zscaler™

Principle networks

WHITE PAPER

State of Cyberthreat and Protection

Abstract: This report analyzes the results of a ViB survey commissioned by Zscaler, that asked IT and security professionals for their views on the most serious threats they face, digital transformation journey, challenges with VPNs, investment in AI, and zero trust. It explores how these issues and trends affect IT and security professionals' outlook for the future. Respondents have serious concerns about worsening threats, but they are hopeful that technologies like AI and zero trust will make a difference going forward—a sentiment reflected in plans to increase budgets in the coming year.

Introduction

IT and security teams today are navigating a landscape filled with diverse and often conflicting pressures. Digital transformation initiatives continue to gather pace, with organizations wholeheartedly adopting cloud-based security tools, migrating applications to the cloud, and implementing cloud-delivered zero trust frameworks. Simultaneously, businesses must grapple with increasingly sophisticated cyberthreats that are becoming more challenging to defend against. This escalating difficulty is largely due to the expanding and intricate enterprise attack surface, which now encompasses cloud environments, SaaS applications, web services, endpoints, generative AI tools, email, and more.

This report, based on a survey conducted by ViB and sponsored by Zscaler, delves into the multifaceted pressures faced by IT and security teams today, providing valuable insights into how organizations can effectively manage and protect their digital assets. It offers a compelling exploration of IT and security professionals' perspectives on the most pressing cyberthreats they encounter, along with their strategic investment plans to counter these risks. Notably, artificial intelligence (AI) stands out as a double-edged sword—while it can exacerbate threats, it also presents a powerful avenue for enhancing security measures. Additionally, the report underscores the growing allure of zero trust as a transformative approach to safeguarding digital assets, offering a more robust and future-proof defense strategy.

Demographic Overview

Zscaler surveyed 227 IT and security professionals for this report. Respondents worked in a variety of industries, primarily in North America, with 19% coming from manufacturing, 15% from healthcare, and 11% from colleges and universities. Organization sizes ranged from 1,000–2,499 employees to over 10,000. Forty-two percent of respondents are in Manager roles, while 39% are Directors. 86% percent either make or influence decisions about cybersecurity strategies and investments. A full breakdown of survey respondent demographics can be found in the Appendix.

The Evolving Threat Landscape

The cyberthreat landscape continues to pose new and dynamic challenges for defenders. 2024 has witnessed a steady pace of attacks, with some stunning incidents like the AT&T data leak, which led to the exposure of 73 million customer accounts, and the theft of 560 million records from Ticketmaster. The latter breach was caused by attacks on Snowflake customer accounts using compromised credentials.

Ransomware remains among the most impactful of attack vectors, with targets including some of the world's highest-profile brands. Zscaler ThreatLabz 2024 Ransomware Report disclosed a ransom payment to Dark Angels, a ransomware group of a record-breaking $75 million in the first half of 2024—higher

than any publicly known amount. From 2023 to now, ThreatLabz identified a 17.8% growth in ransomware attacks blocked in the Zscaler cloud and 57.8% growth in extorted companies on data leak sites.

Advances in AI have led to the technology playing a greater role in cyberattacks than ever before. Criminals used AI-produced "deepfake" videos to defraud a Hong Kong firm of $25 million. Generative AI (GenAI) is capable of creating effective phishing emails and enabling other modes of social engineering. This is expected to further exacerbate phishing attacks which already grew by 58% in 2023. Malicious actors are also using AI to find vulnerabilities more easily than was previously possible.

What's Keeping Security Practitioners Awake at Night?

The threat landscape is a source of worry for security practitioners. In their day-to-day work, though, sources of concern are more pragmatic. They range from issues related to business and technology, such as digital transformation and VPN security, to economic factors, budget, and the like.

Business Transformation Is Driving Increased Complexity and Risk

Technology and security are ultimately about business. Technology enables the business to operate and achieve its objectives. Security is about protecting digital assets so the business can function. The challenge for practitioners is that technology, business, and security never stand still. New technologies, new business requirements, and expectations keep practitioners constantly busy—and worried.

Digital Transformation

Digital transformation is no longer a choice but a necessity in today's rapidly evolving business landscape. Driven by a confluence of technological advancements and shifting work dynamics, this revolution is reshaping how organizations operate, collaborate, and innovate. At its core, digital transformation is about leveraging technologies like cloud computing, mobile devices, and high-speed networks to streamline processes, enhance productivity, and unlock new opportunities. As applications migrate to the cloud and employees work from anywhere on a variety of devices, the traditional data center is giving way to a more distributed, interconnected ecosystem. This shift not only simplifies IT management but also empowers organizations to be more agile, responsive, and competitive in an ever-changing market. A striking 82% of respondents reported that they have one or more active and ongoing digital transformation initiatives. Just 2% said they had no plan to start a digital transformation initiative before 2025.

Specifically, these initiatives involved adopting cloud security tools and infrastructure for 57% of respondents. Forty-three percent said they were moving applications to the cloud as part of their Digital Transformation. Twenty-nine percent said they were adopting a zero trust network architecture (ZTNA).

On the other hand, digital transformation has broadened the attack surface, offering more avenues for threat actors. The growing complexity of IT environments can result in misconfigurations and vulnerabilities, which can be exploited by malicious actors. Moreover, the swift pace of digital change often outpaces the capacity of security teams to maintain comprehensive protection, leading to security gaps. Data privacy issues are also exacerbated, as sensitive information is disseminated and stored across various platforms and locations.

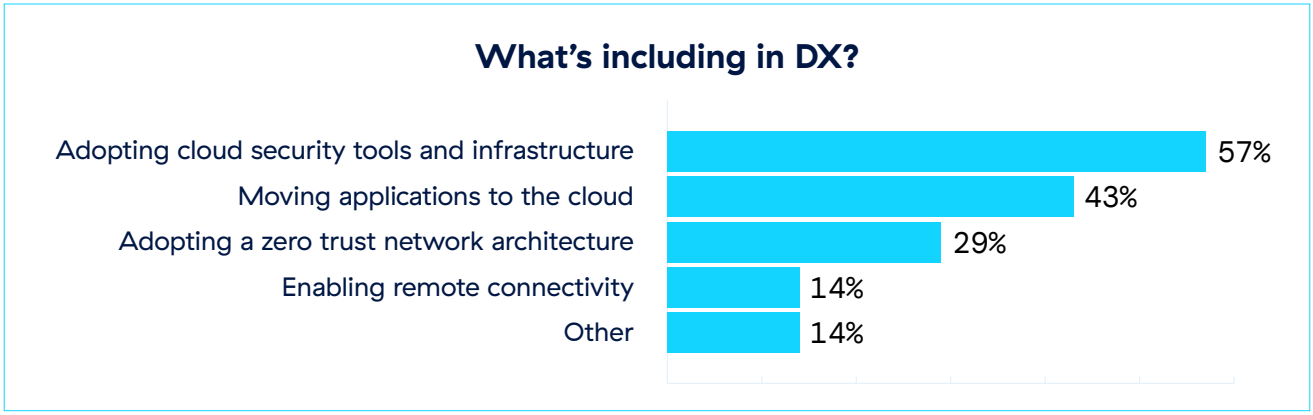


Figure 1 – Responses to the question "Which of the following items are included in your organization's digital transformation (DX)?"

VPN Security Issues

The VPN is emerging as a major point of risk. According to Zscaler ThreatLabz research, 56% of organizations experienced an attack that took advantage of security vulnerabilities on VPN servers. 2024 has been a year of VPN vulnerabilities getting exploited, again and again. For instance, multiple zero-day vulnerabilities in Ivanti's VPN products were exploited by Chinese state-backed hackers taking advantage of flaws described in CVE-2023-46805 and CVE-2023-21887. The adversaries used these vulnerabilities to perform authentication bypass and remote command injection. Once these flaws were patched, attackers bypassed the fixes by leveraging other vulnerabilities (CVE-2024-21888). The workarounds used to circumvent the initial patch allowed attackers to enable privilege escalation and perform server-side request forgery. In February 2024, CISA released another VPN-related alert about an attack on Cisco's Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD). In this case, the Akira ransomware group exploited a vulnerability (CVE-2020-3259) to steal information by leveraging misconfigured instances of WebVPN/AnyConnect. These repeated zero day attacks on VPN show that the real issue is the outdated architecture, not the specific vendors involved.

Survey responses reflected this ominous reality. Twenty-three of respondents expressed that they were "very" or "extremely concerned" about VPN risks and vulnerabilities. One in four are planning to move off of VPN in the next 12 months. Smaller enterprises, perhaps due to lower technical debt and less complex infrastructure, are more likely to have a plan for migrating off of VPN. Two thirds of smaller enterprises (1,000-2,499 employees) have a plan to get off VPN versus just 11% of companies with over 10,000 employees. This discrepancy may be due to inertia at large organizations and the difficulty of making such a major change.

Economic Factors

56% of respondents say that economic uncertainty in 2024 has impacted their organizations' IT/security budgets. In terms of specific impact, for 46% of respondents, economic uncertainty translated into budget cuts. Attrition (18%) and redundancy (14%) were also effects of economic uncertainty.

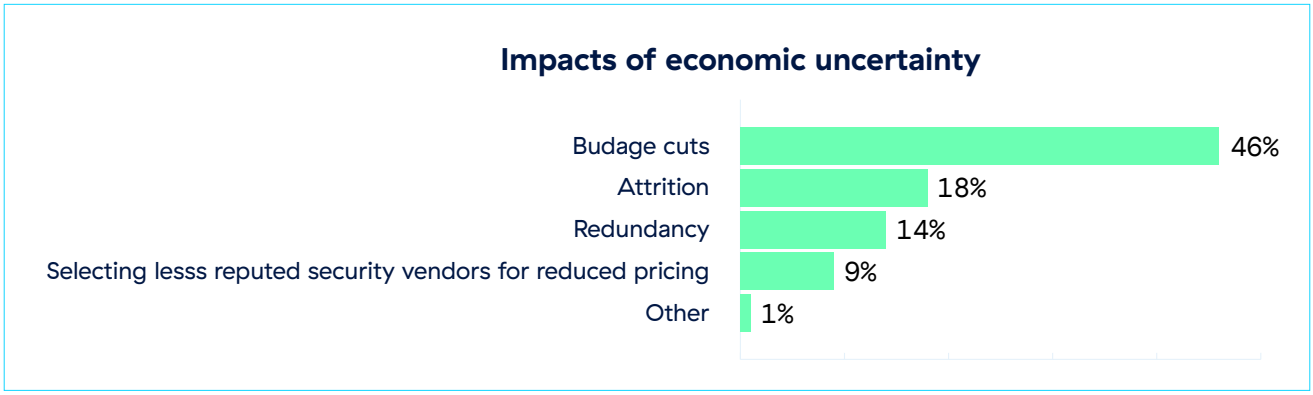


Figure 2 – Responses to the question "What impact did economic uncertainty have on the IT and Security teams?"

Despite this economic uncertainty, budget cuts remain temporary for many organizations. The need for security improvements will drive many enterprises to increase spending next year. Looking ahead, when asked "How, if any, do you expect your security budget to change this year compared to last year?" 54% replied that they would be increasing their budgets. For 19% of respondents, budgets are to increase by over 10%.

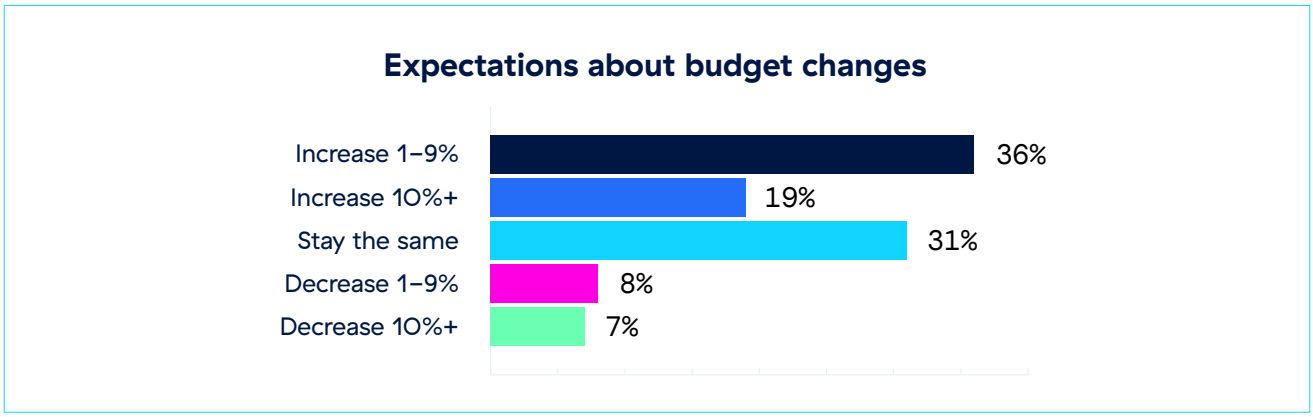


Figure 3 – Responses to the question "How, if any do you expect your security budget to change this year compared to last year?"

Types of Threats They Are Worried About

Security practitioners are anxious about a wide range of threats. Ransomware is certainly top of mind, and was listed as a top cyberthreat concern by 72% of respondents. The Zscaler ThreatLabz 2024 Ransomware Report shows that ransomware attacks will continue to grow more advanced and persistent. What's worse is that it's become increasingly clear that no one is spared as cybercriminals have gone so far as to target the children of corporate executives to force ransom payments.

Phishing (69%) and zero day exploits (48%) were also among the top most concerning cyberthreats. The Zscaler ThreatLabz team observed that phishing threats have reached unprecedented levels of sophistication in the past year, driven by the proliferation of generative AI tools. Transforming how

cybercriminals operate, AI advancements are revolutionizing and reshaping the phishing threat landscape. Moreover, this technology has democratized the ability to orchestrate intricate phishing campaigns, making it easier than ever for even beginners to conduct complex and believable phishing attacks. Specifically, this observed shift is enabling novice cybercriminals to launch highly convincing, personalized scams with ease. As a result, organizations now face a myriad of new challenges in protecting their data and systems from the increasing onslaught of phishing attacks. As the figure shows, the list of threats that cause alarm is quite long.

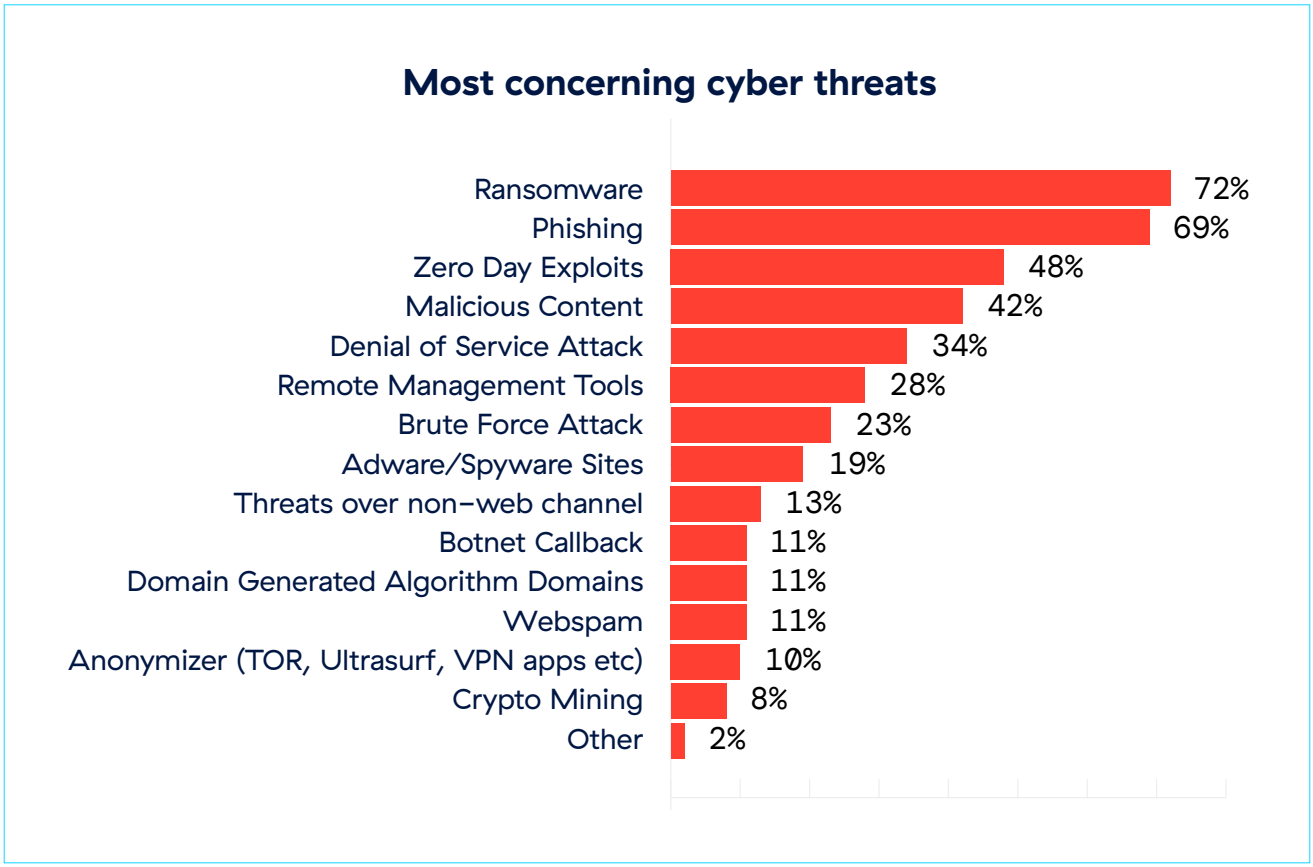


Figure 4 – Responses to the question "What are the cyberthreats that are concerning you the most?" (select all that apply)

External attackers are not the only source of worry, either. Insiders are a significant cause of concern. Thirty-three percent of respondents are either "very" or "extremely concerned" about insider threats. These include malicious as well as non-malicious insiders. As security professionals know, employees can often cause risk exposure by making mistakes with security settings or neglecting to follow security policies.

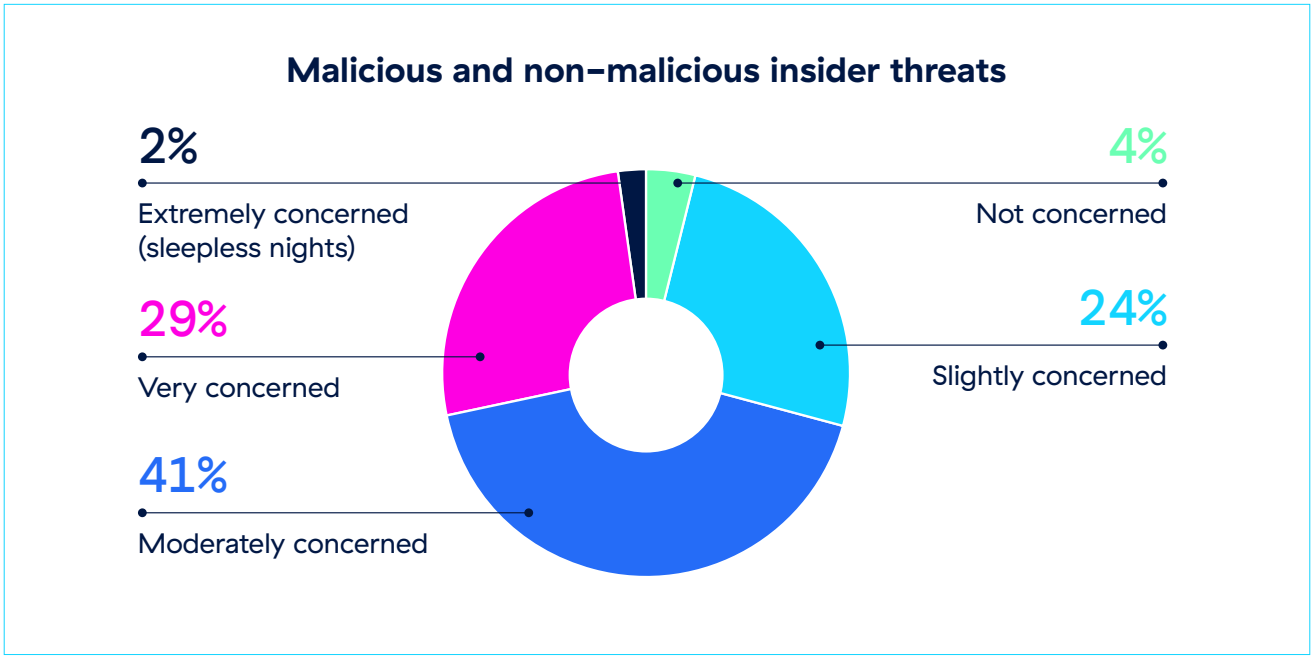


Figure 5 – Responses to the question "How worried are you about malicious and non-malicious Insider Threats?"

Investment Priorities

Given the various threats and areas of concern, how are respondents planning to invest in security going forward? Data security is again the high priority, with 64% of respondents making it their investment category for this year and next year. The emphasis on data security is understandable. After all, data is the ultimate target for ransomware and exfiltration hacks, so it is wise to invest in defending it. Also, given that organizations are looking to securely enable AI tools while protecting enterprise data.

Another top area of investment for security leaders is zero trust. Nearly half of the respondents (45%) say they are planning to invest in zero trust in the future. In fact, Zscaler ThreatLabz 2024 VPN Risk Report with Cybersecurity Insiders found that nearly 78% of organizations plan to implement a zero trust strategy in the next 12 months in response to increasing exploits.

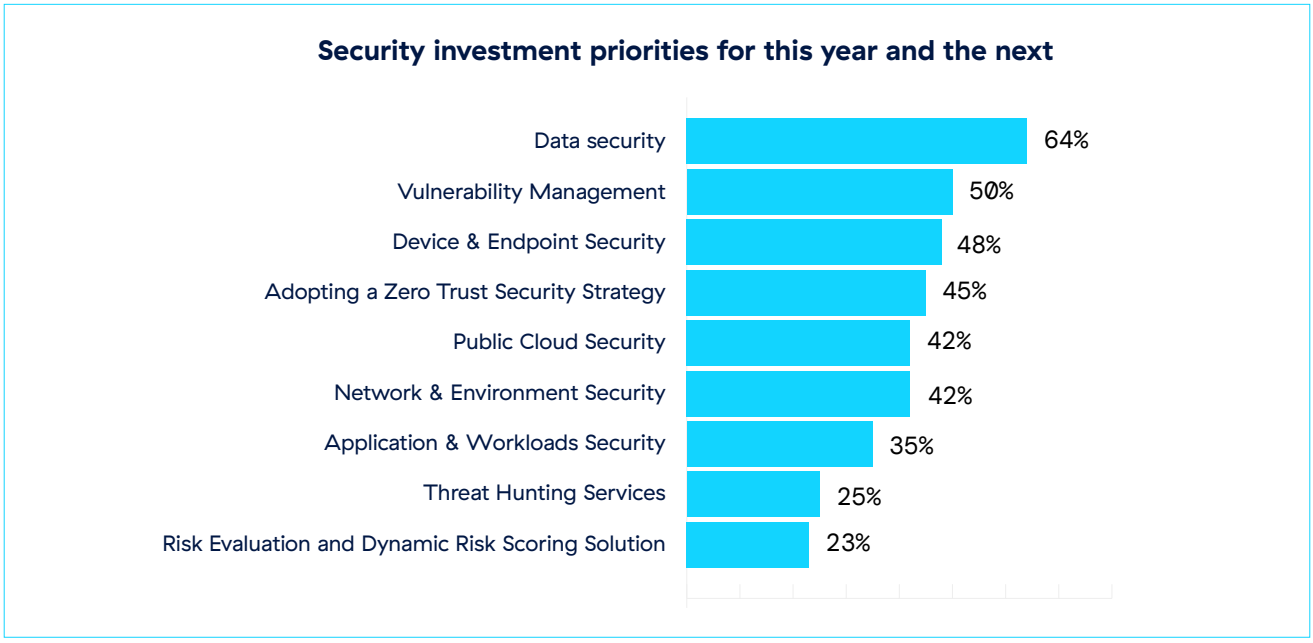


Figure 6 – Responses to the question "Which of the following are your security investment priorities for this year and the next?" (select all that apply)

Organizations seek to consolidate security tools to reduce complexity and improve security outcomes

As security professionals everywhere will relate, our survey found that an excess of security tools is a driver of various problems. Simple tool sprawl is an issue, as is integration between tools. Too many tools means poor visibility into cyber risk data. Reporting is a challenge, as well.

Tool Sprawl

Respondents are worried about tool sprawl, which is the common phenomenon of having more security tools than a department can easily handle. No fewer than 62% of respondents said they were worried about tool sprawl. This is a bigger problem for big companies, with 64% of respondents at companies with over 10,000 employees saying they worry about tool sprawl vs. 50% at companies with 1,000 to 2,499 employees. This makes sense, given that big companies typically have more money to spend on tools, as well as larger, more complex organizations. Mergers and acquisitions (M&A) can compound the problem by combining separate corporations, each of which brings its legacy toolset to the new entity.

Respondents use an average of 15 security tools a day, though some use 50 or even 100. The good news is that organizations seem to be taking action to control this. Of the 62% of respondents who said they worried about tool sprawl, 58% said they plan to consolidate vendors.

Lack of Visibility

Respondents shared that they lacked visibility into cyber risk data. This was expected, as siloed security tools and manual processes paint an incomplete picture of cyber risks and give no meaningful way to remediate them. Sixty-two percent said either "no" they did not have complete visibility or they were "not sure."

It is also worth noting that standalone security risk tools and point products, as well as the manual processes that accompany them, make it impossible for security leaders to holistically assess risks and thoroughly investigate them. As such, more businesses are being disrupted, brands are more vulnerable to damage, and the risk of long-term financial impact has never been higher. No wonder cybersecurity risk management has become a board-level priority.

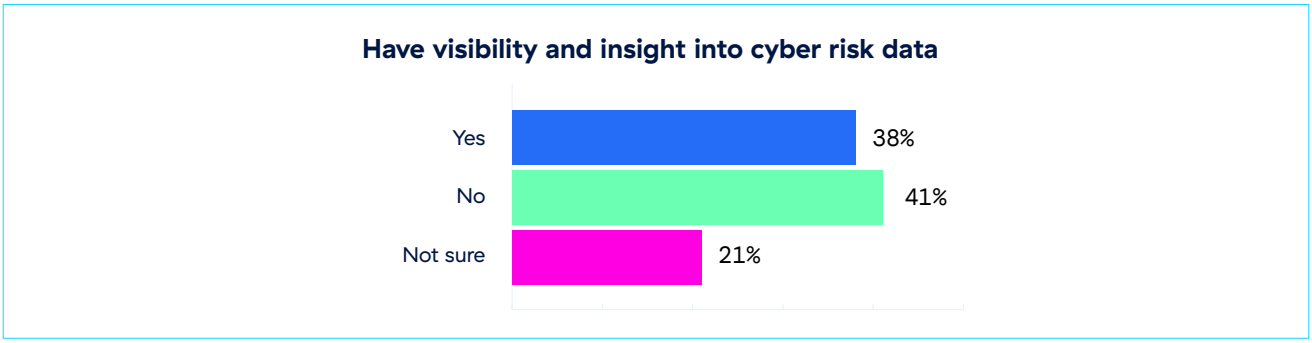


Figure 7 – Responses to the question "Do you have complete visibility and insight into cyber risk data?"

Reporting Challenges

Reporting is a challenge for many respondents.

Asked, "Do you have any framework/solutions in place to consolidate, quantify and visualize risk across your entire IT environment?" 57% said "yes." It also seems that bigger companies are more likely to have a framework/solution in place to consolidate tools. (58% of 10,000+ companies vs. 45% of 1,000-2,499 organizations.)

For the 42 % who said they lacked a framework to consolidate, quantify or visualize risk data, 63% of them said their teams faced challenges for security risk reporting. These barriers to security risk reporting are likely due to having too many tools. It's difficult to generate coherent, complete reports with inputs from multiple tools. Standalone security tools and manual processes hinder security leaders from comprehensively assessing and investigating risks.

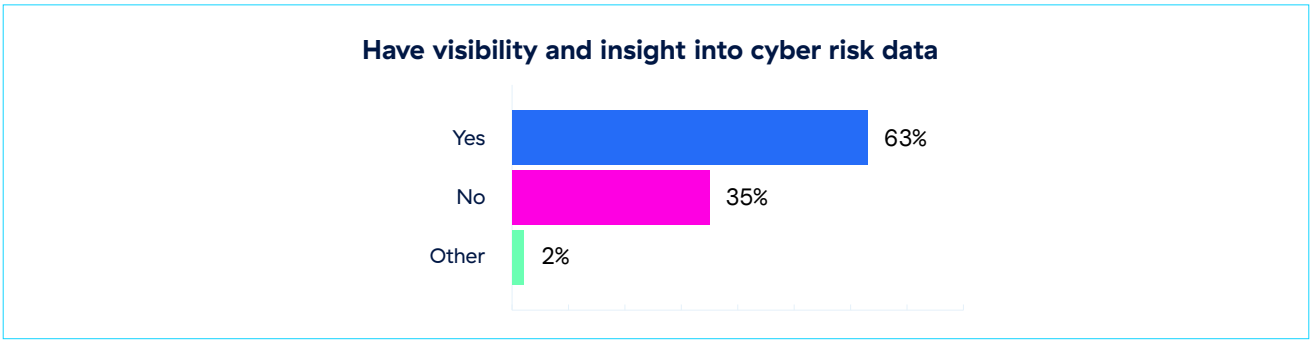


Figure 8 – Of the 42% of respondents who said "No" they didn't have any framework/solutions in place to consolidate, quantify and visualize risk across their entire IT environments, 63% said they face challenges for security risk reporting.

Integration Challenges

Challenges with tool integration are implied by the survey findings. The sheer number of tools in use poses massive management challenges, and often leads to incomplete tool deployments and integrations. The lack of visibility and problems with reporting similarly reflect a likely lack of integration. It is also interesting to note the importance of integration as a success factor in the selection of zero trust solutions. Fifty-three percent of respondents named integration with other systems as an important selection criterion for buying a zero trust solution. (See figure 14.)

AI in Security

AI has evolved beyond just a groundbreaking innovation—it's now an integral part of everyday business operations. As generative AI tools like ChatGPT reshape businesses, AI is becoming deeply embedded in the core of enterprise activities. However, the questions surrounding the secure adoption of these AI tools and the defense against AI-driven threats remain unresolved. It is definitely going to be a balancing act: to reap the full transformative potential of AI, enterprises must work to securely enable AI—that is, to minimize the risks associated with integrating and developing AI tools, while devising strategies to prevent or curtail an explosion of unapproved AI tools in the enterprise, a trend dubbed 'shadow AI.'

Our survey respondents are definitely paying attention. They are likely aware of the massive growth in AI use, though few would guess that enterprise AI transactions grew by nearly 600% from April of 2023 to January of 2024. Asked, "How worried are you about adversarial AI's ability to evade known cybersecurity defenses?" 28% said they were "very" or "extremely concerned." A further 42% said they were "moderately concerned." Only a small fraction was "not" or "slightly concerned.

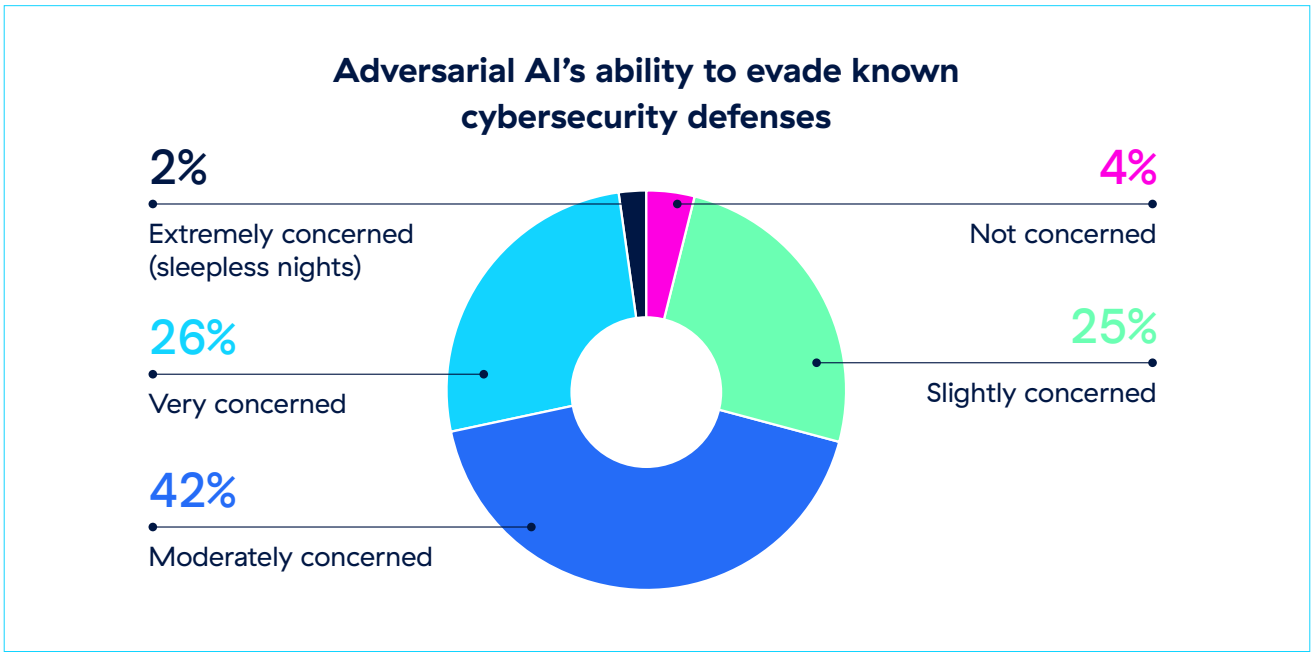


Figure 9 – Responses to the question "How worried are you about adversarial AI's ability to evade known cybersecurity defenses?"

AI is empowering threat actors in unprecedented ways, including for AI-driven phishing campaigns, deepfakes and social engineering attacks, polymorphic ransomware, enterprise attack surface discovery, automated exploit generation, and more. When asked "what types of attacks do respondents think will become more dangerous or serious in the next two to three years due to AI?" Sixty percent said ransomware, followed by 59% for social engineering, which includes phishing, "smishing" using SMS text messages, and "vishing" or voice phishing.

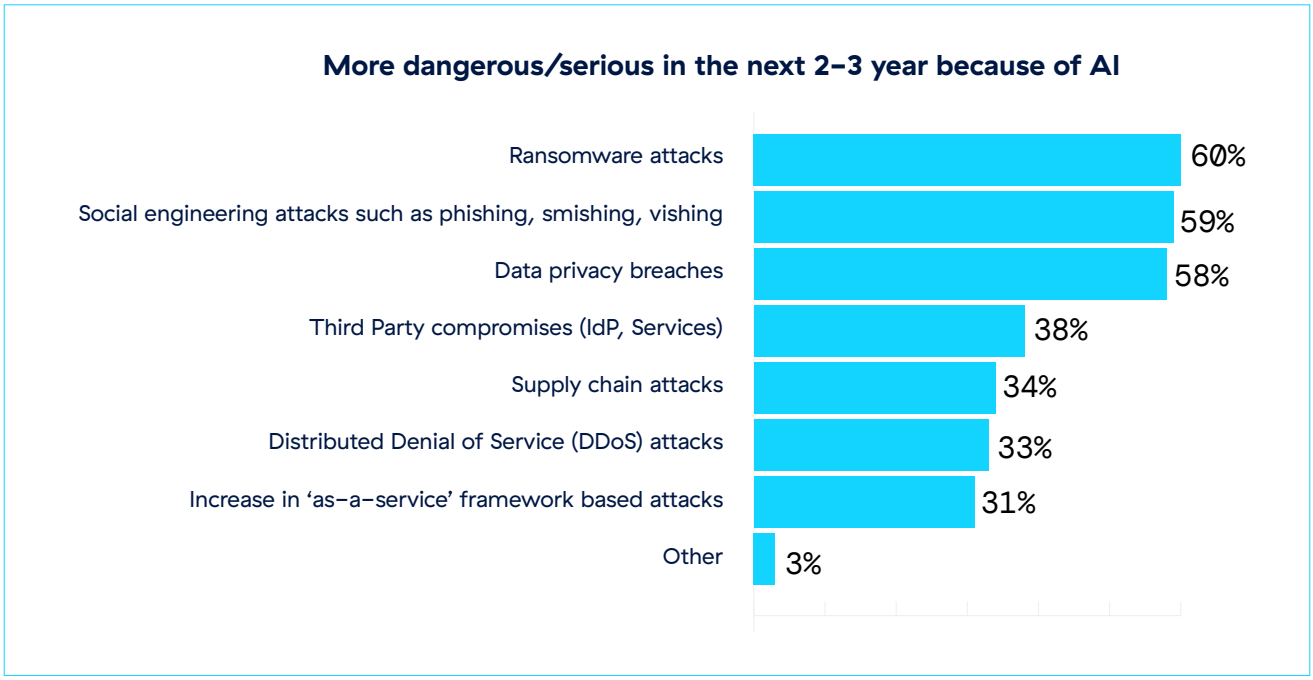


Figure 10 – Responses to the question "Which types of attacks will become more dangerous/serious in the next 2-3 years because of AI?"

AI is empowering security teams, as well. 68% of respondents said they felt AI would help improve security analytics. This figure probably represents an understanding that many cybersecurity tools already use AI for analytics, but that advances in AI promise even more capabilities. Sixty percent said that AI would help make incident response faster, while 55% said it would improve threat prevention and detection. These two concepts are often related, with AI making it possible to automate the detection and analysis of threats, followed by automated enrichment of threat information—speeding up security analyst responses to incidents.

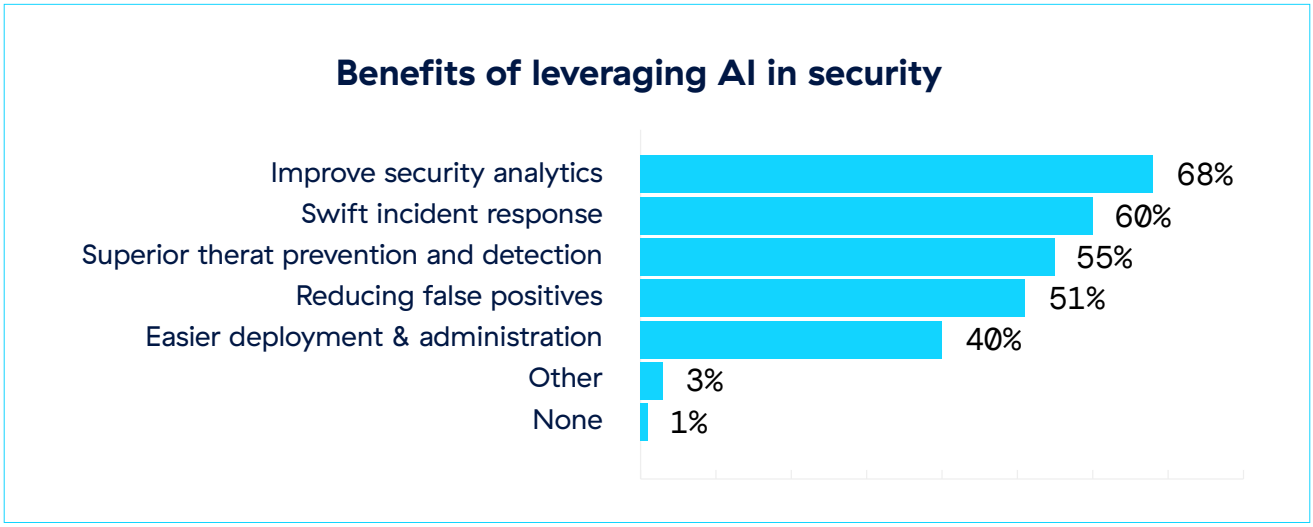


Figure 11 – Responses to the question "What do you think would be the benefits of leveraging AI in security?"

Sixty-two percent of respondents said that they plan to leverage AI capabilities in their cyber defenses within the next two years. It's notable that while 58% worry that AI will make data privacy breaches worse (see figure 10), just 11% plan to use AI for better data security.

Company size affects the findings. Smaller companies are more interested in using AI for risk evaluation and dynamic risk scoring. (40% of 1,000–2,499 organizations plan for it, vs. 17% of 10,000+ companies.) This difference may be attributable to bigger companies already having mature capabilities for risk evaluation and dynamic risk scoring. Or, it could reflect the reality that implementing AI for these workloads is complex and big companies simply cannot scope out the task in the near term.

Bigger companies are more interested in using AI to secure applications and workloads than their smaller counterparts. (34% of 10,000+ companies vs. 26% of 1,000–2,499 companies). This divergence could be due to the fact that large companies often have far more complex and interdependent application environments than smaller businesses. Defending applications is thus more difficult at a bigger firm, so AI is an appealing option for improved application security.

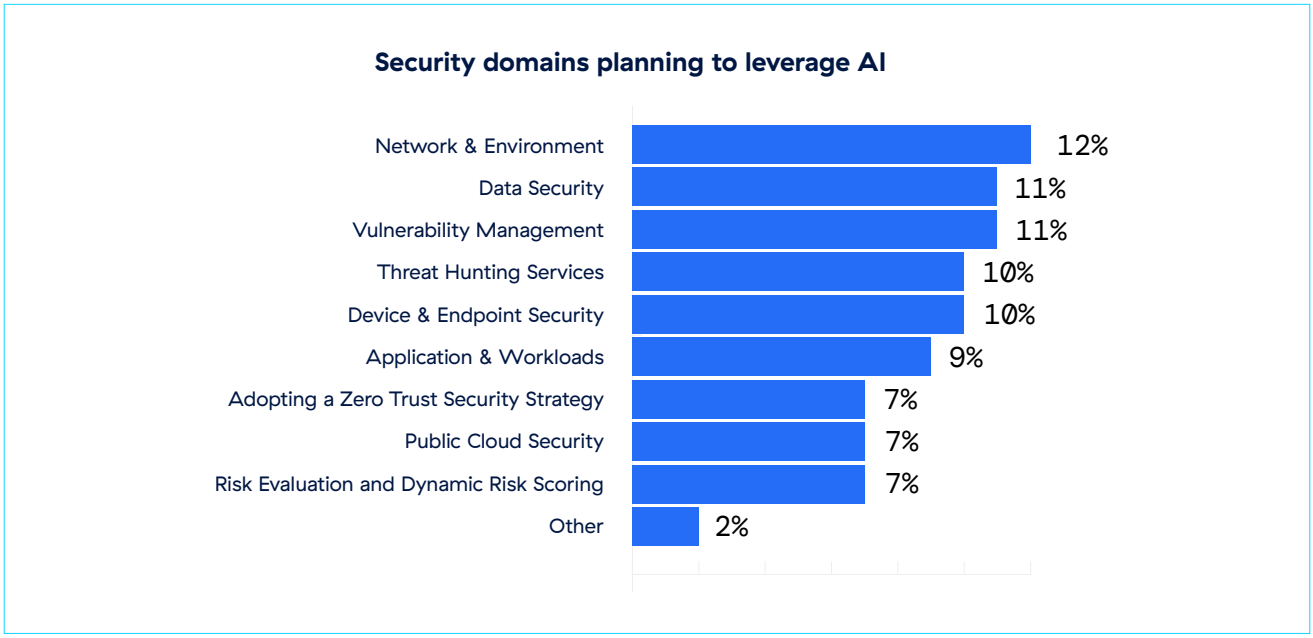


Figure 12 – Responses to the question "Which security domain do you plan to leverage AI capabilities?"

The State of Zero Trust

Zero trust, a cybersecurity strategy wherein security policy is applied based on context established through least-privileged access controls and strict user authentication—not assumed trust—is gaining traction with the companies covered in the survey. Asked, "Do you take a zero trust approach to security in your organization?", a total of 81% of respondents either are in the process of rolling out a zero trust strategy (46%), are planning to do so this year (23%), or already have zero trust tools and strategies deployed (11%).

This high level of interest may be due to the fact that a well-tuned zero trust architecture leads to simpler network infrastructure, a better user experience, and improved cyberthreat defense. Just 15% do not have a plan to embrace zero trust this year.

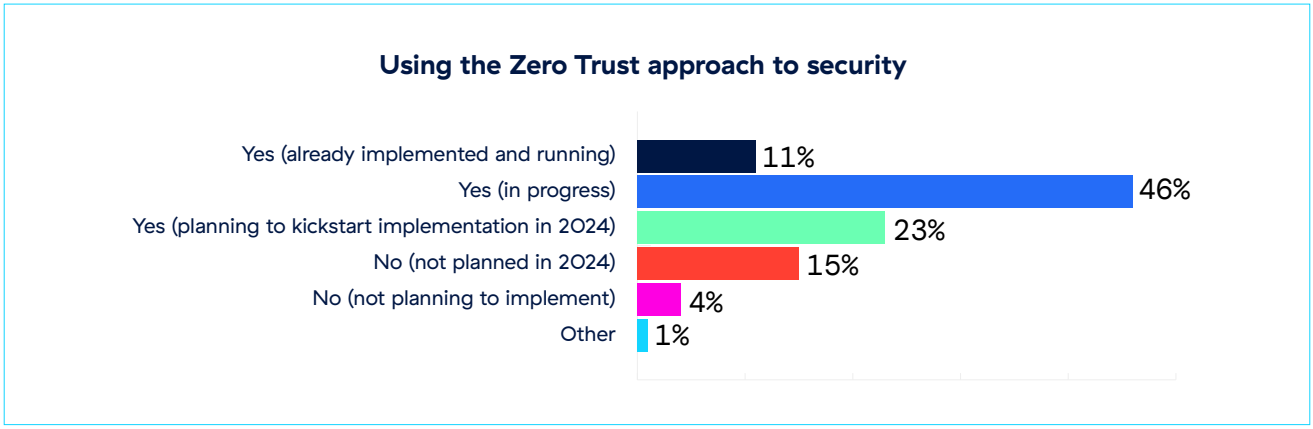


Figure 13 – Responses to the question "Do you take a zero trust approach to security in your organization?"

Given the interest, the respondents who are prospective buyers of zero trust solutions have many selection criteria on their minds. For 56%, price is the most important factor, followed by robustness (54%) and integration with existing security solutions (53%). Ease of use and scalability also matter, as do proven presence in a particular industry and breadth of platform.

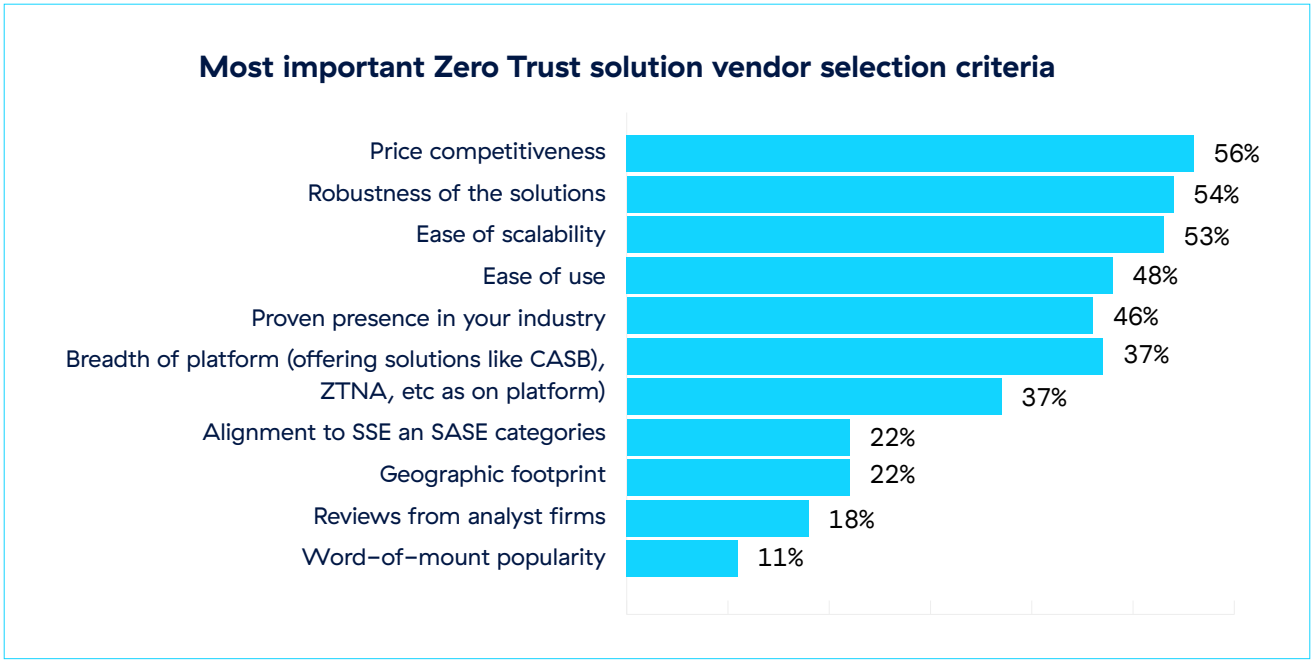


Figure 14 – Responses to the question "What are (or will be) your organization's most important selection criteria when evaluating a Zero Trust solution vendor?"

Predictions for 2025

Amidst rapid change and technological evolution, organizations often struggle to pinpoint where to direct security efforts. Respondents expressed concerns over a lack of visibility into their IT environments. They want to move away from VPNs and embrace zero trust. They are struggling with tool sprawl and worried about the impact of AI on their levels of risk exposure.

What actions will they take to change the way they do things? Here's a recap of plans for this year and the near future:

- 58% said they will focus on vendor consolidation this year
- 54% said they will increase their budgets this year vs. last year
- 81% are utilizing zero trust strategies or plan to implement them this year
- 62% said they plan to leverage AI capabilities in their cyber defenses in the next two years

Based on the data, it's clear that enterprises are actively seeking to streamline and fortify their cybersecurity strategies. Over half of the respondents are looking to consolidate vendors and increase their budgets, indicating a push towards efficiency and investment in security.

The overwhelming majority are adopting or planning to adopt a zero trust approach, signaling a shift towards more robust security architecture. Additionally, with a significant number planning to leverage AI in their cyber defenses in the near future, it's evident that enterprises are increasingly looking to advanced technologies to bolster their security posture. Overall, these trends point to a proactive stance in managing and enhancing cybersecurity capabilities.

How the Zscaler Zero Trust Exchange Can Help

Traditional security architectures, relying on appliances and centralized networks, struggle to provide adequate protection in today's threat landscape. Appliances update slowly, have performance limitations, and are costly to replicate across multiple locations. Moreover, they can't extend consistent security policies to a hybrid workforce expecting to work from anywhere. Effective, scalable protection requires a cloud-native zero trust platform. Cloud-native means designed specifically for the cloud, not just a virtualized traditional appliance. Zero trust abandons the outdated notion of a secure network perimeter, embracing a world where that perimeter no longer exists.

The Zscaler Zero Trust Exchange™ is the only true cloud-native zero trust platform, delivering a comprehensive security service edge (SSE). It connects users, workloads, and devices without exposing them to the network. The Zero Trust Exchange is a fundamentally different approach to cyberthreat protection, with unmatched attack surface reduction and AI-powered advanced threat protection. Users, devices, and workloads connect directly to the resources they need, with inline security controls that operate at the speed of the cloud.

These capabilities help you:

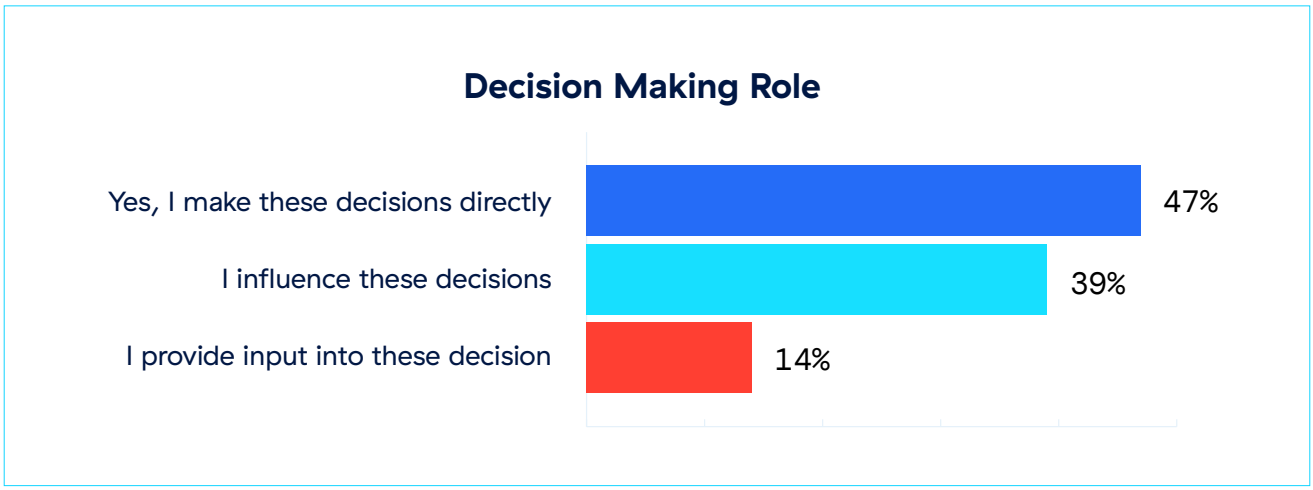
- Eliminate the attack surface: Applications sit behind the exchange, invisible to the open internet, preventing discovery and targeted attacks.
- Prevent compromise: Inspect up to 100% of SSL traffic without performance degradation, and analyze it with context-aware security controls that are kept up-to-date in real time by the world's largest security cloud.
- Stop lateral threat movement: Users connect directly to apps through secure one-to-one tunnels, without network access, to isolate threats.
- Improve user experience: Direct connections to cloud applications are intelligently managed and optimized, giving your users smooth, fast access.
- Reduce costs and complexity: Management and deployment are simple, with no need for VPNs, complex firewall rules, or any new appliances.

Conclusion

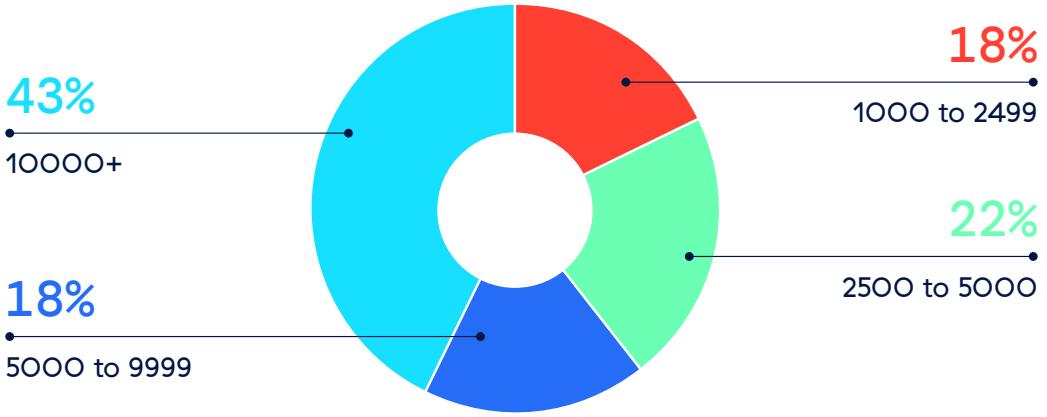
Enterprise applications are swiftly migrating to the cloud, with no signs of slowing down. Embracing the cloud enhances IT agility, reduces costs, and accelerates innovation. Businesses are increasingly dependent on internet services and external SaaS applications for critical needs, and they're transitioning internal applications to public cloud, IaaS, or PaaS for greater agility and access. This is fraught with challenges, including the ever-present threat of ransomware, tool sprawl, limited visibility, and legacy appliance vulnerabilities. Survey respondents are clear: VPNs and firewalls are no longer viable. Security teams are committed to increased spending, vendor consolidation, and the deployment of zero trust architectures.

While AI is recognized as a double-edged sword—capable of powering both advanced threats and innovative countermeasures—IT and security professionals are not deterred. Despite the complex landscape and legitimate concerns, they are focused on practical solutions. The survey results underscore their resolve, demonstrating a clear vision for tackling these challenges head-on with strategies they believe will be effective.

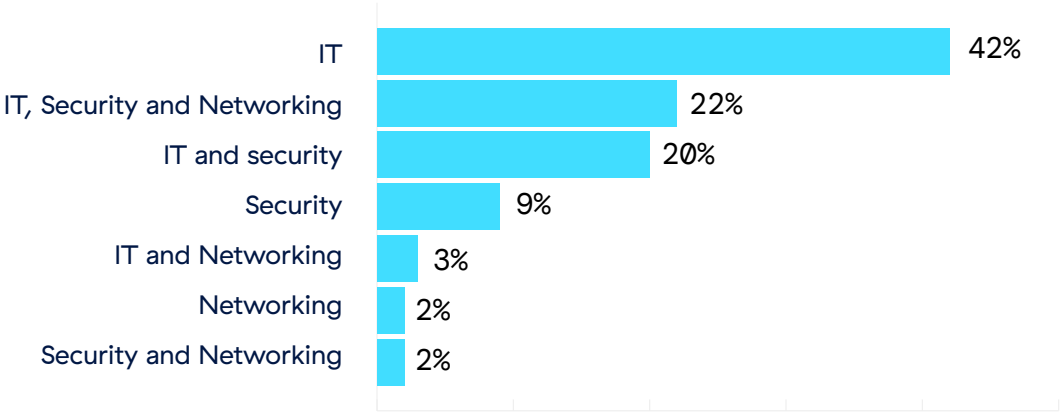
Appendix: Survey Demographics



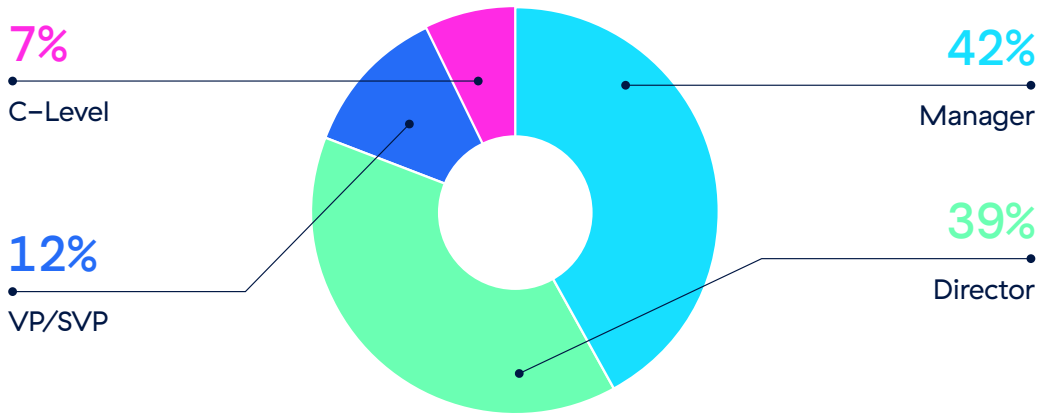
Size of Organization



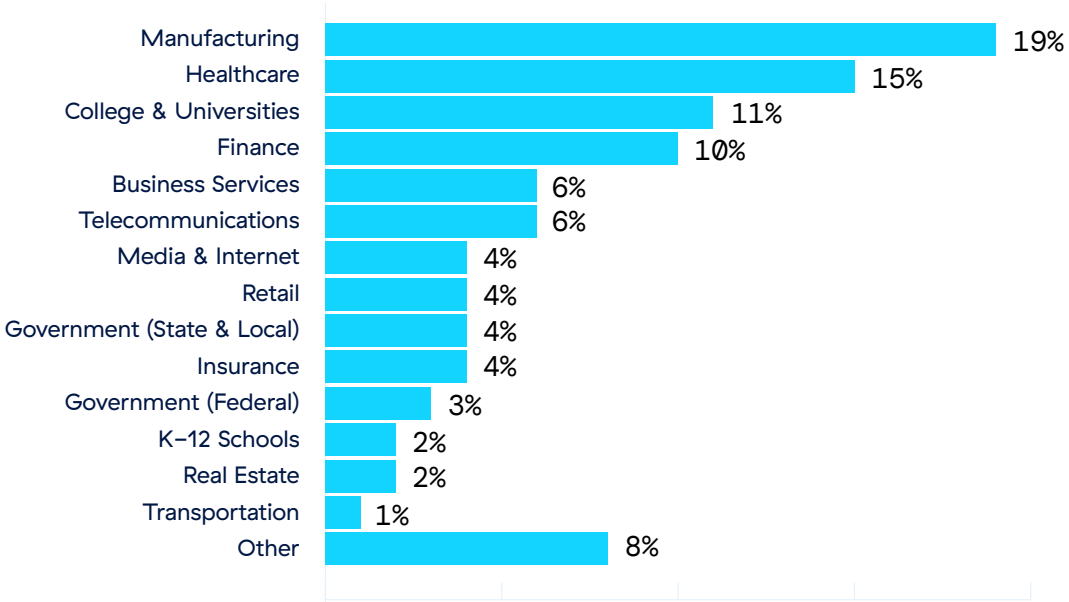
Job Role/Funtion



Size of Organization



Primary Industry



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 SASE–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