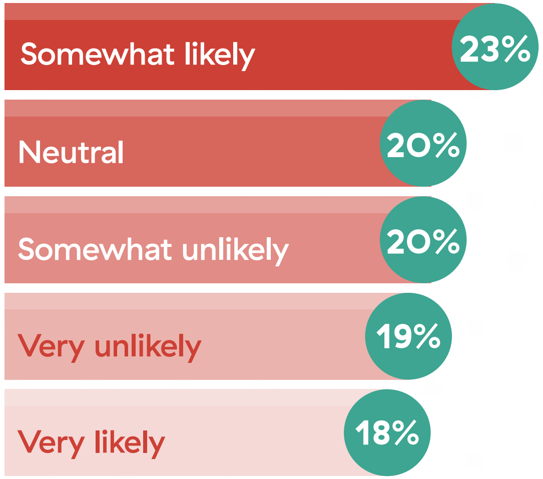
Responses indicate a mix of familiarity with the EU Artificial Intelligence Act, showcasing varying levels of engagement with regulatory frameworks. This highlights the importance of staying informed about evolving legal landscapes in AI governance.



How likely is your organisation to be impacted by the AI Act's regulations on GenAI?

Key insights:

Responses indicate varying perceptions of the potential effects of the AI Act on organisations, reflecting uncertainty and readiness for compliance. This highlights the need for proactive measures to adapt to evolving regulatory landscapes in AI governance.

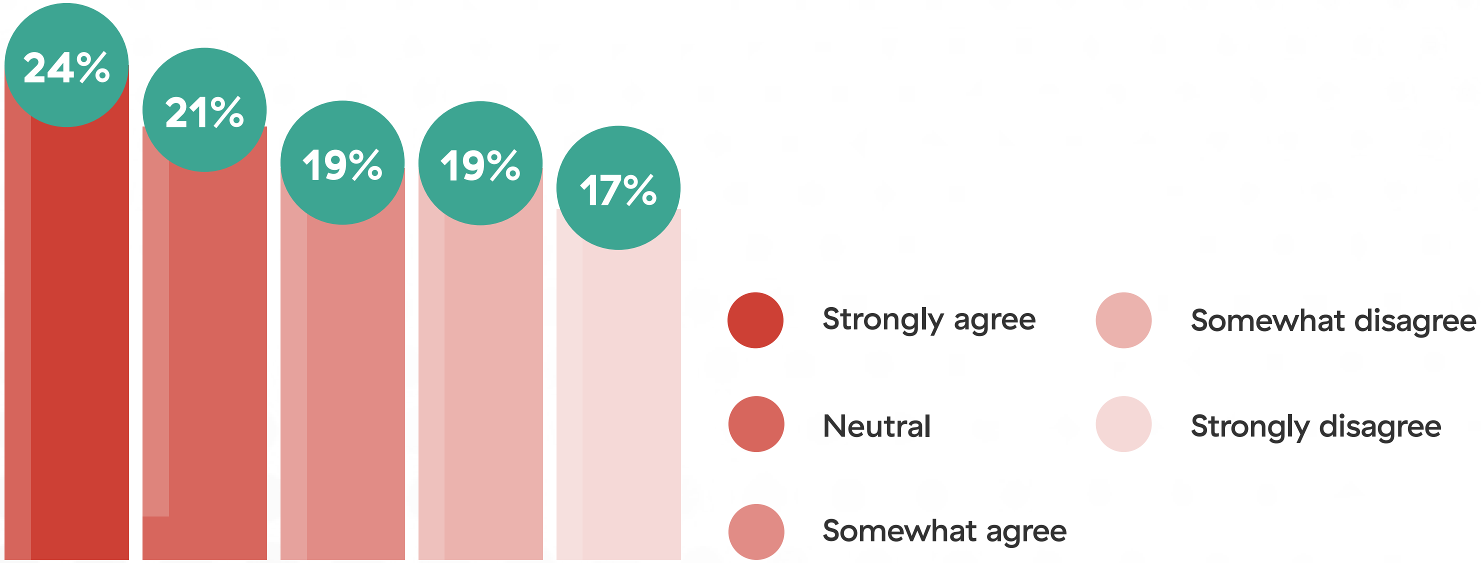


Part 2:
Regulations and priorities

Do you believe the AI Act provides sufficient security and guidance for organisations using GenAI technologies?

Key insights:

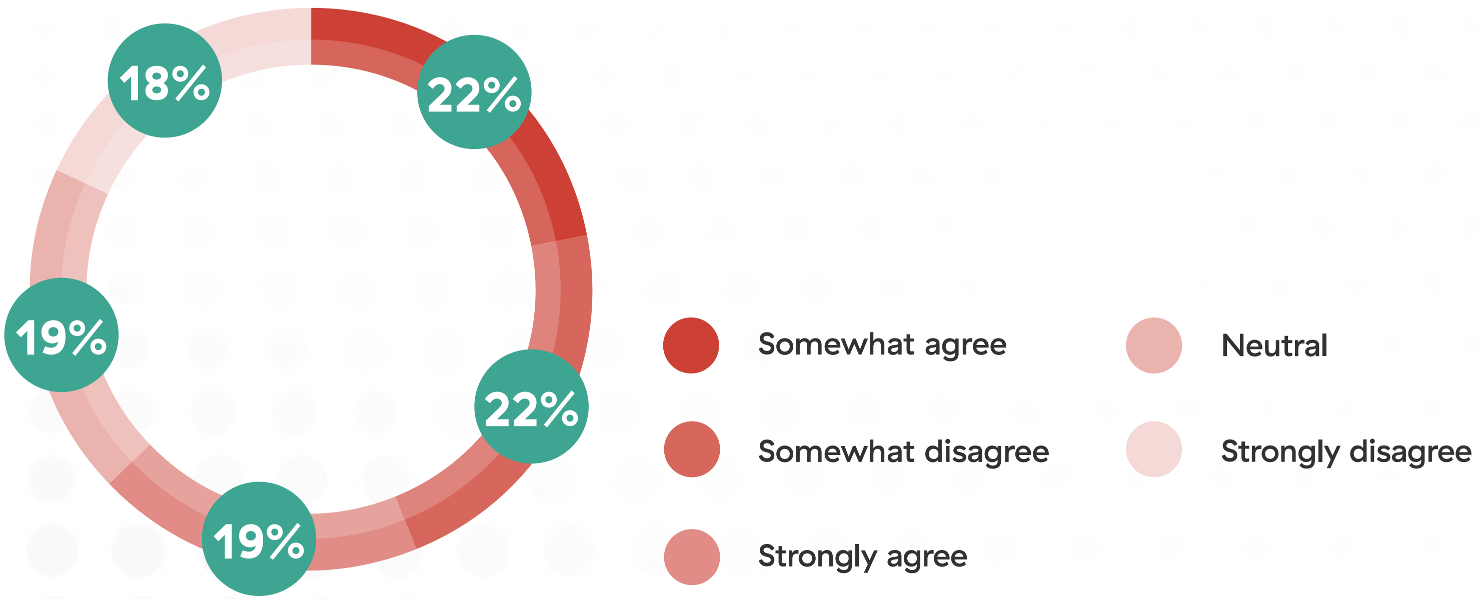
Responses showcase varying degrees of faith in the AI Act's efficacy, indicating diverse perspectives on the adequacy of security provisions. This underscores the complexity of balancing innovation with regulatory oversight and highlights the importance of ongoing dialogue between stakeholders.



To what extent do you agree with the statement “Additional regulations are needed to ensure the safe and secure use of GenAI”?

Key insights:

The data indicates that there is a nuanced understanding of how best to balance innovation and risk mitigation. This highlights the need for ongoing discussions about the appropriate regulatory framework to ensure responsible and secure GenAI deployment within organisations.



zscaler

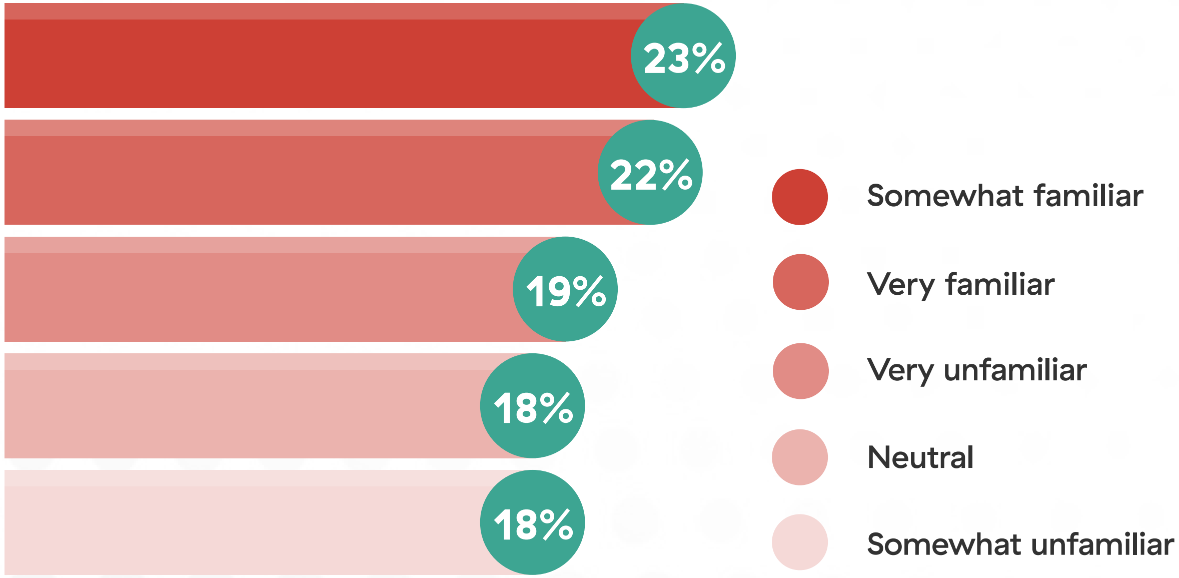
CXO priorities

A Lynchpin Media BRAND

How familiar is your organisation with the key aspects of the EU Network and Information Systems Directive 2 (NIS 2)

Key insights:

The responses reveal a mixed understanding of the EU Network and Information Systems Directive 2 (NIS 2) within organisations. While some are well-versed, others exhibit varying degrees of familiarity. This suggests a spectrum of awareness regarding cybersecurity regulations, highlighting the need for comprehensive education and compliance efforts across the board.

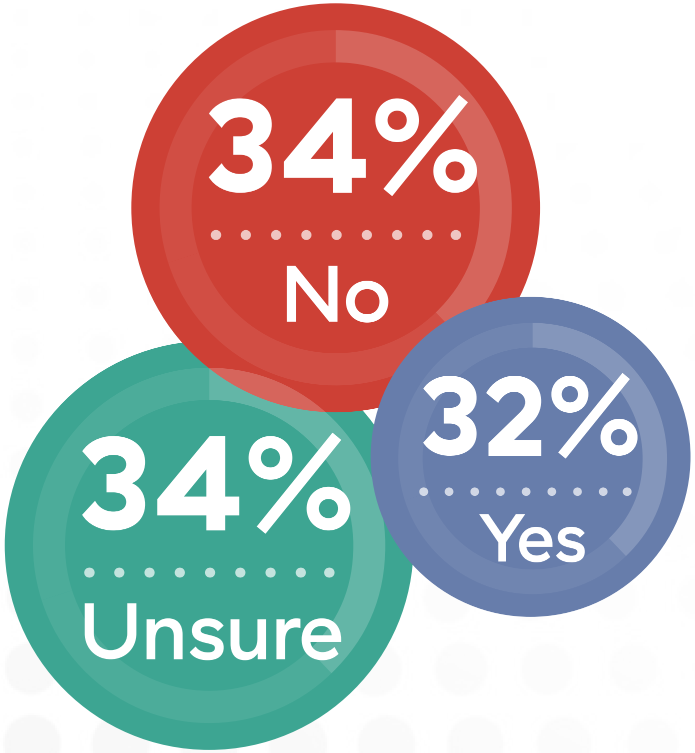


Part 2:
Regulations and priorities

Is your organisation already looking into the specific requirements of NIS2?

Key insights:

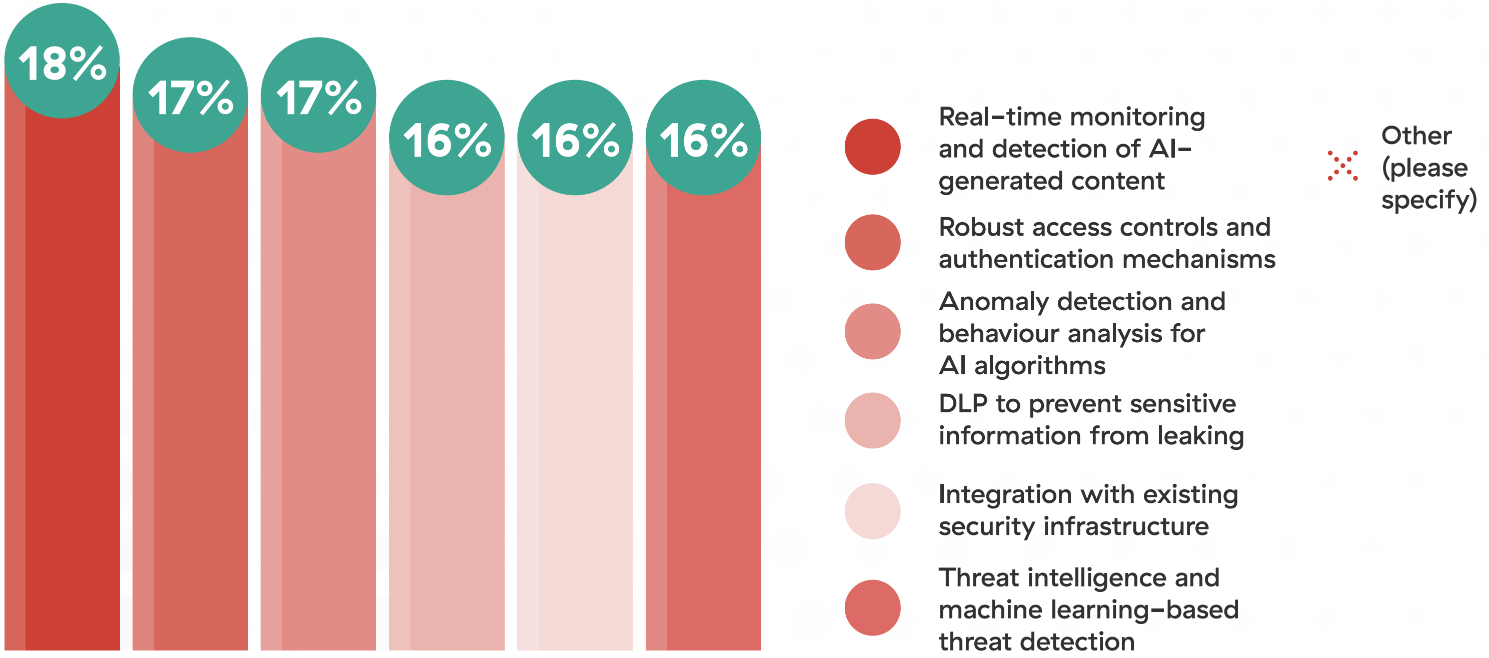
The survey uncovers a mixed understanding of the EU Network and Information Systems Directive 2 (NIS 2) within organisations. This signals a need for enhanced education and compliance efforts to navigate evolving cybersecurity regulations effectively and ensure organisational readiness.



What features or capabilities would you expect from a security solution designed to protect Generative AI technologies?

Key insights:

Themes emerge around proactive monitoring, data protection, access control, anomaly detection, integration and threat intelligence. This demonstrates the multifaceted approach required to address the unique risks posed by AI-generated content, advocating for comprehensive and adaptive security strategies.



What are your top two investment areas for the year ahead?

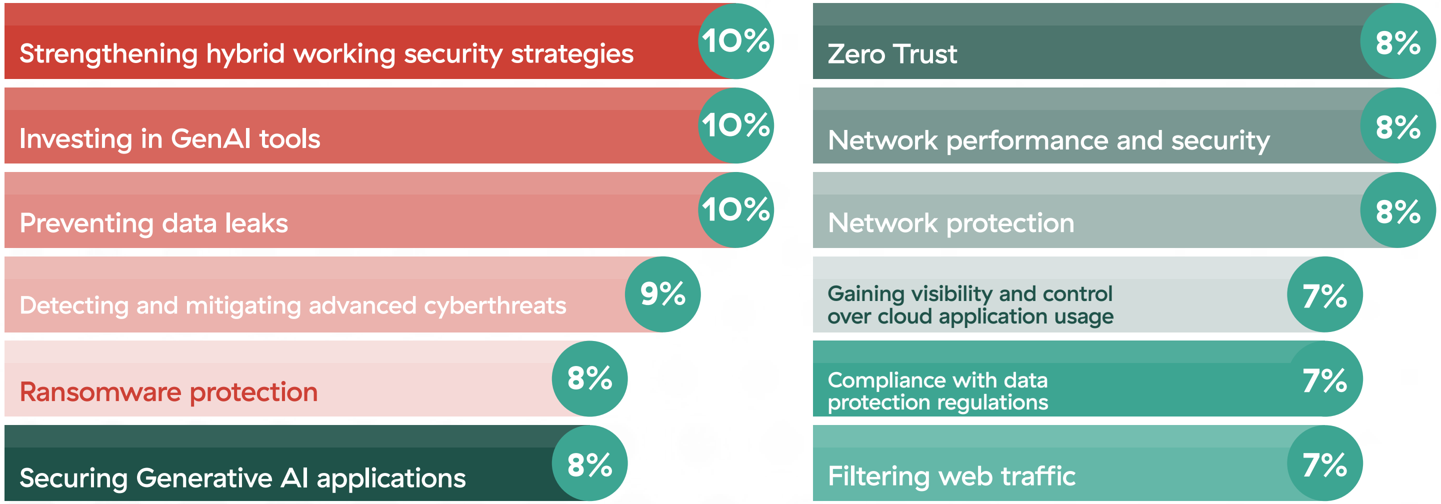
Key insights:

In the year ahead, organisations are prioritising investment in strengthening hybrid working security strategies (10%) and preventing data leaks (10%). The emphasis on hybrid working security reflects the broader trend of remote and flexible work environments becoming the norm. With employees accessing corporate networks from diverse locations, the attack surface has significantly expanded. Investing in strengthening hybrid working security strategies is crucial to safeguarding sensitive data and ensuring secure access to organisational resources.

This involves implementing advanced endpoint protection, secure VPNs and comprehensive identity and access management solutions to mitigate risks associated with remote work.

Preventing data leaks, also prioritised by 10% of organisations, underscores the growing concern over data breaches and loss. As data volumes increase and regulations tighten, organisations must invest in data loss prevention (DLP) technologies, encryption and secure data handling practices. The cost of data breaches, both financial and reputational, necessitates a proactive approach to data security. This focus aligns with the broader trend of heightened regulatory scrutiny and the need for stringent compliance with data protection regulations.

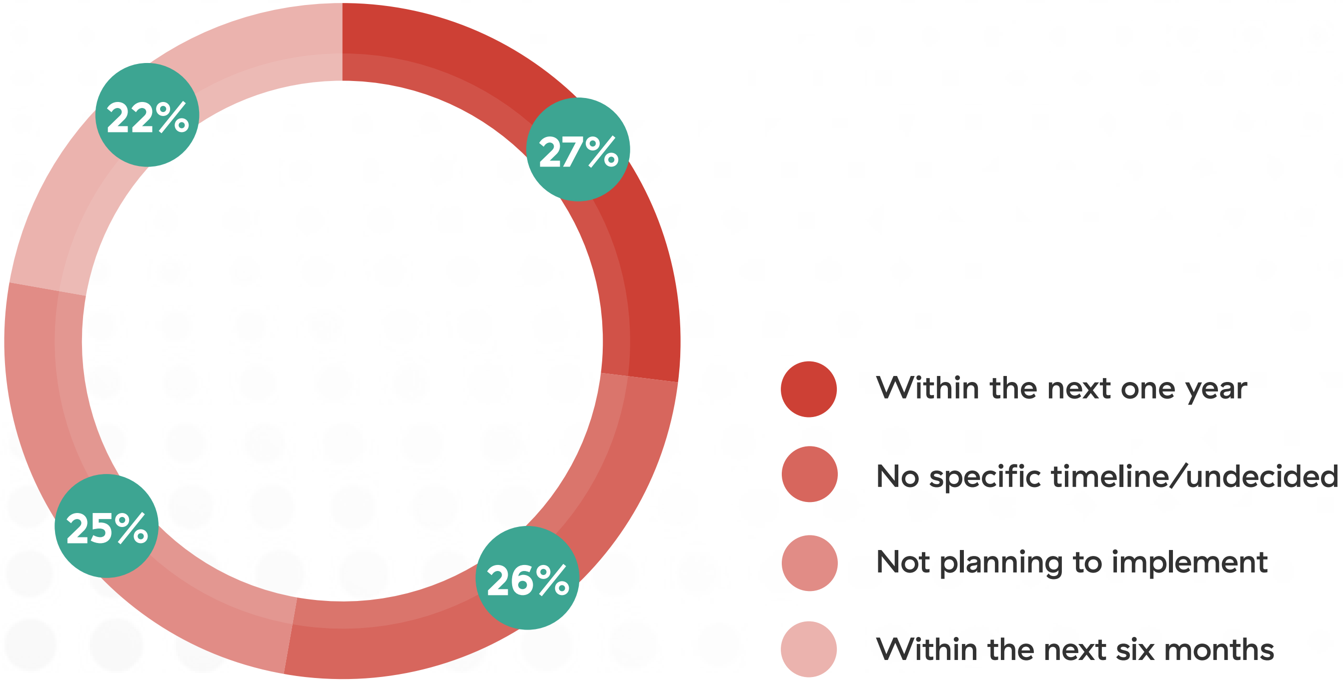
Overall, these investment priorities highlight the evolving cybersecurity landscape, where protecting a dispersed workforce and safeguarding sensitive data are paramount. By addressing these areas, organisations can enhance their security posture and resilience against emerging threats.



When does your organisation plan to implement security measures specifically designed for Generative AI applications?

Key insights:

Respondents present a spectrum of readiness, with varied planning horizons and a significant portion undecided or not planning implementation. This stresses the evolving nature of AI security considerations and the need for strategic foresight in cybersecurity planning.


22%
27%
25%
26%
Within the next one year
No specific timeline/undecided
Not planning to implement
Within the next six months

VIDEO:

Part 3 – How can Zero Trust and Zscaler make the adoption of GenAI safer

Throughout this video series, we unravel the relationship between Zero Trust and Generative AI with a dedicated episode to each of the key elements. Each segment draws attention to the varying aspects of AI and the tools that can make this technology safer for businesses. We focus on the specifics of Zscaler's approach and how the company plans to adapt its security measures to meet the challenges and opportunities.

CLICK/TAP the thumbnail to play the video . . .

Part 3 - How can Zero Trust and Zscaler make the adoption of GenAI safer

Andrea Polesel
Principal Transformation Architect at Zscaler

DEEP DIVE

VIDEO:
Part 4 – Zscaler Gen AI survey

Throughout this video series, we unravel the relationship between Zero Trust and Generative AI with a dedicated episode to each of the key elements. Each segment draws attention to the varying aspects of AI and the tools that can make this technology safer for businesses. We focus on the specifics of Zscaler's approach and how the company plans to adapt its security measures to meet the challenges and opportunities.

CLICK/TAP the thumbnail to play the video . . .

A Lynchpin Media BRAND

INTELLIGENT BRIEFINGS

Part 4 - Zscaler Gen AI survey

Andrea Polesel
Principal Transformation Architect at Zscaler

DEEP DIVE

Conclusion

The report sheds light on the evolving landscape of Generative AI (GenAI) tools and the challenges and opportunities they present for organisations. With a significant portion of respondents indicating a growing interest in GenAI applications, it's evident that these tools are gaining traction across various sectors. However, this interest is accompanied by concerns regarding security risks and regulatory compliance, particularly considering the EU Artificial Intelligence Act (AI Act) and the Network and Information Systems Directive 2 (NIS 2).

Organisations are increasingly aware of the need to implement robust security measures to protect against potential threats introduced by GenAI tools. Concerns such as the manipulation of AI algorithms and unauthorised access to sensitive data highlight the importance of adopting a proactive approach to cybersecurity.

A solutions provider that specialises in Zero Trust architecture and can effectively mitigate the risks introduced by GenAI will undoubtedly lead the market. By prioritising real-time monitoring, robust access controls and anomaly detection, such a provider can help organisations protect their data and employees from emerging threats.

Furthermore, as organisations navigate the complexities of regulatory compliance, solutions that offer comprehensive security features and guidance will be in high demand. The ability to integrate AI-driven security tools seamlessly into existing infrastructure and provide ongoing support and education will set providers apart in a competitive market.

In this rapidly evolving landscape, organisations must focus on protecting their data and employees from emerging threats introduced by GenAI tools. By embracing a Zero Trust approach and partnering with a solutions provider that specialises in in making the adoption if GenAI safer, organisations can ensure they are well-equipped to navigate the challenges of the digital age and stay ahead of evolving threats.

> “The ability to integrate AI-driven security tools seamlessly into existing infrastructure and provide ongoing support and education will set providers apart in a competitive market.

A Lynchpin Media BRAND

Lynchpin Media is a global technology media, data and marketing services company. We help to increase awareness, develop and target key accounts and capture vital information on regional trends. Visit **lynchpinmedia.com** for more information.

CxO Priorities, a Lynchpin Media Brand

63/66 Hatton Garden
London, EC1N 8LE

Find out more: **www.cxopriorities.com**

Sponsored by

www.zscaler.com