ManageEngine

2024 Identity Security Insights

Your engine to manage trends and threats

A report by :

Jane Frankland

Author, advisor, and technologist

Complete findings

Table of Contents

Introduction

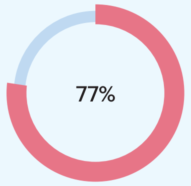
If information is the new oil, then identities are the rigs that allow that oil to be accessed. Everywhere you look, attacks increasingly focus on prying those sensitive keys out of unsuspecting victims' hands–using whatever means necessary. This could include AI-generated phishing campaigns, deeply embedded advanced persistent threats that siphon credentials, and subtly deploy social engineering to con CEOs into revealing their passwords on lookalike sites that specialize in stealing privileged identities.

Do organizations today have what it takes to combat the increasing number of these kind of attacks? If not, how far are they from confidently defending their valuable identities? And how likely are they to take the steps to ensure their safety in the future?

These are questions we pursued relentlessly as we sought experts from four continents, 12 countries, five major industries, and over a dozen different roles to craft our ManageEngine Identity Security Survey 2024. Their answers surprised and intrigued us, and we invite you to see how your company's identity management readiness compares to other organizations around the globe.

Key takeaways

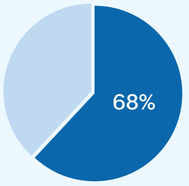
Criminals love our identities! So much so that:



77% of CISOs polled reported experiencing an identity-related cyberattack in 2023.

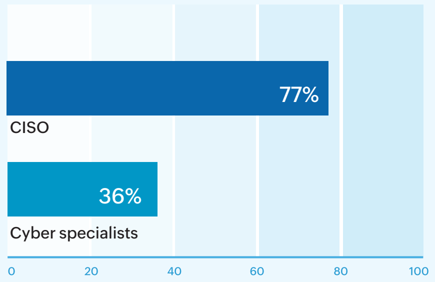
However, Zero Trust access management is (still) at below-zero levels! Indeed, when asked how close they are to having zero standing privileges–or no permanent user access permissions–only 27% could claim that they were "Already there."

Acknowledging these facts,



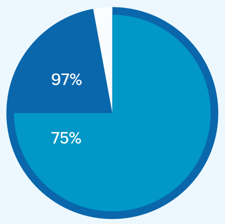
Over two-thirds of those surveyed (68%) felt the need to adopt even more tools to deal with the current need.

And not just any tool. Organizations are ready to "experiment" with AI being an IA (intelligent assistant).



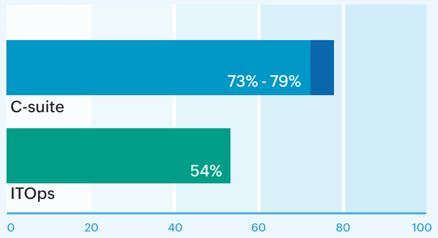
When asked if their organizations would adopt a new AI tool that "promises productivity boosts and faster investigations," even if it took 40 hours to train and four weeks to learn, more than half of respondents in all industries said "Yes," along with 77% of CISOs and a still substantial—but probably unenthusiastic—36% of cyber specialists.

Although money “can’t buy me love”, it certainly can buy more tools!



Although almost every CTO (97%) expressed confidence that their organizations would allocate a budget to invest in identity security tools within the next five years, about 1 in 4 in ITOps don’t share the same view.

Have you noticed that disparity in perception? Well, it wasn’t the only one we identified!



When asked how capable their organization’s security stack was for meeting current identity security needs, between 73% and 79% of those in the C-suite responded “Very capable;” however, only 54% in ITOps agreed.

Bonus takeaway:

Survey respondents were asked to name a few IT and security threats that organizations must be prepared to handle in the next three to five years.

AI-generated deepfakes, AI-driven social engineering attacks, and AI-enabled ransomware attacks that rapidly exploit zero-day vulnerabilities were the top responses.

AI is not only an incredible assistant, but it can also be a formidable opponent!

Perceptions and reality of the IT ecosystem visibility and control

“You can’t protect what you don’t know,” goes the famous security motto. Maintaining complete visibility over privileged resources and identities is critical for sectors handling sensitive data. Due to the valuable information they maintain, the finance, government, education, and healthcare segments are prime targets for cyberattacks. Without comprehensive oversight, these sectors risk unauthorized access, data breaches, and compliance violations. Robust visibility enables proactive threat detection, swift incident response, and effective risk management, safeguarding essential services and sensitive information.

However, the distance between theory and practice can sometimes be worrying. For example, almost all industries still lack visibility and control over at least a quarter of their privileged resources, survey results indicate. This is alarmingly worrying, especially if you consider that representatives in the finance, healthcare, education, and government sectors say they are 68% confident they have “complete visibility” into their privileged (and critical) assets. Unsurprisingly, the situation is not different across all continents.

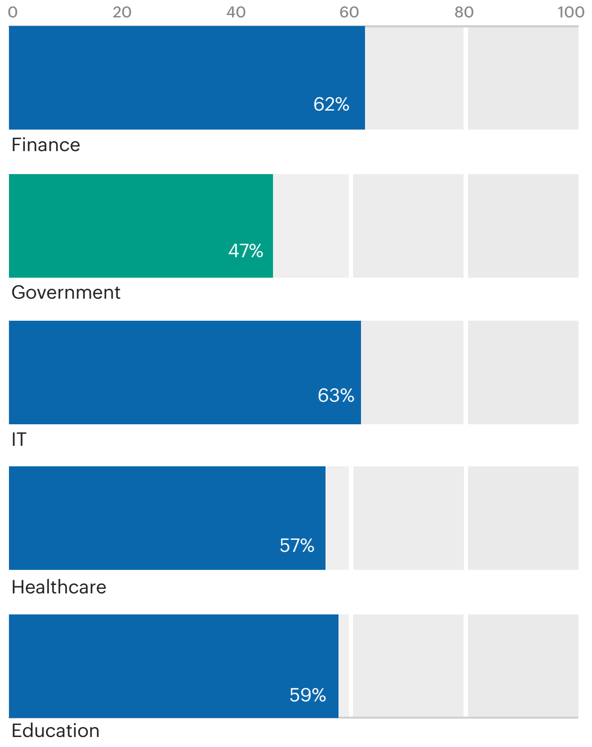


Figure 1: Percentage of respondents in different industries who have complete visibility over the privileged identities that they manage and control.

Although many in IT acknowledge the critical role identities play in protecting data and systems, many businesses seem to be dismissive of the need to effectively manage digital identities across their life cycle. Only 62% of financial institutions report they can successfully inventory all privileged identities, with the government segment being as low as 47% (see Figure 1).

To be fair, there are factors contributing to this visibility gap:

1. **Legacy systems:**
   These sectors often rely on outdated systems that lack modern security features and are challenging to integrate with current identity management solutions.

2. **Regulatory complexity:**
   Stringent regulations like HIPAA, the GDPR, and FISMA create a complex compliance landscape, sometimes leading to a focus on checkbox compliance rather than comprehensive security.

3. **Decentralized IT environments:**
   Many organizations in these sectors have grown through mergers or have multiple departments with independent IT systems, creating siloed environments that hinder centralized visibility.

4. **Resource constraints:**
   Budgetary limitations and skill shortages can prevent organizations from implementing and maintaining advanced identity management solutions.

5. **Rapid digital transformation:**
   The push to modernize and adopt cloud services often outpaces security measures, leaving gaps in identity oversight.

6. **Complex attack surfaces:**
   The increasing use of IoT devices, mobile technologies, and distributed workforces expands the attack surface, making it harder to maintain comprehensive visibility.

Although there is uniformity across industries and regions, the disparity of perceptions between business and security executives and security practitioners on the ground is more alarming. For example, while 92% of CISOs reported having full visibility and control over their enterprise's applications, servers, devices, and other resources, only 48% of their ITOps and infrastructure experts agreed with this assessment, and a slightly higher number of cyber specialists (59%) concurred.

The disparity continues in managing privileged identities. CISOs claimed to have "Complete visibility" into 92% of privileged identities, while ITOps professionals put the number at 44%. This is a potential overestimation of double the amount. This drastic difference raises questions about the accuracy of self-assessment and the potential for blind spots in security strategies.

However, security gaps might emerge because businesses rely on IT resources beyond their immediate control. Globally, at least 85% of respondents across all countries oversee assets outside their direct control. While this reflects the reality of modern cloud and SaaS adoption, it introduces significant risk.

The varying perceptions within the business of how secure these external channels are—85% of CTOs believe so versus a mere 42% of CISOs and 65% of ITOps—is a fascinating and concerning phenomenon that usually stems from differing perspectives and priorities:

- CTOs typically focus on technology innovation and operational efficiency. Their high confidence (85%) might reflect optimism about the advanced features and compliance certifications of external services.

- CISOs, being security-focused, are more attuned to potential vulnerabilities and risks. Their lower confidence (42%) likely stems from a deeper understanding of the threat landscape and potential security gaps.

- ITOps, with their middle-ground perspective (65%), balance day-to-day operations with security concerns, resulting in a more moderate view.

However, this disparity might also indicate a deeper cultural issue, where communication gaps and insufficient sharing of security insights and concerns across these different roles lead to misaligned perceptions.

Perhaps most worrying is the overconfidence in security tools. While most respondents believe they have sufficient protection, this optimism is often misplaced. The fact is telling that 26% of cyber specialists—those closest to the day-to-day security operations—indicate they need additional solutions.

The importance of identity security

As traditional network boundaries blur with cloud adoption and remote work, digital identities now serve as the primary gateway to our most sensitive resources and data.

The importance of identity security in the modern enterprise cannot be overstated. It's no longer just about protecting user accounts; it's about safeguarding the very core of how we conduct business, collaborate, and innovate. Every interaction, transaction, and data access point hinges on the integrity and security of digital identities.

As cybercriminals increasingly target identities as their attack vector of choice, robust identity security has evolved from a best practice to an absolute necessity. It's the linchpin that holds together Zero Trust architectures, enables secure digital transformation, and ultimately determines an organization's resilience against today's sophisticated cyberthreats.

Across industries, the recognition of the critical role of identity security is nearly universal. It's particularly telling that the government and IT sectors lead the pack, with 91% rating it as "Very important." This aligns with the complex identity ecosystems these sectors manage and the sensitive nature of their data. What truly stands out is the overwhelming consensus among C-suite executives. When 97% of CIOs and CTOs emphasize the paramount importance of identity security, it's clear that this isn't just a technical concern, it's a business imperative.

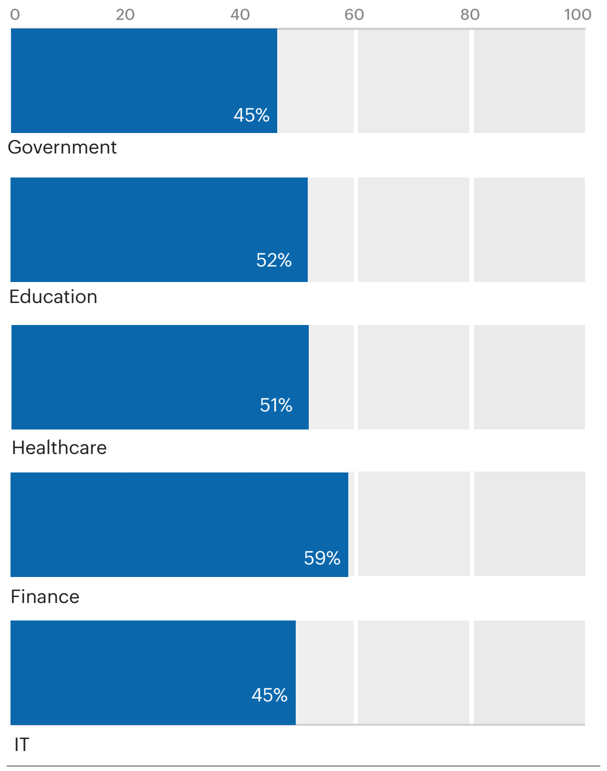


Figure 2. Percentage of respondents across different industries who reported facing an identity security related attack in 2023.

The threat landscape further underscores why identity security is crucial. Social engineering emerges as the top concern across multiple sectors and countries. This isn't surprising; a single compromised identity can unravel even the most sophisticated security measures.

What's particularly alarming is the prevalence of identity-related attacks. When 59% of finance sector respondents report facing such attacks in 2023 (as shown in Figure 2), it's clear that this isn't a hypothetical threat. It's a daily reality. The disparity in attack reporting between CISOs (77%) and ITOps (29%) is a critical issue that points to several underlying problems in organizational cybersecurity structures.

For example, this disparity likely indicates a severe lack of information sharing between departments. CISOs, with their bird's-eye view of the security landscape, are aware of more incidents, while ITOps teams might only be privy to a subset of attacks they directly encounter or mitigate. This disparity is a hidden vulnerability and a dangerous one. It suggests that a significant number of identity-related attacks might be unnoticed or unreported by the teams responsible for day-to-day IT operations. This gap in awareness can lead to delayed incident response, incomplete risk assessments, inadequate security measures, and potential compliance violations.

The identity security tech stack

The identity security tech stack represents the front line of defense against a myriad of sophisticated cyberthreats. It's no longer just about password protection or basic access controls. Modern identity security encompasses a complex ecosystem of tools and technologies designed to authenticate, authorize, and audit every digital interaction within an organization.

From adaptive and phishing-resistant MFA and privileged access management to identity governance and administration, each component of the tech stack plays a crucial role in maintaining the integrity and security of our digital identities. These technologies not only protect against external threats but also mitigate risks from insider threats and accidental misuse.

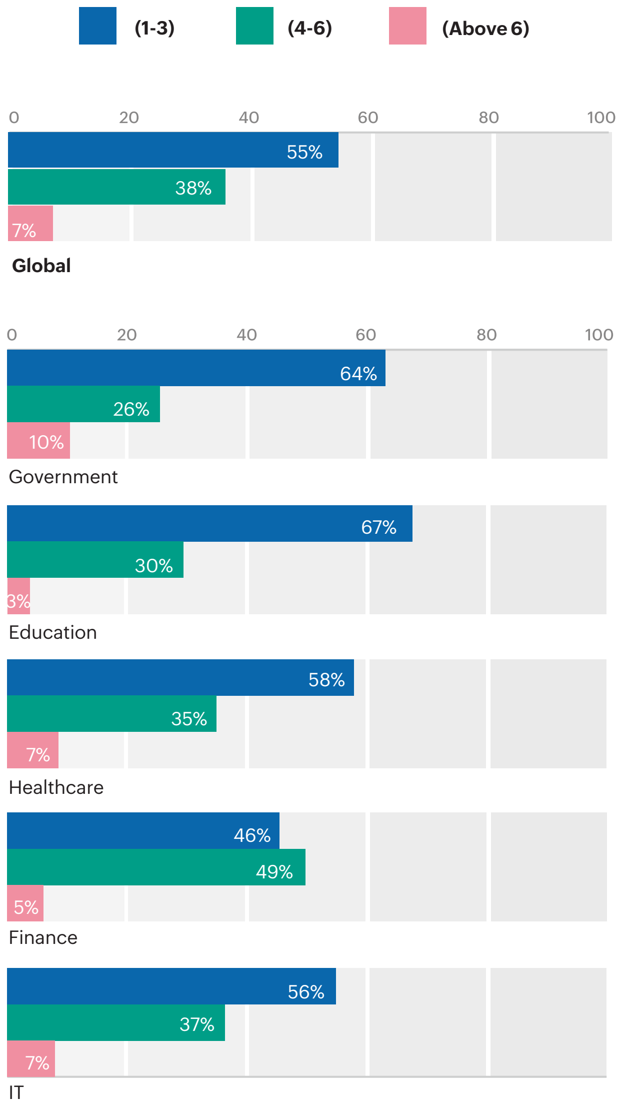


Figure 3 : The number of different vendors that enterprises rely on to manage their identity security stack.

The widespread adoption of identity management solutions is encouraging, with over 82% of respondents across all industries and 84% of global businesses using these tools. However, the choice of solutions varies significantly. The government and education sectors primarily rely on password managers, while the finance, IT, and healthcare sectors lean towards more sophisticated SSO solutions.

This disparity hints at differing maturity levels in identity security strategies.

What's particularly intriguing is the tool sprawl we're witnessing. In the finance sector, 54% of respondents report using four or more identity management vendors (refer to Figure 3).

The tools sprawl trend is a double-edged sword. While it demonstrates a commitment to comprehensive security, it also raises concerns about integration complexity and potential security gaps between solutions.

- Different vendors often use proprietary protocols or data formats, making seamless integration difficult. This can lead to siloed systems that don't communicate, coordinate, or operate effectively. Managing multiple systems requires diverse skill sets and more time, potentially leading to configuration errors or oversight.
- Poorly integrated systems can cause latency, affecting user experience and potentially encouraging risky work-arounds.
- Different tools might interpret and enforce security policies differently, creating inconsistencies in access controls.

Perhaps most telling is the appetite for additional tools. Despite high adoption rates, many respondents, particularly in the finance (68%) and government (74%) sectors, feel the need for more solutions. This sentiment is strongest among cyber specialists, with 79% advocating for additional tools.

This desire for more tools, coupled with the optimism about future budget allocations (94% of respondents in the finance sector expect increased investments), signals both an awareness of evolving threats and a potential over-reliance on technology as a silver bullet.

However, as we navigate this complex landscape, it's crucial to remember that tool proliferation isn't always the answer. A strategic, integrated approach to identity security, focusing on interoperability and comprehensive coverage, is often more effective—both operationally and cost-wise—than simply adding more tools to the stack. This is a trend that we saw in some regions. For example, EU countries like Spain are the least likely to adopt more identity security tools, which could indicate a satisfaction with simplicity or current strategy, or a need for a more robust approach.

The identity security posture of organizations

The landscape of identity security is rapidly evolving, and our survey reveals a complex picture of how organizations are adapting to these changes.

One of the most striking findings is the gap between perception and reality when it comes to the capabilities of current identity security solutions. While 73-79% of C-suite executives believe their current solutions are "Very" capable of meeting today's identity management challenges (as shown in Figure 4), only 58% of cyber specialists and just 54% of ITOps and infrastructure professionals share this confidence.

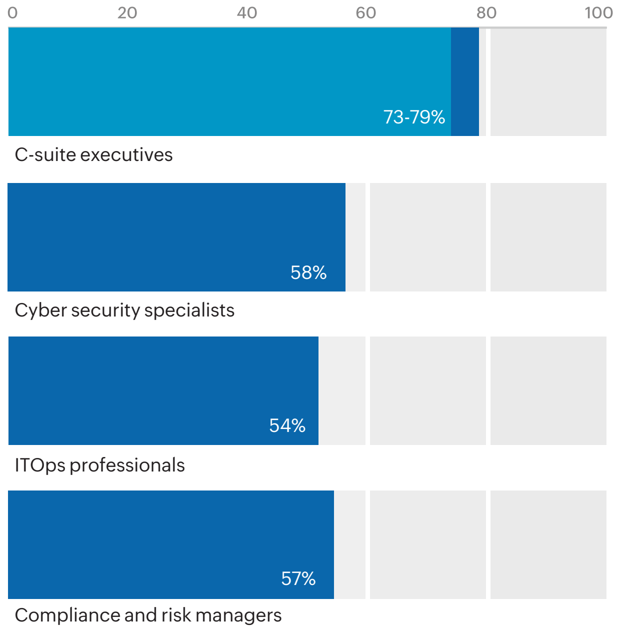


Figure 4: Percentage of respondents across different roles who believe their current identity security solutions are "Very capable" of managing their identity security challenges.

This disparity is concerning, as it suggests a potential disconnect between strategic vision and operational reality:

- When C-suite executives overestimate the capabilities of their security solutions, they might also underestimate the actual risks facing the organization. This can lead to inadequate resource allocation, leaving critical vulnerabilities unaddressed.
- Strategic decisions made based on an overly optimistic view of security capabilities might not address the real challenges faced by IT and security teams. This can result in investments in solutions that don't address the most pressing operational needs.
- This disparity suggests a significant communication gap between executives and operational staff. If ITOps and cyber specialists aren't effectively communicating their challenges and concerns up the chain, critical security issues might go unnoticed and unaddressed at the strategic level.

The adoption of Zero Trust strategies for identity security is encouraging, with 80% of financial organizations leading the charge. However, the fact that only 64% of government agencies have such strategies in place is worrying, given the critical nature of the data and systems they protect. This lag in adoption among government entities could represent a significant vulnerability in our national cybersecurity posture.

Perhaps most telling is the state of standing privileges within organizations. The concept of "zero standing privileges"—where no user has permanent, unfettered access to critical systems—is a cornerstone of modern identity security. Yet, our survey shows that only 25% of organizations in any industry have achieved this goal (elaborated in Figure 5). The primary obstacle? A lack of processes is cited consistently across industries and roles.

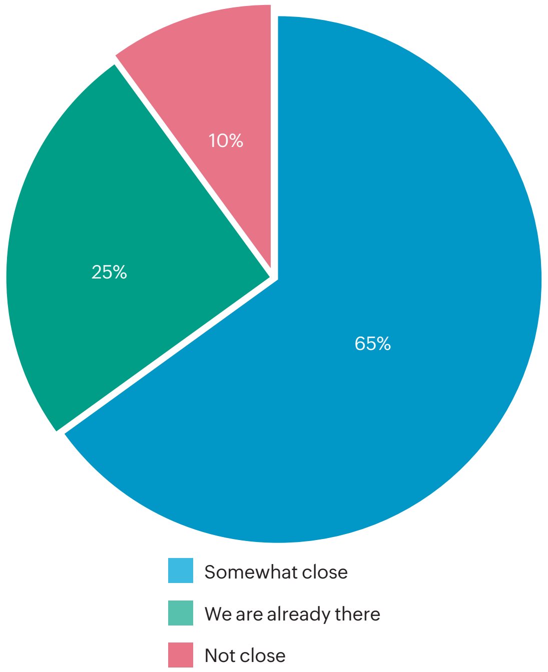


Figure 5: How close do respondents believe their organization is towards having zero standing privileges?

This finding underscores a critical point: effective identity security is not just about technology but also about people and processes. While organizations might invest in cutting-edge identity management tools, without the right processes in place, these investments might fall short of their potential.

The path to a robust identity security posture is clearly still a work in progress for many organizations. However, by addressing the gaps identified, businesses can significantly enhance their resilience against identity-based threats in today's digital landscape.

Future threats

As we stand at the precipice of a new era in cybersecurity, the landscape of threats looming on the horizon is both daunting and complex. The next three to five years promise to usher in a paradigm shift in how we approach identity security, driven by rapid technological advancements and evolving attack vectors.

In this section, we delve into the collective insights of cybersecurity professionals across various industries, roles, and geographies. Their perspectives paint a vivid picture of the challenges that lie ahead—a future where the lines between physical and digital identities blur, AI becomes both a formidable threat and a powerful ally, and the human element remains both our greatest vulnerability and our strongest defense.

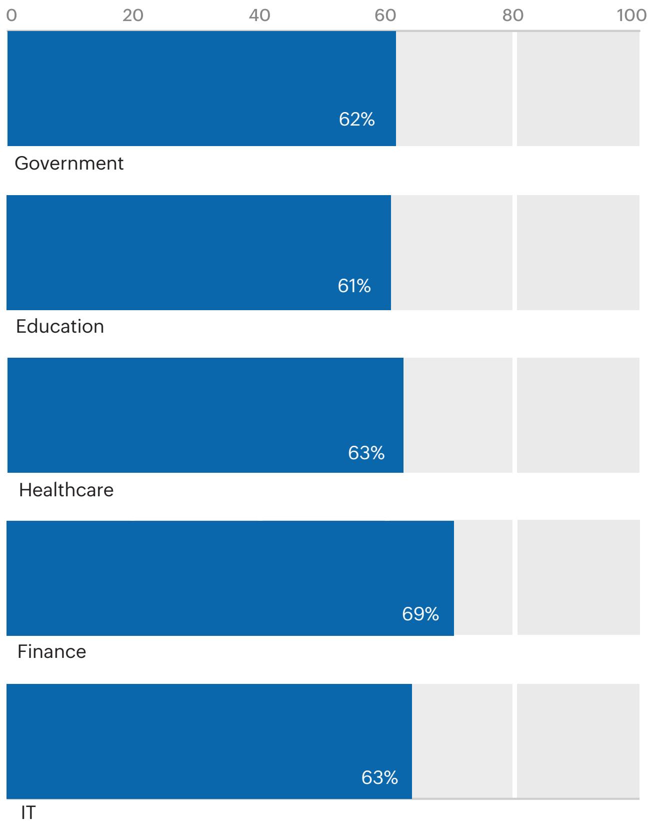


Figure 6: The percentage of respondents from different sectors that believe in AI's ability to strengthen their identity security strategies.

Artificial Intelligence emerges as a dominant theme in future threat predictions. The rise of deepfakes, AI-powered social engineering attacks, and the potential for AI to create sophisticated phishing attempts are top concerns across multiple sectors. A healthcare professional warned of "artificial intelligence creating deepfake profiles to access sensitive information," while a CIO emphasized the need to "protect online identities from AI that can create a deepfake video of your face using only a picture."

However, it's noteworthy that despite these concerns, there's a strong belief in AI's potential to strengthen identity security. Between 61% and 69% of all sectors surveyed believe that AI could bolster their security strategies (see Figure 6). Reactions were mixed among geographies, but close to half or more put faith in AI-based identity security enhancements. This duality of AI as both a threat and a solution underscores the complex role it will play in shaping the future of cybersecurity.

Social engineering attacks continue to be a significant concern, with many respondents highlighting the evolving nature of these threats. The shift to remote work has created new vulnerabilities, with one education sector respondent noting the "evolving social engineering [attacks] that target a more distributed workforce, preying on the isolation and potential lack of awareness of remote workers."

The skills gap and lack of security awareness among users remain pressing issues. Multiple respondents emphasized the need for better training and education, with one Singapore-based professional stating, "Users need to attend cybersecurity training classes to operate with security in mind, and management also needs to educate their staff to improve IT."

Ransomware, supply chain attacks, and the security challenges posed by remote work are also prominent concerns. A finance sector professional warns of "highly organized criminal gangs that lurk in the network for a long time for intelligence gathering or sabotage."

Looking at organizational readiness for these future threats, there's a notable disparity between private sector companies and government agencies. While 84-89% of private sector companies report their IT stacks as future-ready, only 73% of government agencies share this confidence. This gap is concerning, given the critical nature of government systems and data, and can be attributed to several factors:

- Private sector companies often have more flexibility in allocating resources and adjusting budgets to address emerging threats quickly. Government agencies, on the other hand, often face bureaucratic hurdles and rigid budget cycles that can slow down the adoption of new technologies and strategies.

- Private companies, especially in tech-driven industries, tend to have shorter technology adoption cycles. They can often implement new solutions more rapidly. Government agencies typically have longer procurement processes and stricter regulations governing technology adoption, which can lead to slower modernization.

- Government agencies often rely on legacy systems that are difficult to update or replace due to their critical nature and the potential for service disruption.

- Government agencies face a unique threat landscape, often dealing with nation-state actors and highly sophisticated attacks targeting critical infrastructure. This elevated threat level might contribute to a more cautious assessment of their readiness.

The willingness to adopt new AI-driven cybersecurity solutions, despite significant time investments for training and proficiency, is encouraging. However, the disparity between CISOs' enthusiasm (77% extremely likely to adopt) and cyber specialists' caution (only 36% extremely likely) highlights a potential disconnect between strategic vision and operational realities.

CISOs often face pressure from boards and executives to adopt cutting-edge technologies to stay competitive. Thus, they focus on long-term strategy, seeing AI as a crucial investment for future-proofing their security infrastructure. On the other hand, cyber specialists have a more pragmatic approach to cybersecurity since they are concerned about tool fatigue and workload pressure, given that their teams are often understaffed.

A final word

The purpose of our research was to discover how well various demographics understood the plight of privileged identities, how prepared they believed their organizations were to secure them, and what they thought was standing in the way.

When asked, most industries saw a lack of budget as the number one obstacle preventing them from creating a security stack that could withstand the threats of the future. Second was complex legacy IT infrastructure, which remains a problem for the healthcare and financial services sectors in particular. Whatever the challenges, however, the answers in this survey also provide hopeful clues on how to solve them.

It is significant, for instance, that up to two-thirds of all surveyed would adopt new AI-based tools if they thought they could better secure vulnerable identities—even if training took an entire work week plus another month to learn the technology. Also encouraging is that roughly 70-90% anticipate further investment in identity management within the next five years, and that 60-80% already have a Zero Trust-focused identity and security plan in place.

Notwithstanding the challenges, these facts indicate that a significant number of decision-makers worldwide recognize the criticality of privileged identities enough to make steep sacrifices to secure them.

ManageEngine's PAM360 is a comprehensive enterprise privileged access management solution that empowers IT teams to effectively manage and secure privileged access. With over two decades of experience in developing cutting-edge IT management tools, ManageEngine has created a robust and reliable PAM solution.

PAM360's effectiveness is evidenced by its adoption by more than 5,000 organizations worldwide, including government agencies. Gartner named ManageEngine a Challenger in the 2024 Magic Quadrant™ for Privileged Access Management.

ManageEngine's expertise in IT management, combined with its focus on security, results in a PAM tool that meets the stringent requirements of both leading corporations and governmental bodies. PAM360 stands as a testament to ManageEngine's commitment to providing resilient, trustworthy solutions for today's complex security landscape.

Learn more about ManageEngine PAM360.

About ManageEngine

ManageEngine is the enterprise IT management division of Zoho Corporation. Established and emerging enterprises—including 9 of every 10 Fortune 100 organizations—rely on ManageEngine's real-time IT management tools to ensure optimal performance of their IT infrastructure, including networks, servers, applications, endpoints, and more. ManageEngine has offices worldwide, including in the United States, the United Arab Emirates, the Netherlands, India, Colombia, Mexico, Brazil, Singapore, Japan, China and Australia, as well as 200+ global partners to help organizations tightly align their business and IT. For more information, please visit manageengine.com

Addendum: Demographics

ManageEngine surveyed 3,000+ global enterprises spanning a wide range of industries, roles, and demographics to learn what they have to say about the current state of identity security.

- United States
- Canada
- United Kingdom
- Spain
- United Arab Emirates
- Saudi Arabia
- Singapore
- India
- Malaysia
- Indonesia
- Philippines
- Thailand
- Vietnam

Respondents belonged to one of the following five industries: financial services, government, IT, healthcare, and education. Their companies ranged from fewer than 500 employees to over 5,000, and roles included:

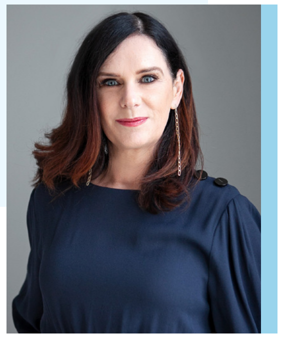
- Executive leadership : CEO, CISO, CMO, CTO, CIO, CFO, CMO, Founder/Owner, Partner, President
- Senior leadership: Executive Vice President, Senior Vice President, Assistant Vice President, Vice President, Director, Group Director, Senior Director
- Compliance and risk management
- IT operations and infrastructure
- Cyber specialists

Among participants, 31% worked fully in the office, 19% were exclusively remote, and 50% were employed in a hybrid work environment.

About the author:

Jane Frankland is a highly respected thought leader in cybersecurity and technology, celebrated for her impactful collaborations with top brands and governments. She made history by founding the first female-owned global hacking firm in the 1990s, paving the way for women's representation in a traditionally male-dominated field. Her work has played a pivotal role in launching ground-breaking initiatives such as CREST, Cyber Essentials, and Women4Cyber, demonstrating her leadership and pioneering efforts in advancing security and promoting diversity. With prestigious accolades to her name and a successful career including her role as Managing Director at Accenture, Jane is not only a seasoned professional but also an author of the bestselling book "IN Security" and associated movement which has empowered more than 400 women through scholarships worth $800,000. Her insights have reached millions through renowned media outlets like The Sunday Times, BBC, The Guardian, and Forbes. As a sought-after speaker at global events, including the EU Commission and UN Women, Jane continues to inspire aspirations across the tech community. Presently, as the CEO of KnewStart, Jane harnesses her expertise to promote innovation and inclusivity, ensuring that her remarkable journey leaves a lasting impact in the field of cybersecurity.

linkedin.com/in/janefrankland/



ManageEngine

PAM360

Full-stack PAM solution for modern enterprises

Zoho Corporation
4708 HWY 71 E
Del Valle, TX 78617, USA

Contact: hello-pam360@manageengine.com
Media : me-pr@manageengine.com
Phone : +1.925.924.9500
+1.888.720.9500