Ponemon INSTITUTE

The Hidden Cybersecurity Threat in Organizations: Disconnected Applications

Sponsored by Cerby

Independently conducted by Ponemon Institute LLC

Publication Date: April 2023

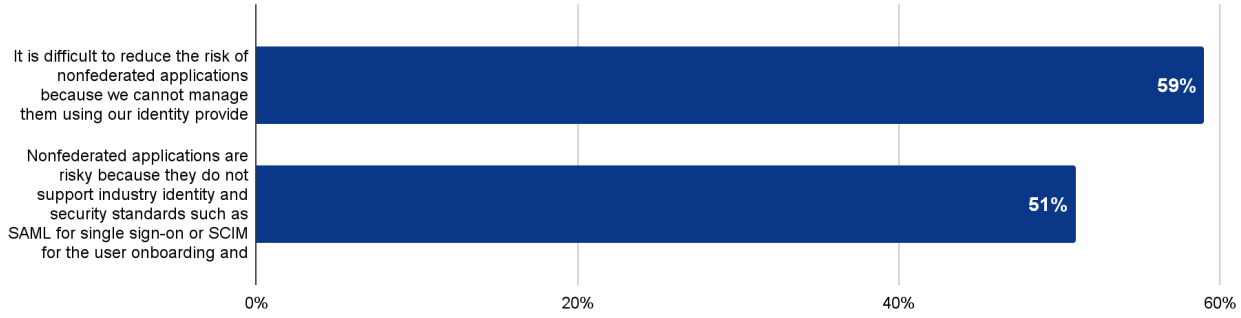
Part 1. Introduction

Disconnected applications pose an unseen and severe threat because in most organizations there is a lack of visibility into who has access to what and how accounts are secured. Sponsored by Cerby, Ponemon Institute surveyed 595 IT and security practitioners in the United States involved in their organization's identity and access management strategy. The study aims to determine an organization's level of understanding of the risks created by disconnected applications and the steps that can be taken to mitigate the risk.

A key takeaway from the research is that organizations don't know what they don't know when it comes to disconnected applications. Less than half (49 percent) of organizations track the number of disconnected applications they have that are not managed and accessed by their identity provider (IdP[1]). Of those respondents who track disconnected applications, 23 percent say they have between 101 to 250. The average number is 96. Despite efforts to have an accurate inventory, only 21 percent of these respondents are highly confident that they know all the disconnected applications used throughout the enterprise.

As shown in Figure 1, disconnected applications are risky because they cannot be centrally managed using the organizations' IdP, (59 percent of respondents). Fifty-one percent of respondents say they are risky because they do not support industry identity and security standards such as Security Assertion Markup Language (SAML) for single sign-on or System for Cross-domain Identity Management (SCIM) for the user onboarding and offboarding process. As defined in this research, disconnected applications lack support for the security standards organizations need to manage at scale. In the cloud and on-premises, these applications do not support common industry security standards.

Figure 1. Understanding the risk of disconnected applications
Strongly agree and agree responses combined



The following findings are evidence of the risk posed by disconnected applications.

- **The cost and time of provisioning and deprovisioning access to applications quickly add up.** Before analyzing the risks, it is crucial to understand the costs. Seven hours is the average time spent provisioning access to a standard set of applications for one employee. At an average $62.50[2] hourly pay rate, the cost is **$437.50 per employee**. To deprovision one employee takes an average of 8 hours, costing **$500 per employee**. Organizations can use this benchmark to calculate the process's impact based on the annual turnover of employees and contractors.

[1] An IdP is a service that stores and manages digital identities. The use of an IdP can simplify the process of managing user identities and access, as it allows users to use a single set of credentials across multiple systems and applications. Many organizations use IdPs to manage user access to internal and external systems, such as cloud-based applications or partner networks.

[2] IT and IT security fully loaded pay rate per hour is $62.50 (source: Ponemon Institute)

- Salaries also need to be considered. An average of 8 people are involved in the provisioning and deprovisioning process in addition to their other responsibilities. The average annual salary per staff member is $81,000[3]. Consequently, the total annual staff cost is **$648,000**, with a significant portion allocated to the time-consuming manual work of provisioning and deprovisioning, which could be better utilized elsewhere.

- **The total average annual cost to investigate and remediate cybersecurity incidents involving disconnected applications is $292,500.** This is based on 47 hours each week, or 2,444 annually, to investigate potential unauthorized access and 43 hours weekly, or 2,236 annually, to investigate and remediate cybersecurity incidents caused by unauthorized access to disconnected applications.

- **Disconnected applications are represented across all application categories and are not limited to a single business unit.** As discussed previously, only 49 percent of organizations track using disconnected applications. Only 21 percent of these respondents say their organizations are confident in knowing all the disconnected applications being used. Disconnected application use across business units underscores the difficulty in managing them.

- **Fifty-two percent of respondents say their organizations have experienced a cybersecurity incident caused by the inability to secure disconnected applications.** Sixty-three percent of these respondents say their organizations had a minimum of 4 and more than 5 incidents. Loss of customers and business partners are the primary consequences of a cybersecurity incident caused by the inability to secure disconnected applications, according to 43 percent and 36 percent of respondents, respectively.

- **Security and identity teams are often left out of managing and manually controlling access to disconnected applications.** According to the research, shared management of disconnected applications leads to a decentralized approach. Business units (63 percent of respondents) are most likely to manage these applications, followed by IT teams (54 percent of respondents). Only 45 percent of respondents say the security and/or identity teams are responsible for managing these applications. Moreover, 54 percent of respondents say business units control the granting and revoking of access.

- **Organizations are using inefficient manual processes to grant and revoke access to applications.** An average of 84 applications in organizations represented in this research require an admin to manually log in to add, remove or update access, meaning the application doesn't support SCIM and the organization cannot leverage automation through its IdP. The primary reasons for not automating the process are SCIM is not supported (33 percent of respondents) and the cost (31 percent of respondents).

- **Organizations rely upon business units to report their use of disconnected applications.** While there are several methods used to collect information about current disconnected applications, business units are most likely to self-report their use of disconnected applications (62 percent of respondents), followed by the use of a cloud access security broker (CASB) (48 percent of respondents) and endpoint detection tools (47 percent of respondents). Only 39 percent of respondents say business units complete a form to confirm the disconnected applications used.

- **An average of more than half of tracked disconnected applications do not support single sign-on (SSO).** As discussed previously, there is an average of 96 disconnected applications in organizations that track their use, and respondents estimate that an average of 50 of these do not support SSO. As described in the research, the benefit of SSO is that it permits a user to have one

[3] Source: GlassDoor, published in CSO magazine, July 19,2021

set of login credentials—for example, a username and password to access multiple applications. Thus, SSO eases the management of multiple credentials.

- **Organizations lack an effective process to prevent employees from putting data in disconnected applications at risk.** Few organizations report that they are effective in preventing employees' reuse of passwords, retaining access to critical systems after they leave or change roles, and preventing the disabling of MFA.

- **There is a desire to prioritize disconnected application security, but the risk is underestimated due to a lack of awareness**. While only 34 percent of respondents say their organizations do not make the security of disconnected applications a priority, 44 percent of respondents say management underestimates the cybersecurity risks. When educated on the risks, 82 percent of respondents say the importance of securing disconnected applications increased.

- **Employees are sharing their account login credentials, making it critical to have the proper security safeguards in place.** Seventy-six percent of respondents say employees are sharing account login credentials with both employees and external collaborators (35 percent), sharing account login credentials with other employees (21 percent), and sharing with external collaborators (20 percent).

- **Exposing, failing to rotate passwords, and being unable to track who is accessing a shared account are top security concerns.** Forty-one percent of respondents say employees or collaborators share accounts without concealing the password, and another 41 percent say passwords are not rotated. Reused or weak credentials also create risk (36 percent of respondents).

- **Organizations are not able to reduce the cybersecurity risks caused by shared accounts.** Half of the respondents (50 percent) say their organizations' access management strategy enables employees to share login credentials securely when required by the application. However, only 27 percent of respondents say their organizations are very or highly effective in reducing cybersecurity risks from shared accounts. Of those respondents (73 percent) who rank their organization's effectiveness as low, 56 percent are motivated to reduce the cybersecurity risk.

- **Organizations lack processes and policies to make disconnected applications secure.** Only 41 percent of respondents have a process to make disconnected applications secure and compliant with their organizations' policies, and only 35 percent of respondents say they have a policy that prevents the trial use of new disconnected applications. Thirty-nine percent of respondents say the use of disconnected applications is limited. This research shows that organizations do not like to limit the use of disconnected applications because it can affect employee morale and productivity.

- **The challenge for organizations is that they don't know what they don't know.** The top two challenges to securing disconnected applications are the inability to know and manage all disconnected applications because of the lack of visibility and not having an accurate inventory. This is followed by the inefficient use of manual processes to secure disconnected applications. Budget and in-house expertise are not considered as much of a challenge.

- **Most organizations do not follow up to ensure password and MFA policies adherence.** Fifty-seven percent of respondents say employees are required and reminded to turn on MFA, and about half (48 percent of respondents) say employees are required and reminded to rotate passwords regularly. However, only 40 percent of respondents say they follow up with every account to ensure MFA is turned on and passwords are rotated following their policies.

Part 2. Key findings

The complete audited findings are shown in the Appendix of this report. The report is organized according to the following topics about disconnected applications.

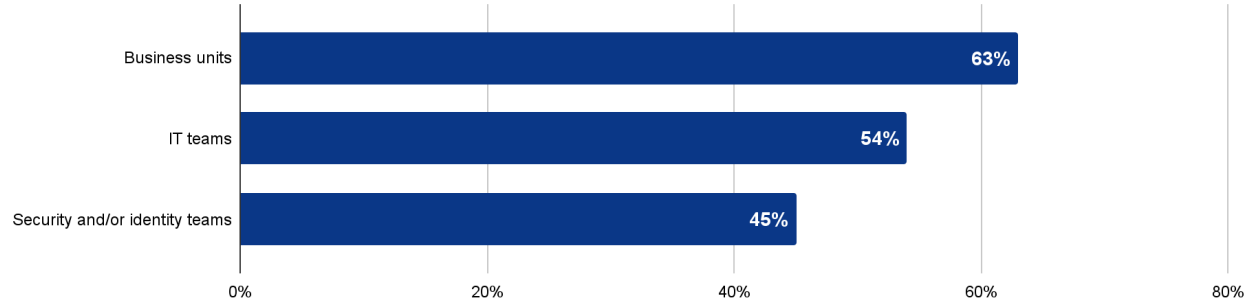
- What organizations understand about the risks
- Why organizations are vulnerable to a potential cybersecurity incident
- The cost of disconnected application management and risk
- Solutions: Managing the risks of disconnected applications

What organizations understand about the risks

Security and identity teams are often left out of managing and manually controlling access to disconnected applications. According to the research, shared management of disconnected applications leads to a decentralized approach. As shown in Figure 2, business units (63 percent of respondents) are most likely to manage disconnected applications, followed by IT teams (54 percent of respondents). Only 45 percent of respondents say the security and/or identity teams are responsible for managing these applications. Moreover, 54 percent of respondents say business units control the granting and revoking of access.

Figure 2. Who manages disconnected applications?

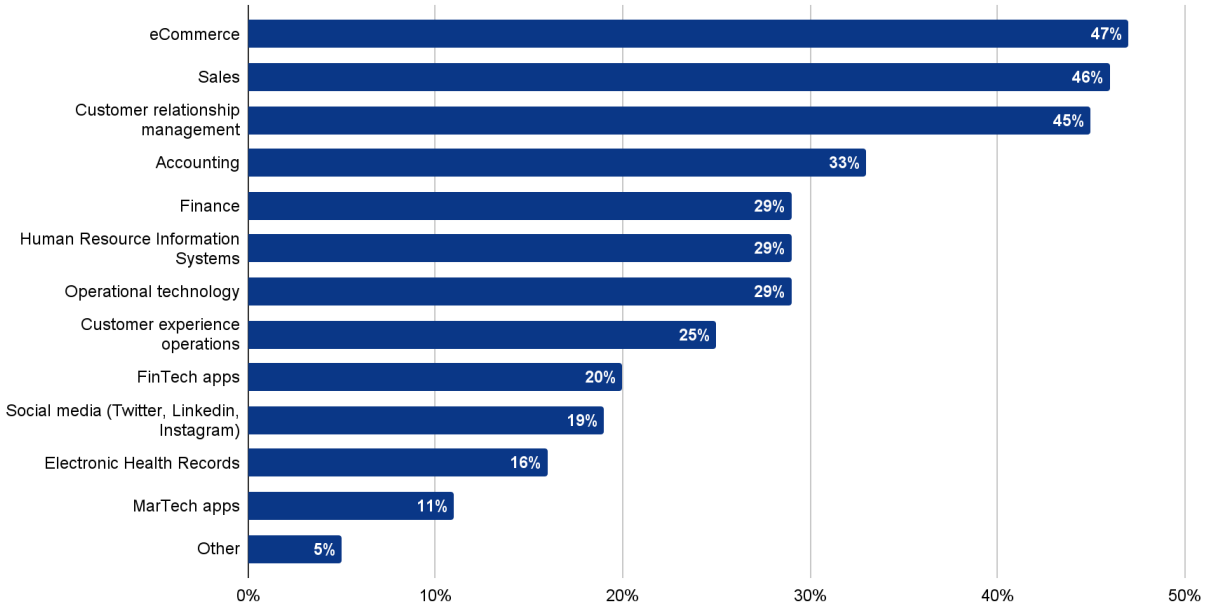
More than one response permitted



Disconnected applications are widely used across application categories from eCommerce to electronic health records and underscore their extensive use and risk. Only 49 percent of organizations are tracking the use of disconnected applications, and only 21 percent of these respondents say their organizations are confident in knowing all the disconnected applications being used. If they do know what applications they have, the primary types of applications used are eCommerce (47 percent), sales (46 percent), and CRM (45 percent), as shown in Figure 3.

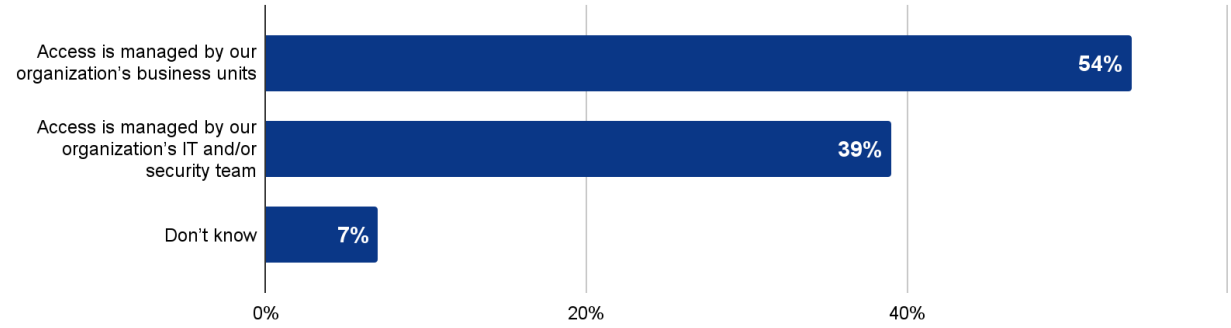
Figure 3. What categories of disconnected applications does your organization have?

More than one response permitted



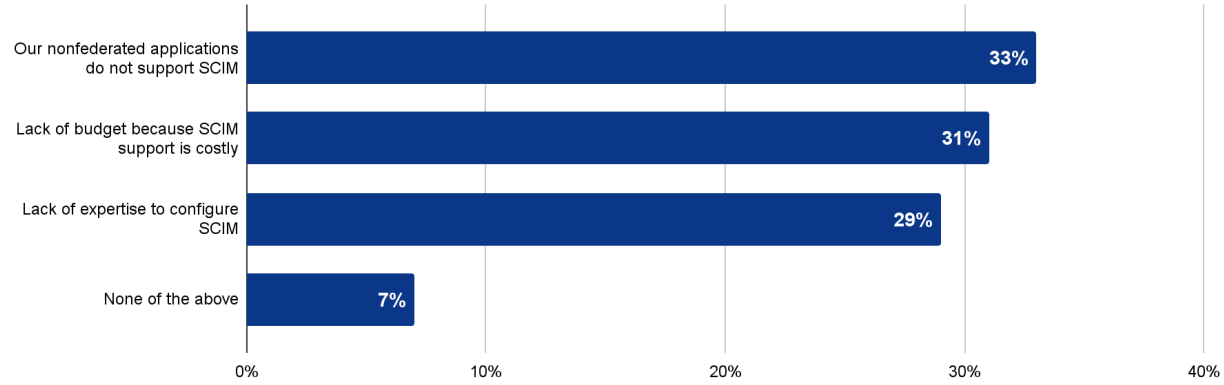
Business units are mostly managing access to disconnected applications. As shown in Figure 4, 54 percent of respondents say the granting and revoking of access to each disconnected application are controlled by business units.

Figure 4. How does your organization manually grant and revoke access to each disconnected application?



Organizations are using inefficient manual processes to grant and revoke access to applications. An average of 84 applications in organizations represented in this research require an admin to log in to add, remove or update access manually. Manual processes are used as the applications don't support SCIM, and the organization cannot leverage automation through its IdP. According to Figure 5, the primary reasons for not automating the process are SCIM is not supported (33 percent of respondents) and the cost (31 percent of respondents).

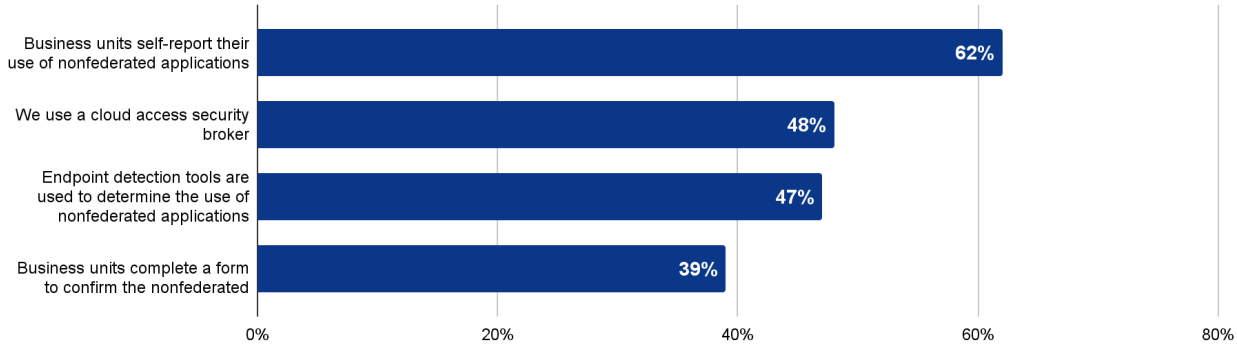
Figure 5. Why does your organization manually grant and revoke access to each disconnected application?



Organizations rely upon business units to report their use of disconnected applications. According to Figure 6, while there are several methods used to collect information about current disconnected applications, business units are most likely to self-report their use of disconnected applications (62 percent of respondents) followed by the use of a CASB (48 percent of respondents) and endpoint detection tools (47 percent of respondents). Only 39 percent of respondents say business units complete a form to confirm the disconnected applications used.

Figure 6. How do you collect information about the current disconnected applications used across different business units?

More than one response permitted

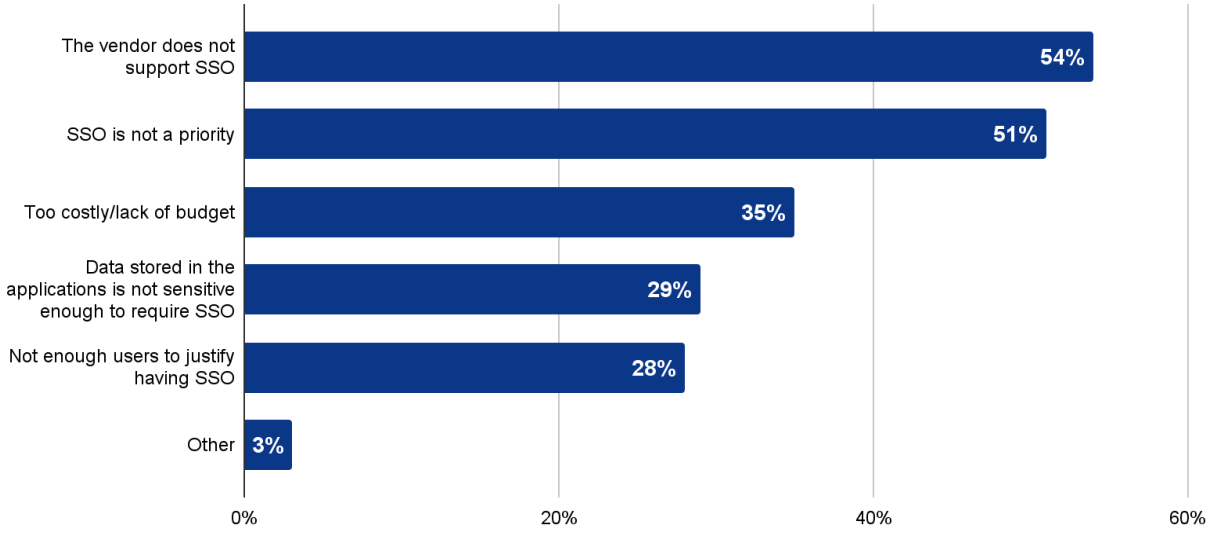


An average of more than half of tracked disconnected applications do not support SSO. As discussed previously, there is an average of 96 disconnected applications in organizations, and respondents estimate that an average of 50 of these disconnected applications do not support SSO. As described in the research, the benefit of SSO is that it permits a user to have one set of login credentials—for example, a username and password to access multiple applications. Thus, SSO eases the management of multiple credentials and reduces password reuse.

The primary reasons for not supporting SSO are lack of vendor support (54 percent of respondents), and SSO is not a priority (51 percent of respondents), as shown in Figure 7.

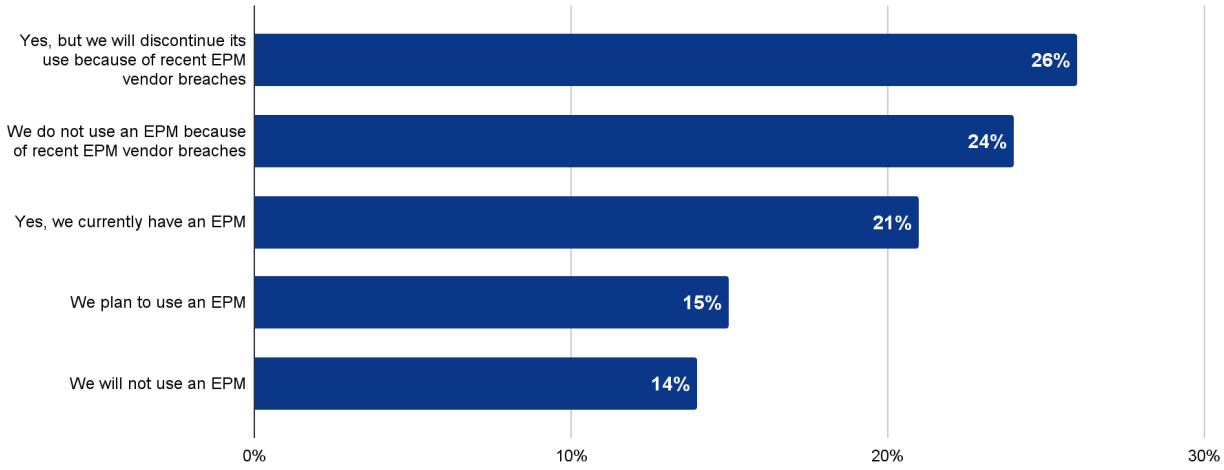
Figure 7. What are the primary reasons your organization's disconnected applications do NOT support SSO?

Two responses permitted



Recent vendor breaches negatively impacted enterprise decisions to use enterprise password managers (EPMs). Fifty percent of respondents (26 percent + 24 percent) will discontinue or plan not to use an EPM because of vendor breaches. EPMs generate strong, unique passwords and allow employees to store secrets from SSH keys to passwords. According to Figure 8, only 21 percent of respondents say they currently have an EPM, and 15 percent of respondents say they plan to use an EPM.

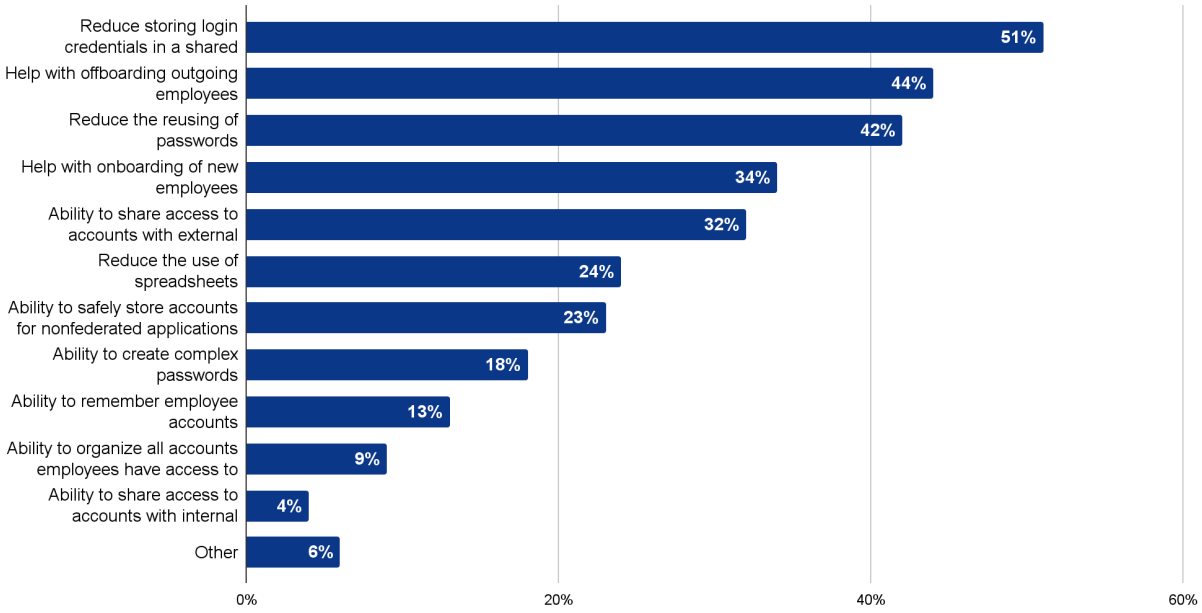
Figure 8. Does your organization use an EPM?



According to Figure 9, of the 21 percent of respondents currently using an EPM, 23 percent cite the ability to safely store accounts for disconnected applications as a benefit. Coupled with the 50 percent who will discontinue or remove EPMs from deployment plans due to recent breaches, organizations have a shrinking arsenal of tools to combat the risks of disconnected applications.

Figure 9. Benefits of an EPM

More than one response permitted



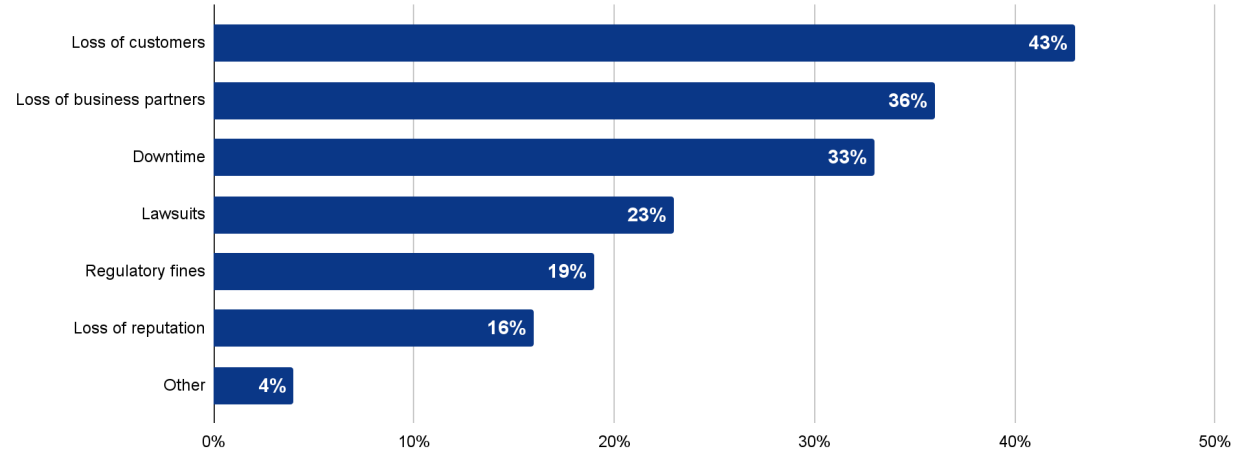
Why organizations are vulnerable to a potential cybersecurity incident

Fifty-two percent of respondents say their organizations have experienced a cybersecurity incident caused by the inability to secure disconnected applications. Sixty-three percent of these respondents say their organizations had a minimum of 4 and more than 5 incidents.

Loss of customers and business partners are the primary consequences of a cybersecurity incident caused by the inability to secure disconnected applications, according to 43 percent and 36 percent of respondents, respectively (Figure 10). These losses prove the need to know and secure disconnected applications used across the application and business spectrum.

Figure 10. What were the consequences of a cybersecurity incident caused by the inability to secure disconnected applications?

More than one response permitted

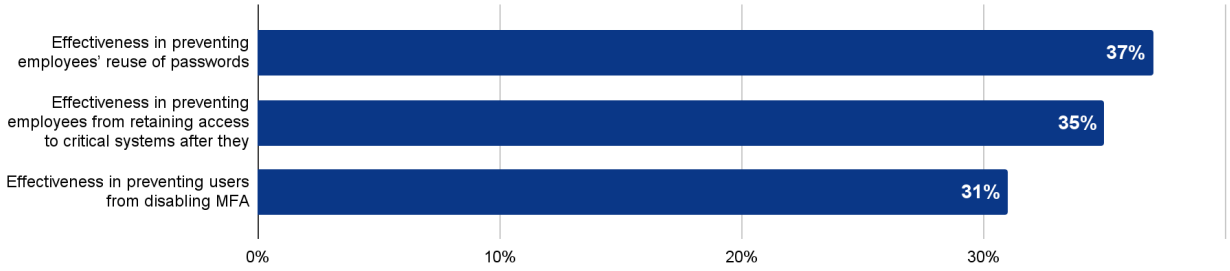


Organizations lack an effective process to prevent employees from putting data in disconnected applications at risk. Respondents were asked to rank their organizations' effectiveness in safeguarding disconnected applications on a scale from 1 = low effectiveness to 10 = high effectiveness.

Figure 11 presents the 7+ responses (very or highly effective). As shown, few organizations report that they are effective in preventing employees' reuse of passwords, retaining access to critical systems after they leave or change roles, and preventing the disabling of MFA.

Figure 11. Practices that create risks caused by disconnected applications

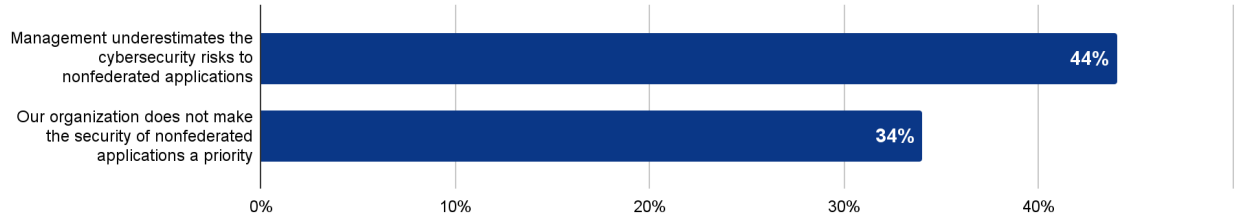
On a scale from 1 = low effectiveness to 10 = high effectiveness, 7+ responses presented



There is a desire to prioritize disconnected application security, but the risk is underestimated due to a lack of awareness. While only 34 percent of respondents say their organizations do not make the security of disconnected applications a priority, 44 percent of respondents say management underestimates the cybersecurity risks (Figure 12).

Figure 12. Perceptions about disconnected applications

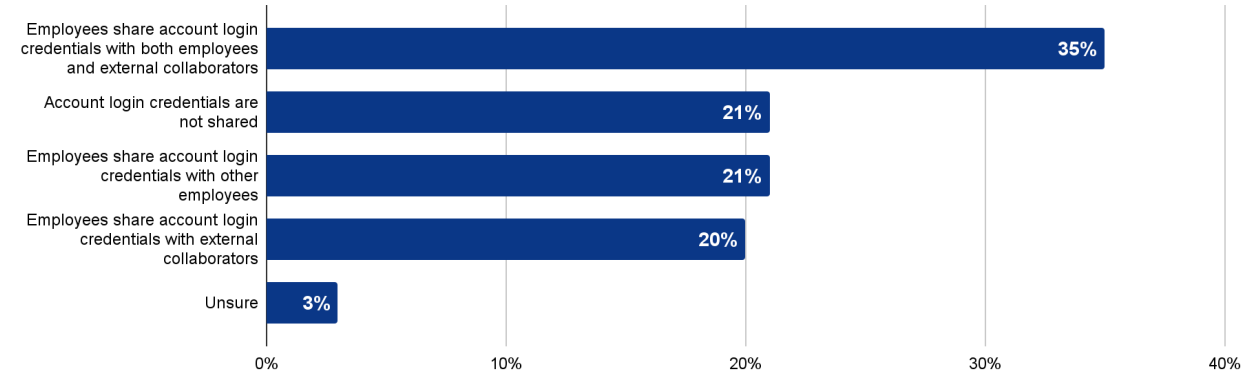
Strongly agree and Agree responses combined



Employees are sharing their account login credentials, making it critical to have the proper security safeguards in place. According to Figure 13, 76 percent of respondents say employees are sharing account login credentials with both employees and external collaborators (35 percent), sharing account login credentials with other employees (21 percent), and sharing with external collaborators (20 percent). Only 21 percent of respondents say account login credentials are not shared, and 3 percent are unsure.

Shared access of accounts requires organizations to know who accesses what and when, verify that MFA is active, and routinely conduct password rotations for shared accounts. As discussed previously, the management of disconnected applications is decentralized, making it difficult to ensure users adhere to the processes and policies organizations may have in place to secure access and comply with industry regulations.

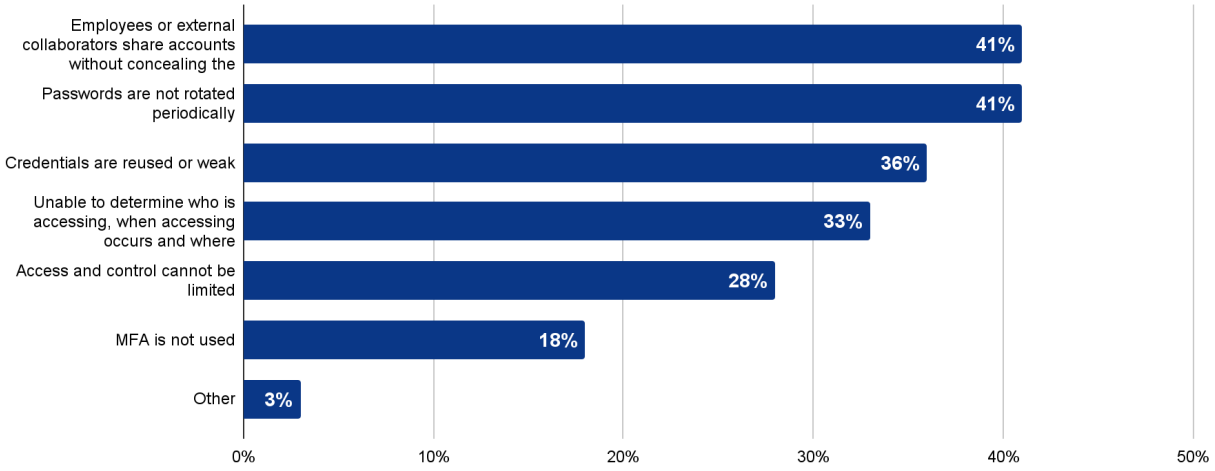
Figure 13. Do employees share account login credentials?



Exposing, failing to rotate passwords, and being unable to track who is accessing a shared account are top security concerns. Figure 14 presents the top cybersecurity risks caused by shared accounts. Forty-one percent of respondents say employees or collaborators share accounts without concealing passwords, and another 41 percent say passwords are not rotated. Reused or weak credentials also create risk (36 percent of respondents).

Figure 14. What are the top two cybersecurity risks caused by shared accounts?

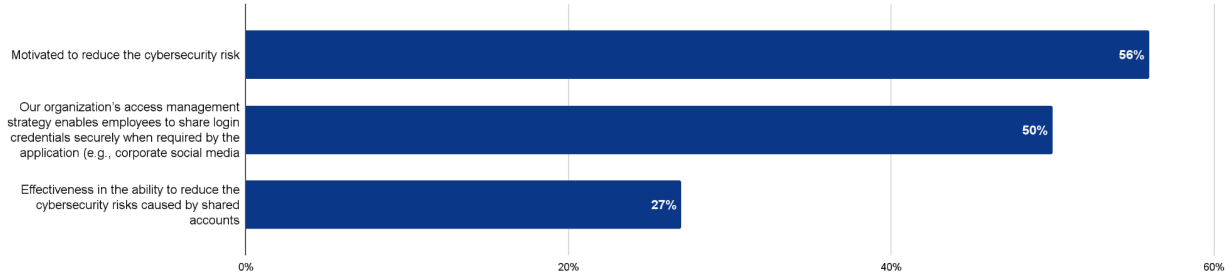
Two responses permitted



Organizations are not able to reduce the cybersecurity risks caused by shared accounts. According to Figure 15, only half (50 percent) of respondents say their organizations' access management strategy enables employees to share login credentials securely when required by the application. However, only 27 percent of respondents say their organizations are very or highly effective in reducing cybersecurity risks from shared accounts. Of those respondents (73 percent) who rank their organization's effectiveness as low, 56 percent are motivated to reduce the cybersecurity risk.

Figure 15. Perceptions about the risk of shared accounts

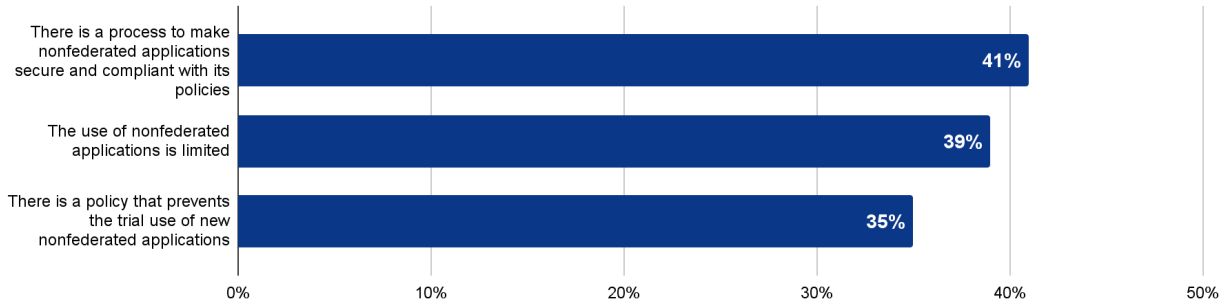
Agree, highly effective and highly motivated responses presented



Organizations lack processes and policies to make disconnected applications secure. According to Figure 16, only 41 percent of respondents have a process to make disconnected applications secure and compliant with their policies and only 35 percent of respondents say they have a policy that prevents the trial use of new disconnected applications. Only 39 percent of respondents say the use of disconnected applications is limited. As shown in this research, organizations do not like to limit the use of disconnected applications because it can affect employee morale and productivity.

Figure 16. Processes and policies to make disconnected applications secure

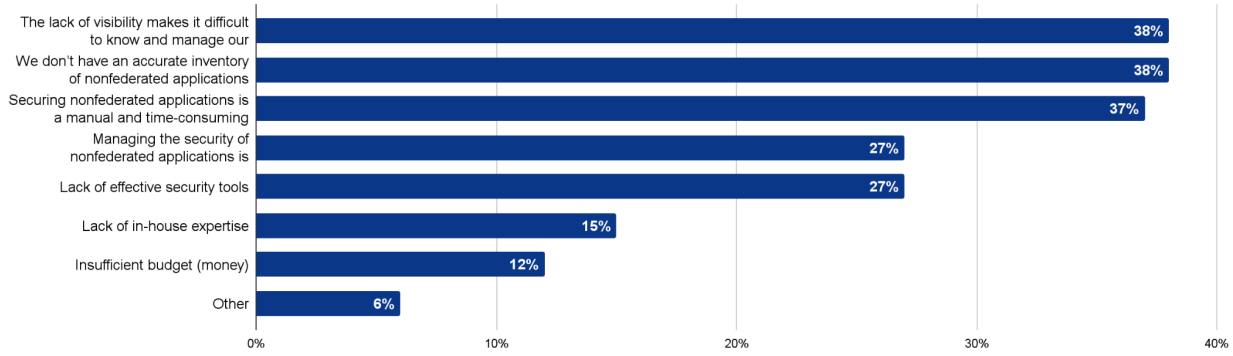
Yes responses presented



The challenge for organizations is that they don't know what they don't know. As shown in Figure 17, the top two challenges to securing disconnected applications are the inability to know and manage all the disconnected applications in use and not having an accurate inventory. This is followed by the inefficient use of manual processes to secure disconnected applications. Budget and in-house expertise are not considered as much of a challenge.

Figure 17. What are the top two challenges to securing disconnected applications?

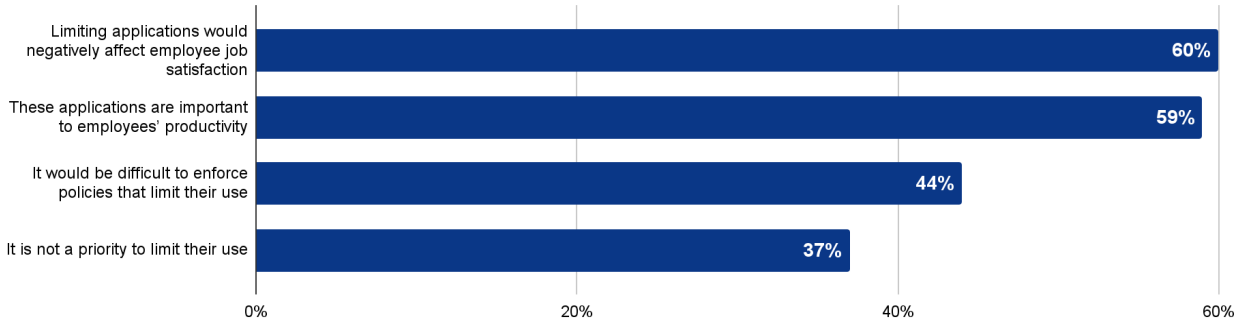
Two responses permitted



Job satisfaction and productivity are some of the reasons for not limiting the use of disconnected applications, as shown in Figure 18. Because organizations are not limiting their business units' use of disconnected applications, policies that govern their use should be enacted. Steps also should be taken to track these applications and secure them as part of the organization's identity and access management strategy.

Figure 18. Why does your organization not limit the use of disconnected applications?

Two responses permitted

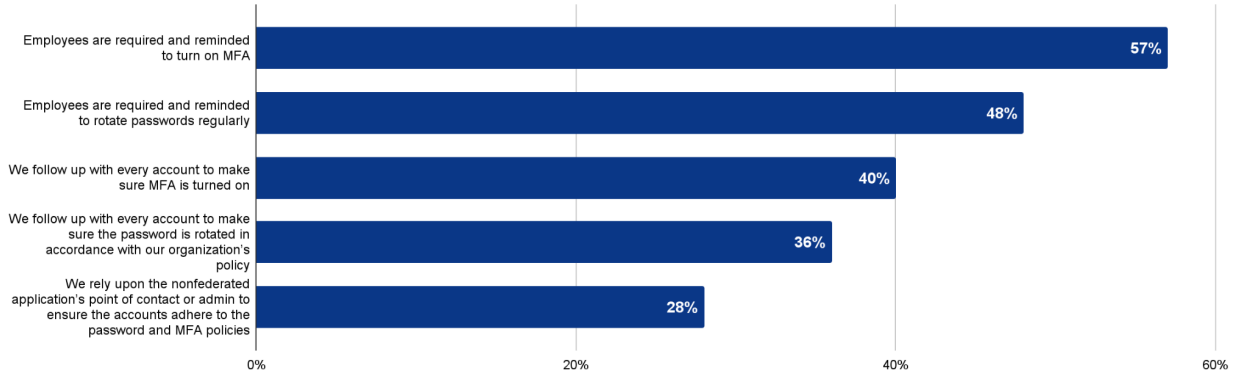


Most organizations do not follow up to ensure adherence to password and MFA policies. As shown in Figure 19, 57 percent of respondents say employees are required and reminded to turn on MFA, and about half (48 percent of respondents) say employees are required and reminded to rotate passwords regularly. However, only 40 percent of respondents say they follow up with every account to ensure MFA is turned on and passwords are rotated following their policies.

This “trust but do not verify” approach further illustrates the unchecked cyber risk of disconnected applications not managed centrally through an identity provider.

Figure 19. How do you ensure that employees’ accounts in disconnected applications adhere to the organization’s password and multi-factor authentication (MFA) policies

More than one response permitted



The cost of disconnected application management and risk

The cost of provisioning and deprovisioning access to applications quickly adds up. As shown in Table 1, 7 hours is the average time spent provisioning access to a standard set of applications for one employee. At an average $62.50[4] hourly pay rate, the cost averages **$437.50 per employee**. To deprovision one employee takes an average of 8 hours, costing **$500 per employee**. This benchmark can be used to calculate the process's negative productivity impact based on the annual turnover of employees and contractors.

The provisioning process involves collecting new employee information, logging in, and manually granting access to needed applications. Deprovisioning involves collecting an outgoing employee's information, searching for applications to which they are granted access, and revoking access to all relevant applications.

Deprovisioning can take significantly longer than onboarding due to the number of applications an employee or contractor may have gained access to over their tenure. Salaries also need to be considered. An average of 8 people are involved in the provisioning and deprovisioning process, in addition to their other responsibilities, and the average annual salary per staff member is $81,000[5]. Consequently, the total annual staff cost is **$648,000**, with a significant portion allocated to the time-consuming manual work of provisioning and deprovisioning, which could be better utilized elsewhere.

Table 1.

Time spent provisioning and deprovisioning access to applications	Average hours per employee	Cost per employee
Time spent provisioning access to a standard set of applications per employee	7 hours	$437.50
Time spent deprovisioning access to a standard set of applications per employee	8 hours	$500.00
Total hours for provisioning and deprovisioning **per** employee	15 hours	$937.50

[4] IT and IT security fully loaded pay rate per hour is $62.50 (source: Ponemon Institute)
[5] Source: GlassDoor, published in CSO magazine, July 19,2021

As shown in Table 2, the total average annual cost to investigate and remediate cybersecurity incidents involving disconnected applications is $292,500. This is based on 47 hours each week or 2,444 annually to investigate potential unauthorized access and 43 hours weekly, or 2,236 annually, to investigate and remediate cybersecurity incidents caused by unauthorized access to disconnected applications.

Table 2.

Time spent investigating and remediating cybersecurity incidents[6] involving disconnected applications	Aggregate hours of IT and IT security staff weekly	Aggregate Hours of IT and IT security staff annually
Investigating potential unauthorized access to disconnected applications	47 hours	2,444
Investigating and remediating cybersecurity incidents caused by unauthorized access to disconnected applications	43 hours	2,236
Average total hours weekly/annually	90 hours	4,680
Average total cost weekly/monthly	$5,625	$292,500

Solutions: Managing the risks of disconnected applications

Now that the many risks associated with disconnected applications have been outlined, what steps can organizations take to address the previously hidden threat? We recommend the following considerations.

- Enhance your organization's security posture by increasing visibility and assessing risks associated with disconnected application usage across all types, including on-premise, OT, legacy, and cloud.
- Adopt a proactive approach rather than merely blocking access, which may negatively impact productivity. Opt for solutions that redirect employees to approved cloud and on-premise applications, minimizing the expansion of disconnected applications.
- Centralize disconnected application management by implementing solutions that bridge the gap between your organization's IdP and these applications across all categories. Assign security and/or identity teams to manage access, as business units may not adhere to security best practices, contributing to potential cybersecurity incidents.
- To streamline onboarding and offboarding processes, leverage automation solutions to centralize access around your organization's IdP for all disconnected applications, including on-premise, OT, legacy, and cloud. Organizations can significantly reduce manual workload and costs by implementing solutions that extend the complete identity lifecycle to disconnected applications. Our research indicates that the total annual staff cost is $648,000, with a substantial portion dedicated to time-consuming manual tasks like provisioning and deprovisioning. By focusing on cost savings and optimizing resource allocation, businesses can achieve a considerable ROI and direct staff efforts toward more value-added activities.
- Utilize platforms that facilitate tracking user activity within disconnected applications, as access to these applications is often obscured from security platforms. For shared accounts, such as

[6] The aggregate hours of the IT and security teams spent weekly and annually

corporate social media or administrative accounts, find solutions to track individual access across various application types. Centralize all access to disconnected applications and integrate them with SIEM platforms for further analysis.

Part 3. Methodology

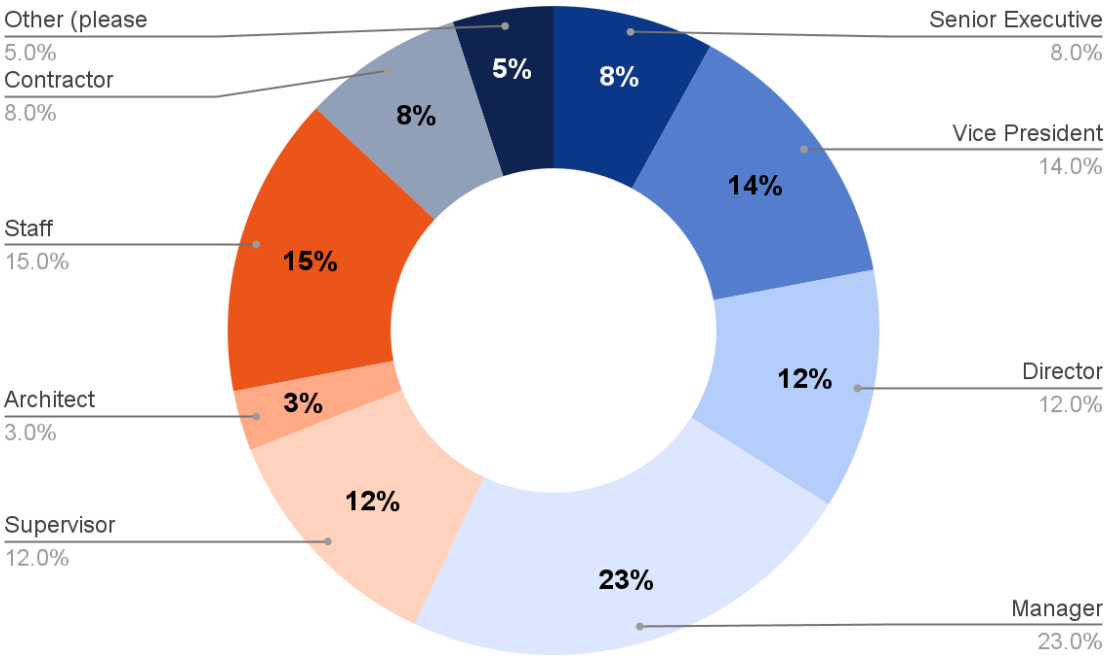
A sampling frame of 15,880 IT and security practitioners in the United States involved in their organization's identity and access management strategy were selected as participants in this survey. Table 3 shows 669 total returns. Screening and reliability checks required the removal of 74 surveys. Our final sample consisted of 595 surveys or a 3.7 percent response.

Table 3

Sample response	Freq	Pct%
Sampling frame	15,880	100.0%
Total returns	669	4.2%
Rejected or screened surveys	74	0.5%
Final sample	595	3.7%

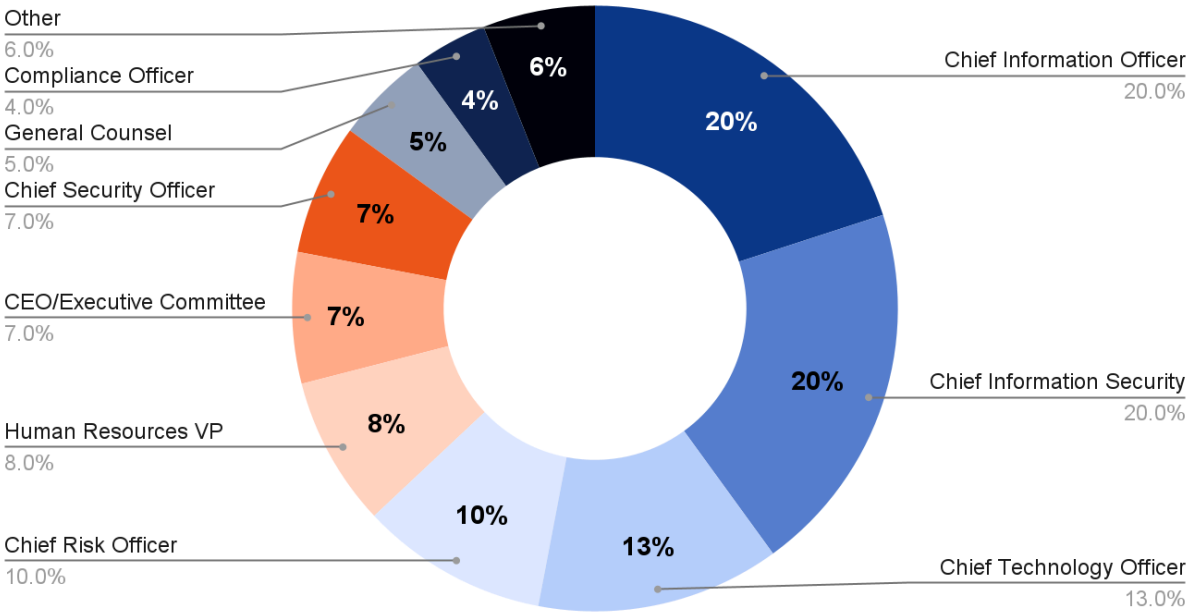
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, more than half (69 percent) of respondents are at or above the supervisory levels. The largest category, at 23 percent of respondents, is manager.

Pie Chart 1. Current position within the organization



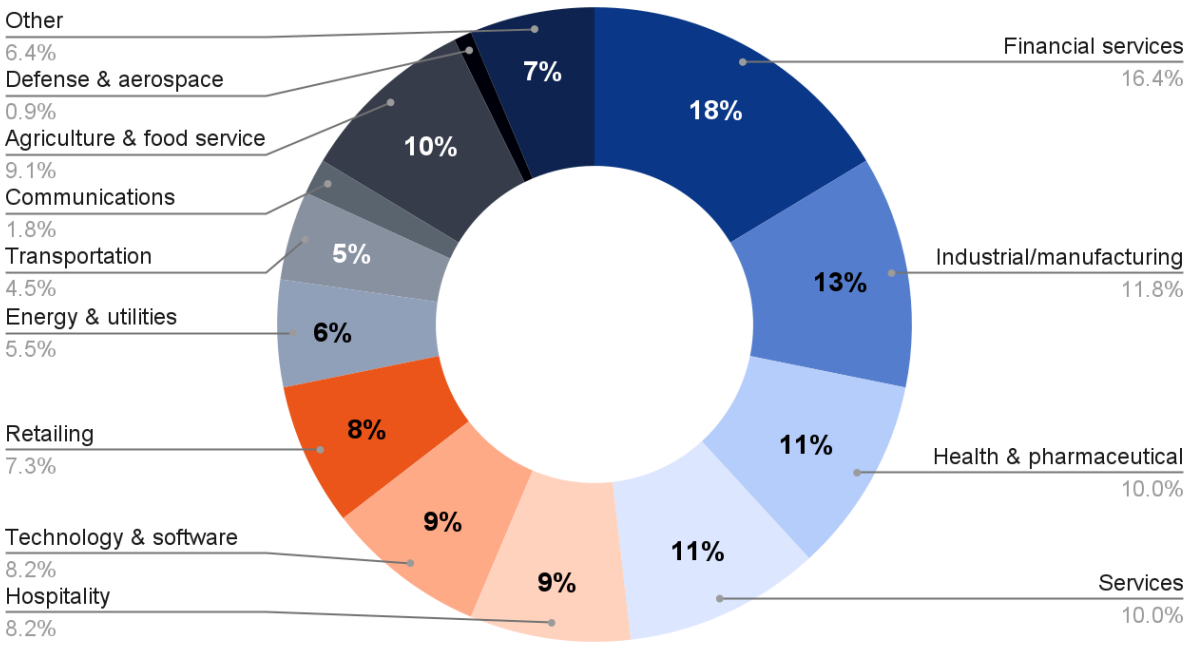
Pie Chart 2 reports the primary person the respondent reports to within the organization. Twenty percent of respondents report to the chief information officer, 20 percent report to the chief information security officer, 13 percent report to the chief technology officer, and 10 percent report to the chief risk 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 respondents' organizations. This chart identifies financial services (18 percent) as the most prominent industry focus, which includes banking, investment management, insurance, brokerage, payments, and credit cards. This is followed by industrial manufacturing (13 percent of respondents), healthcare and pharmaceuticals (11 percent of respondents), services (11 percent of respondents), technology and software (9 percent of respondents), and retailing (9 percent of respondents).

Pie Chart 3. Primary industry focus



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 individuals who are IT and IT Security practitioners. 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.

Note on Terminology Update – October 2024

As of October 2024, we have updated the term "nonstandard applications" to "disconnected applications" throughout this whitepaper. This change reflects our ongoing commitment to clarity and better aligns with the evolving language used in the industry to describe applications that fall outside of centralized identity management systems. While the terminology has been updated, the core findings and recommendations remain unchanged.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to al survey questions. All survey responses were captured in February and March 2023.

Survey response	Freq
Total sampling frame	15,880
Total survey returns	669
Rejected surveys	74
Final sample	595
Response rate	3.7%

Part 1. Screening Questions

S1. How involved are you in your organization's identity and access strategy?	Pct%
Highly involved	20%
Involved	45%
Somewhat involved	35%
Not involved (Stop)	0%
Total	100%

S2. What is the headcount of your organization?	Pct%
Less than 1,000 (Stop)	0%
1,000 to 5,000	43%
5,001 to 25,000	32%
25,001 to 75,000	17%
75,000+	8%
Total	100%

Part 2. Background

Q1a. Does your organization track the number of disconnected applications it has that are not managed and accessed by its IdP?	Pct%
Yes	49%
No (please skip to Q3)	51%
Total	100%

Q1b. If yes, how many disconnected applications are used in your organization?	Pct%
1 to 5	6%
6 to 10	11%
11 to 20	15%
21 to 50	18%
51 to 100	17%
101 to 250	21%
More than 250	12%
Total	100%
Average number of disconnected applications	96

Q2. Using the following 10-point scale, please rate your organization's confidence in knowing all the disconnected applications being used from 1 = low confidence to 10 = high confidence.	Pct%
1 or 2	31%
3 or 4	31%
5 or 6	17%
7 or 8	13%
9 or 10	8%
Total	100%

Q3. What categories of disconnected applications does your organization have? Please select all that apply.	Pct%
Accounting	33%
eCommerce	47%
Operational technology (OT)	29%
Human Resource Information Systems (HRIS)	29%
Customer relationship management (CRM)	45%
Finance	29%
Sales	46%
Customer experience operations	25%
Social media (Twitter, LinkedIn, Instagram)	19%
FinTech apps	20%
MarTech apps	11%
Electronic Health Records (EHR)	16%
Other (please specify)	5%
Total	354%

Q4. Does your organization have a process to make disconnected applications secure and compliant with its policies?	Pct%
Yes	41%
No	59%
Total	100%

Q5. Who manages disconnected applications? Please select all that apply.	Pct%
Business units	63%
IT teams	54%
Security and/or identity teams	45%
Total	162%

Q6. How do you collect information about the current disconnected applications used across different business units? Please select all that apply.	Pct%
Business units self-report their use of disconnected applications	62%
Business units complete a form to confirm the disconnected applications used	39%
Endpoint detection tools are used to determine the use of disconnected applications	47%
We use a cloud access security broker (CASB)	48%
Total	196%

Q7. Does your organization have a policy that prevents the trial use of new disconnected applications?	Pct%
Yes	35%
No	65%
Total	100%

Q8a. Does your organization limit the use of disconnected applications?	Pct%
Yes (please skip to Q9)	39%
No	61%
Total	100%

Q8b. If no, why? Please select two choices only.	Pct%
These applications are important to employees' productivity	59%
Limiting applications would negatively affect employee job satisfaction	60%
It would be difficult to enforce policies that limit their use	44%
It is not a priority to limit their use	37%
Total	200%

Part 3. The risks to disconnected applications

Q9. Using the following 10-point scale, please rate your organization's effectiveness in preventing users from disabling MFA on a scale from 1 = low effectiveness to 10 = high effectiveness.

	Pct%
1 or 2	13%
3 or 4	36%
5 or 6	20%
7 or 8	18%
9 or 10	13%
Total	100%

Q10. Using the following 10-point scale, please rate your organization's effectiveness in preventing employees' reuse of passwords on a scale from 1 = low effectiveness to 10 = high effectiveness.

	Pct%
1 or 2	19%
3 or 4	27%
5 or 6	17%
7 or 8	21%
9 or 10	16%
Total	100%

Q11. Using the following 10-point scale, please rate your organization's effectiveness in preventing employees from retaining access to critical systems after they leave or change roles on a scale from 1 = low effectiveness to 10 = high effectiveness.

	Pct%
1 or 2	21%
3 or 4	26%
5 or 6	18%
7 or 8	20%
9 or 10	15%
Total	100%

Q12. What are the top two challenges to securing disconnected applications? Please select your top two challenges.

	Pct%
Insufficient budget (money)	12%
Lack of effective security tools	27%
Lack of in-house expertise	15%
We don't have an accurate inventory of disconnected applications	38%
The lack of visibility makes it difficult to know and manage our disconnected applications	38%

Managing the security of disconnected applications is decentralized in the business units	27%
Securing disconnected applications is a manual and time-consuming process	37%
Other (please specify)	6%
Total	200%

Please rate the statement using the scale provided below each item.

Q13a. Management underestimates the cybersecurity risks to disconnected applications.	Pct%
Strongly agree	20%
Agree	24%
Unsure	12%
Disagree	18%
Strongly disagree	26%
Total	100%

Q13b. Our organization does not make the security of disconnected applications a priority.	Pct%
Strongly agree	14%
Agree	20%
Unsure	14%
Disagree	29%
Strongly disagree	23%
Total	100%

Q13c It is difficult to reduce the risk of disconnected applications because we cannot manage them using our identity provider.	Pct%
Strongly agree	32%
Agree	27%
Unsure	11%
Disagree	18%
Strongly disagree	12%
Total	100%

Q13d. disconnected applications are risky because they do not support industry identity and security standards such as SAML for single sign-on or SCIM for the user onboarding and offboarding process.	Pct%
Strongly agree	25%
Agree	26%
Unsure	13%

Disagree	20%
Strongly disagree	16%
Total	100%

Q14. How do you ensure that employees' accounts in disconnected applications adhere to the organization's password and multi-factor authentication (MFA) policies?	Pct%
Employees are required and reminded to turn on MFA	57%
Employees are required and reminded to rotate passwords regularly	48%
We follow up with every account to make sure MFA is turned on	40%
We follow up with every account to make sure the password is rotated in accordance with our organization's policy	36%
We rely upon the disconnected application's point of contact or admin to ensure the accounts adhere to the password and MFA policies	28%

Q15a. Has your organization experienced a cybersecurity incident caused by the inability to secure disconnected applications?	**Pct%**
Yes	52%
No (please skip to Q16a)	40%
Unsure (please skip to Q16a)	8%
Total	100%

Q15b. If yes, how many?	**Pct%**
1 to 3	37%
4 to 5	45%
More than 5	18%
Total	100%

Q16a. Has your organization failed to meet regulatory compliance regulations due to the inability to secure disconnected applications?	**Pct%**
Yes	47%
No (please skip to Q17a)	46%
Unsure (please skip to Q17a)	7%
Total	100%

Q16b. If yes, what were the consequences? Please select all that apply.	Pct%
Lawsuits	23%
Regulatory fines	19%
Loss of customers	43%
Loss of business partners	36%
Downtime	33%
Loss of reputation	16%
Other (please specify)	4%
Total	174%

Q17a. Do all disconnected applications support SSO (i.e., SAML, SSO or OIDC)?	Pct%
Yes (please skip to Q19a)	47%
No	34%
Unsure because our organization does not have accurate visibility into all applications (please skip to Q19a	19%
Total	100%

Q17b. If no, how many applications used by your organization do NOT support single sign-on (i.e., SAML, SSO or OIDC)? Please select one choice only.	Pct%
1 to 5	3%
6 to 10	12%
11 to 20	17%
21 to 50	20%
51 to 75	18%
76 to 100	12%
101 to 250	10%
More than 250	8%
Total	100%
Average number of applications that do not support SSO	50.24

Q18. What are the two primary reasons your organization's disconnected applications do NOT support SSO? Please select the top two reasons only.	Pct%
Too costly/lack of budget	35%
Not enough users to justify having SSO	28%
Data stored in the applications is not sensitive enough to require SSO	29%
SSO is not a priority	51%
The vendor does not support SSO	54%
Other (please specify)	3%
Total	200%

Q19a. Does your organization use Enterprise Password Managers (EPM)? Please select one choice only.	Pct%
Yes, we currently have an EPM	21%
Yes, but we will discontinue its use because of recent EPM vendor breaches	26%
We plan to use an EPM	15%
We do not use an EPM because of recent EPM vendor breaches (please skip to Q20)	24%
We will not use an EPM (please skip to Q20)	14%
Total	100%

Q19b. If yes, what are the top three benefits of an EPM? Please select the top three benefits only.	Pct%
Ability to create complex passwords	18%
Ability to organize all accounts employees have access to	9%
Ability to remember employee accounts	13%
Ability to safely store accounts for disconnected applications	23%
Ability to share access to accounts with external collaborators	32%
Ability to share access to accounts with internal employees	4%
Help with onboarding of new employees	34%
Help with offboarding outgoing employees	44%
Reduce storing login credentials in a shared document	51%
Reduce the reusing of passwords	42%
Reduce the use of spreadsheets	24%
Other (please specify)	6%
Total	300%

Part 4. Risk of sharing account login credentials

Q20. Do employees share account login credentials? Please select one choice only.	Pct%
Yes, employees share account login credentials with other employees	21%
Yes, employees share account login credentials with external collaborators	20%
Yes, employees share account login credentials with both employees and external collaborators	35%
Account login credentials are not shared (please skip to Q22)	21%
Unsure	3%
Total	100%

Q21. What are the top two cybersecurity risks caused by shared accounts? Please select two choices only.	Pct%
Credentials are reused or weak	36%
Passwords are not rotated periodically	41%
Access and control cannot be limited	28%
MFA is not used	18%
Unable to determine who is accessing, when accessing occurs and where	33%
Employees or external collaborators share accounts without concealing the password	41%
Other (please specify)	3%
Total	200%

Please rate the statement using the scale provided below each item

Q22. Our organization's access management strategy enables employees to share login credentials securely when required by the application (e.g., corporate social media applications, privileged administration accounts).	Pct%
Strongly agree	21%
Agree	29%
Unsure	9%
Disagree	18%
Strongly disagree	23%
Total	100%

Q23. How effective is your organization's ability to reduce the cybersecurity risks caused by shared accounts on a scale from 1 = low effectiveness to 10 = high effectiveness?	Pct%
1 or 2	13%
3 or 4	35%
5 or 6	25%
7 or 8	18%
9 or 10	9%
Total	100%

Q24. If effectiveness is low, how motivated is your organization to reduce the risk on a scale from 1 = not motivated to 10 = highly motivated.	Pct%
1 or 2	9%
3 or 4	11%
5 or 6	24%
7 or 8	31%
9 or 10	25%
Total	100%

Part 5. The cost of managing and securing disconnected applications

Q25. How many applications require an admin to manually login to add, remove or update access, meaning the application doesn't support SCIM and your organization's IdP can't leverage automation?	Pct%
1 to 5	6%
6 to 10	9%
11 to 20	10%
21 to 50	23%
51 to 100	19%
101 to 250	15%
More than 250	11%
None (please skip to Q28)	0%
Unsure because we don't have accurate visibility into all applications (please skip to Q28)	7%
Total	100%
Average number of applications	84.29

Q26. How does your organization manually grant and revoke access to each disconnected application?	Pct%
Access is managed by our organization's IT and/or security team	39%
Access is managed by our organization's business units	54%
Don't know	7%
Total	100%

Q27. Why does your organization manually grant and revoke access to each disconnected application? Please select one choice only.	Pct%
Lack of budget because SCIM support is costly	31%
Lack of expertise to configure SCIM	29%
Our disconnected applications do not support SCIM	33%
None of the above	7%
Total	100%

Q28. Approximately how much time is spent provisioning access to a standard set of applications for one new employee (e.g. collecting new employee information, logging in and manually granting access to the applications they need)?	Pct%
Less than 30 minutes	8%
30 minutes to 59 minutes	23%
1 hour to 2 hours	21%
3 hours to 5 hours	17%
6 hours to 12 hours	9%
13 hours to 24 hours	16%
More than 24 hours	6%
Total	100%
Average time spent provisioning access (hours)	6.78

Q29. Approximately how much time is spent deprovisioning access to a standard set of applications for an outgoing employee (e.g. collecting outgoing an employee's information, revoking access to all relevant applications)?	Pct%
Less than 30 minutes	4%
30 minutes to 59 minutes	13%
1 hour to 2 hours	14%
3 hours to 5 hours	29%
6 hours to 12 hours	12%
13 hours to 24 hours	22%
More than 24 hours	6%
Total	100%
Average	8.43

Q30. Approximately how many people are involved in the provisioning and deprovisioning process at your company?	Pct%
1 person	8%
2 to 4 people	19%
5 to 7 people	23%
8 to 10 people	30%
More than 10 people	20%
Total	100%
Average	7.73

Q31. Approximately how much time each week is spent investigating potential unauthorized access to disconnected applications? Please estimate the aggregate hours of the IT and Security (SecOps) teams.	Pct%
Less than 5 hours	6%
5 to 10 hours	9%
11 to 25 hours	15%
26 to 50 hours	24%
More than 50 hours	46%
Total	100%
Average	47.15

Q32. Approximately how much time each week is spent investigating and remediating cybersecurity incidents resulting from unauthorized access to disconnected applications?	Pct%
Less than 5 hours	6%
5 to 10 hours	11%
11 to 25 hours	20%
26 to 50 hours	23%
More than 50 hours	40%
Total	100%
Average	43.32

Part 6. Conclusion

Q33. After completing the survey, has the importance of securing disconnected applications changed?	Pct%
Significantly increased in importance	23%
Increased in importance	34%
Somewhat increased in importance	25%
No change in importance	18%
Total	100%

Q34. How satisfied are you with your current solutions to reduce the cybersecurity risks to disconnected applications?	Pct%
Very satisfied	20%
Satisfied	24%
Somewhat satisfied	30%
Not satisfied	26%
Total	100%

Part 7. Your role

D1. What organizational level best describes your current position?	Pct%
Senior Executive	8%
Vice President	14%
Director	12%
Manager	23%
Supervisor	12%
Architect	3%
Staff	15%
Contractor	8%
Other (please specify)	5%
Total	100%

D2. Check the Primary Person you, your IT or Security leader reports to within the organization.	Pct%
CEO/Executive Committee	7%
Chief Financial Officer	0%
General Counsel	5%
Chief Information Officer	20%
Chief Technology Officer	13%
Compliance Officer	4%
Human Resources VP	8%
Chief Security Officer	7%
Chief Information Security Officer	20%
Chief Risk Officer	10%
Other	6%
Total	100%

D3. What industry best describes your organization's industry focus?	Pct%
Agriculture & food service	1%
Communications	2%
Defense & aerospace	0%
Energy & utilities	6%
Financial services	18%
Health & pharmaceutical	11%
Hospitality	9%
Industrial/manufacturing	13%
Retailing	8%
Services	11%
Technology & software	9%
Transportation	5%
Other (please specify)	7%
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.