Ponemon INSTITUTE

The State of Identity and Access Management (IAM) Maturity

Sponsored by GuidePoint Security

Independently conducted by Ponemon Institute LLC

Publication Date: May 2025

The State of Identity and Access Management (IAM) Maturity

May 2025

Part 1. Executive Summary

Identity and Access Management (IAM) Maturity refers to the extent to which an organization effectively manages user identities and access across its systems and applications. It's a measure of how well an organization is implementing and managing Identity and Access Management (IAM) practices. A mature IAM program ensures that only authorized users have access to the resources they need, enhancing security, reducing risks and improving overall efficiency.

Most organizations remain in the early to mid-stages of IAM maturity, leaving them vulnerable to identity-based threats. This new study of 626 IT professionals by the Ponemon Institute, sponsored by GuidePoint Security, highlights that despite growing awareness of insider threats and identity breaches, IAM is under-prioritized compared to other IT security investments. All participants in this research are involved in their organizations' IAM programs.

Key Insights:

- **IAM is underfunded and underdeveloped.**

  Only 50 percent of organizations rate their IAM tools as very or highly effective, and even fewer (44 percent) express high confidence in their ability to prevent identity-based incidents. According to 47 percent of organizations, investments in IAM technologies trail behind other security investment priorities.

- **Manual processes are stalling progress.**

  Many organizations still rely on spreadsheets, scripts and other manual efforts for tasks like access reviews, deprovisioning and privileged access management—introducing risk and inefficiencies.

- **High performers show the way forward.**

  High performers in this research are those organizations that self-report their IAM technologies and investments are highly effective (23 percent). As a result, they report fewer security incidents and stronger identity controls. These organizations also lead other organizations represented in this research in adopting biometric authentication, authentication, identity threat detection and integrated governance platforms.

- **Technology and expertise gaps persist.**

  A lack of tools, skilled personnel and resources is preventing broader progress. Many IAM implementations are driven by user experience goals rather than security or compliance needs.

Bottom Line:

Achieving IAM maturity requires a strategic shift—moving from reactive, manual processes to integrated, automated identity security. Organizations that treat IAM as foundational to cybersecurity, not just IT operations, are best positioned to reduce risk, streamline access and build trust in a dynamic threat landscape.

Part 2. Introduction: Including a Peek at High Performer Trends

The purpose of an Identity and Access Management (IAM) program is to manage user identities and access across systems and applications. A mature IAM program ensures that only authorized users have access to the resources they need to enhance security, reduce risks and improve overall efficiency.

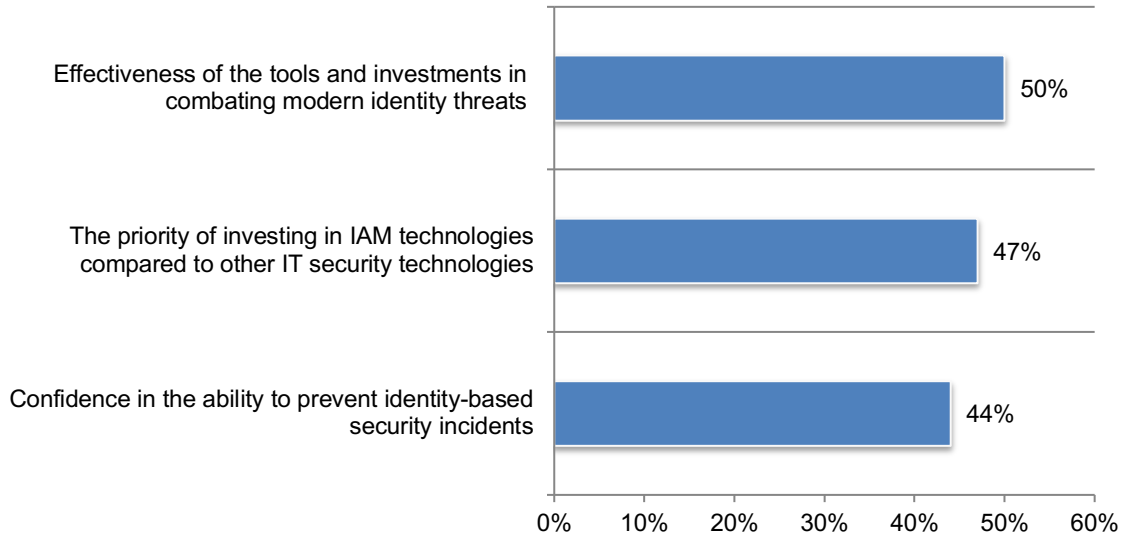
This survey, sponsored by GuidePoint Security, was designed to understand how effective organizations are in achieving IAM maturity and which tools and practices are critical components of their identity and access management programs. A key takeaway from the research is that organizations' continued dependency on manual processes as part of their IAM programs is a barrier to achieving maturity and reducing insider threats. Such a lack of maturity can lead to data breaches and security incidents caused by negligent or malicious insiders.

Recent examples of such events include former Tesla employees in 2023 who leaked sensitive data about 75,000 current and former employees to a foreign media outlet[1]. In August 2022, Microsoft experienced an insider data breach where employees inadvertently shared login credentials for GitHub infrastructure, potentially exposing Azure servers and other internal systems to attackers.

According to the research, investments in IT security technologies are prioritized over IAM technologies. Without the necessary investments in IAM, organizations lack confidence in their ability to prevent identity-based security incidents**.** Respondents were asked to rate effectiveness in their organizations' tools and investments in combating modern identity threats on a scale from 1 = not effective to 10 = highly effective, their confidence in the ability to prevent identity-based security incidents from 1 = not confident to 10 = highly confident and the priority of investing in IAM technologies compared to other security technologies from 1 = not a priority to 10 = high priority.

Figure 1 shows the very effective/very confident/high priority responses (7+ on the 10-point scale). As shown, only half (50 percent of respondents) believe their tools and investments are very effective and only 44 percent of respondents are very or highly confident in their ability to prevent identity-based security incidents. Less than half of the organizations (47 percent of respondents) say investing in IAM technologies compared to other IT security technologies is a high priority.

Figure 1. Effectiveness, confidence and priority in reducing identity threat threats
Very effective/high priority/high confidence 7+ responses shown



[1] Tesla: Insiders Responsible for Major Data Breaches, Infosecurity Magazine, August 2023.

Best practices in achieving a strong identity security posture

To identify best practices in achieving a strong identity security posture, we analyzed the responses of the 23 percent of IT professionals who rated the effectiveness of their tools and investments in combating modern identity threats as highly effective (9+ on a scale from 1 = low effectiveness to 10 = high effectiveness). We refer to these respondents and their organizations as high performers. Seventy-seven percent of respondents rated their effectiveness on a scale from 1 to 8. We refer to this group as "other" in the report.

Organizations that have more effective tools and investments to combat modern identity threats are less likely to experience an identity-based security incident. Only 39 percent of high performers had an identity-based security incident.

High performers are outpacing other organizations in the adoption of automation and advanced identity security technologies.

- Sixty-four percent of high performers vs. 37 percent of other respondents have adopted biometric authentication.
- Fifty-nine percent of high performers vs. 34 percent of other respondents use automated mechanisms that check for compromised passwords.
- Fifty-six percent of high performers vs. 23 percent of other respondents have a dedicated PAM platform.
- Fifty-three percent of high performers vs. 31 percent of other respondents use IAM platforms and/or processes used to manage machine, service and other non-human accounts or identities.

High performers are significantly more likely to assign privileged access to a primary account (55 percent vs. 30 percent). Only 25 percent of high performers vs. 33 percent of other respondents use manual or scripted processes to temporarily assign privileged accounts.

High performers are leading in the adoption of ITDR, ISPM and IGA platforms.

- Thirty-seven percent of high performers vs. 12 percent of other respondents have adopted IDTR.
- Thirty-five percent of high performers vs. 15 percent of other respondents have adopted ISPM.
- Thirty-one percent of high performers vs. 9 percent of other respondents have adopted IGA platforms.

Barriers and challenges to achieving IAM maturity

Following are highlights from organizations represented in this research

Identity verification solutions are systems that confirm the authenticity of a person's identity, typically in digital contexts, such as online transactions or applications. These solutions use various methods to verify a person's identity and ensures only authorized users have access to the resources they need.

Few organizations use identity verification solutions and services to confirm a person's claimed identity. Only 39 percent of respondents say their organizations use identity verification solutions and services. If they do use identity verification solutions and services, they are mainly for employee and contractor onboarding (37 percent of respondents). Thirty-three percent of respondents say it is part of customer registration and vetting, and 30 percent of respondents say it is used for both employee/contractor and customer.

Reliance on manual processes stalls organizations' ability to achieve maturity. Less than half of organizations (47 percent) have an automated mechanism that checks for compromised passwords. If they do automate checks for compromised passwords, 37 percent of respondents say it is for both customer and workforce accounts, 34 percent only automate checks for customer accounts, and 29 percent only automate checks for workforce accounts.

To close the identity security gap, organizations need technologies, in-house expertise and resources. However, as discussed previously, more resources are allocated to investments in IT security. Fifty-four percent of respondents say there is a lack of technologies. Fifty-two percent say there is a lack of in-house expertise, and 45 percent say it is a lack of resources.

Security is not a priority when making IAM investment decisions. Despite many high-profile examples of insider security breaches, 45 percent of respondents say the number one priority for investing in IAM is to improve user experience. Only 34 percent of respondents say investments are prioritized based on the increase in number of regulations or industry mandates or the constant turnover of employees, contractors, consultants and partners (31 percent of respondents).

To achieve greater maturity, organizations need to improve the ability of IAM platforms to authenticate and authorize user identities and access rights. Respondents were asked to rate the effectiveness of their IAM platform in user access provisioning lifecycle from onboarding through termination, and its effectiveness authenticating and authorizing on a scale of 1 = not effective to 10 = highly effective. Only 46 percent of respondents say their IAM platform is very or highly effective for authentication and authorization. Fifty percent of respondents rate the effectiveness of their IAM platforms' user access provisioning lifecycle from onboarding through termination as very or highly effective.

Policies and processes are rarely integrated with IAM platforms in the management of machine, service and other non-human accounts or identities. Forty-four percent of respondents say their IAM platform and/or processes are used to manage machine, service and other non-human accounts or identities. Thirty-nine percent of respondents say their organizations are in the adoption stage of using their IAM platform and/or processes to manage machine, service and other non-human accounts. Of these 83 percent of respondents (44 percent + 39 percent), 39 percent say the use of the IAM platform to manage machine, service and other non-human accounts or identities is ad hoc. Only 28 percent of these respondents say management is governed with policy and/or processes and integrated with the IAM platform.

IAM platforms and/or processes are used to perform periodic access review, attestation, certification of user accounts and entitlements but mostly it is manual. While most organizations conduct periodic access review, attestation and certification of user accounts and entitlements, 34 percent of respondents say it is manual with spreadsheets, and 36 percent say their organizations use custom in-house built workflows. Only 17 percent of respondents say it is executed through the IAM identity governance platform. Only 41 percent of respondents use internal applications and resources based on their roles and needs, to streamline onboarding, offboarding and access management. An average of 38 percent of internal applications are managed by their organizations' IAM platforms.

Deprovisioning non-human identities, also known as non-human identity management (NHIM), focuses on removing or disabling access for digital entities like service accounts, APIs, and IoT devices when they are no longer needed. This process is crucial for security, as it helps prevent the misuse of credentials by automated systems that could lead to data breaches or system compromises.

Deprovisioning user access is mostly manual. Forty-one percent of respondents say their organizations include non-human identities in deprovisioning user access. Of those respondents, 40 percent say NHI deprovisioning is mostly a manual process. Twenty-seven percent of respondents say the process is automated with a custom script and 26 percent say it is automated with a SaaS tool or third-party solution.

Few organizations are integrating privileged access with other IAM systems and if they do the integration is not effective. Forty-two percent of respondents say PAM is running a dedicated platform. Twenty-seven percent say privileged access is integrated with other IAM systems, and 31 percent of respondents say privileged access is managed manually. Of these 27 percent of respondents, only 45 percent rate the effectiveness of their organizations' IAM platforms for PAM as very or highly effective.

Part 3. Key findings

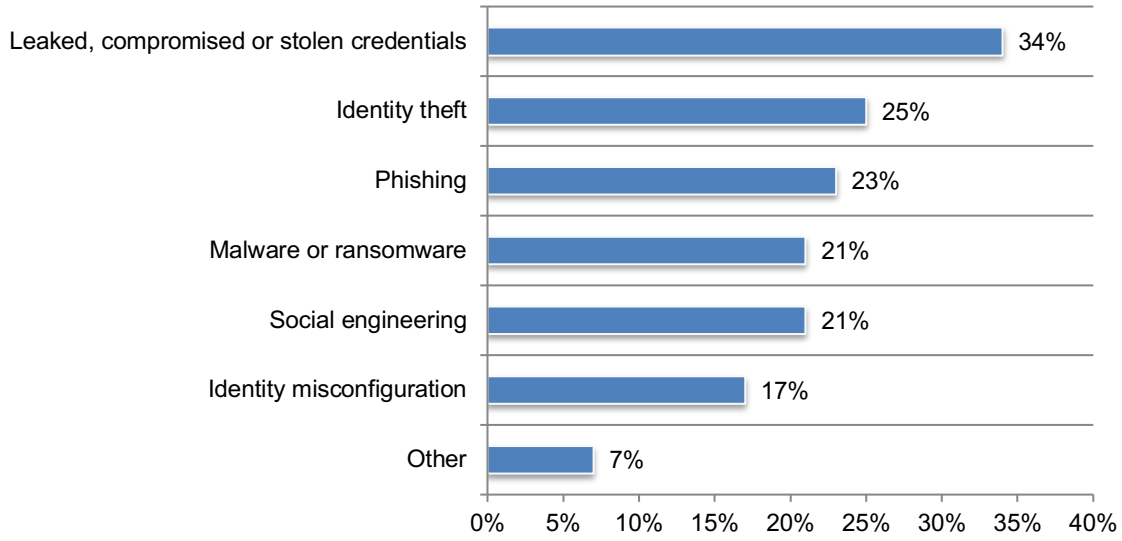
In this section of the report, we present an analysis of the findings. The complete findings are presented in the Appendix. We have organized the report according to the following topics.

- Risks to identity security
- Managing user access & IT privileges in the IAM platform
- Current and future trends in identity security technologies
- Best practices in achieving a strong identity security posture

Risks to identity security

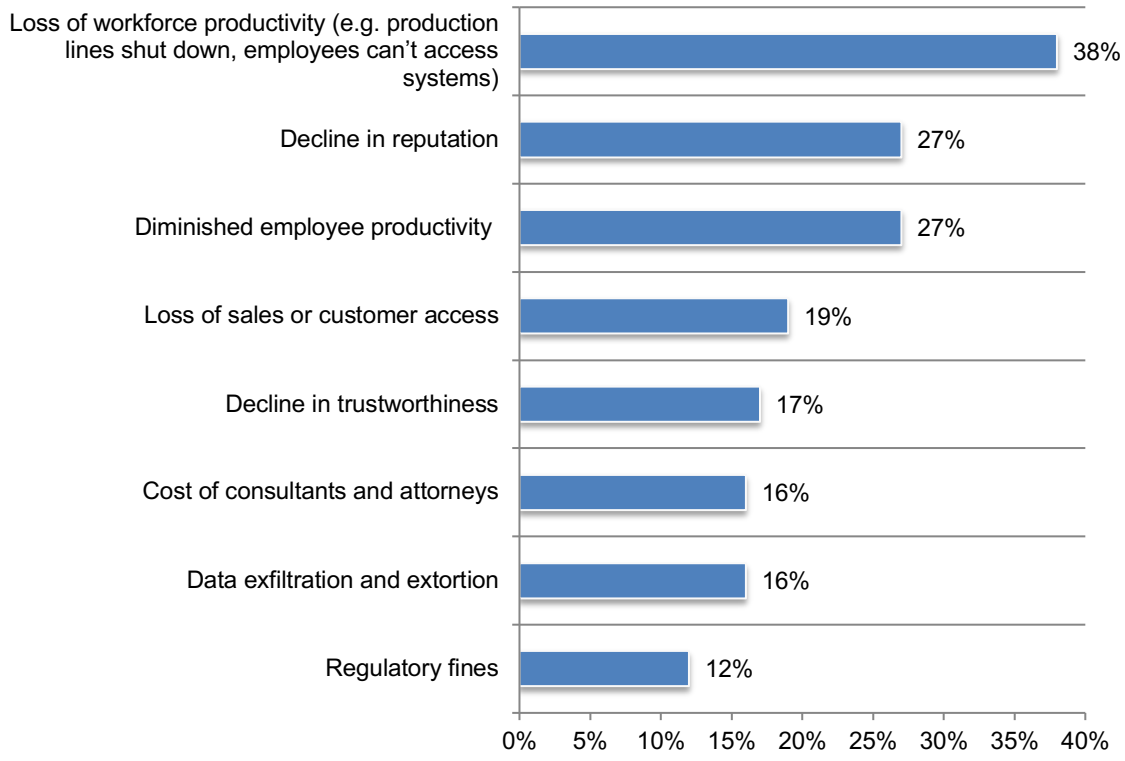
Leaked, compromised or stolen credentials were most likely to cause an identity-based security incident. In the past 12 months, 50 percent of organizations represented in this research had an identity-based security incident. According to Figure 2, the number one cause was leaked, compromised or stolen credentials (34 percent of respondents). Other primary causes were identity theft (25 percent of respondents) and phishing (23 percent of respondents).

Figure 2. What were the causes of the identity-based security incident(s)?
More than one response permitted



In addition to the possibility of fines and other financial consequences, identity-based security incidents cause declines in workforce and employee productivity. Respondents were asked how the incident affected their organizations. As shown in Figure 3, organizations experienced such serious consequences as the loss of workforce productivity because employees couldn't access systems (38 percent of respondents) and diminishment of employee productivity (27 percent of respondents). Reputation of the organization also declined (27 percent of respondents).

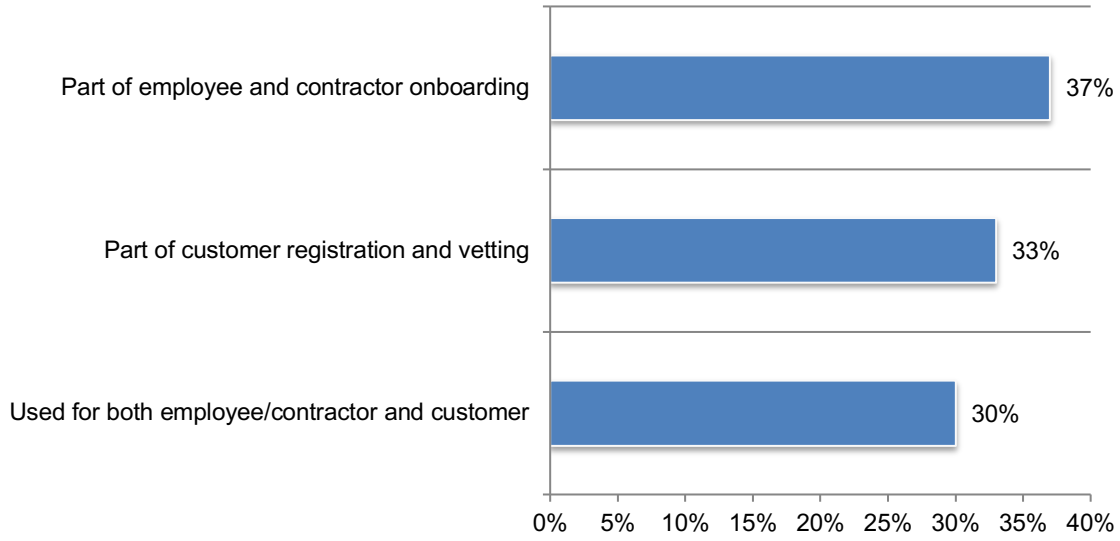
Figure 3. What was the impact of the identity-based security incident(s)?
More than one response permitted



Few organizations use identity verification solutions and services to confirm a person's claimed identity. Identity verification solutions are systems that confirm the authenticity of a person's identity, typically in digital contexts, such as online transactions or applications. These solutions use various methods to verify a person's identity, ensuring they are who they claim to be.

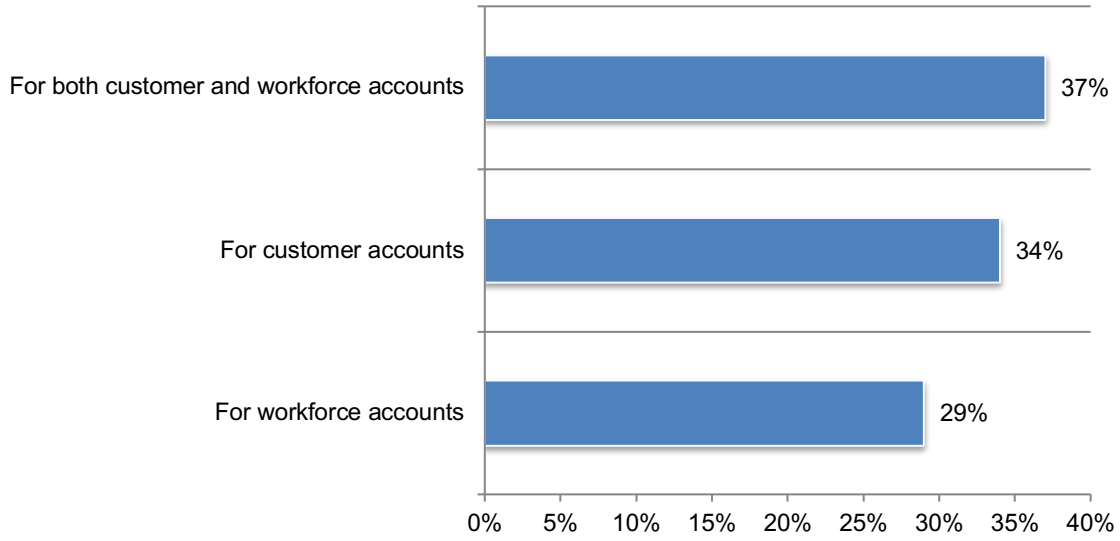
Only 39 percent of respondents say their organizations use identity verification solutions and services. As shown in Figure 4, if they do use identity verification solutions and services, it is mainly for employee and contractor onboarding (37 percent of respondents). Thirty-three percent of respondents say it is part of customer registration and vetting, and 30 percent of respondents say it is used for both employee/contractor and customer.

Figure 4. How are identity verification solutions and services used?



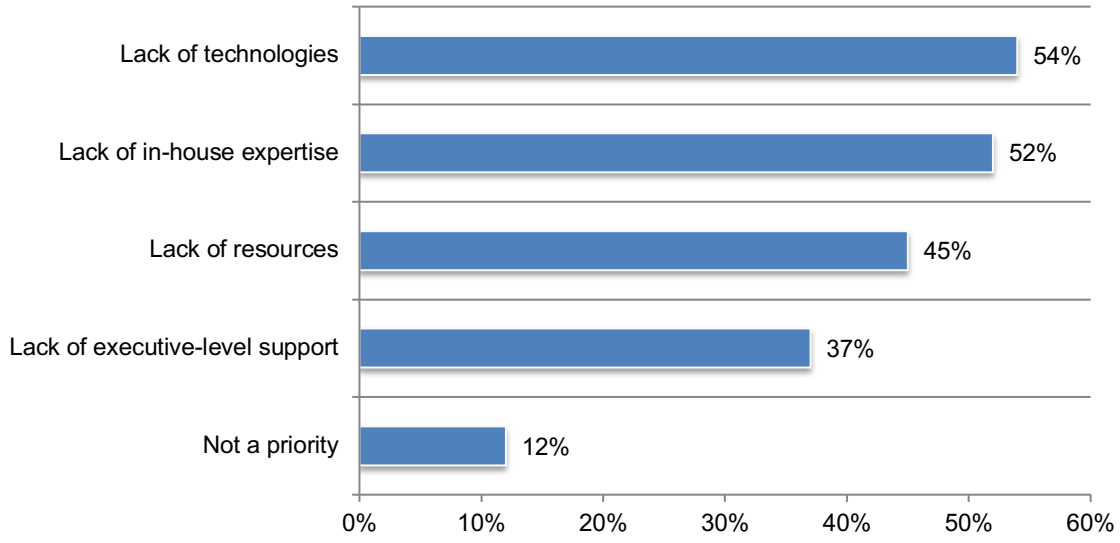
Less than half of organizations (47 percent) have an automated mechanism that checks for compromised passwords. According to Figure 5**,** if they automate checks for compromised passwords, 37 percent of respondents say it is for both customer and workforce accounts. Thirty-four percent only automate checks for customer accounts, and 29 percent only automate checks for workforce accounts.

Figure 5. How are these automated mechanisms used?



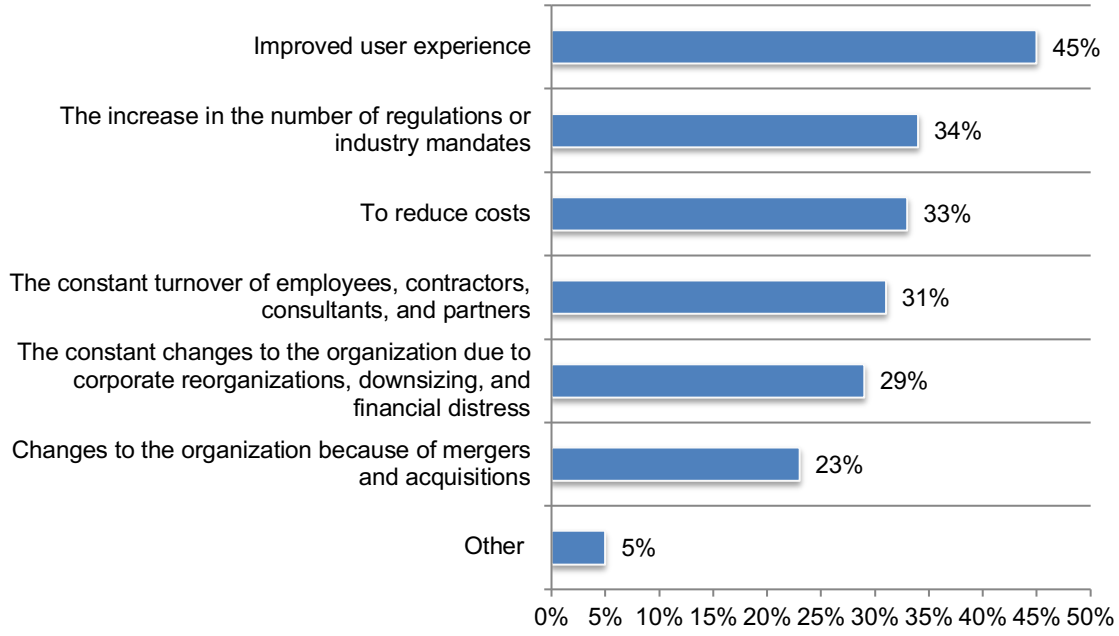
To close the identity security gap, organizations need technologies, in-house expertise and resources. As shown in Figure 6, the top three gaps in identity security are the lack of technologies (54 percent of respondents), lack of in-house expertise (52 percent of respondents), and lack of resources (45 percent of respondents).

Figure 6. What are the biggest challenges to effectively implementing an identity-based security strategy?
Two responses permitted



Security is not the highest priority when making IAM investment decisions. Despite the many high-profile examples of insider security breaches, 45 percent of respondents say the number one priority for investing in IAM is to improve user experience, according to Figure 7. Similarly, investments are not prioritized to address weaknesses caused by the increase in number of regulations or industry mandates (34 percent of respondents), or the constant turnover of employees, contractors, consultants and partners (31 percent of respondents).

Figure 7. What are the most important drivers for investing in IAM security?
Two responses permitted



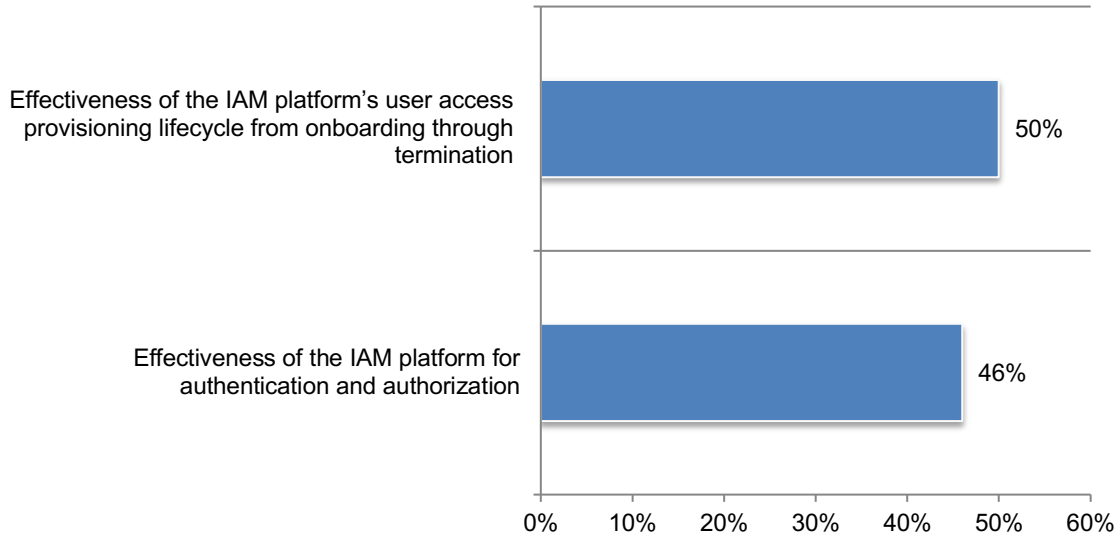
Managing user access & IT privileges in the IAM platform

IAM platforms utilize various data sources to manage user identities and access rights. These include directory services, user accounts, and application and resource information. They also integrate with external systems like HR databases and IT systems for comprehensive identity management. An average of 86 data sources are integrated in the IAM platform.

To achieve greater maturity, organizations need to improve the ability of IAM platforms to authenticate and authorize user identities and access rights. Respondents were asked to rate the effectiveness of their IAM platform in user access provisioning lifecycle from onboarding through termination, and its effectiveness authenticating and authorizing on a scale of 1 = not effective to 10 = highly effective.

According to Figure 8, only 46 percent of respondents say their IAM platform is very or highly effective for authentication and authorization. Fifty percent of respondents rate the effectiveness of their IAM platforms' user access provisioning lifecycle from onboarding through termination as very or highly effective.

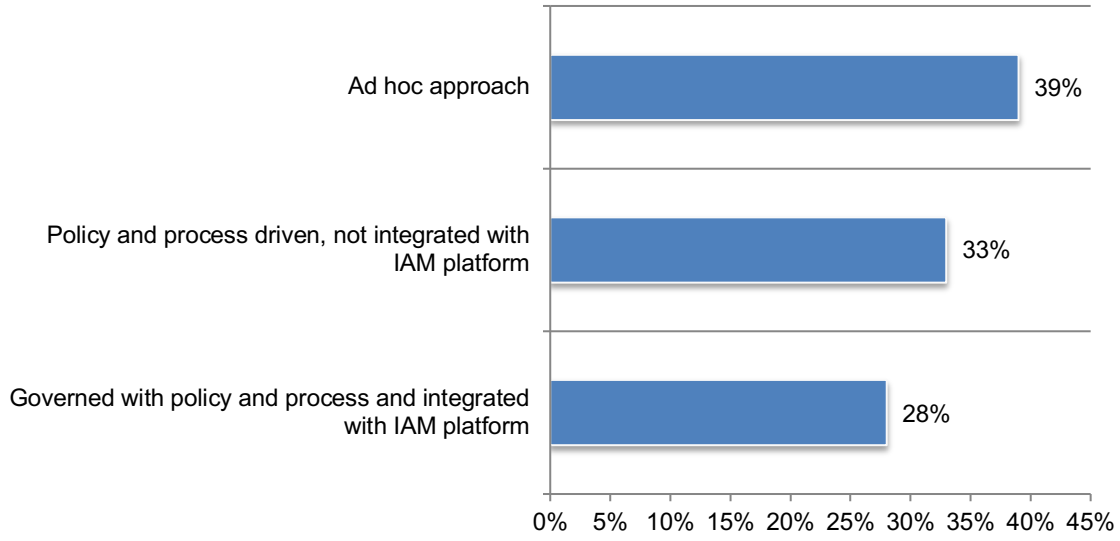
Figure 8. The effectiveness of an IAM platform's user access provisioning
On a scale from 1 = not effective to 10 = highly effective, 7+ responses presented



Policies and processes are rarely integrated with IAM platforms to manage machine, service and other non-human accounts or identities. Forty-four percent of respondents say their IAM platform and/or processes are used to manage machine, service and other non-human accounts or identities. Thirty-nine percent of respondents say their organizations are at the adoption stage of using their IAM platform and/or processes to manage machine, service and other non-human accounts.

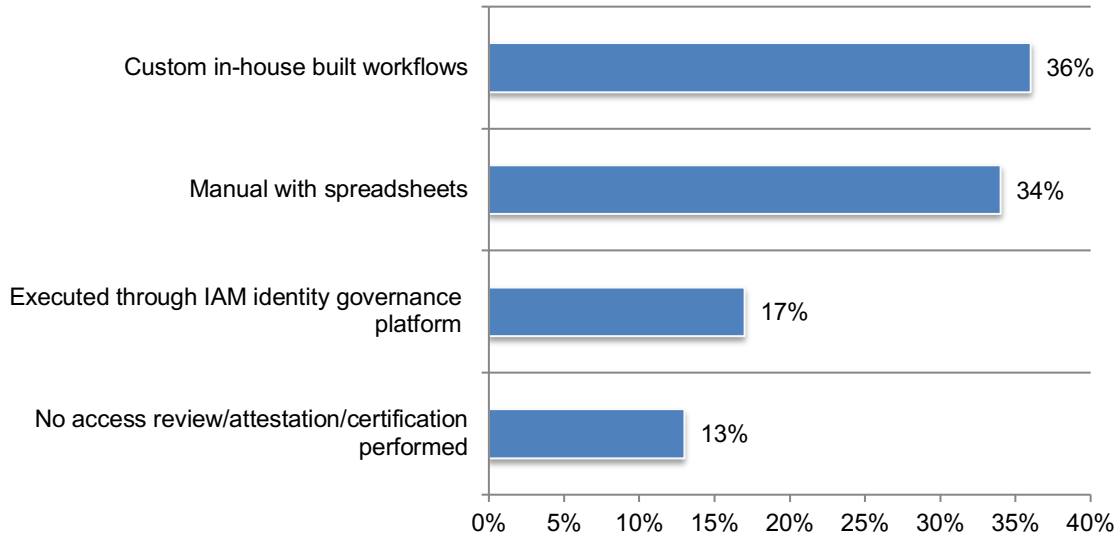
As shown in Figure 9, of these 83 percent of respondents (44 percent + 39 percent), 39 percent say the use of the IAM platform to manage machine, service and other non-human accounts or identities is ad hoc. Only 28 percent of these respondents say management is governed with policy and process integrated with the IAM platform.

Figure 9. How does your organization use its IAM platform and/or processes to manage machine, service and other non-human accounts or identities?



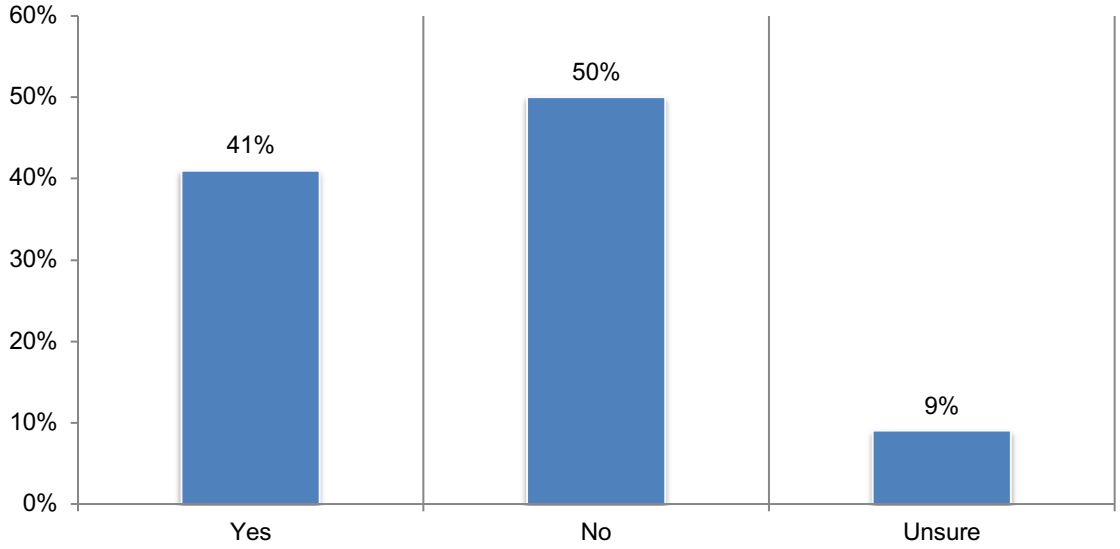
Periodic access to review/attestation/certification of user accounts and entitlements is mostly manual. Eighty-seven percent of respondents say their organization performs access review/attestation/certification. According to Figure 10, 36 percent of respondents say their organizations use custom in-house built workflows, 34 percent of respondents say it is manual with spreadsheets, and 17 percent of respondents say it is executed through the IAM identity governance platform.

Figure 10. What are the most important processes to perform periodic access review/attestation/certification of user accounts and entitlements?



According to Figure 11, only 41 percent of respondents use internal applications and resources based on their roles and needs to streamline onboarding, offboarding and access management. An average of 38 percent of internal applications are managed by their organizations' IAM platforms.

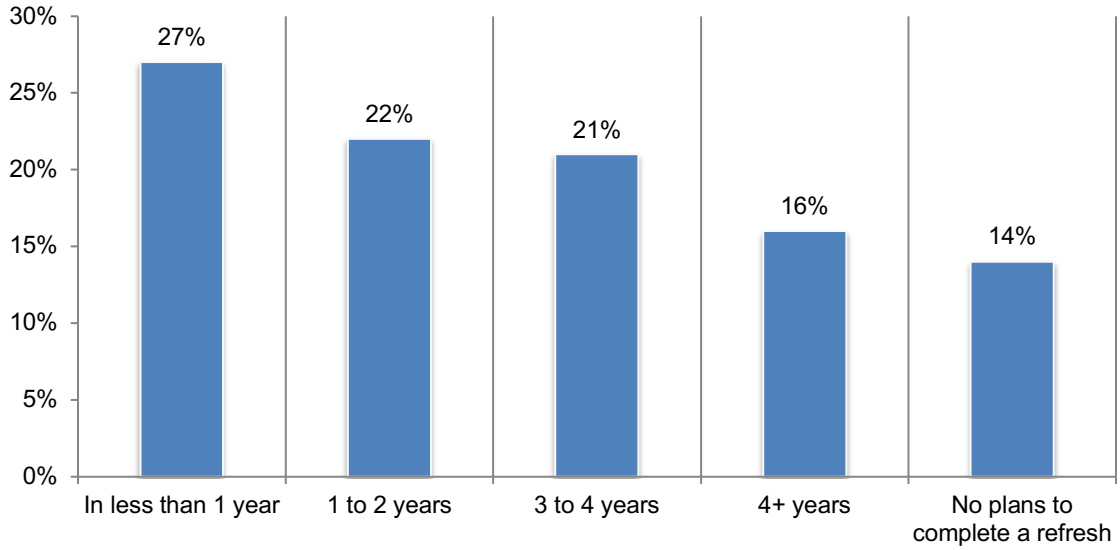
Figure 11. Does your organization use internal application provisions to grant users access to internal applications and resources based on their roles and needs, streamlining onboarding, offboarding and access management?



More organizations will complete a refresh to a cloud-or SaaS-delivered IAM platform for user access provisioning, lifecycle from onboarding to termination. Currently, 39 percent of respondents have completed a refresh.

As shown in Figure 12, 86 percent of respondents say their organizations will complete a refresh in less than 1 year (27 percent), 1 to 2 years (22 percent), 3 to 4 years (21 percent) or 4+ years (16 percent).

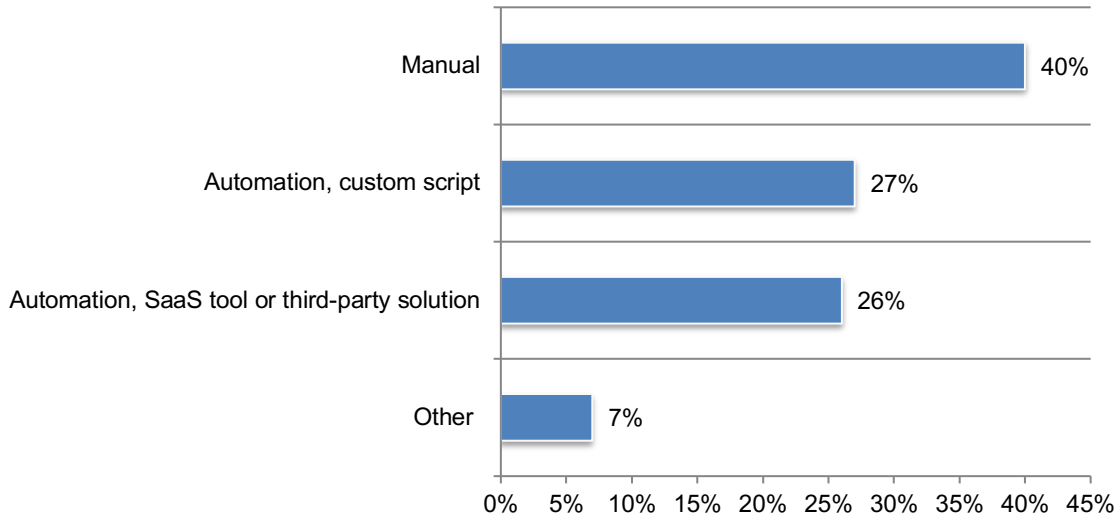
Figure 12. If no, will your organization complete a refresh to a cloud-or SaaS-delivered IAM platform for user access provisioning, lifecycle from onboarding to termination?



Deprovisioning non-human identities, also known as non-human identity management (NHIM), focuses on removing or disabling access for digital entities like service accounts, APIs, and IoT devices when they are no longer needed. This process is crucial for security, as it helps prevent the misuse of credentials by automated systems that could lead to data breaches or system compromises.

Deprovisioning user access is mostly manual. Forty-one percent of respondents say their organizations include non-human identities when deprovisioning user access. According to Figure 13, this is mostly a manual process (40 percent of respondents). Twenty-seven percent of respondents say the process is automated with a custom script, and 26 percent say it is automated with a SaaS tool or third-party solution.

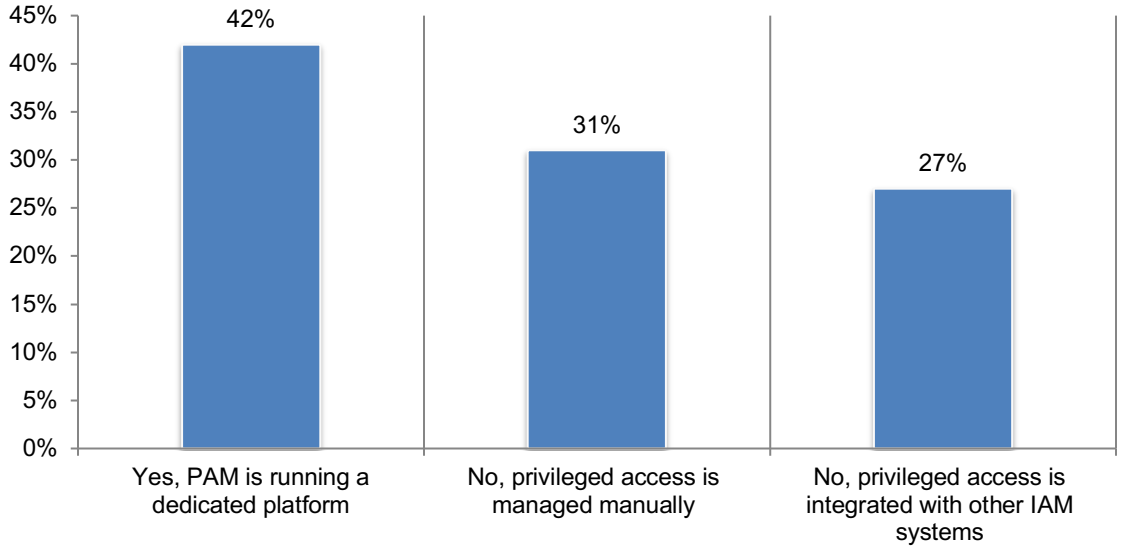
Figure 13. How does your organization deprovision user access?



A PAM (Privileged Access Management) platform is a cybersecurity technology that secures, manages and monitors privileged accounts across an IT environment. It focuses on accounts with elevated permissions, like administrator accounts, and uses techniques like credential vaulting, session monitoring, and access controls to protect sensitive resources. PAM ensures only authorized users can access critical systems and data, minimizing the risk of breaches and operational disruptions.

Few organizations are integrating privileged access with other IAM systems, and if they do, the integration is not effective. According to Figure 14, 42 percent of respondents say PAM is running on a dedicated platform. Twenty-seven percent say privileged access is integrated with other IAM systems, and 31 percent of respondents say privileged access is managed manually. Of these 27 percent of respondents, only 45 percent rate the effectiveness of their organizations' IAM platforms for PAM as very or highly effective.

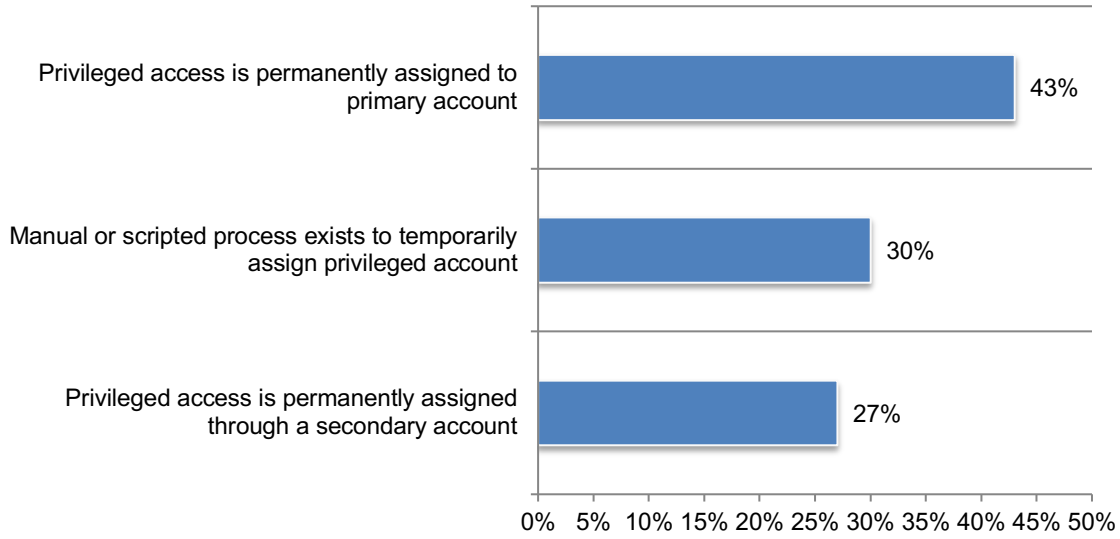
Figure 14. Does your organization have a dedicated PAM platform?



Privileged access refers to the ability of individuals or entities to access resources and systems with higher-than-standard permissions, often including administrative or superuser-level access. This access allows them to perform sensitive operations and manage critical aspects of the organization's infrastructure.

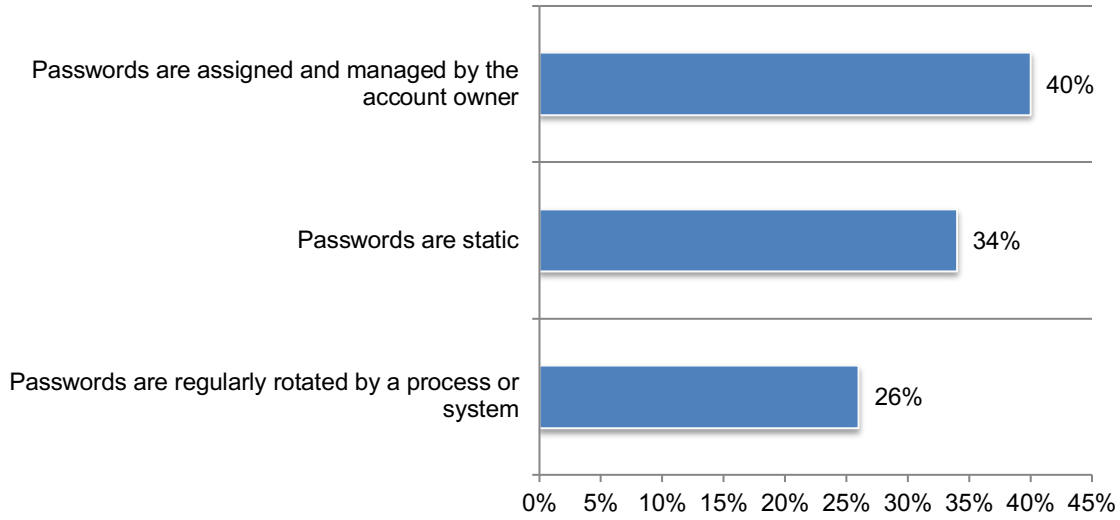
As shown in Figure 15, 43 percent of respondents say privileged access is permanently assigned to a primary account, 30 percent of respondents say a manual or script exists to temporarily assign a privileged account, and 27 percent of respondents say privileged access is permanently assigned through a secondary account.

Figure 15. How does your organization assign privileged access?
Only one choice permitted



As shown in Figure 16, 40 percent of respondents say the management of privileged access passwords, including privileged access assigned to service accounts, is managed by the account owner. Thirty-four percent of respondents say passwords are static, and 26 percent of respondents say passwords are regularly rotated by a process or system.

Figure 16. How does your organization manage privileged access passwords, including privileged access assigned to service accounts?

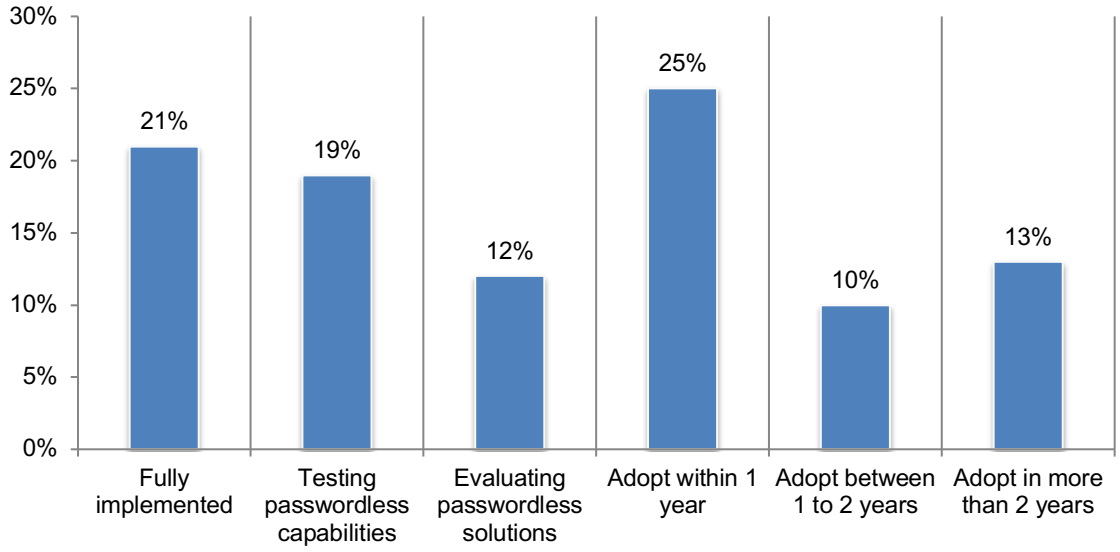


Current and future trends in identity security technologies

Passwordless authentication is a means to verify a user's identity without using a password. Instead passwordless uses more secure alternatives like possession factors, one-time passwords (OTP), registered smartphones or biometrics.

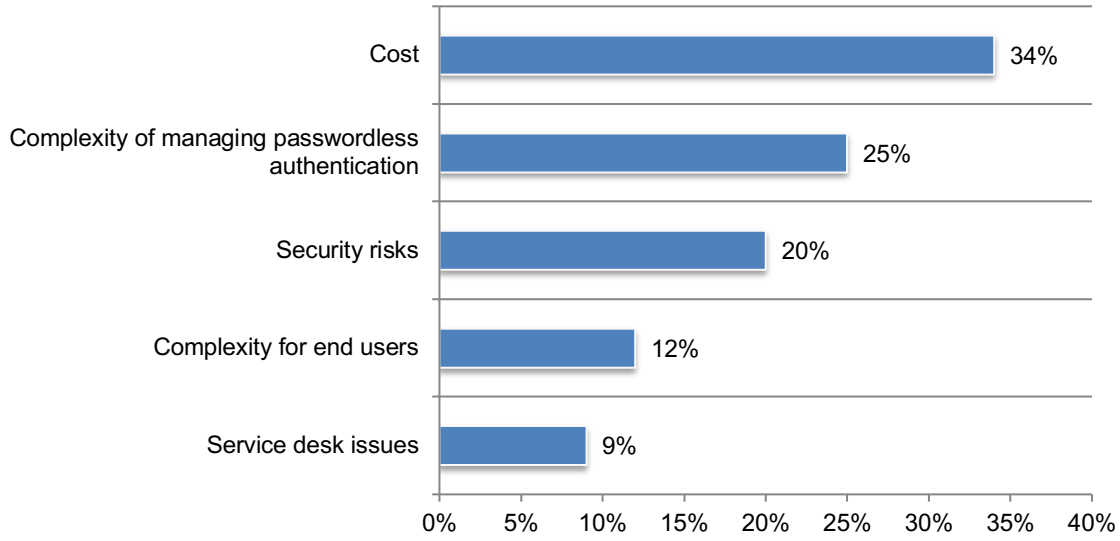
The adoption of passwordless authentication is in its early stages. Fifty-five percent of respondents say their organizations have adopted or plan to adopt passwordless authentication. However, only 21 percent of these respondents say it is fully implemented in their organizations, as shown in Figure 17.

Figure 17. What best describes your organization's adoption or plan to adopt passwordless authentication?



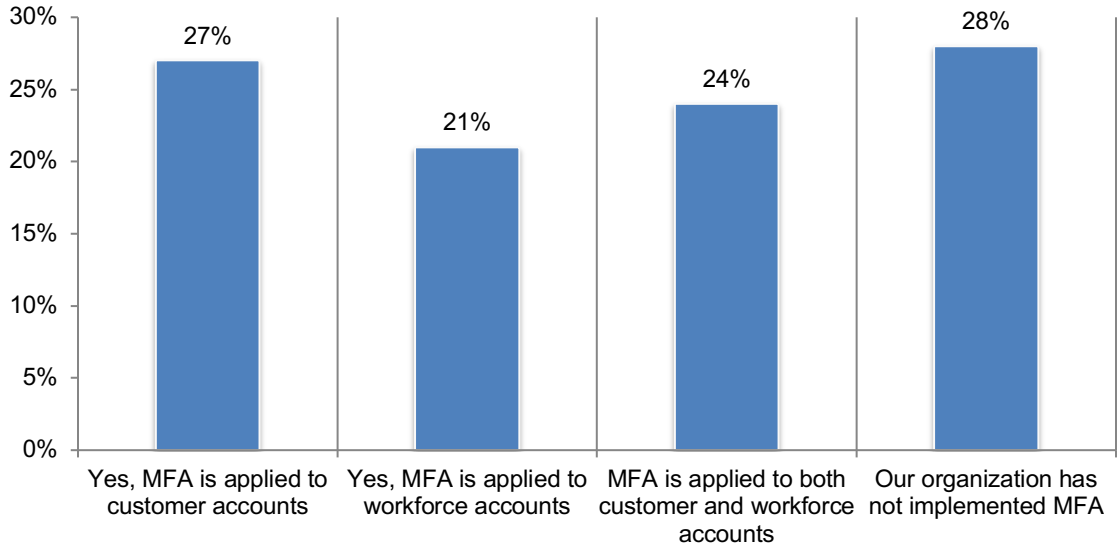
Cost and complexity deter the adoption of passwordless authentication. Of the 45 percent of respondents who say their organizations have no plans to adopt passwordless authentication, 34 percent say it is the cost, and 25 percent say it is the complexity of managing passwordless authentication, as shown in Figure 18.

Figure 18. Why would your organization not adopt passwordless authentication?



Seventy-two percent of organizations have implemented multifactor authentication MFA. According to Figure 19, 27 percent of respondents say MFA is applied to customer accounts only, 24 percent of respondents say MFA is applied to both customer and workforce accounts, and 21 percent of respondents say MFA is applied to workforce accounts only.

Figure 19. Has your organization implemented multifactor authentication (MFA)?



Fifty percent of organizations in this research are adopting biometric authentication. Biometric authentication refers to a cybersecurity process that verifies a user's identity using their unique biological traits such as fingerprints, voices, retinas, and facial features. Biometric authentication systems store this information to verify a user's identity when that user accesses their account. According to Figure 20, the most biological traits used are fingerprints (42 percent of respondents), voice patterns (33 percent of respondents) and facial (29 percent of respondents).

Figure 20. What types of biometric authentication does your organization use?
More than one response permitted

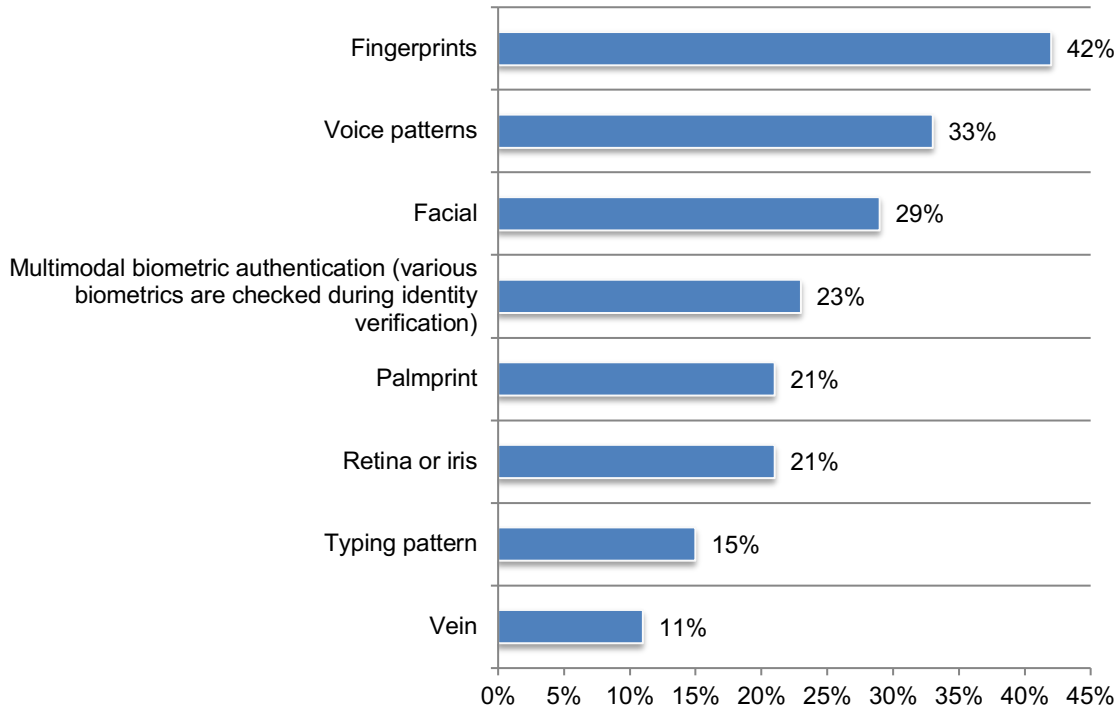


Figure 21. Presents the state of adoption for the following tools, frameworks and processes. As shown, Artificial Intelligence (AI) and Identity Threat Detection and Response (IDTR) lead the adoption.

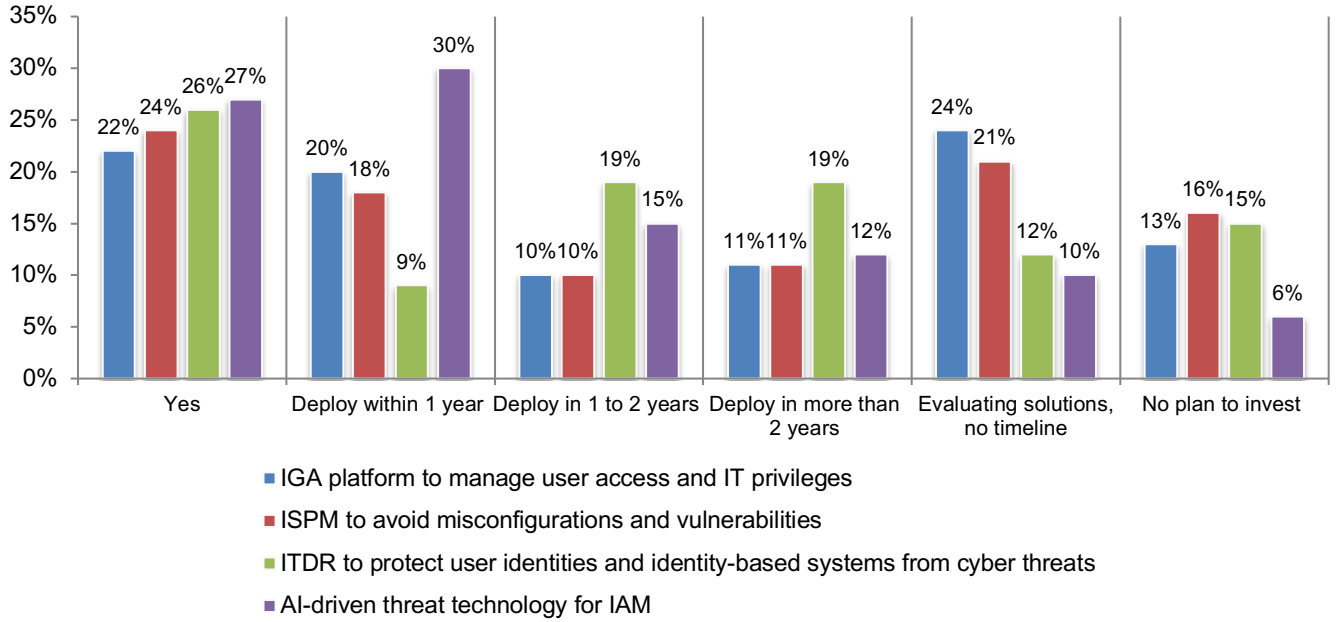
Identity Governance and Administration (IGA) is a set of processes and tools that manage and monitor digital identities and access rights across an organization, ensuring only the right people have access to the right resources at the right time, improving security and compliance. Twenty-two percent of respondents use an IGA to manage user access and IT privileges. Forty-one percent of respondents say they will deploy IGA within 1 year (20 percent), in 1 to 2 years (10 percent), and in more than 2 years (11 percent).

Identity Security Posture Management (ISPM) is a framework used to strengthen and maintain the security posture of an organization's identity infrastructure to prevent breaches. ISPM involves monitoring and analyzing identities, access rights and authentication processes across the enterprise. Twenty-four percent of respondents have a ISPM framework. Thirty-nine percent of respondents say they will deploy ISPM within 1 year (18 percent), in 1 to 2 years (10 percent), or in more than 2 years (11 percent).

Identity Threat Detection and Response (ITDR) focuses on protecting user identities and identity-based systems from cyber threats. ITDR involves a combination of security tools, processes and best practices to effectively prepare for, as well as detect and respond, to identity-related threats. Twenty-six percent of respondents say their organizations use ITDR to protect user identities and identity-based systems from cyber threats. Forty-seven percent of respondents say they will deploy IDTR in 1 year (9 percent), in 1 to 2 years (19 percent), or in more than 2 years (19 percent).

Organizations plan to deploy AI-driven threat technology to reduce identity-based security incidents. Only six percent of respondents do not plan to invest in AI. Twenty-seven percent of respondents say their organizations use AI-driven threat technology specifically to reduce identity-based security incidents, and 30 percent say they will deploy within 1 year.

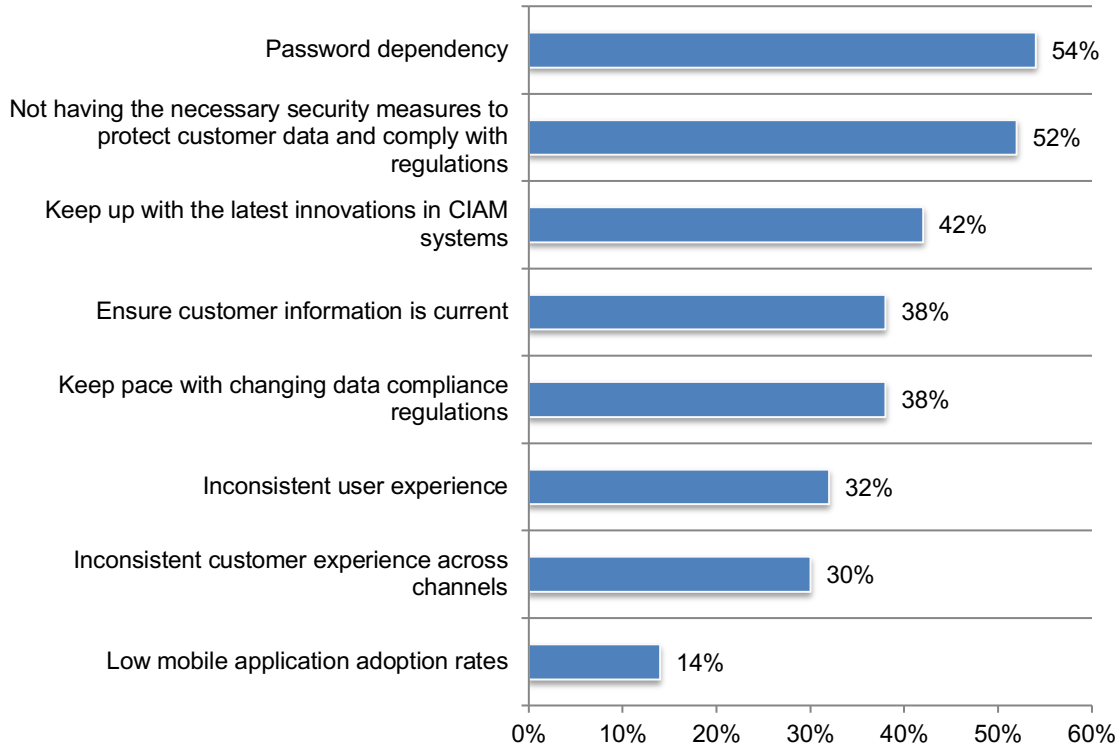
Figure 21. Does your organization use IGA, ISPM, ITDR and AI



Customer Identity and Access Management (CIAM) is a set of technologies and processes that incorporates advanced security methods like multifactor authentication to ensure that only authorized individuals can access sensitive information. Only 26 percent of respondents say their organizations have implemented CIAM. The functions most responsible for CIAM are the digital team (23 percent), IT security (17 percent) or IT (16 percent).

According to Figure 22, password dependency (54 percent of respondents) and not having the necessary security measures to protect customer data and comply with regulations (52 percent of respondents) are the biggest challenges to the success of CIAM.

Figure 22. What are the challenges to having a successful CIAM?
Three responses permitted

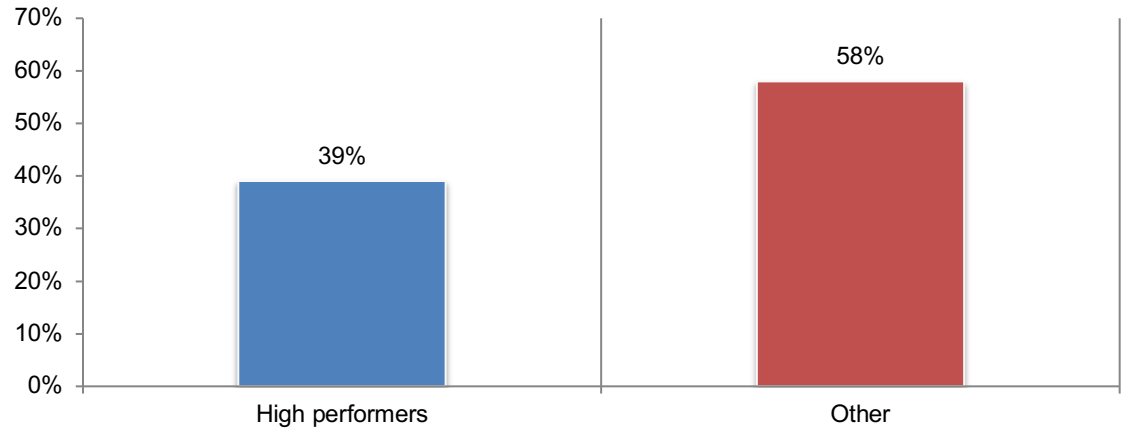


Best practices in achieving a strong identity security posture

In this section, we provide an analysis of high performers based on how respondents rated the effectiveness of their tools and investments in combating modern identity threats on a scale from 1 = low effectiveness to 10 = high effectiveness. The high performer organizations are highly effective based on rating their organizations' effectiveness from 9 to 10 and represent 23 percent of the final sample. Seventy-seven percent of respondents rate their effectiveness from 1 to 8 on the 10-point scale. We refer to this sample as other in the figures below.

Organizations that have effective tools and investments in combating modern identity threats are less likely to experience an identity-based security incident. Only 39 percent of high performers had an identity-based security incident, as shown in Figure 23.

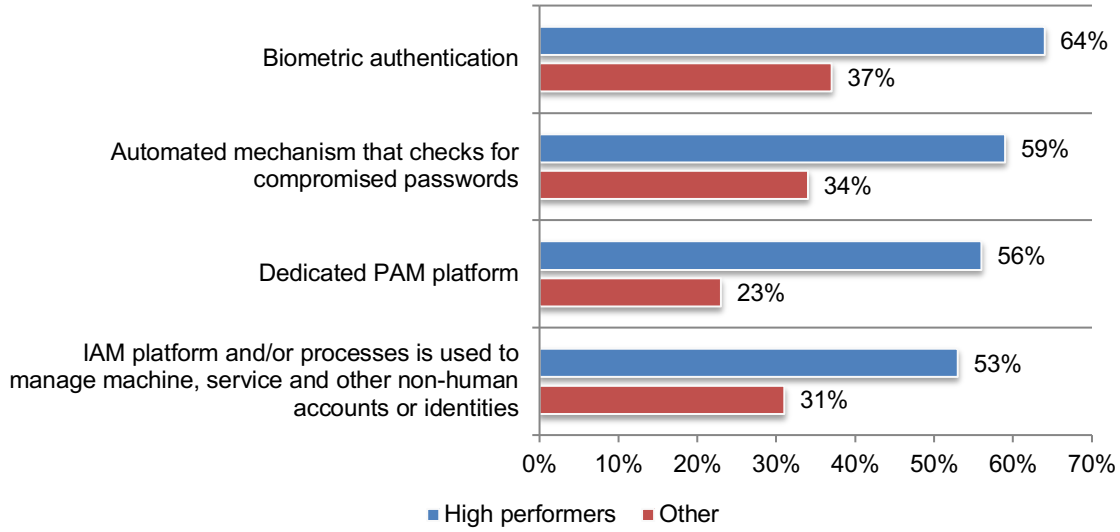
Figure 23. In the past 12 months, did your organization experience an identity-based security incident?
Yes responses



Following are the differences in the tools and investments between the high performers and others in the research. High performers are outpacing other respondents in the adoption of automation and advanced identity security technologies.

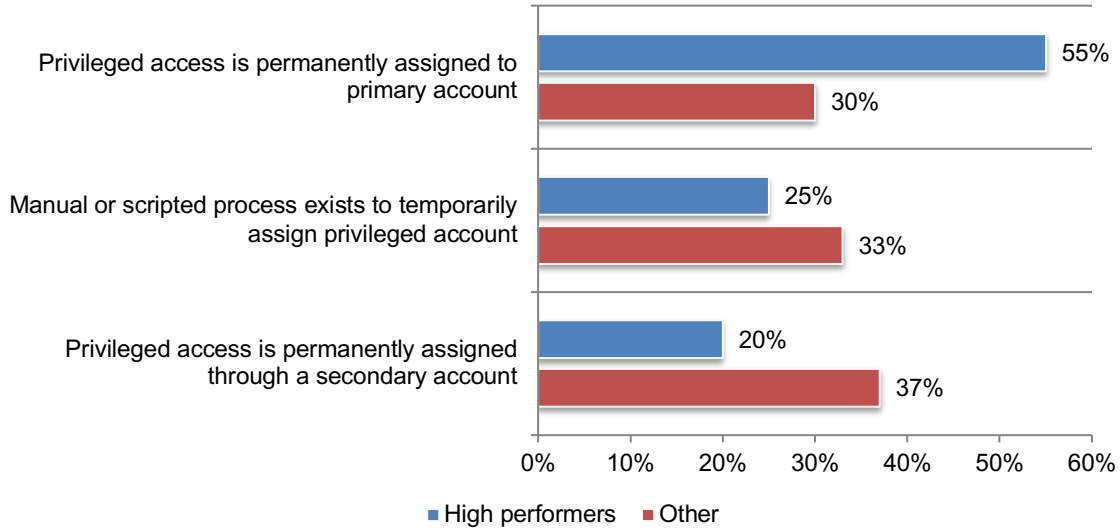
According to Figure 24, 64 percent of high performers vs. 37 percent of other respondents have adopted biometric authentication. Fifty-nine percent of high performers vs. 34 percent of other respondents use automated mechanisms that check for compromised passwords. Fifty-six percent of respondents of high performers vs. 23 percent of other respondents have a dedicated PAM platform, and 53 percent of high performers vs. 31 percent of other respondents use IAM platforms and/or processes used to manage machine, service and other non-human accounts or identities.

Figure 24. The differences in tools and investments between high performer and other respondents
Yes responses



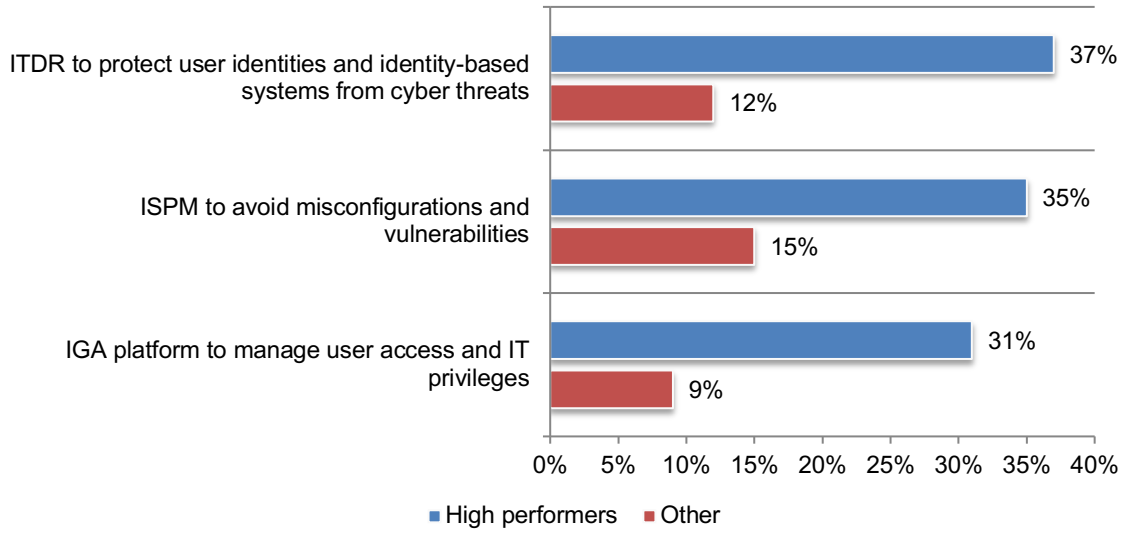
More high performers assign privileged access to a primary account (55 percent vs. 30 percent). Fewer high performers use manual or scripted processes to temporarily assign privileged accounts (25 percent of high performers vs. 33 percent of other respondents), as shown in Figure 25.

Figure 25. How does your organization assign privileged access?



High performers are leading in the adoption of ITDR, ISPM and IGA platforms, as shown in Figure 26. Thirty-seven percent of high performers vs. 12 percent of other respondents have adopted IDTR, 35 percent of high performers vs. 15 percent of other respondents have adopted ISPM, and 31 percent of high performers vs. 9 percent of other respondents have adopted IGA platforms.

Figure 26. Technologies to manage user access, misconfigurations and vulnerabilities and detect identity threats.
Yes responses



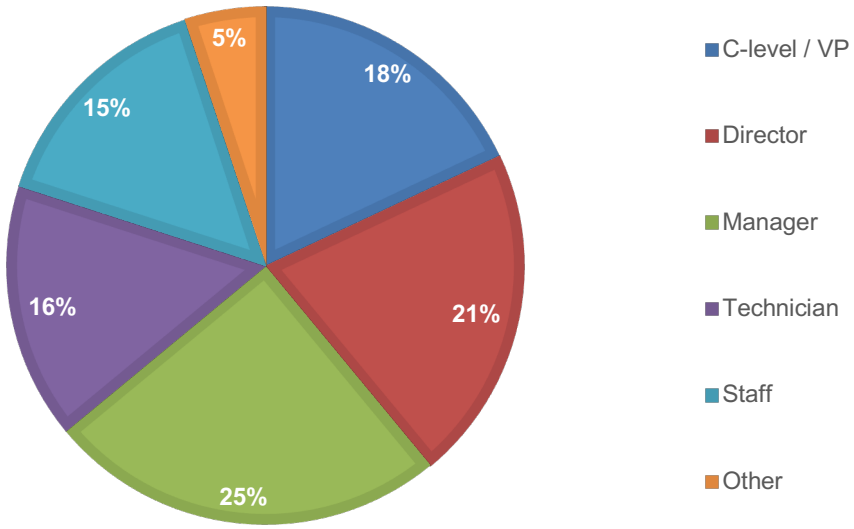
Part 4. Methodology

A sampling frame of 16,900 IT and IT security practitioners in the U.S. who are involved in their organizations' identity and access management program were selected as participants to this survey. Table 1 shows 695 total returns. Screening and reliability checks required the removal of 69 surveys. Our final sample consisted of 626 surveys or a 3.7 percent response.

Table 1. Sample response	Freq	Pct%
Sampling frame	16,900	100.0%
Total returns	695	4.1%
Rejected or screened surveys	69	0.4%
Final sample	626	3.7%

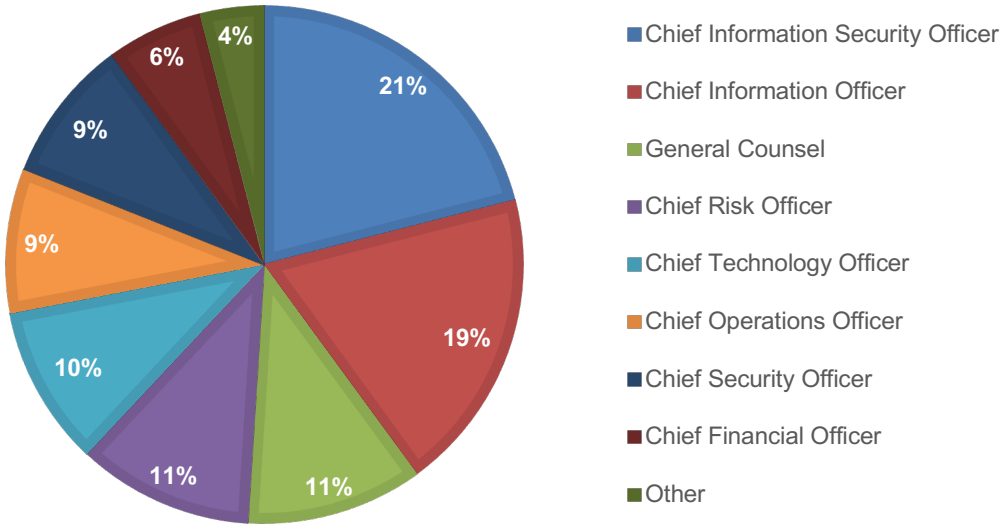
Pie Chart 1 reports the respondent's current position within the organization. Eighteen percent of respondents report their current position as C-level/VP, 21 percent of respondents are directors, 25 percent of respondents are manager, as shown in Pie Chart 1.

Pie Chart 1. Respondents current position within the organization



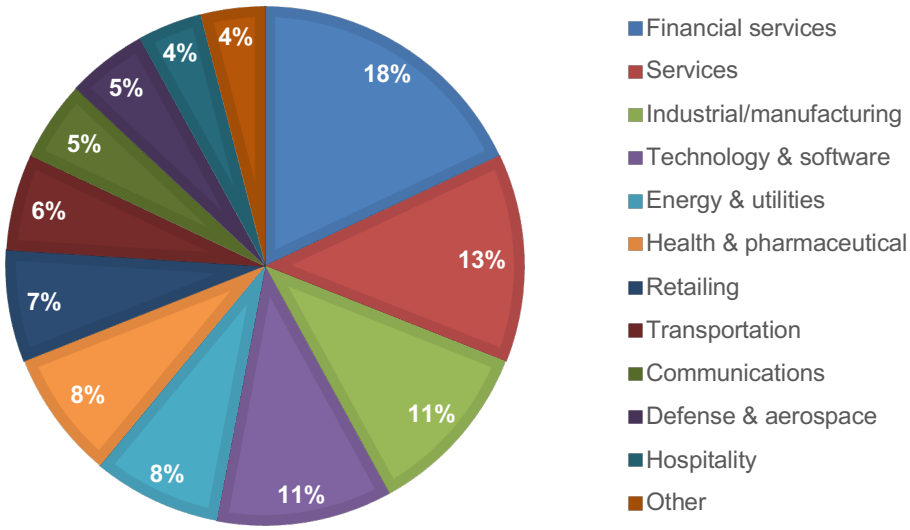
Pie Chart 2 reports the primary person the respondent reports to within the organization. Twenty-one percent of respondents report to the chief information security officer, 19 percent of respondents report to the chief information officer, 11 percent report to the general counsel, 11 percent of respondents report to the chief risk officer, 10 percent of respondents report to the chief technology officer, as shown in Pie Chart 2.

Pie Chart 2. Primary person respondent reports to within the organization



Pie Chart 3 reports the industry focus of the respondent's organizations. This chart identifies financial services (18 percent) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by services[2] (13 percent of respondents), industrial manufacturing (11 percent of respondents), technology and software (11 percent of respondents), energy and utilities, and health and pharmaceuticals (each at 8 percent of respondents).

Pie Chart 3. Primary industry focus



[2] Services include, but are not limited to, law and accounting firms and major consulting firms.

Part 5. Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of IT decision makers and security professionals. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Part 6. Appendix with the detailed audited findings

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in March 2025.

Survey Response	Freq
Total sampling frame	16,900
Total survey returns	695
Rejected or failed surveys	69
Final sample	626
Response rate	3.7%

Part 1: Screening questions

S1. Which best describes your role and involvement in your organization's IAM program. Please select all that apply.	Pct%
Setting IAM program priorities	32%
Managing budget	39%
Selecting IAM vendors and contractors	48%
Determining strategy	35%
Evaluating IAM effectiveness	33%
Mitigating IAM security risk	41%
IAM engineering or support	47%
Digital user experience	28%
Managing IAM personnel, teams, and projects	26%
IAM end user	54%
None of the above (Stop)	0%

S2. What is the headcount of your organization?	Pct%
Less than 500 (Stop)	0%
500 to 2,000	10%
2,001 to 10,000	20%
10,001 to 25,000	22%
25,001 to 50,000	25%
50,001 to 75,000	13%
More than 75,000	10%
Total	100%

Part 2: Organization's IAM coverage and investment

Q1. How effective are your organization's tools and investments in combating modern identity threats from 1 = not effective to 10 = highly effective.	Pct%
1 or 2	11%
3 or 4	16%
5 or 6	23%
7 or 8	27%
9 or 10	23%
Total	100%

Q2. What describes your organization's IT environment? Please select one choice only.	Pct%
On-premise	29%
Cloud	41%
Hybrid	30%
Total	100%

Q3. Does your organization include non-human identities in deprovisioning user access?	Pct%
Yes	41%
No	52%
Unsure	7%
Total	100%

Q4. If yes, how does your organization deprovision user access?	Pct%
Manual	40%
Automation, custom script	27%
Automation, SaaS tool or third-party solution	26%
Other (please specify)	7%
Total	100%

Q5. How many data sources are integrated into your organization's IAM platform?	Pct%
None	10%
1 to 50	12%
51 to 100	29%
101 to 150	33%
150+	11%
Unsure	5%
Total	100%

Q6. Does your organization use internal application provisions to grant users access to internal applications and resources based on their roles and needs, streamlining onboarding, offboarding, and access management?	Pct%
Yes	41%
No	50%
Unsure	9%
Total	100%

Q7. If yes, what percentage of internal applications are managed by your organization's IAM platform?	Pct%
None	9%
1 to 25%	29%
26 to 50%	30%
51 to 75%	20%
76 to 100%	12%
Total	100%

Q8. Approximately, what is the dollar range that best describes your organization's IT security budget in 2025?	Pct%
< $5 million	11%
$5 to $10 million	18%
$11 to $50 million	27%
$51 to $100 million	22%
> $100 million	22%
Total	100%

Q9 Using the following 10-point scale, please rate the priority of investing in IAM technologies compared to other IT security technologies from 1 = not a priority to 10 = high priority.	Pct%
1 or 2	10%
3 or 4	16%
5 or 6	27%
7 or 8	22%
9 or 10	25%
Total	100%

Part 3: Potential IAM security risks and exposures

Q10. In the past 12 months, did your organization experience an identity-based security incident?	Pct%
Yes	50%
No (please skip to Q13)	46%
Unsure (please skip to Q13)	4%
Total	100%

Q11. If yes, what were the causes of the identity-based security incident(s)? Please select all that apply.	Pct%
Identity misconfiguration	17%
Leaked, compromised or stolen credentials	34%
Phishing	23%
Social engineering	21%
Identity theft	25%
Malware or ransomware	21%
Other	7%
Total	148%

Q12. What was the impact of the identity-based security incident? Please select all that apply.	Pct%
Loss of workforce productivity (e.g. production lines shut down, employees can't access systems)	38%
Loss of sales or customer access	19%
Data exfiltration and extortion	16%
Diminished employee productivity	27%
Cost of consultants and attorneys	16%
Decline in reputation	27%
Decline in trustworthiness	17%
Regulatory fines	12%
Other (please specify)	0%
Unsure	0%
Total	172%

Q13. Does your organization use identity verification solutions and services to confirm a person's claimed identity?	Pct%
Yes	39%
No	57%
Unsure	4%
Total	100%

Q14. If yes, how are these identity solutions used? Please select one choice only.	Pct%
Part of employee and contractor onboarding	37%
Part of customer registration and vetting	33%
Used for both employee/contractor and customer	30%
Total	100%

Q15. Does your organization have an automated mechanism that checks for compromised passwords?	Pct%
Yes	47%
No	50%
Unsure	3%
Total	100%

Q16. If yes, how are these automated mechanisms used? Please select one choice only.	Pct%
For customer accounts	34%
For workforce accounts	29%
For both customer and workforce accounts	37%
Total	100%

Part 4: Understanding IAM and strategies

Q17. Using the following 10-point scale, please rate the effectiveness of your IAM platform's user access provisioning lifecycle from onboarding through termination from 1 = not effective to 10 = highly effective.	Pct%
1 or 2	12%
3 or 4	21%
5 or 6	17%
7 or 8	29%
9 or 10	21%
Total	100%

Q18. Using the following 10-point scale, please rate the effectiveness of your IAM platform for authentication and authorization from 1 = not effective to 10 = highly effective.	Pct%
1 or 2	14%
3 or 4	19%
5 or 6	21%
7 or 8	27%
9 or 10	19%
Total	100%

Q19. Using the following 10-point scale, please rate your organization's confidence in its ability to prevent identity-based security incidents from 1 = not confident to 10 = highly confident.	Pct%
1 or 2	18%
3 or 4	20%
5 or 6	18%
7 or 8	24%
9 or 10	20%
Total	100%

Q20. Has your organization completed a refresh to a cloud-or SaaS-delivered IAM platform for user access provisioning, lifecycle from onboarding to termination?	Pct%
Yes	39%
No	61%
Total	100%

Q21. If no, will your organization complete a refresh to a cloud-or SaaS-delivered IAM platform for user access provisioning, lifecycle from onboarding to termination?	Pct%
In less than 1 year	27%
1 to 2 years	22%
3 to 4 years	21%
4+ years	16%
No plans to complete a refresh	14%
Total	100%

Q22. What are the biggest challenges to effectively implementing an identity-based security strategy? Please select the top two challenges.	Pct%
Lack of technologies	54%
Lack of resources	45%
Lack of executive-level support	37%
Lack of in-house expertise	52%
Not a priority	12%
Total	200%

Q23. What are the most important drivers for investing in IAM security? Please select the top two choices.	Pct%
The increase in the number of regulations or industry mandates	34%
The constant turnover of employees, contractors, consultants, and partners	31%
Improved user experience	45%
To reduce costs	33%
The constant changes to the organization due to corporate reorganizations, downsizing, and financial distress	29%
Changes to the organization because of mergers and acquisitions	23%
Other (please specify)	5%
Total	200%

Q24. Does your organization use its IAM platform and/or processes to manage machine, service and other non-human accounts or identities?	Pct%
Yes	44%
Adoption in process of IAM platform and/or processes to manage machine, service and other non-human accounts or identities	39%
No plans to adopt (please skip to Q26)	17%
Total	100%

Q25. If yes, how does your organization use its IAM platform and/or processes to manage machine, service and other non-human accounts or identities? Please select one choice only.	Pct%
Ad hoc approach	39%
Policy and process driven, not integrated with IAM platform	33%
Governed with policy and process and integrated with IAM platform	28%
Total	100%

Q26. How does your organization use its IAM platform and/or processes to perform periodic access review/attestation/certification of user accounts and entitlements?	Pct%
Manual with spreadsheets	34%
Custom in-house built workflows	36%
Executed through IAM identity governance platform	17%
No access review/attestation/certification performed	13%
Total	100%

Q27. Has your organization implemented multifactor authentication (MFA)? Please select one choice only.	Pct%
Yes, MFA is applied to customer accounts	27%
Yes, MFA is applied to workforce accounts	21%
MFA is applied to both customer and workforce accounts	24%
Our organization has not implemented MFA	28%
Total	100%

Q28. Does your organization use biometric authentication?	Pct%
Yes	50%
No (please skip to Q30)	37%
Unsure	13%
Total	100%

Q29. If yes, what types do you use? Please select all that apply.	Pct%
Facial	29%
Voice patterns	33%
Retina or iris	21%
Fingerprints	42%
Palmprint	21%
Vein	11%
Typing pattern	15%
Multimodal biometric authentication (various biometrics are checked during identity verification)	23%
Total	195%

Q30. Does your organization have a dedicated PAM platform?	Pct%
Yes, PAM is running a dedicated platform	42%
No, privileged access is integrated with other IAM systems (please skip to Q32)	27%
No, privileged access is managed manually (please skip to Q32)	31%
Total	100%

Q31. Using the following 10-point scale, please rate the effectiveness of your organization's IAM platform(s) for PAM from 1 = not effective to 10 = highly effective.	Pct%
1 or 2	20%
3 or 4	17%
5 or 6	18%
7 or 8	22%
9 or 10	23%
Total	100%

Q32. How does your organization assign privileged access? Please select one choice only.	Pct%
Privileged access is permanently assigned to primary account	43%
Privileged access is permanently assigned through a secondary account	27%
Manual or scripted process exists to temporarily assign privileged account	30%
Total	100%

Q33. How does you organization manage privileged access passwords, including privileged access assigned to service accounts? Please select one choice only.	Pct%
Passwords are assigned and managed by the account owner	40%
Passwords are regularly rotated by a process or system	26%
Passwords are static	34%
Total	100%

Q34. Has your organization adopted or plan to adopt passwordless authentication?	Pct%
Yes	55%
No plans to adopt (please skip to Q37)	45%
Total	100%

Q35. If yes, what describes your organization's adoption or plan to adopt passwordless authentication?	Pct%
Fully implemented	21%
Testing passwordless capabilities	19%
Evaluating passwordless solutions	12%
Plan to adopt within 1 year	25%
Plan to adopt between 1 to 2 years	10%
Plan to adopt in more than 2 years	13%
Total	100%

Q36. Why would your organization not adopt passwordless authentication?	Pct%
Cost	34%
Complexity of managing passwordless authentication	25%
Complexity for end users	12%
Service desk issues	9%
Security risks	20%
Other (please specify)	0%
Total	100%

Q37. Does your organization use an Identity Governance and Administration (IGA) platform to manage user access and IT privileges?	Pct%
Yes	22%
Currently evaluating solutions, no timeline	24%
Plan to deploy within 1 year	20%
Plan to deploy between 1 and 2 years	10%
Plan to deploy in more than 2 years	11%
No plan to invest in IGA	13%
Total	100%

Q38. Does your organization use Identity Security Posture Management (ISPM) to avoid misconfigurations and vulnerabilities?	Pct%
Yes	24%
Currently evaluating solutions, no timeline	21%
Plan to deploy within 1 year	18%
Plan to deploy between 1 and 2 years	10%
Plan to deploy in more than 2 years	11%
No plan to invest in ISPM	16%
Total	100%

Q39. Does your organization use Identity Threat Detection Response (ITDR) to protect user identities and identity-based systems from cyber threats?	Pct%
Yes	26%
Currently evaluating solutions, no timeline	12%
Plan to deploy within 1 year	9%
Plan to deploy between 1 and 2 years	19%
Plan to deploy in more than 2 years	19%
No plan to invest in ITDR	15%
Total	100%

Q40. Has your organization implemented Customer Identity and Access Management (CIAM)?	Pct%
Yes	26%
No (Please skip to Q43)	74%
Total	100%

Q41. Who has primary responsibility for CIAM? Please select one choice only.	Pct%
Marketing/sales	9%
IT	16%
IT security	17%
Finance	11%
Digital team	23%
Risk	8%
Legal/compliance	16%
Total	100%

Q42. What are the challenges to having a successful CIAM? Please select three choices only.	Pct%
Keep up with the latest innovations in CIAM systems	42%
Password dependency	54%
Inconsistent user experience	32%
Keep pace with changing data compliance regulations	38%
Not having the necessary security measures to protect customer data and comply with regulations	52%
Ensure customer information is current	38%
Inconsistent customer experience across channels	30%
Low mobile application adoption rates	14%
Total	300%

Q43. Does your organization use AI-driven threat technology for IAM?	Pct%
Yes	27%
Currently evaluating solutions, no timeline	30%
Plan to deploy within 1 year	15%
Plan to deploy between 1 and 2 years	12%
Plan to deploy in more than 2 years	10%
No plan to invest in AI for IAM	6%
Total	100%

Q44. Would or does your organization use AI security technology to continuously monitor authenticated user sessions to prevent unauthorized access?	Pct%
Yes	34%
No (please skip to Part 6)	60%
Unsure (please skip to Part 6)	6%
Total	100%

Q45. Has your organization adopted generative AI for threat detection and response to identity-based security incidents?	Pct%
Yes	41%
No	51%
Unsure	8%
Total	100%

Part 5: Demographics

D1. What organizational level best describes your current position?	Pct%
C-level / VP	18%
Director	21%
Manager	25%
Technician	16%
Staff	15%
Other	5%
Total	100%

D2. Check the primary person you report to within the organization.	Pct%
Chief Financial Officer	6%
Chief Operations Officer	9%
General Counsel	11%
Chief Information Officer	19%
Chief Technology Officer	10%
Chief Information Security Officer	21%
Chief Security Officer	9%
Chief Risk Officer	11%
Other	4%
Total	100%

D3. What industry best describes your organization's industry focus?	Pct%
Agriculture & food service	1%
Communications	5%
Defense & aerospace	5%
Energy & utilities	8%
Financial services	18%
Health & pharmaceutical	8%
Hospitality	4%
Industrial/manufacturing	11%
Retailing	7%
Services	13%
Technology & software	11%
Transportation	6%
Other (please specify)	3%
Total	100%

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or call at 1.800.887.3118.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.