Ponemon INSTITUTE

The State of Enterprise Identity

Sponsored by

Saviynt

Independently conducted by Ponemon Institute LLC

Publication Date: June 2022

The State of the Enterprise Identity

Ponemon Institute, June 2022

Part 1. Introduction

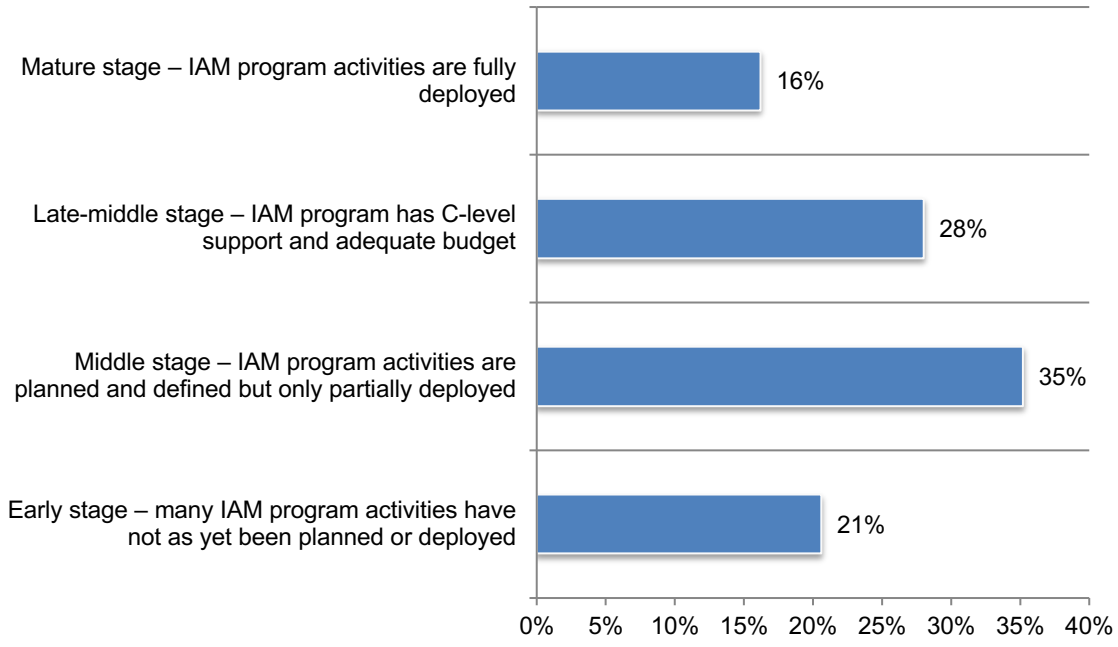
The purpose of this research is to determine enterprise security risks associated with identity & access and what is being done to manage these risks. Sponsored by Saviynt, Ponemon Institute surveyed more than 1,000 IT and IT security practitioners in the United States (627) and EMEA (416). These participants are knowledgeable about their organizations' programs and solutions used to mitigate cybersecurity, identity & access and compliance risks.

Zero trust is becoming an important strategy to support efforts to reduce identity & access risk. According to the research, an important benefit of the adoption of zero trust is greater visibility of the actions of privileged users. Currently, 52 percent of respondents say their organizations have implemented a zero-trust privileged access strategy. Of these respondents, 54 percent of respondents say it has improved visibility into where, when and how access is used and when it is being abused.

Most identity and access (IAM) programs have not achieved maturity which is affecting organizations' ability to reduce identity & access risks. Very few respondents have confidence in their organizations' controls to reduce identity & access risks. Part of this lack of confidence could be attributed to not having a fully mature IAM program. According to Figure 1, only 16 percent of respondents say their organizations have reached the mature stage, which is described as having all program activities fully deployed and C-level executives and the board of directors are regularly informed about the efficiency and effectiveness of the program. Only 28 percent of respondents say the IAM program has C-level support and adequate budget (late-middle stage).

Thirty-five percent of respondents say IAM program activities are only partially deployed (middle stage). Twenty-one percent of respondents say many IAM program activities have not been planned or deployed. Response to threats is reactive and ad hoc. Resources are not sufficient for staffing and investment in the program (early stage).

Figure 1. What best describes the maturity of your organization's IAM program?



The following findings reveal the security gaps and the steps taken to improve current identity and access management programs.

A lack of comprehensive identity controls or policies puts organizations at risk for a data breach or access-related security incident. In the past two years, 56 percent of respondents say their organizations had an average of three data breaches or other access-related security incidents. Fifty-two percent of these respondents say the breach was due to a lack of comprehensive identity controls or policies. Top abuses by both insiders and outsiders who are intent on circumventing controls include accessing sensitive data not associated with their role or function (70 percent of respondents) and making multiple requests for access to tools or resources not needed (70 percent of respondents).

Enterprise-wide visibility is critical to reducing risks in privileged user access but changes to IT resources make it difficult. Only 36 percent of respondents say their organizations are confident that they can determine if privileged users are compliant with policies. Sixty-one percent say the primary reason is not keeping up with the changes occurring to on-boarding, off-boarding and outsourcing. This is followed by having user account information but not privileged user entitlement information.

Delays in granting and enforcing user access rights create risks to sensitive and confidential information. Primarily, not having sufficient staff to monitor and control all privileged users (56 percent of respondents) and the inability to keep pace with the number of access change requests that are received regularly (51 percent of respondents) are the primary problems.

Organizations struggle to prioritize cybersecurity initiatives because of problems in the collection and assessment of risks. Fifty-four percent of respondents say the lack of a defined risk assessment framework is the biggest challenge facing organizations when prioritizing cybersecurity initiatives. Forty-four percent of respondents say their organizations collect risk data but do not use it to prioritize cybersecurity initiatives.

Cost reduction and frictionless identity and resource access are the top two benefits of a converged IGA and PAM solution. Fifty-seven percent of respondents have an IGA solution and of these respondents, 51 percent say it is converged with a PAM solution. Forty-two percent of respondents say a converged IGA and PAM solution reduces costs and provides frictionless identity and resource access.

The adoption of a converged platform is gaining traction to improve IAM processes. Forty-three percent of respondents say their organizations **do not** have an IGA solution and 49 percent of respondents say their organizations have an IGA solution but **do not** have a PAM solution converged with an IGA solution. Of both groups of respondents, 71 percent say they will consider (43 percent) or will adopt a platform (28 percent) that converges PAM and IGA solutions as well as being integrated with other external PAM solutions.

Organizations need solutions that determine if remote workers are securely accessing the network. Currently, the number one step to secure the hybrid, remote workforce is screening new employees (37 percent of respondents). Only 28 percent of respondents say their organizations are determining if remote workers are securely accessing the network.

Monitoring privileged users and acting upon threat intelligence and user behavior are primarily used to reduce access risks. Only 40 percent of respondents say their organizations remove standing privilege and only issue privileged access for a specific time for a specific account to do specific things. Sixty-three percent of respondents say their organizations monitor and review the activity of privileged users on the target system or through the PAM solution

followed by 57 percent of respondents who say their organizations rely upon threat intelligence and user behavior.

Analytics are used to identify suspicious insider activities. Analytics and PAM tooling capabilities are the most often used technologies, according to 67 percent and 59 percent of respondents, respectively. Processes used are monitoring and reviewing log files and manual oversight by supervisors and managers, according to 60 percent and 38 percent of respondents, respectively.

Critical to securing access is the ability to have efficient review cycles and remediations. Sixty-two percent of respondents say their organizations measure the effectiveness of their access governance programs. Of these respondents, 62 percent say their organizations measure how fast their access review cycles and remediations are. This is followed by total cost of ownership and a decline in audit findings and improvements in compliance posture according to 60 percent and 50 percent of respondents, respectively.

Part 2. Key findings

In this section, we provide an analysis of the research findings. The complete findings are presented in the Appendix of this report. The report is organized according to the following topics.

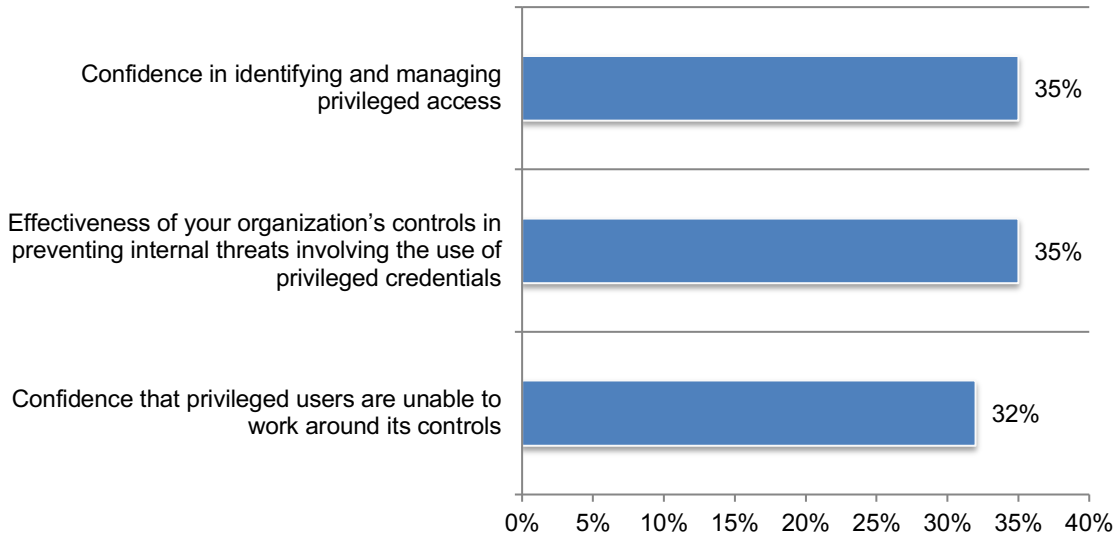
- The state of cybersecurity risks based on organizations' identity & access practices
- The impact of cloud adoption on IAM
- Convergence, zero-trust and other solutions to securing identity & access practices

The state of cybersecurity risks based on organizations' identity & access practices

Confidence and effectiveness is low in reducing privileged access misuse. Respondents were asked to rate their confidence in important components of their privileged access management programs and effectiveness in preventing internal threats involving the use of privileged credentials on a scale from 1 = low confidence/low effectiveness to 10 = high confidence/high effectiveness.

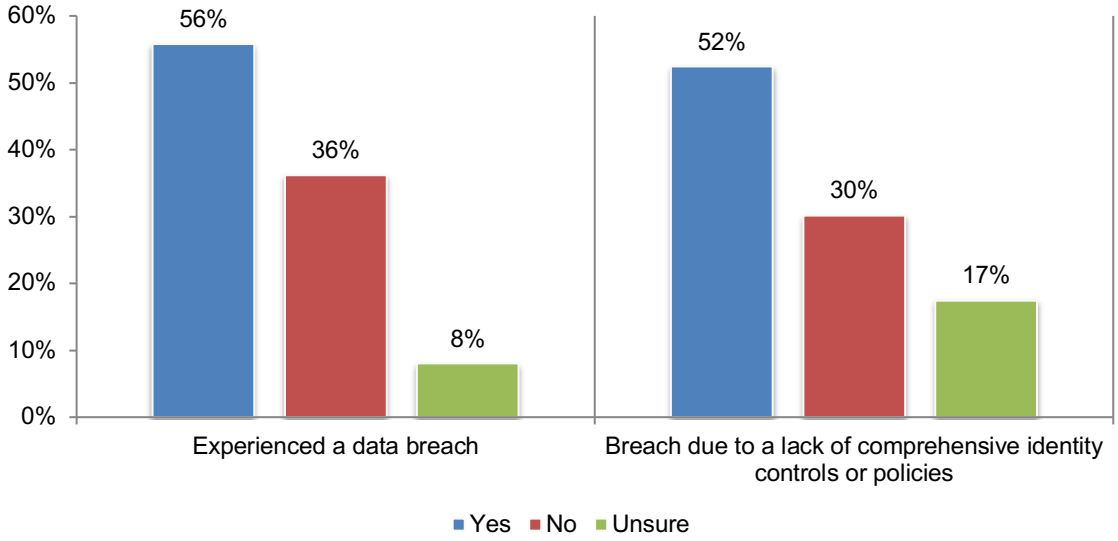
Figure 2 shows the high confidence and high effectiveness responses (7+ responses on the 10-point scale). Only 35 percent of respondents say their organizations are confident in the ability to identify and manage privileged access and only 32 percent of respondents are confident that privileged users are unable to work around its controls. Only 35 percent rate the effectiveness of current controls in preventing internal threats involving the use of privileged credentials as high.

Figure 2. Confidence and effectiveness is low in reducing privileged access misuse.
On a scale from 1 = low confidence/effectiveness to 10 = high confidence/effectiveness, 7+ responses presented



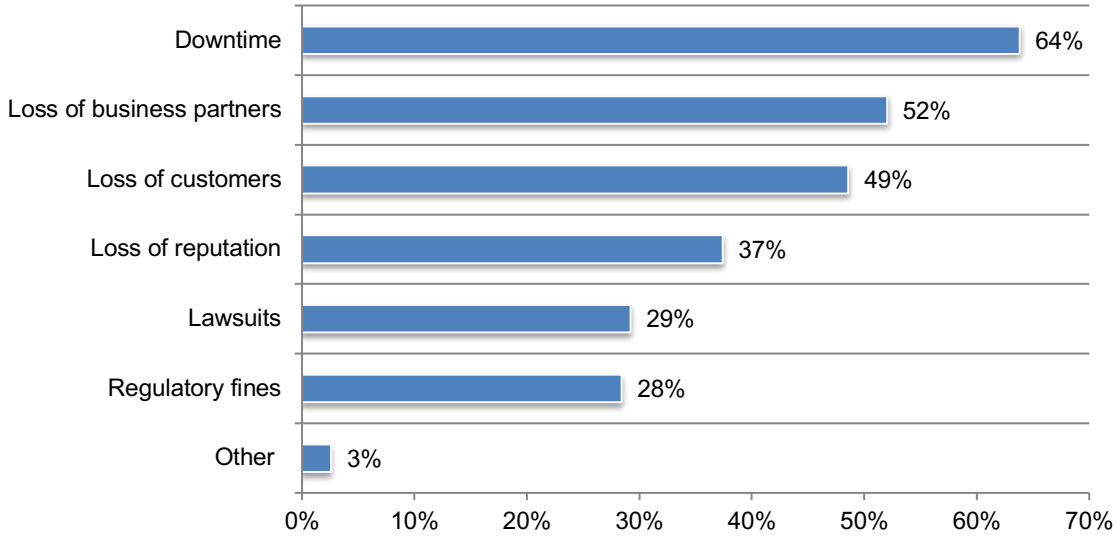
A lack of comprehensive identity controls or policies puts organizations at risk for a cyberattack, data breach or access-related security incident. In the past two years, as shown in Figure 3, 56 percent of respondents say their organizations had an average of three data breaches or other access-related security incidents. Fifty-two percent of these respondents say the breach was due to a lack of comprehensive identity controls or policies.

Figure 3. Did your organization have a data breach within the last two years and was it due to a lack of comprehensive security controls or policies?



Downtime is the most significant consequence of the failure to comply with regulations. In In the past two years, 46 percent of respondents say their organizations failed to comply with regulations because of the inability to secure access to their information assets. As shown in Figure 4, of these respondents, 64 percent say the primary consequence is downtime followed by loss of business partners (52 percent) and loss of customers (49 percent). In the context of this research, downtime is the time during which an IT system is offline or not operational.

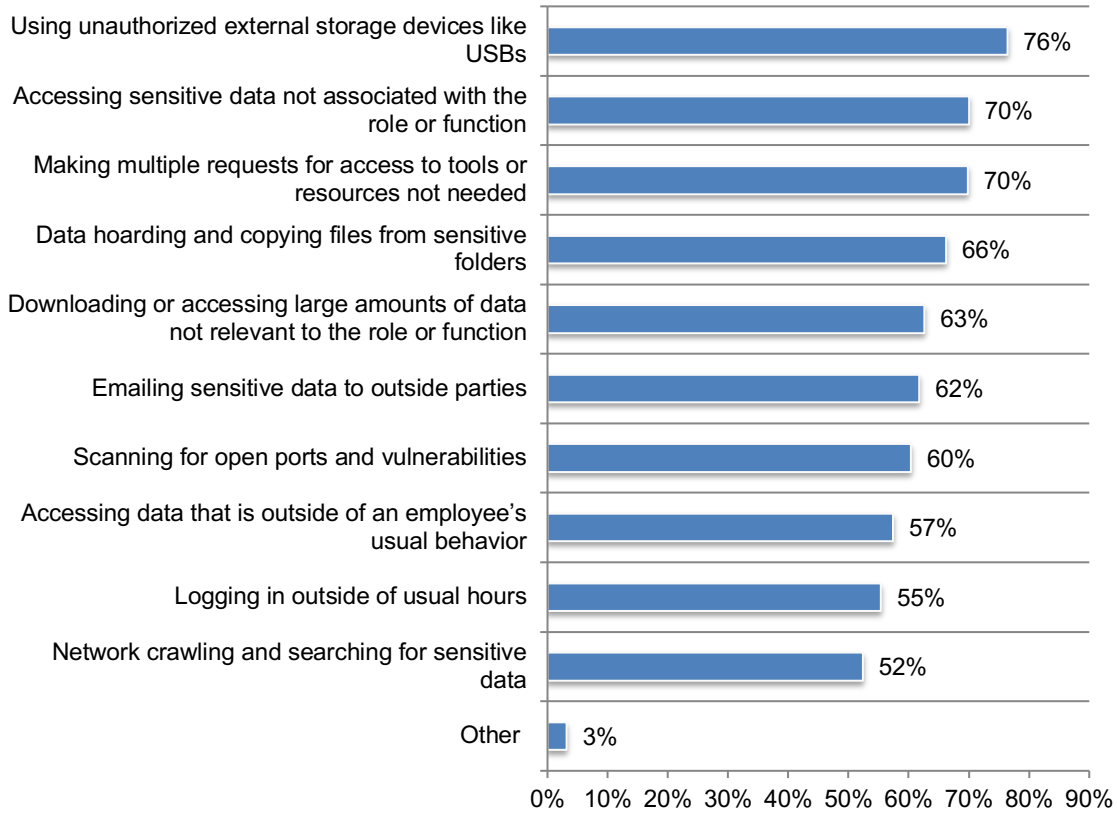
Figure 4. What were the consequences of a failure to comply with regulations due to the lack of secure access to information assets?
More than one response permitted



Access controls have been circumvented putting data at risk. Figure 5 presents a list of how controls have been circumvented internally or externally thus putting sensitive and confidential information at risk. The three top abuses by both insiders and outsiders who are intent on circumventing controls include using unauthorized external storage devices like USBs (76 percent of respondents), accessing sensitive data not associated with the role or function (70 percent of respondents) and making multiple requests for access to tools or resources not needed (70 percent of respondents).

Figure 5. In the past two years, how have controls been circumvented internally and/or externally?
More than one response permitted

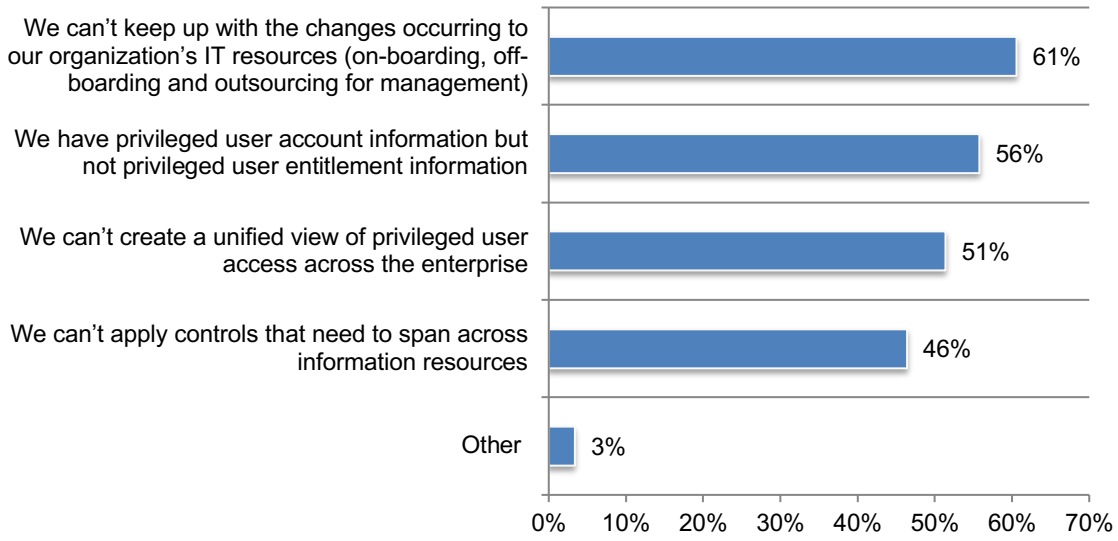
Because the frequency of responses sums to more than 100% the responses cannot be aggregated.



Enterprise-wide visibility is critical to reducing risks in privileged user access but changes to IT resources make it difficult. Only 36 percent of respondents say their organizations are confident that they can determine if privileged users are compliant with policies. The reasons for not having confidence are shown in Figure 6. Sixty-one percent say the primary reason is not keeping up with the changes occurring when on-boarding, off-boarding and outsourcing. This is followed by having user account information but not privileged user entitlement information.

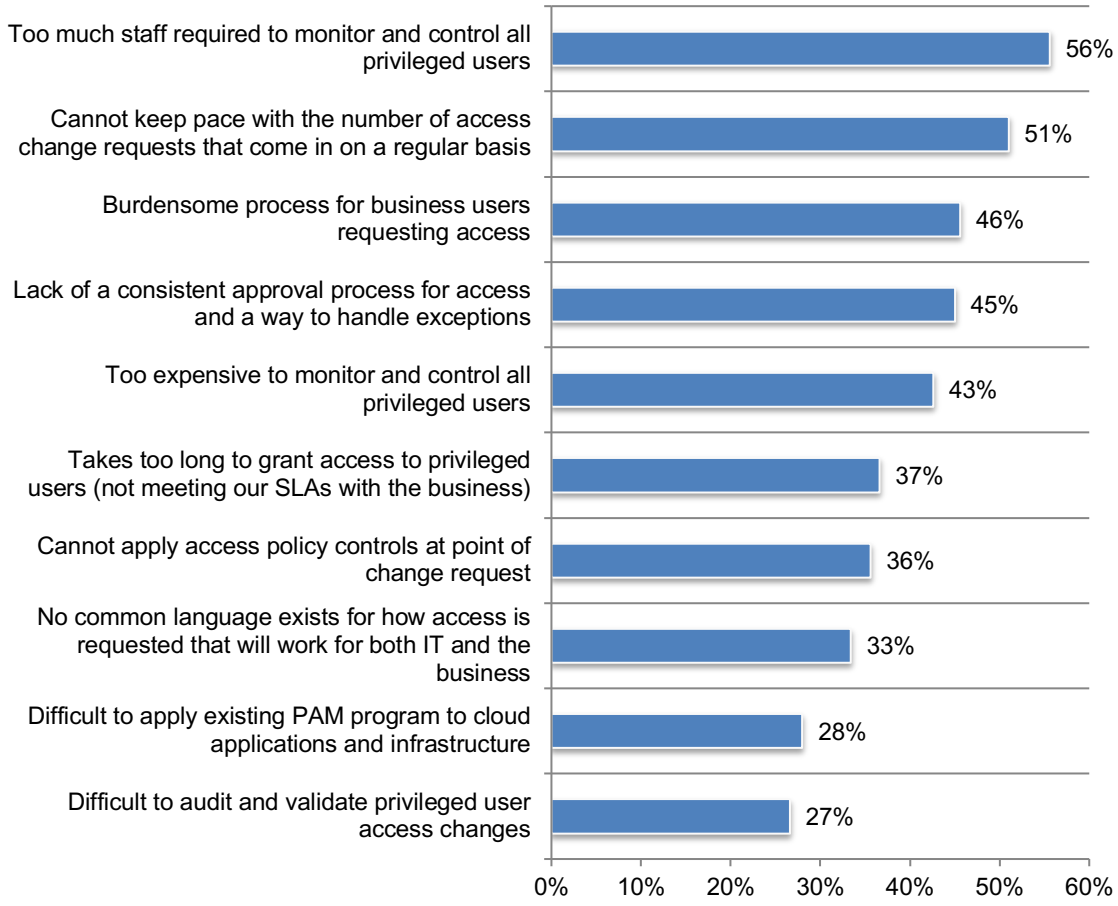
Figure 6. Reasons for having a lack of confidence in achieving visibility of privileged user access

More than one response permitted



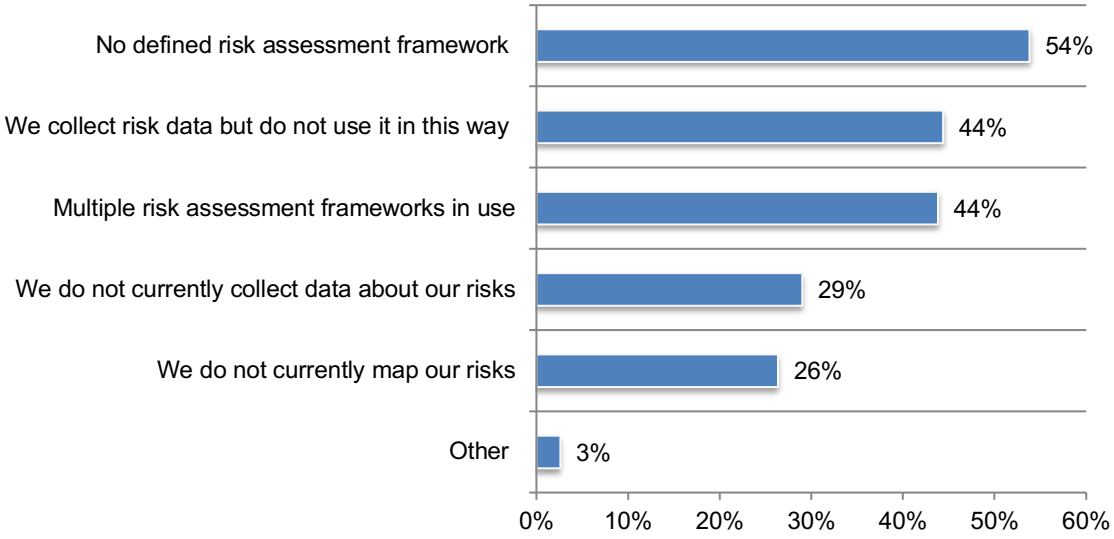
Delays in granting and enforcing user access rights create risks to sensitive and confidential information. Figure 7 lists the problems organizations face when providing timely granting of user access rights and then ensuring enforcement of these rights which can affect the security of sensitive and confidential information. Primarily, not having sufficient staff to monitor and control all privileged users (56 percent of respondents) and the inability to keep pace with the number of access change requests that are received regularly (51 percent of respondents) are the main problems.

Figure 7. What are the main problems in granting and enforcing privileged user access rights?
Four responses permitted



Organizations struggle to prioritize cybersecurity initiatives because of problems in the collection and assessment of risks. As shown in Figure 8, 54 percent of respondents say the lack of a defined risk assessment framework is the biggest challenge facing organizations when prioritizing cybersecurity initiatives. Forty-four percent of respondents say their organizations collect risk data but do not use it to prioritize cybersecurity initiatives.

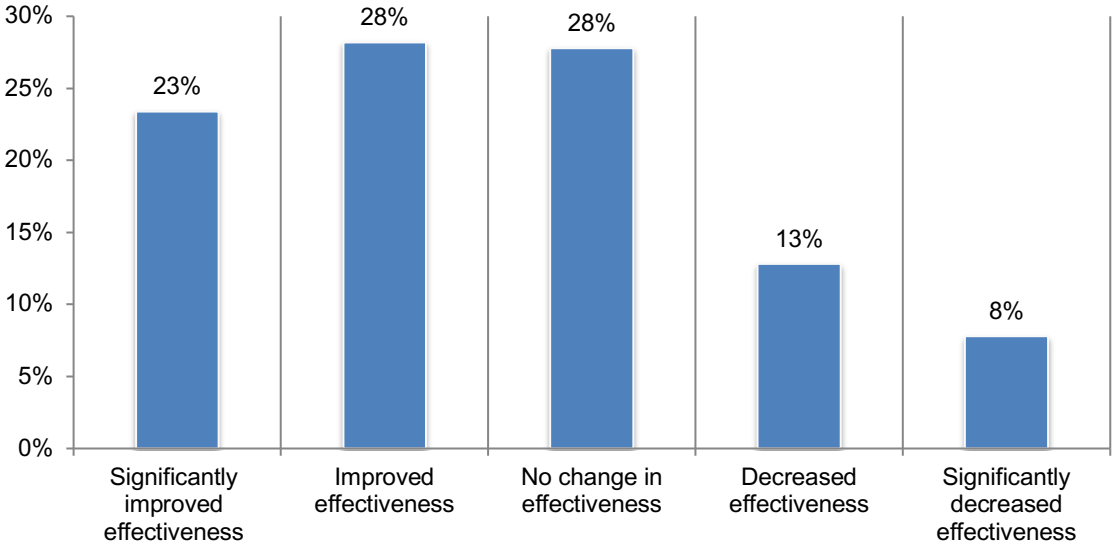
Figure 8. The primary challenges in using risk data to prioritize cybersecurity initiatives
Two responses permitted



The impact of cloud adoption on IAM

The cloud improves the effectiveness of enterprise IAM programs. An average of 56 percent of organizations' IT infrastructure and applications have migrated to the cloud and 52 percent of respondents say their organizations' cloud IT program is integrated with their IAM. According to Figure 9, 51 percent of respondents say cloud services have significantly improved effectiveness (23 percent) or improved effectiveness (28 percent) of IAM effectiveness.

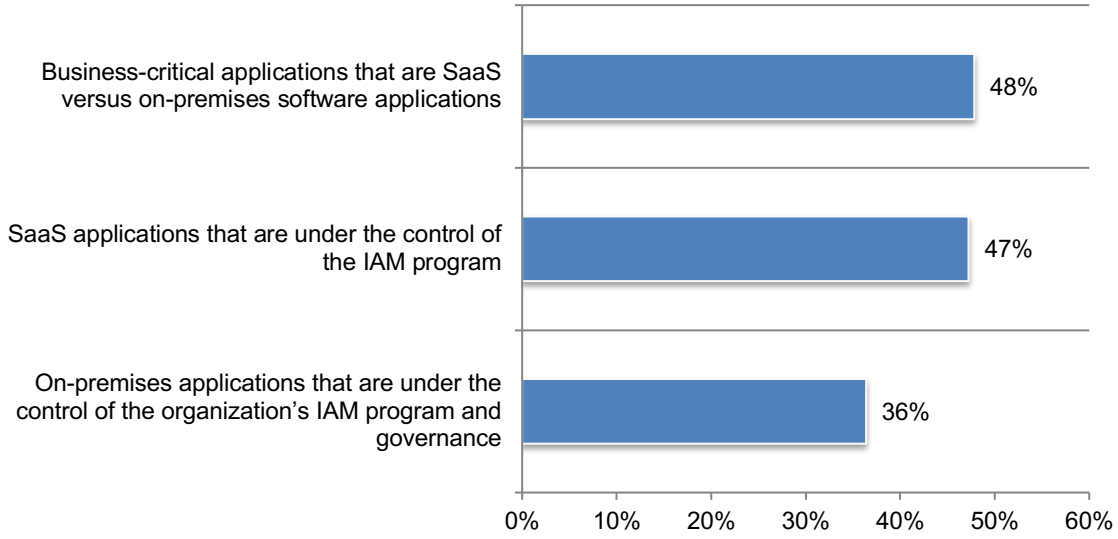
Figure 9. How has the use of cloud services affected IAM effectiveness?



More SaaS applications than on-premises applications are under the control of the organization's IAM program. Ninety-two percent of respondents say their organizations are heavy (33 percent), moderate (29 percent) or light users (30 percent) of SaaS resources from cloud service providers.

As shown in Figure 10, an average of 48 percent of business-critical applications are SaaS versus on-premises software applications. Organizations have an average of 241 SaaS applications and an average of 47 percent of these applications are under the control of the IAM program. Organizations have an average of 243 on-premises applications and 36 percent of these applications are under the control of the IAM program

Figure 10. Percentage of business-critical applications are SaaS and under the control of the IAM program
Extrapolated values presented



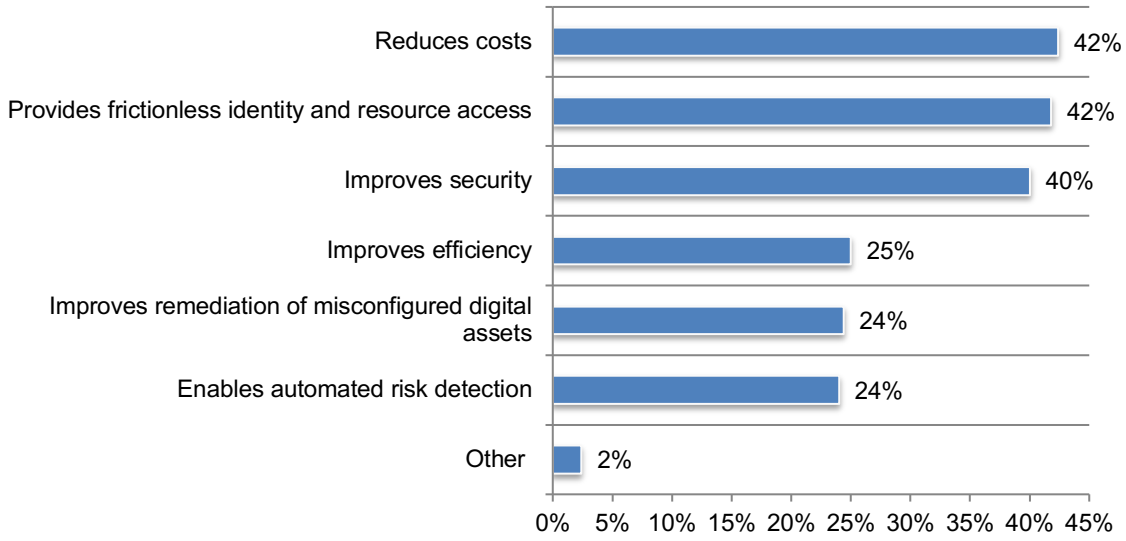
Convergence, zero trust and other solutions to securing IAM processes

Cost reduction and frictionless identity and resource access are the top two benefits of a converged IGA and PAM solution. Identity Governance & Administration (IGA) is a policy-based approach to identity management and access control. IGA systems merge identity governance and identity administration to provide additional functionality beyond traditional identity and access management (IAM) tools.

Privileged Access Management (PAM) is intended to secure and manage an organization's privileged access to information resources. The goals of PAM are to protect critical data and ensure availability of essential business systems, reduce the likelihood that privileged credentials will be compromised or misused, reduce the impact if compromise or misuse does occur and pinpoint which user is responsible for actions taken by a shared account.

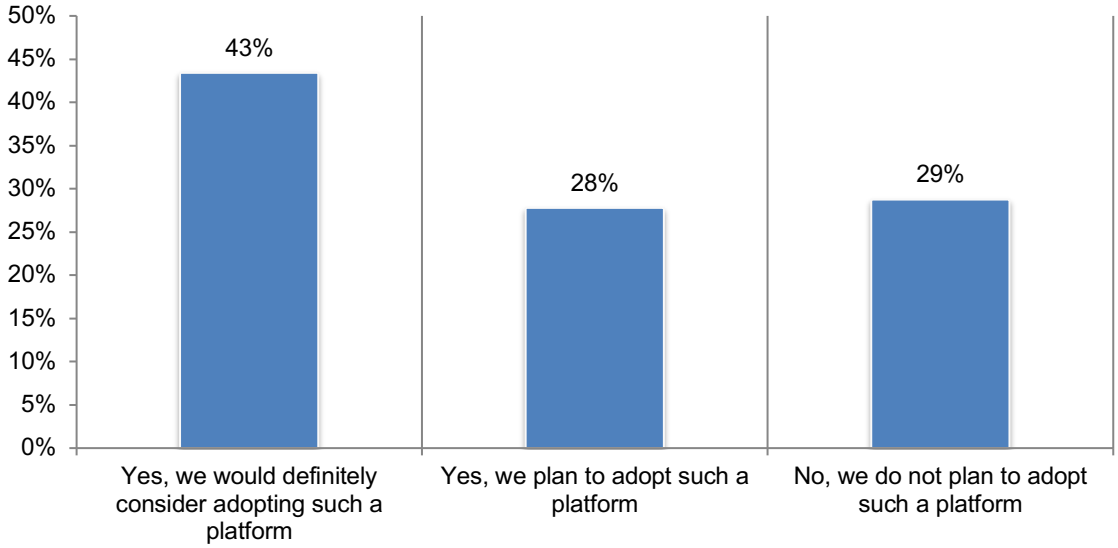
Fifty-seven percent of respondents have an IGA solution and of these respondents, 51 percent say it is converged with a Privileged Access Management (PAM) solution. According to Figure 11, 42 percent of respondents say a converged IGA and PAM solution reduces costs and provides frictionless identity and resource access.

Figure 11. The benefits of a converged IGA and PAM solution
Two responses permitted



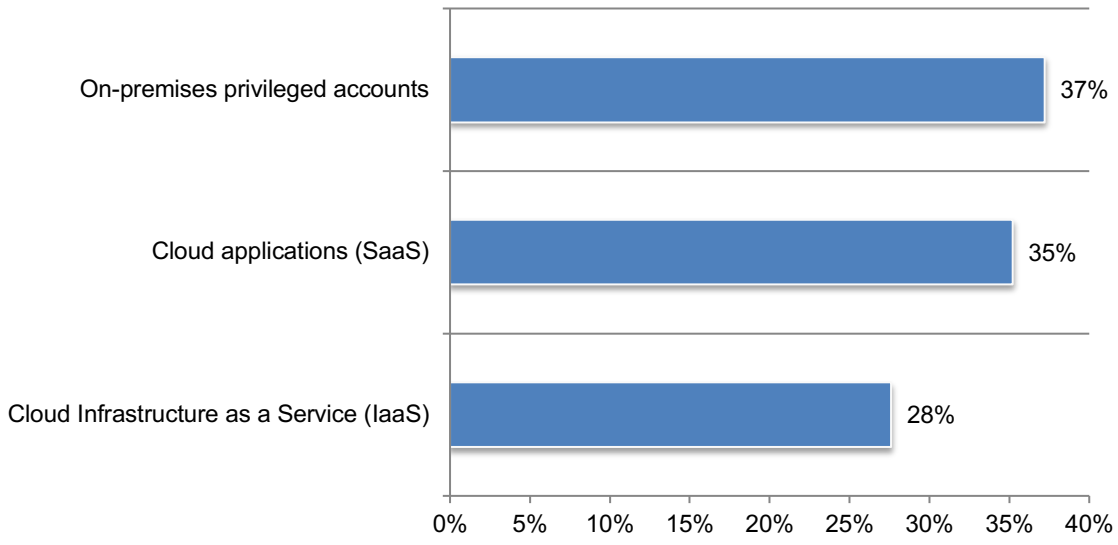
The adoption of a converged platform is gaining traction to improve IAM processes. Forty-three percent of respondents say their organizations **do not** have an IGA solution and 49 percent of respondents say their organizations have an IGA solution but **do not** have a PAM solution converged with an IGA solution. Of both groups of respondents, 71 percent say their organizations will consider (43 percent) or will adopt a platform (28 percent) that converges PAM and IGA solutions as well as being integrated with other external PAM solutions.

Figure 12. Will your organization consider a platform with a PAM solution combined with an IGA solution and integrated with other external PAM solutions?



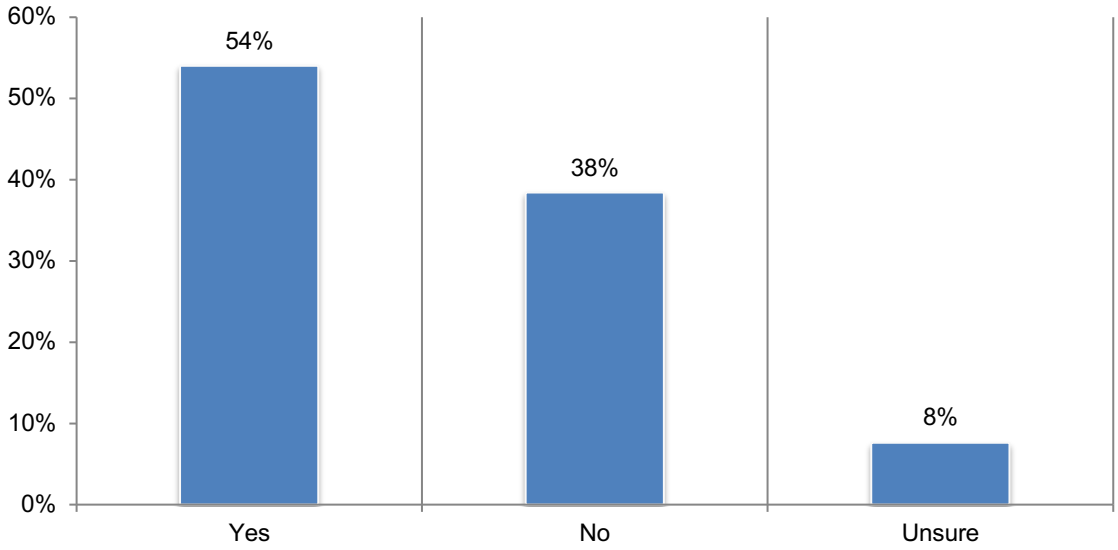
PAM solutions are primarily used to manage cloud applications and infrastructure. According to Figure 13, 63 percent of respondents say the PAM solution manages privileged access in cloud applications (SaaS) (35 percent) or cloud Infrastructure as a Service (IaaS).

Figure 13. In which of the following does the PAM solution manage privileged access?
Only one choice permitted



An important benefit of the adoption of zero-trust is greater visibility of the actions of privileged users. Currently, 52 percent of respondents say their organizations have implemented a zero-trust privileged access strategy. As shown in Figure 14, of these respondents, 54 percent say zero-trust has improved visibility into where, when and how privileged access is used and when it is being abused.

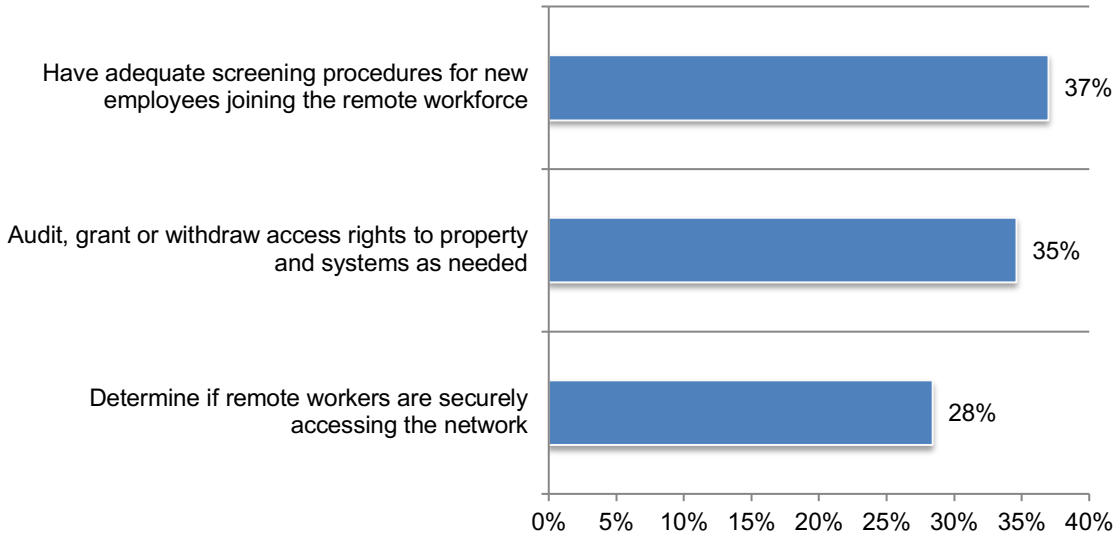
Figure 14. Has a zero-trust privileged access strategy improved visibility into where, when and how privileged access is used and when it is being abused?



Organizations need solutions that determine if remote workers are securely accessing the network. An average of 41 percent of organizations' employees work both off-site and on-site. When asked to rate their confidence in reducing risks created by a hybrid remote workforce on a scale from 1 = low confidence to 10 = high confidence, only 33 percent rate their confidence as high to very high (7+ responses on the 10-point scale).

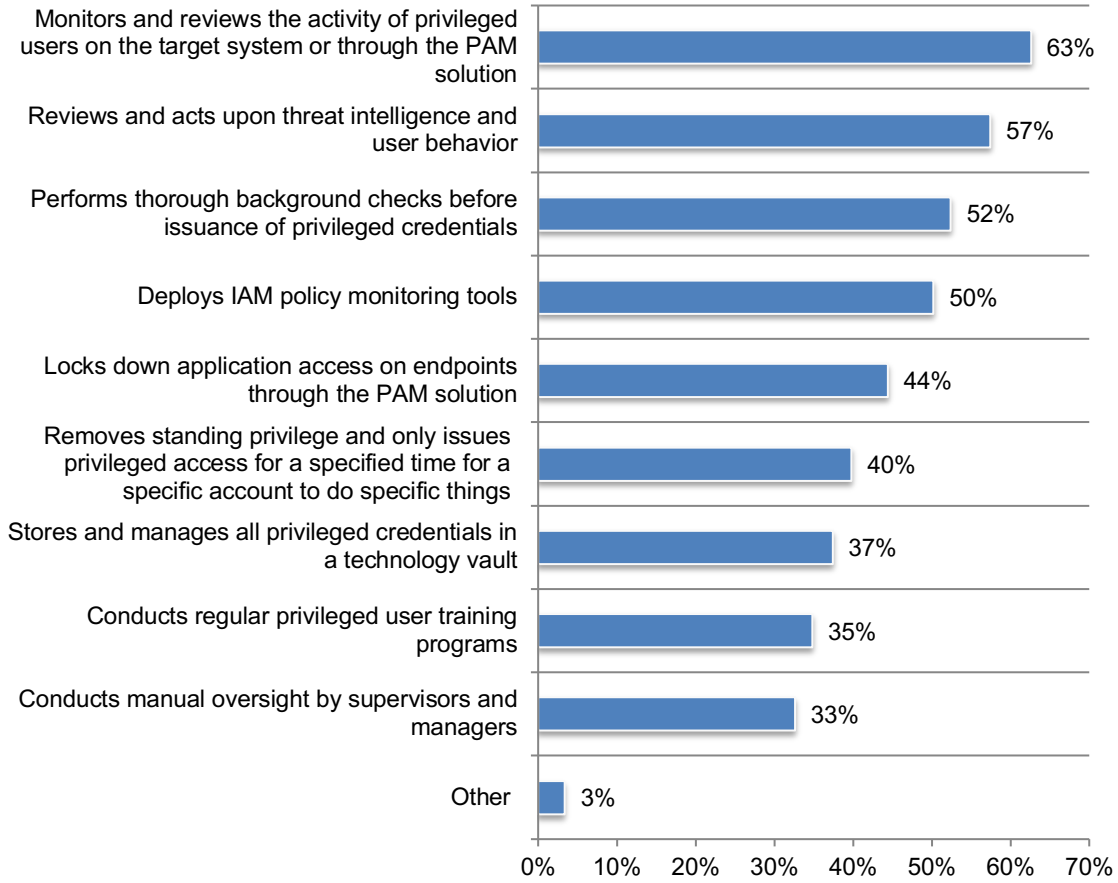
Figure 15 provides the actions being taken to reduce risk. The number one is screening new employees (37 percent of respondents). Only 28 percent of respondents say their organizations are determining if remote workers are securely accessing the network.

Figure 15. What steps are taken to secure the hybrid, remote workforce as part of the access governance program?
Only one choice permitted



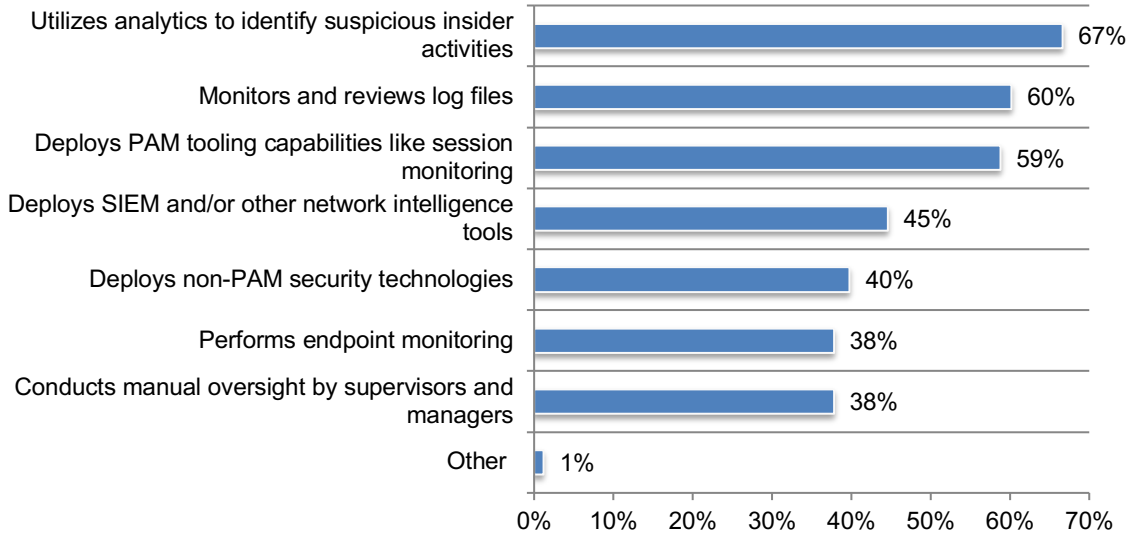
Monitoring privileged users and acting upon threat intelligence and user behavior are primarily used to reduce access risks. Figure 16 presents a list of steps taken to prevent privileged access abuse. Sixty-three percent of respondents say their organizations monitor and review the activity of privileged users on the target system or through the PAM solution followed by 57 percent of respondents who say their organizations rely upon threat intelligence and user behavior. Only 40 percent of respondents say their organizations remove standing privilege and only issue privileged access for a specific time for a specific account to do specific things.

Figure 16. What steps are taken to prevent privileged access abuse?
More than one response permitted



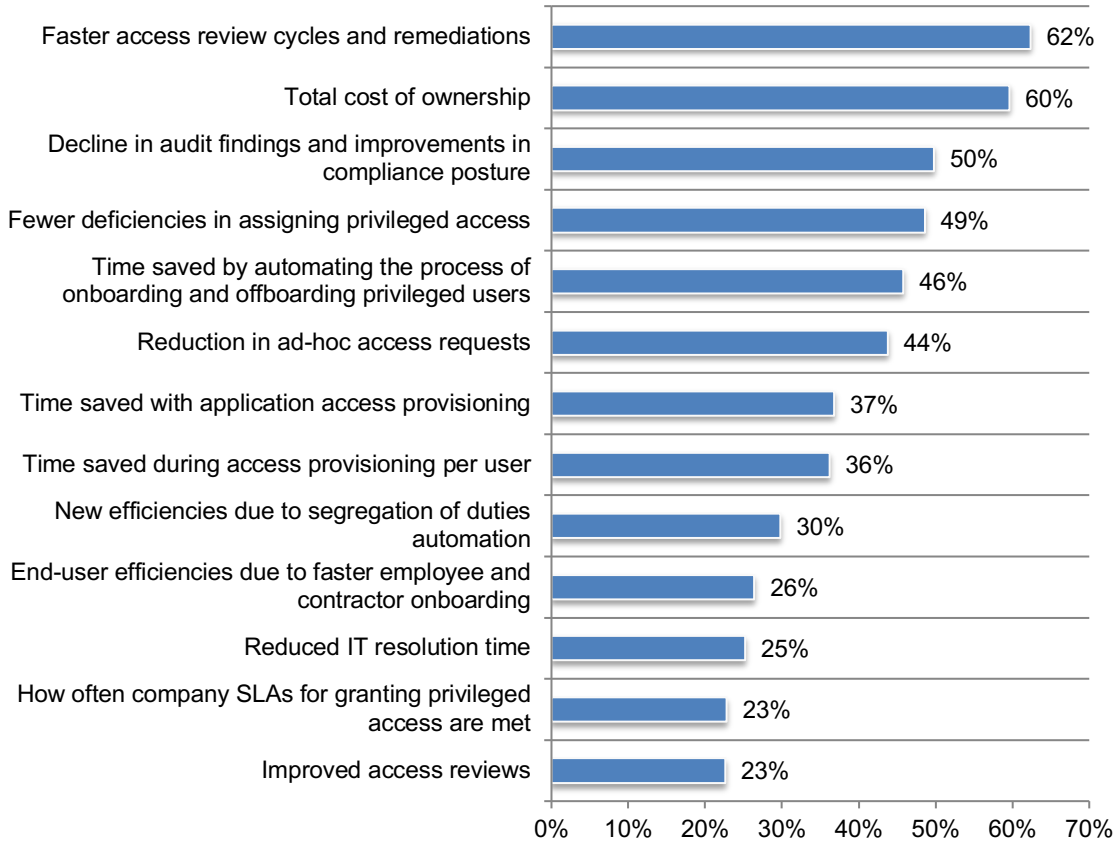
Analytics are used to identify suspicious insider activities. Figure 17 lists the technologies and processes used to identify privileged user threats. Analytics and PAM tooling capabilities are the most often used technologies, 67 percent of respondents and 59 percent of respondents, respectively. Processes used are monitoring and reviewing log files and manual oversight by supervisors and managers, according to 60 percent and 38 percent of respondents, respectively.

Figure 17. How does your organization determine if an action taken by a privileged user is a threat?
More than one response permitted



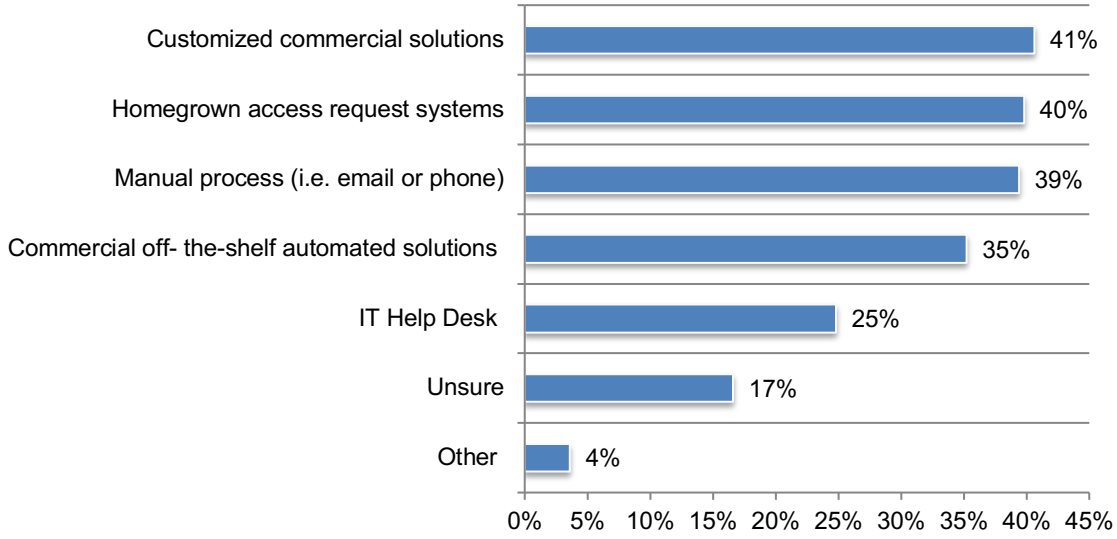
Critical to securing access is the ability to have efficient review cycles and remediations. According to Figure 18, 62 percent of respondents say their organizations measure the effectiveness of their access governance programs. Of these respondents, 62 percent say their organizations measure how fast their access review cycles and remediations are. This is followed by total cost of ownership and a decline in audit findings and improvements in compliance posture, 60 percent of respondents and 50 percent of respondents respectively.

Figure 18. How does your organization measure the effectiveness of its access governance programs?
More than one response permitted



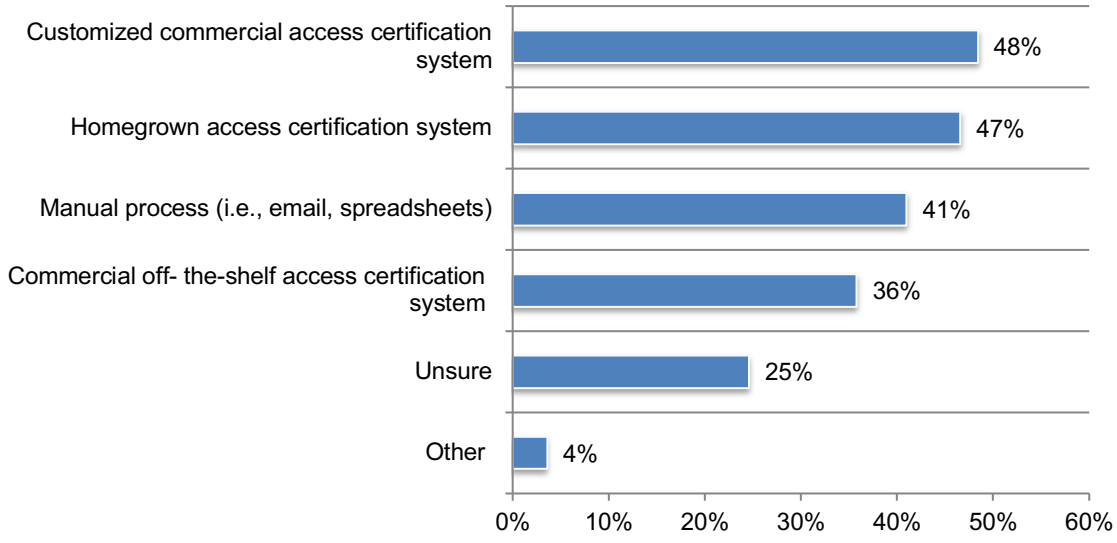
Customized commercial solutions are primarily used to grant, review and certify privileged user access. As shown in Figure 19, 41 percent of respondents use customized commercial solutions and 40 percent of respondents say their organizations have a homegrown access request system. Only 25 percent of respondents say their organizations use IT help desks to grant access to IT resources, possibly because of the cost.

Figure 19. What are the processes used to grant users access to IT resources?
Two responses permitted



As shown in Figure 20, almost half of respondents (48 percent) say their organizations use a customized commercial access certification system followed by 47 percent of respondents who say their organizations use homegrown access certification systems.

Figure 20. What are the processes used to review and certify privileged access?
Two responses permitted



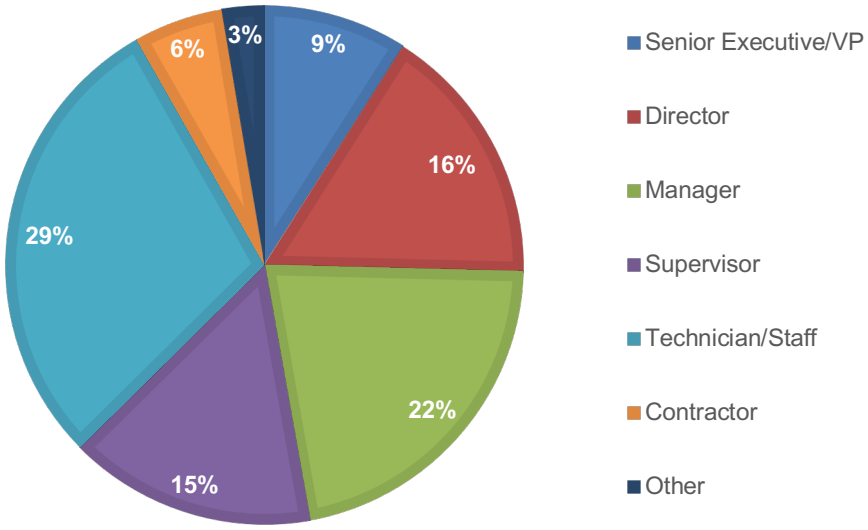
Part 3. Methodology

A sampling frame of 29,167 IT and IT security professionals in the United States and EMEA in organizations with a privileged access management program (PAM) currently or who will have a PAM in the next six months to one year were selected as participants to this survey. Table 1 shows 1,140 total returns. Screening and reliability checks required the removal of 97 surveys. Our final sample consisted of 1,043 surveys or a 3.6 percent response.

Table 1. Sample response	Freq	Pct%
Sampling frame	29,167	100.0%
Total returns	1,140	3.9%
Rejected or screened surveys	97	0.3%
Final sample	1,043	3.6%

Figure 21 reports the respondent's organizational level within participating organizations. By design, more than half (62 percent) of respondents are at or above the supervisory levels. The largest category at 29 percent of respondents is technician or staff.

Figure 21. Current position within the organization



As shown in Figure 22, 33 percent of respondents report to the chief information officer, 17 percent of respondents report to the chief information security officer, 15 percent of respondents report to the chief technology officer, 8 percent of respondents report to the CEO/executive committee and 7 percent of respondents report to the chief risk officer.

Figure 22. Direct reporting channel

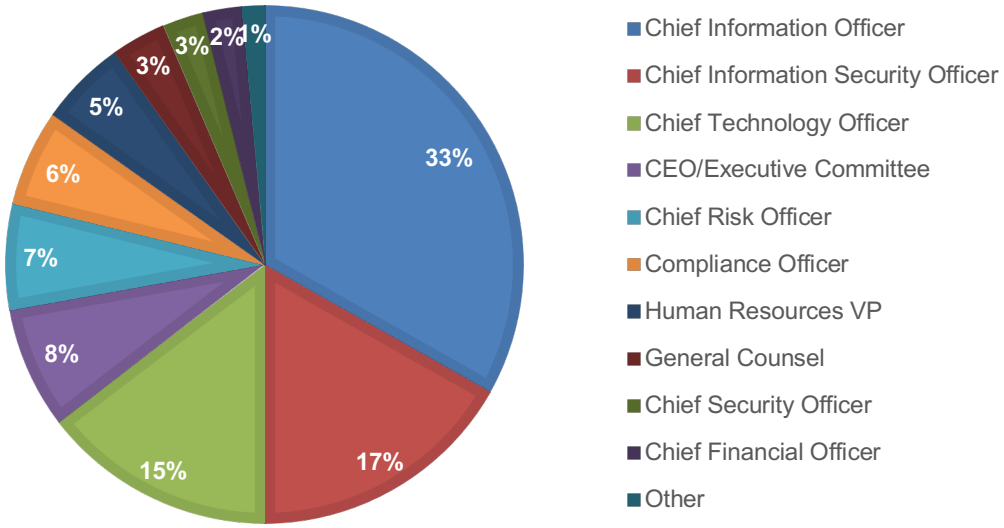
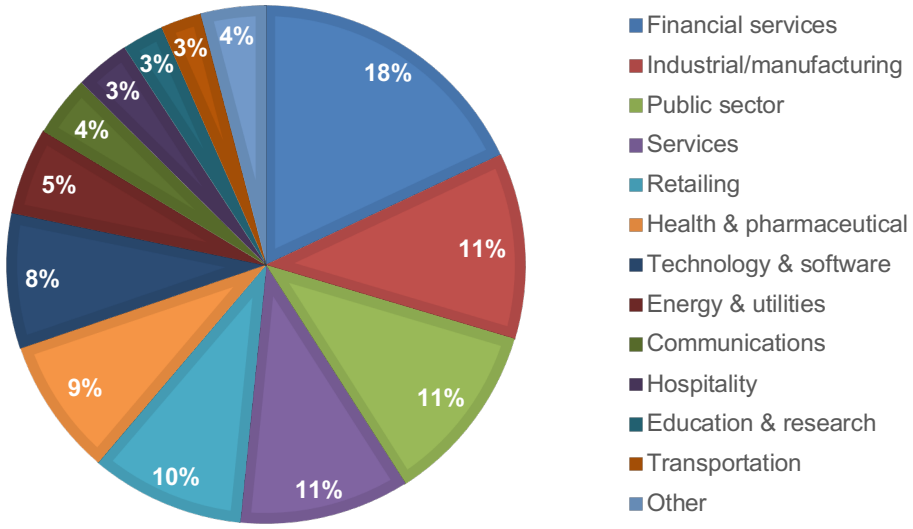


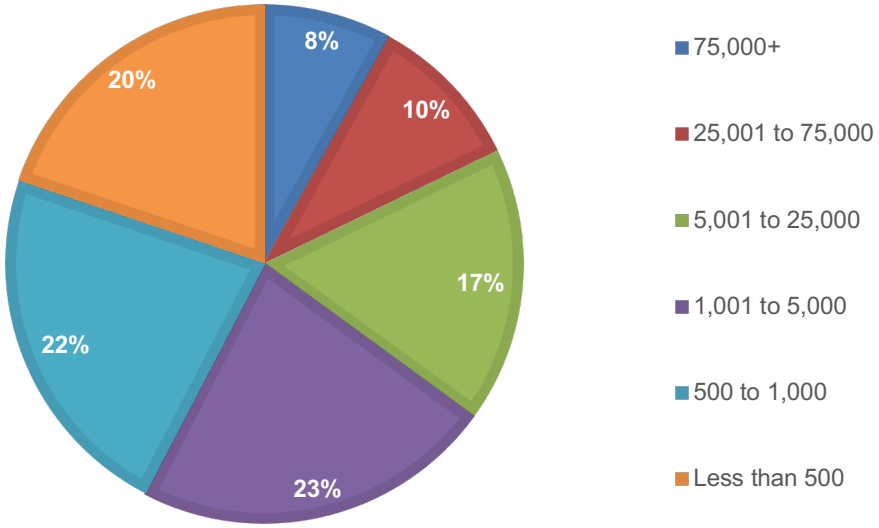
Figure 23 reports the industry focus of respondents' organizations. This chart identifies financial services (18 percent) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by industrial and manufacturing (11 percent of respondents), public sector (11 percent of respondents), services (11 percent of respondents), retailing (10 percent of respondents) and healthcare and pharmaceuticals (9 percent of respondents).

Figure 23. Primary industry focus



As shown in Figure 24, 58 percent of respondents are from organizations with a global headcount of more than 1,000 employees.

Figure 24. Global full-time headcount



Part 4. 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 or IT security professionals in the United States and EMEA. 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 5. Appendix with the detailed audited findings

The following tables provide the percentage frequency of responses to all survey questions. All survey responses were captured in February 2022

Survey Response	Total
Total sampling frame	29,167
Total survey returns	1,140
Rejected surveys	97
Final sample	1,043
Response rate	3.6%
Sample weights	1.00

Part 1. Screening Questions

S1. Does your organization have a privileged access management program (PAM)?	Total
Yes	55%
No, but will have a program within the next six months to one year	45%
No (Stop)	0%
Total	100%

S2. How knowledgeable are you about your organization's PAM program?	Total
Very knowledgeable	39%
Knowledgeable	36%
Somewhat knowledgeable	25%
No knowledge (Stop)	0%
Total	100%

S3. How knowledgeable and involved are you in your organization's solutions to mitigate cybersecurity, identity access and compliance risks?	Total
Very knowledgeable and very involved	38%
Knowledgeable and involved	34%
Somewhat knowledgeable and somewhat involved	28%
No knowledge and/or no involvement (Stop)	0%
Total	100%

Part 2. Background

Q1. Does your organization have an Identity Governance & Administration (IGA) solution as defined above?	Total
Yes	57%
No (please skip to Q4)	43%
Total	100%

Q2. If yes, has it converged with a Privileged Access Management (PAM) solution?	Total
Yes	51%
No (please skip to Q4)	49%
Total	100%

Q3. If yes, what do you consider the main benefits of a converged IGA and PAM solution? Please select the top two choices.	Total
Reduces costs	42%
Improves efficiency	25%
Improves security	40%
Provides frictionless identity and resource access	42%
Enables automated risk detection	24%
Improves remediation of misconfigured digital assets	24%
Other (please specify)	2%
Total	200%

Q4. Would your organization consider adopting a platform that provides its own PAM solution that is combined with an IGA solution as well as integrated with other external PAM solutions?	Total
Yes, we would definitely consider adopting such a platform	43%
Yes, we plan to adopt such a platform	28%
No, we do not plan to adopt such a platform	29%
Total	100%

Q5. How does your organization protect itself from privileged access abuse? Please select all that apply.	Total
Performs thorough background checks before issuance of privileged credentials	52%
Conducts manual oversight by supervisors and managers	33%
Stores and manages all privileged credentials in a technology vault	37%
Monitors and reviews the activity of privileged users on the target system or through the PAM solution	63%
Reviews and acts upon threat intelligence and user behavior	57%
Locks down application access on endpoints through the PAM solution	44%
Removes standing privilege and only issues privileged access for a specified time for a specific account to do specific things (just-in-time access)	40%
Deploys IAM policy monitoring tools	50%
Conducts regular privileged user training programs	35%
Other (please specify)	3%
Total	415%

Q6. How does your organization determine if an action taken by a privileged user is truly a threat? Select all that apply.	Total
Monitors and reviews log files	60%
Conducts manual oversight by supervisors and managers	38%
Deploys SIEM and/or other network intelligence tools	45%
Utilizes analytics to identify suspicious insider activities	67%
Deploys PAM tooling capabilities like session monitoring	59%
Deploys non-PAM security technologies	40%
Performs endpoint monitoring	38%
Other (please specify)	1%
Total	347%

Q7. Which part of your organization is responsible for granting privileged access? Please select all that apply.	Total
Information technology	63%
Information security	36%
Compliance/general counsel	11%
Internal audit	10%
Human resources	18%
Risk management	14%
Lines of business	38%
Other (please specify)	2%
Total	192%

Q8. In which of the following does the PAM solution manage privileged access?	Total
On-premises privileged accounts	37%
Cloud applications (SaaS)	35%
Cloud Infrastructure as a Service (IaaS)	28%
Total	100%

Q9. What percentage of privileged access is managed by the PAM solution?	Total
Less than 10%	14%
10% to 25%	19%
26% to 50%	23%
51% to 75%	25%
75% to 100%	19%
Total	100%
Extrapolated value	45%

Q10. What best describes the maturity of your organization's IAM program?	Total
Early stage – many IAM program activities have not as yet been planned or deployed. Response to threats is reactive and ad hoc. Resources are not sufficient for staffing and investment in the program.	21%
Middle stage – IAM program activities are planned and defined but only partially deployed. Efforts are being made to establish security protocols, prioritize risks and increase investments.	35%
Late-middle stage – IAM program has C-level support and adequate budget. Risks are regularly assessed.	28%
Mature stage – IAM program activities are fully deployed, and C-level executives and the board of directors are regularly informed about the efficiency, effectiveness and security of the program.	16%
Total	100%

Part 3. The challenges and risks of identity management and governance

Q11a. Has your organization experienced a data breach or other access-related security incident within the past 2 years?	Total
Yes	56%
No	36%
Unsure	8%
Total	100%

Q11b. If yes, how many?	Total
One	19%
2 to 3	37%
4 to 5	29%
More than 5	15%
Total	100%
Extrapolated value	3.3

Q11c. If yes, was the breach due to a lack of comprehensive identity controls or policies?	Total
Yes	52%
No	30%
Unsure	17%
Total	100%

Q12a. Has your organization failed to meet regulatory compliance regulations due to the inability to secure access to its information assets in the past two years?	Total
Yes	46%
No	37%
Unsure	17%
Total	100%

Q12b. If yes, what were the consequences? Please select all that apply.	Total
Lawsuits	29%
Regulatory fines	28%
Loss of customers	49%
Loss of business partners	52%
Downtime	64%
Loss of reputation	37%
Other (please specify)	3%
Total	262%

Q13. In the past two years, have any controls been circumvented internally and/or externally to do any of the following? Please select all that apply.	Total
Downloading or accessing large amounts of data not relevant to the role or function	63%
Accessing sensitive data not associated with the role or function	70%
Accessing data that is outside of an employee's usual behavior	57%
Making multiple requests for access to tools or resources not needed	70%
Using unauthorized external storage devices like USBs	76%
Network crawling and searching for sensitive data	52%
Data hoarding and copying files from sensitive folders	66%
Emailing sensitive data to outside parties	62%
Scanning for open ports and vulnerabilities	60%
Logging in outside of usual hours	55%
Other (please specify)	3%
Total	636%

Q14. Using the following 10-point scale, please rate the effectiveness of your organization's controls in preventing internal threats involving the use of privileged credentials from 1 = low effectiveness to 10 = high effectiveness.	Total
1 or 2	21%
3 or 4	21%
5 or 6	23%
7 or 8	18%
9 ot 10	17%
Total	100%
Extrapolated value	5.24

Q15. Using the following 10-point scale, please rate your organization's confidence that privileged users are unable to work around its controls from 1 = low confidence to 10 = high confidence.	Total
1 or 2	18%
3 or 4	22%
5 or 6	29%
7 or 8	17%
9 or 10	15%
Total	100%
Extrapolated value	5.26

Q16. Using the following 10-point scale, please rate your organization's confidence in identifying and managing privileged access from 1 = low confidence to 10 = high confidence.	Total
1 or 2	18%
3 or 4	17%
5 or 6	29%
7 or 8	21%
9 or 10	14%
Total	100%
Extrapolated value	5.41

Q17a. Using the following 10-point scale, how confident is your organization that it has enterprise-wide visibility for privileged user access and can determine if these users are compliant with policies? Please use the 10-point scale below, where 1 = low confidence to 10 = high confidence.	Total
1 or 2	22%
3 or 4	23%
5 or 6 (please skip to Q18)	18%
7 or 8 (please skip to Q18)	12%
9 or 10 (please skip to Q18)	24%
Total	100%
Extrapolated value	5.37

Q17b. If your confidence is low (responses 1 to 4), please select all that apply.	Total
We can't create a unified view of privileged user access across the enterprise	51%
We have privileged user account information but not privileged user entitlement information	56%
We can't apply controls that need to span across information resources	46%
We can't keep up with the changes occurring to our organization's IT resources (on-boarding, off- boarding and outsourcing for management)	61%
Other (please specify)	3%
Total	218%

Q18. What are the predominant processes used for granting users privileged access to IT resources? Please select no more than two choices.	Total
Manual process (i.e. email or phone)	39%
Homegrown access request systems	40%
Commercial off- the-shelf automated solutions	35%
Customized commercial solutions	41%
IT Help Desk	25%
Unsure	17%
Other (please specify)	4%
Total	200%

Q19. What are the predominant processes used to review and certify privileged access? Please select no more than two choices.	Total
Manual process (i.e. email, spreadsheets)	41%
Homegrown access certification system	47%
Commercial off- the-shelf access certification system	36%
Customized commercial access certification system	48%
Unsure	25%
Other (please specify)	4%
Total	200%

Q20a. Does your organization measure the effectiveness of its access governance programs?	Total
Yes	62%
No	38%
Total	100%

Q20b. If yes, what do you measure? Please select all that apply.	Total
Reduction in ad-hoc access requests	44%
Decline in audit findings and improvements in compliance posture	50%
Time saved during access provisioning per user	36%
Time saved by automating the process of onboarding and offboarding privileged users	46%
Fewer deficiencies in assigning privileged access	49%
Faster access review cycles and remediations	62%
Total cost of ownership	60%
Time saved with application access provisioning	37%
New efficiencies due to segregation of duties automation	30%
Improved access reviews	23%
End-user efficiencies due to faster employee and contractor onboarding	26%
Reduced IT resolution time	25%
How often company SLAs for granting privileged access are met	23%
Total	510%

Q21. What are the main problems your organization faces in granting and enforcing privileged user access rights? Please select your top four choices.	Total
Takes too long to grant access to privileged users (not meeting our SLAs with the business)	37%
Too expensive to monitor and control all privileged users	43%
Too much staff required to monitor and control all privileged users	56%
Cannot apply access policy controls at point of change request	36%
Cannot keep pace with the number of access change requests that come in on a regular basis	51%
Lack of a consistent approval process for access and a way to handle exceptions	45%
Difficult to audit and validate privileged user access changes	27%
Difficult to apply existing PAM program to cloud applications and infrastructure	28%
Burdensome process for business users requesting access	46%
No common language exists for how access is requested that will work for both IT and the business	33%
Total	400%

Part 4. Cloud adoption and IAM

Q22. What percentage of your organization's IT infrastructure and applications have migrated to the cloud?	Total
Less than 25%	15%
25% to 50%	25%
51% to 75%	32%
75% to 100%	28%
Total	100%
Extrapolated value	56%

Q23. How has the use of cloud services affected the effectiveness of IAM?	Total
Significantly improved effectiveness	23%
Improved effectiveness	28%
No change in effectiveness	28%
Decreased effectiveness	13%
Significantly decreased effectiveness	8%
Total	100%

Q24. Is your cloud IT program integrated with your IAM?	Total
Yes	52%
No	41%
Unsure	7%
Total	100%

Q25. Does your organization use SaaS resources from cloud service providers?	Total
Yes, heavy use	33%
Yes, moderate use	29%
Yes, light use	30%
No (Please skip to Q30)	8%
Total	100%

Q26. What percent of your organization's business-critical applications are SaaS versus on-premises software applications?	Total
Less than 25%	28%
Between 25 to 50%	26%
Between 51 to 75%	24%
Between 76% to 100%	22%
Total	100%
Extrapolated value	48%

Q27. How many SaaS applications does your organization have?	Total
Less than 100	30%
101 to 250	35%
251 to 500	21%
More than 500	14%
Total	100%
Extrapolated value	241

Q28. How many on-premises applications does your organization have?	Total
Less than 100	24%
101 to 250	35%
251 to 500	33%
More than 500	8%
Total	100%
Extrapolated value	243

Q29. What percentage of SaaS applications are under the control of your IAM program?	Total
Less than 25%	19%
Between 25 to 50%	38%
Between 51 to 75%	28%
Between 76% to 100%	15%
Total	100%
Extrapolated value	47%

Q30. What percentage of on-premises applications are under the control of your organization's IAM program and governance?	Total
Less than 25%	35%
Between 25 to 50%	42%
Between 51 to 75%	16%
Between 76% to 100%	7%
Total	100%
Extrapolated value	36%

Q31. What are the primary challenges your organization faces to using risk data to inform cybersecurity initiative prioritization and decision making? Please select the top two choices.	Total
No defined risk assessment framework	54%
Multiple risk assessment frameworks in use	44%
We collect risk data but do not use it in this way	44%
We do not currently collect data about our risks	29%
We do not currently map our risks	26%
Other (please specify)	3%
Total	200%

Q32a. Do any of your employees and contractors work both off-site and on-site (e.g. hybrid or remote workforce)?	Total
Yes	41%
No (please skip to Q34a)	59%
Total	100%

Q32b. If yes, using the following 10-point scale, please rate your organization's confidence in reducing the insider threats created by a hybrid, remote workforce from 1 = low confidence to 10 = high confidence.	Total
1 or 2	20%
3 or 4	22%
5 or 6	26%
7 or 8	19%
9 or 10	13%
Total	100%
Extrapolated value	5.15

Q33. What steps are you taking to secure the hybrid, remote workforce as part of your organization's access governance program? Please select one choice only.	Total
Audit, grant or withdraw access rights to property and systems as needed	35%
Have adequate screening procedures for new employees joining the remote workforce	37%
Determine if remote workers are securely accessing the network	28%
Total	100%

Q34a. Has your organization implemented a zero-trust strategy?	Total
Yes, we have implemented a zero-trust privileged access strategy	52%
No, but we plan to in the next six months	20%
No, but we plan to in the next year	12%
No, but we plan to in the next two years	17%
Total	100%

Q34b. If yes, has your organization improved its visibility into where privilege is used, when it is used, how it is used and when it is being abused?	Total
Yes	54%
No	38%
Unsure	8%
Total	100%

Part 5. Your role

D1. What organizational level best describes your current position?	Total
Senior Executive/VP	9%
Director	16%
Manager	22%
Supervisor	15%
Technician/Staff	29%
Contractor	6%
Other	3%
Total	100%

D2. Check the **Primary Person** you or your IT security leader reports to within the organization.	Total
CEO/Executive Committee	8%
Chief Financial Officer	2%
General Counsel	3%
Chief Information Officer	33%
Chief Technology Officer	15%
Compliance Officer	6%
Human Resources VP	5%
Chief Security Officer	3%
Chief Information Security Officer	17%
Chief Risk Officer	7%
Other	1%
Total	100%

D3. What industry best describes your organization's industry focus?	Total
Agriculture & food service	1%
Communications	4%
Defense & aerospace	1%
Education & research	3%
Energy & utilities	5%
Financial services	18%
Health & pharmaceutical	9%
Hospitality	3%
Industrial/manufacturing	12%
Public sector	11%
Retailing	10%
Services	11%
Technology & software	8%
Transportation	3%
Other	2%
Total	100%

D4. What is the worldwide headcount of your organization?	Total
Less than 500	20%
500 to 1,000	23%
1,001 to 5,000	23%
5,001 to 25,000	17%
25,001 to 75,000	10%
75,000+	8%
Total	100%

Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.

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.