ConductorOne

2024

Identity Security Outlook Report

Table of Contents

Executive Summary

Navigating identity, access, and permissions has become an overwhelmingly complicated challenge for security teams. The explosion of SaaS and the complexity of hybrid environments have created an intricately tangled web of permissions. This complexity is heightened as the extended enterprise takes hold, with contractors, partners, and suppliers now having access to sensitive company systems. The rise of non-human identities is also quickly expanding the risk associated with managing access and permissions within organizations.

These challenges go far beyond traditional identity priorities like passwords, authentication, or ease of access. Critical systems and sensitive data are now at risk from overprivileged users, birthright access, orphaned and unused accounts, and widespread permissions sprawl. Additionally, gaining visibility into and managing user access across systems is often a highly manual and time-consuming endeavor for security teams.

The *2024 Identity Security Outlook Report* was conducted to shine a light on the current identity security and access management challenges and opportunities security leaders face. For the study, ConductorOne surveyed 523 US-based IT security professionals — director level and higher — at companies with 250 to 10,000 employees. The results paint a clear picture of the technological and organizational complexity creating a new wave of identity risks. The study found that

- Most organizations have experienced firsthand just how risky identity issues have become. **The majority of security leaders said their organization has faced a cyberattack or data breach in the last 12 months** due to improper access or overprivileged users.
- **Complexity was cited as the number one identity security challenge today,** with most organizations dealing with numerous SaaS apps, hybrid environments, and external entities like contractors having access to systems.
- Despite nearly half of respondents stating their identity strategy is hindering team productivity, **risk reduction is the top priority for security leaders** when it comes to identity and access.
- **The concept of zero standing privileges is gaining traction** and is widely viewed as an effective strategy to reduce access risks.

Key Findings

1. The majority (77%) of security leaders said there have been instances of cyberattacks or data breaches at their organization in the past 12 months due to improper access or overprivileged users.

2. Respondents' top identity and access management challenges were
   - Complexity of existing systems (47%)
   - Employees' resistance to change (38%)
   - Limitations due to the tools they have available (33%)
   - Executives' resistance to change (32%)

3. The majority (76%) of respondents said their company has a hybrid environment.

4. 97% of security leaders reported that their company involves external entities like contractors, partners, or suppliers who have access to their various systems, applications, and resources.

5. 81% of respondents expressed concern about non-human identities and the risk they pose to their company, with 38% stating they are very concerned.

6. When asked what they perceive to be the biggest pressure they face in their role, 24% of security leaders cited keeping up with the rapid pace of technological change and new attack vectors.

7. Almost half (47%) of respondents said that their company's identity security strategy and access policies hinder team productivity.

8. Nearly three in four respondents (73%) said they frequently or very frequently negotiate higher security budgets due to increasing security risks and responsibilities.

9. 93% of respondents said they believe zero standing privileges is effective at reducing access risks within their organization, with 52% believing it to be highly effective.

10. Respondents' top priorities for access management include
    - Reducing risk (55%)
    - Improving team productivity (50%)
    - Automating processes (47%)
    - Improving user experience (46%)

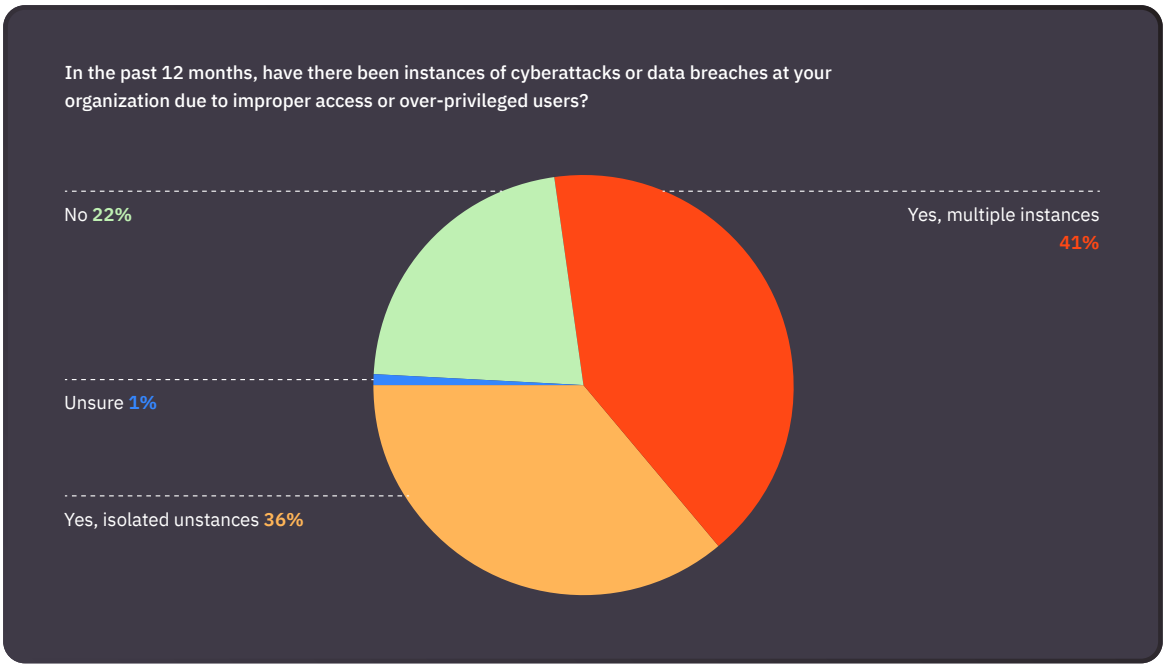
Security Leaders Face Mounting Identity Threats

The threat landscape has evolved significantly over the past decade. To counter rising threats, many companies have turned to zero trust as a guiding principle of defense. Based on the concept of "never trust, always verify," businesses have gone to great lengths to ensure that nothing inside or outside of their environment is trusted by default.

Because zero trust has worked so well, it's become much more difficult for attackers to gain access to companies' systems via traditional methods. In response, attackers are increasingly shifting their tactics toward identity-based attacks. Now, instead of "breaking in," attackers are "logging in" to gain access to sensitive systems and data.

Improper Access Is Resulting in a High Percentage of Cyberattacks and Breaches

Of the security leaders surveyed for this report, 77% said their organization has suffered from instances of cyberattacks or data breaches in the past 12 months due to improper access or overprivileged users.



Furthermore, 41% of respondents said there had been *multiple instances* of cyberattacks or data breaches due to the same improper access issues.

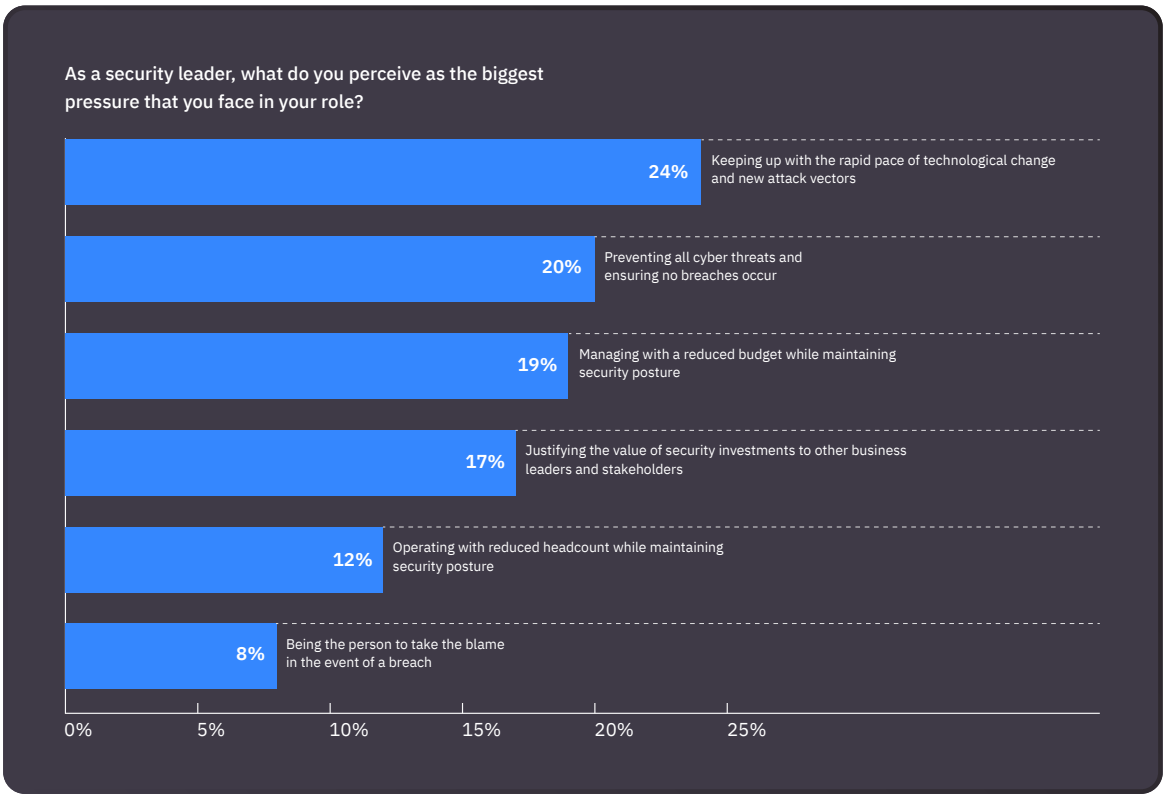
Smaller businesses seem to be feeling the pain more acutely — 85% of respondents at companies of 250-500 employees said they had experienced a breach or attack in the last 12 months.

Adversarial Advancement Cited as a Top Pressure

With identity-based attacks on the rise, security leaders are facing significant pressure to keep their businesses safe and stay one step ahead of attackers.

When asked what they perceive to be the biggest pressure they face in their role, 24% cited keeping up with the rapid pace of technological change and new attack vectors.

This was followed by preventing all cyber threats and ensuring no breaches occur (20%), managing with a reduced budget while maintaining security posture (19%), and justifying the value of security investments to other business leaders and stakeholders (17%).



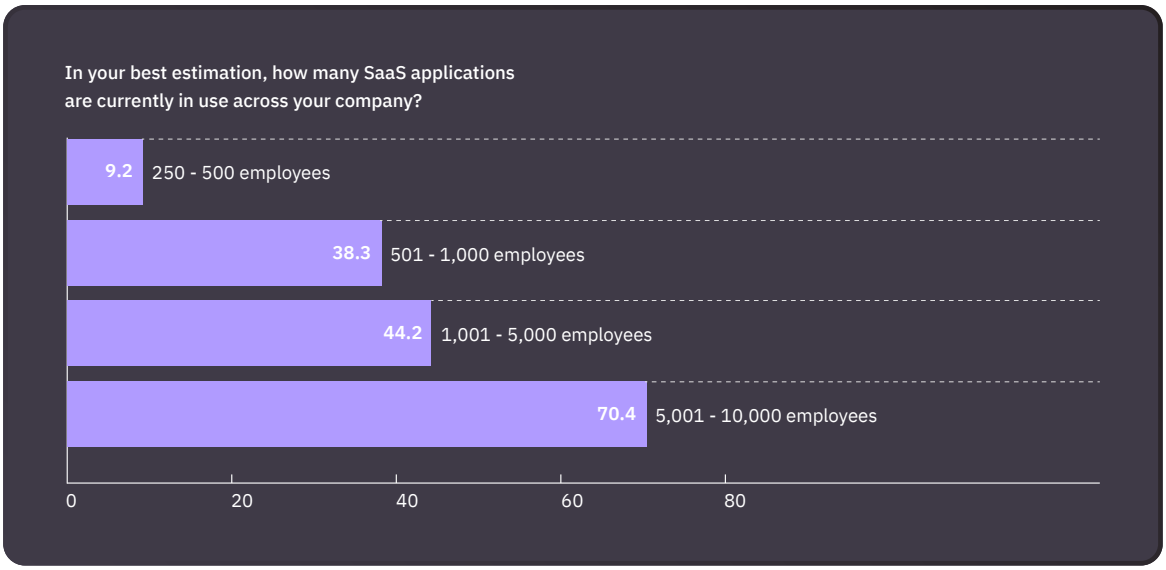
Complex Environments Lead to Identity Risks

It's clear that businesses need to find ways to reduce their identity and access attack surface. However, the complexity of modern technology environments has made identity security and access management an overwhelming challenge.

SaaS Sprawl

As SaaS becomes more pervasive, it creates new layers of complexity for IT and security departments. To better understand the issue, the *Identity Security Outlook Report* asked respondents how many SaaS apps were in use across their company. On average, security leaders estimated 39.5 apps in use.

As anticipated, the results show that the larger the organization, the more SaaS applications were reportedly in use. Smaller companies with 250-500 employees had 9.2 SaaS apps in use, whereas larger companies with 5,001-10,000 employees had an average of 70.4 apps.



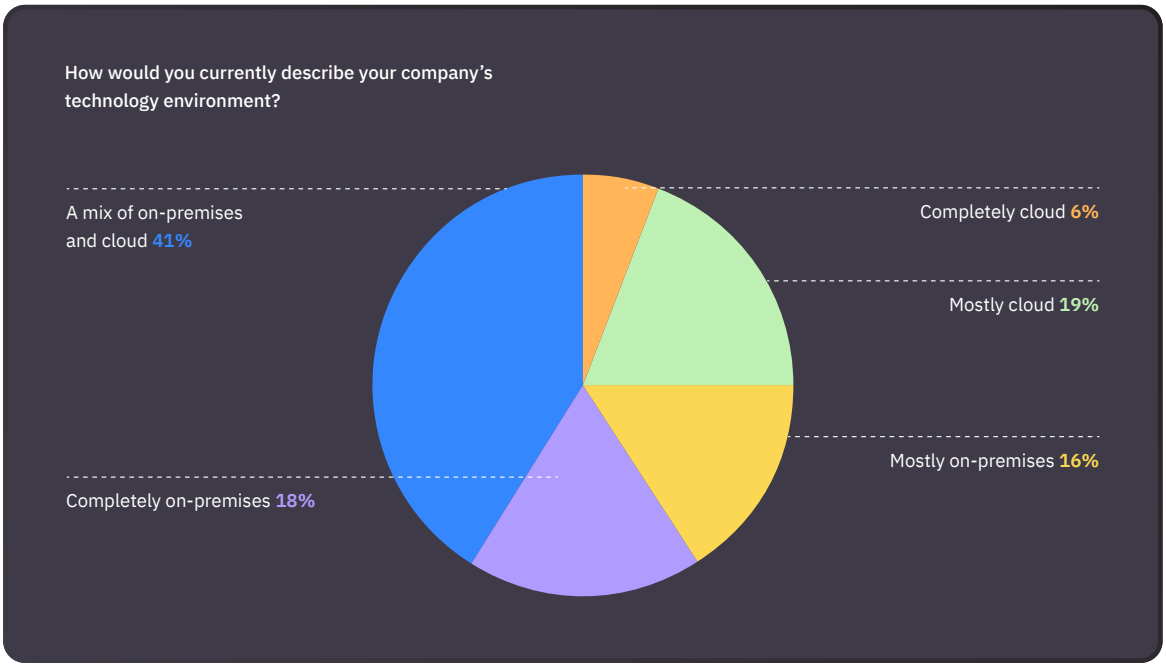
While this correlation between company size and number of SaaS apps was expected, the volume of reported SaaS apps was surprisingly low. For example, according to Statista, the average company used 130 SaaS apps as of 2022.

The low reported volume of SaaS in the *Identity Security Outlook Report* could indicate that some organization's apps are not under the purview of the security team, highlighting the growing threat vector of shadow or rogue SaaS applications not sanctioned or managed by the security team.

Hybrid IT

Cloud migration is well underway for most organizations today, yet many still operate with some on-premises systems. The majority (76%) of survey respondents indicated that their company currently has a hybrid environment.

The survey results demonstrate that hybrid IT is the new normal. Only a small percentage of respondents (6%) said their environment is completely in the cloud, and only 18% stated that their company's technology environment is completely on premises.



Interestingly, of the respondents who experienced multiple instances of cyberattacks or breaches due to improper access or overprivileged users in the past 12 months, 55% said their company's technology environment was mostly or completely on-premises. This percentage is notably higher compared to the 35% of respondents from the broader survey who reported the same.

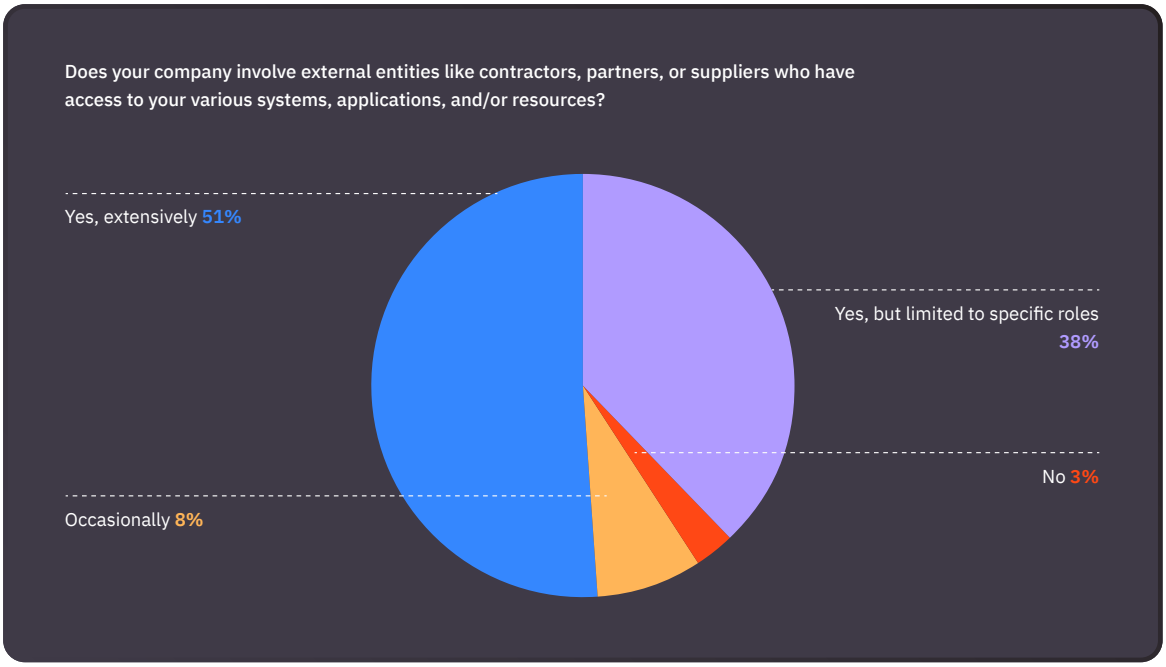
Extended Enterprise

The concept of the extended enterprise continues to gain traction, as the vast majority of companies now bring data, users, and systems from third-party organizations into their own environments.

Granting third-party users access to internal systems can be important for collaboration and productivity, but it can also put sensitive data and systems in jeopardy. Because a business cannot control an external entity's own security protocols or tools, this practice may open the business up to increased risk.

Nearly all security leaders (97%) reported that their company works with external entities like contractors, partners, or suppliers who have access to their various systems, applications, and/or resources.

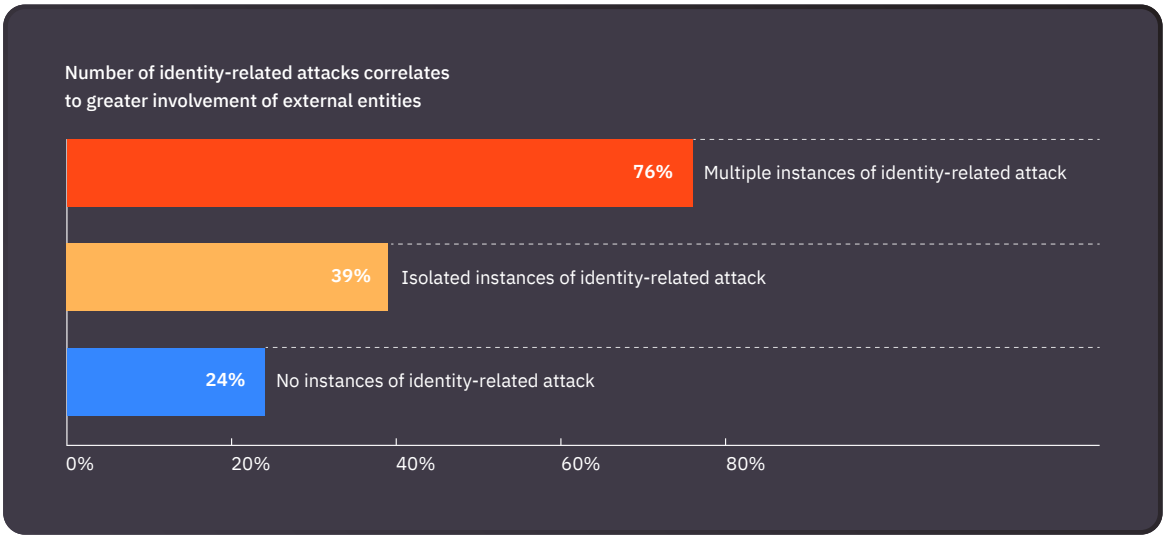
More than half (51%) of respondents said their company *extensively* involves external entities, while 38% say these contractors, partners or suppliers are limited to specific roles.



The study also found a correlation between the number of cyberattacks due to improper access in the last year and the extensive involvement of external entities.

For example, of the respondents who experienced multiple instances of cyberattacks or breaches due to improper access or overprivileged users in the past year, 76% said their company extensively involves external entities. Of those who only experienced isolated attacks, that number decreased to 39%.

Of the respondents who did *not* experience any breach or attack, only 24% said their company extensively involves external entities. This indicates that the involvement of external entities could result in greater risk for the organization.

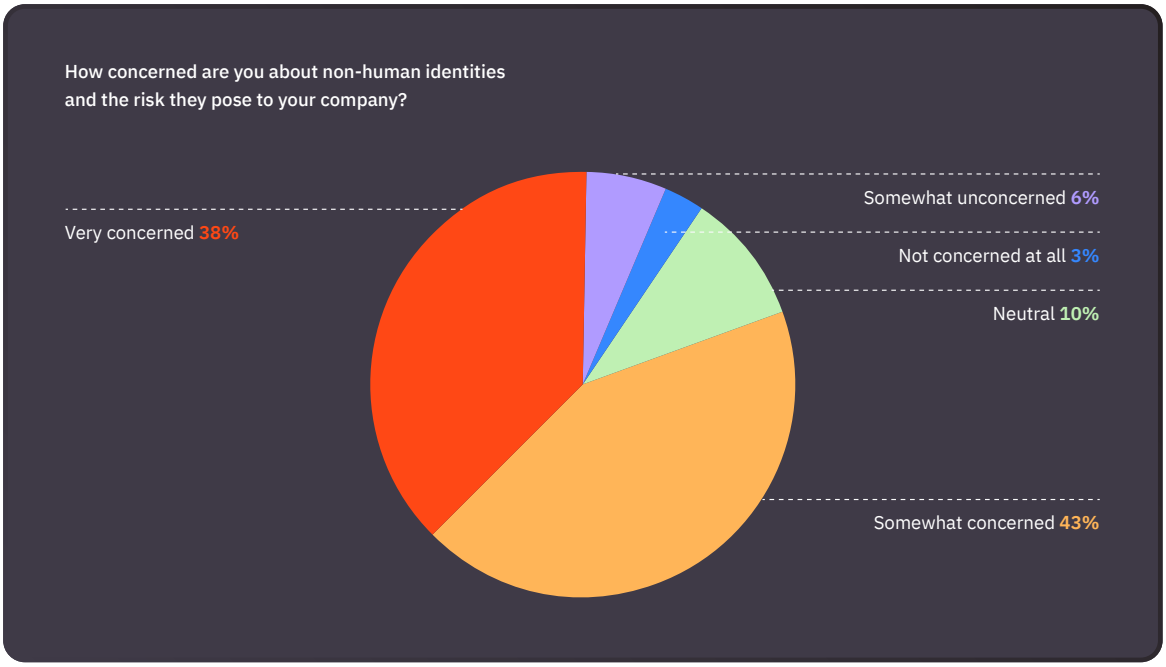


Non-Human Identities

Also known as machine identities, non-human identities such as service accounts, API tokens, OAuth tokens, and more are becoming a significant challenge for security teams. Just like human users, these non-human identities can have privileged access to an organization's system and data.

Therefore, it's no wonder that the majority (81%) of respondents stated they are concerned about non-human identities and the risk they pose to their company, with 38% stating they are very concerned.

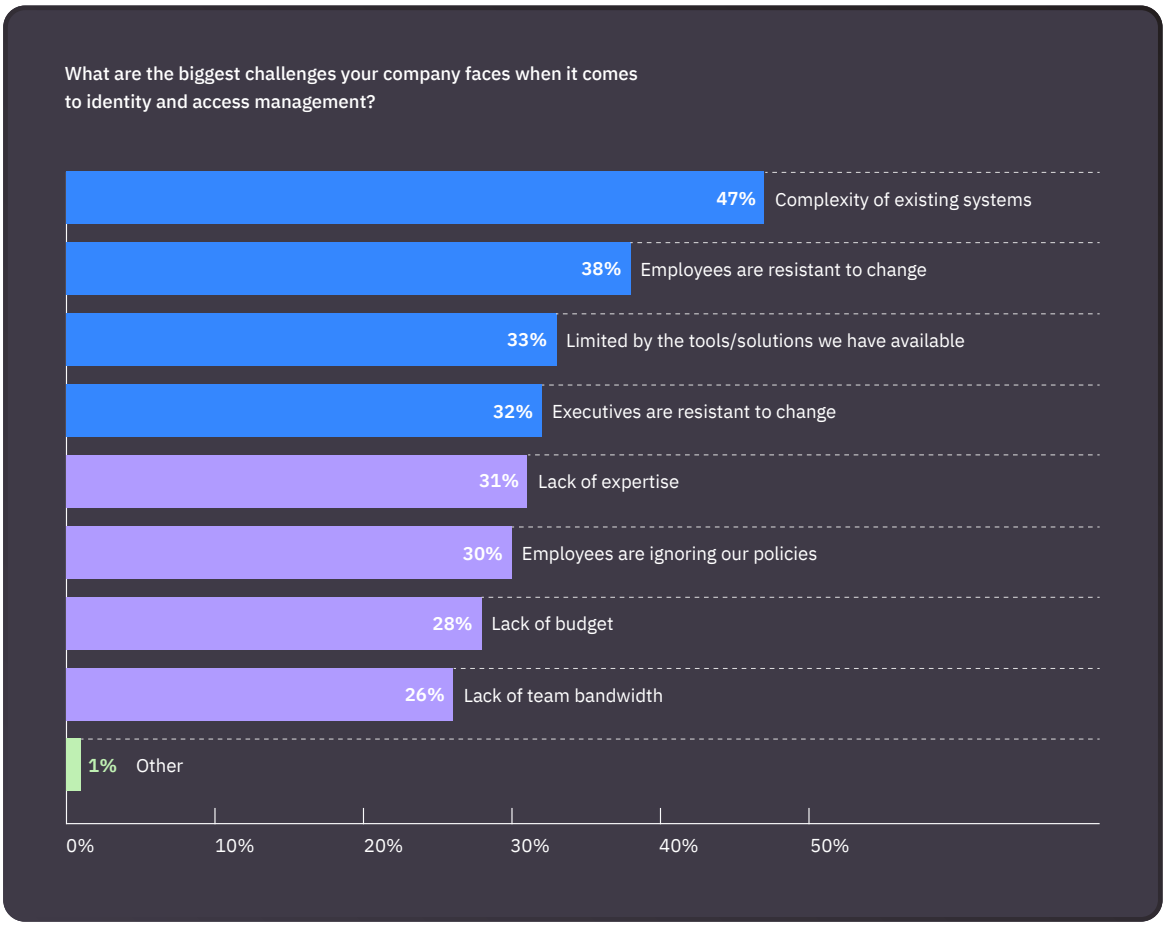
The number of "very concerned" respondents increased to 56% across those who had experienced multiple instances of cyberattacks due to improper access in the past year.



Top Identity and Access Management Challenges

Given the high degree of complexity associated with SaaS, hybrid IT, the extended enterprise, and non-human identities, it's no surprise that "complexity of existing systems" was cited as the top identity and access management challenge by 47% of survey respondents.

This was followed by employees' resistance to change (38%), limitations due to the tools or solutions available (33%), and executives' resistance to change (32%). Other challenges include lack of expertise (31%), employees ignoring policies (30%), lack of budget (28%), and lack of team bandwidth (26%).



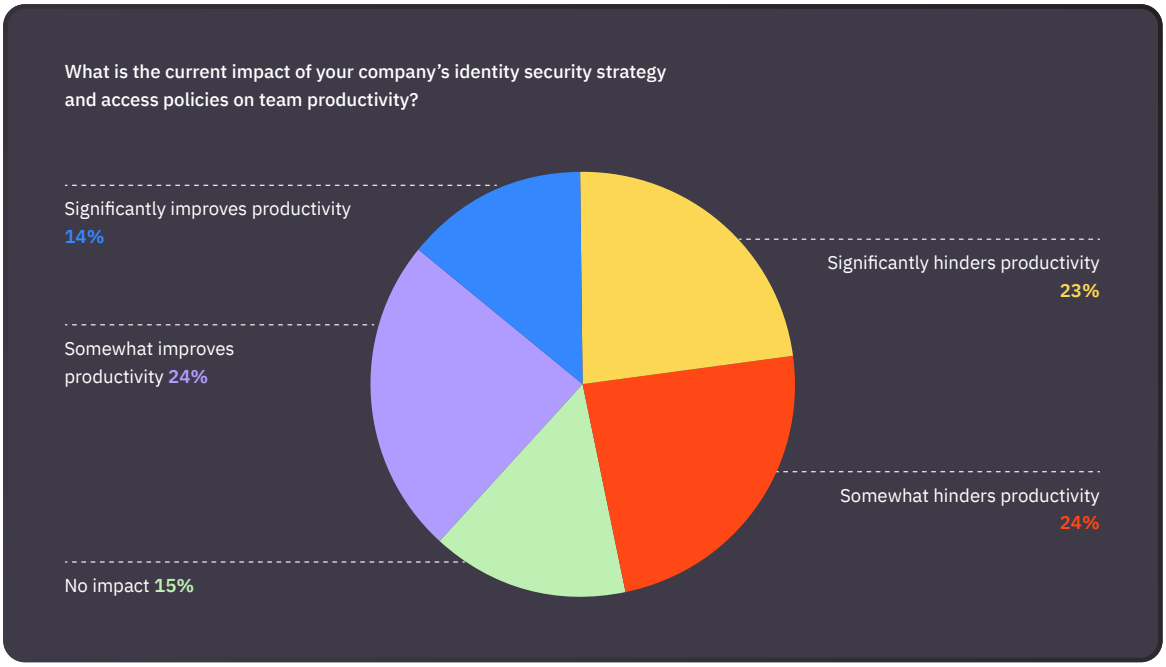
Complexity of existing systems was cited as the top challenge across all company sizes. However, this was not the case among respondents who experienced multiple instances of cyberattacks or breaches due to improper access or overprivileged users in the past 12 months. For this group, executives' resistance to change (46%) and employees' resistance to change (42%) were cited as the top challenges.

Impact of Identity Security Strategies on Team Productivity

In years past, identity and access management safeguards have been notoriously viewed as a hindrance to team productivity. Employees have long begrudged additional layers of passwords, multifactor authentication, and other access protocols as hoops they must jump through to access their company's critical systems.

While many identity and access management tools have vastly improved the employee experience, some organizations are still stuck in the age-old battle between security and productivity.

This is evidenced by the nearly half (47%) of survey respondents who reported that their company's identity security strategy and access policies hinder team productivity, with 23% citing a *significant hindrance* on productivity. Smaller organizations (250-500 employees) were more likely to state that their policies significantly hinder productivity, at 42%.



Respondents who did *not* experience any instances of breach or attack due to improper access were far less likely to cite a significant hindrance on productivity, at only 4%. This could indicate that organizations whose identity security strategies prioritize a seamless user experience may be more likely to achieve employee compliance with internal policies, thus reducing their overall risk.

Encouragingly, 38% of respondents said their current identity security strategies and access policies have actually *improved* team productivity.

Current Processes to Manage Risk

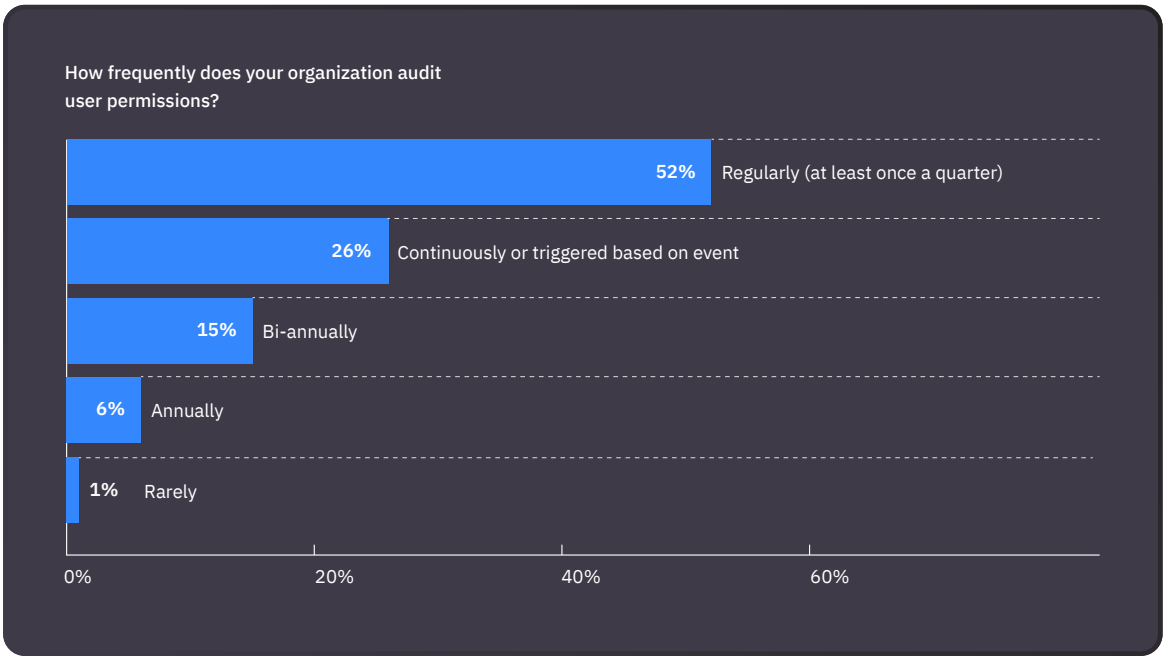
With a wide range of identity and access management challenges to contend with, security leaders must take steps to reduce risk and stay ahead of attacks without introducing friction into the business — all while staying on budget.

Auditing User Access

Auditing user access and permissions is a critical step for organizations to maintain compliance, reduce standing privileges, and improve security.

Nearly all (95%) of respondents responded they are confident in their company's ability to audit identities and access rights across all systems. Larger companies (5,001-10,000 employees) were somewhat less confident than their smaller-size counterparts, at 89%.

More than half (52%) of respondents said their organization audits user permissions regularly — at least once a quarter — with another 26% stating their user permissions audits are either continuous or triggered based on events.

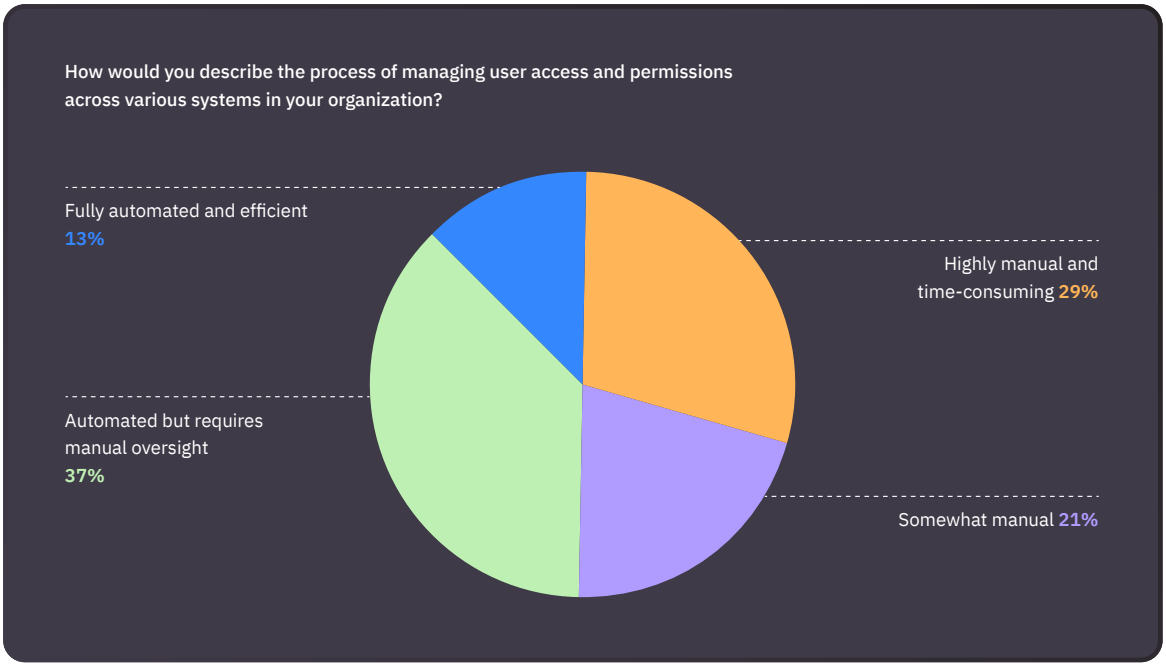


Managing User Access and Permissions

Granting and revoking user access can be a tedious process, especially as the number of systems and users grows along with the business.

When asked who manages permissions for their company's systems, applications, and resources, 46% stated a central IT department, 15% said individual departmental admins, and 38% said permissions are managed by a mix of both IT and department admins.

When it comes to automated vs. manual processes for managing user access and permissions, respondents are evenly split: 50% described their process as manual, while the other 50% described their process as automated. However, 29% of respondents described their process as highly manual and time-consuming, compared to only 13% who stated their process was fully automated and efficient.



Of the respondents who experienced multiple instances of cyberattacks or breaches due to improper access or overprivileged users in the past 12 months, almost half (49%) stated their process was highly manual and time consuming. This could indicate that manual processes might introduce error or inaccuracy, leading to greater risk.

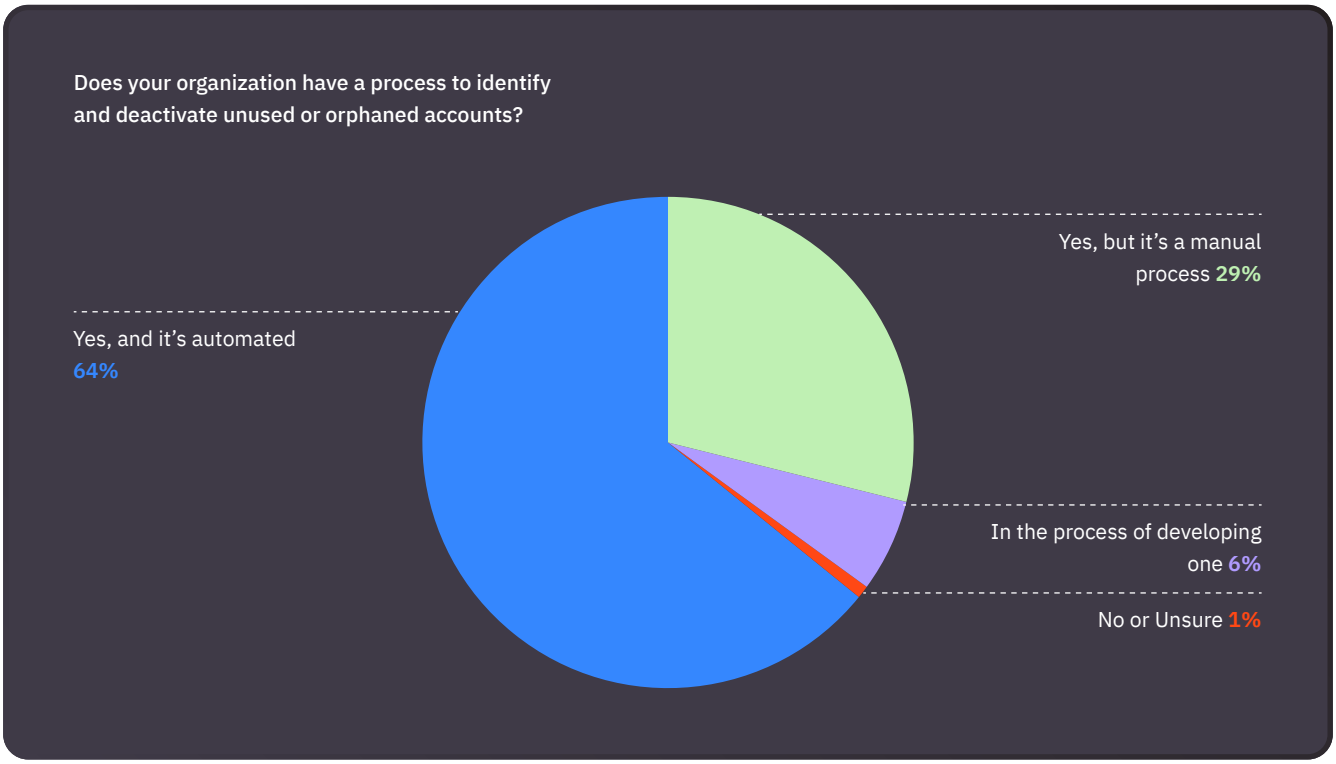
Among the respondents who said their process is automated, 75% stated their process still requires manual oversight. This could point toward the trend of human-in-the-loop (HITL) automation, in which humans are involved in automation workflows at key decision-making points to ensure accuracy. However, this could also indicate that the automation in use among these respondents is not sophisticated and still requires significant human intervention.

Identifying Privileged Users and Orphaned Accounts

Overprivileged users, orphaned accounts, and unused accounts represent a growing security risk that must be managed. Overprivileged users have more access rights than necessary for their roles, whereas orphaned accounts are those that are not deactivated when an employee leaves the organization. Unused accounts include permissions held by users who either aren't using them or no longer need access to certain systems. In these scenarios, the accounts can become easy targets for attack.

More than half (61%) of respondents reported that their company has a strictly enforced policy to manage and restrict overprivileged users. However, 32% said that enforcement of their policy is inconsistent, while 7% say they either don't have a policy in place or their policy is still under development.

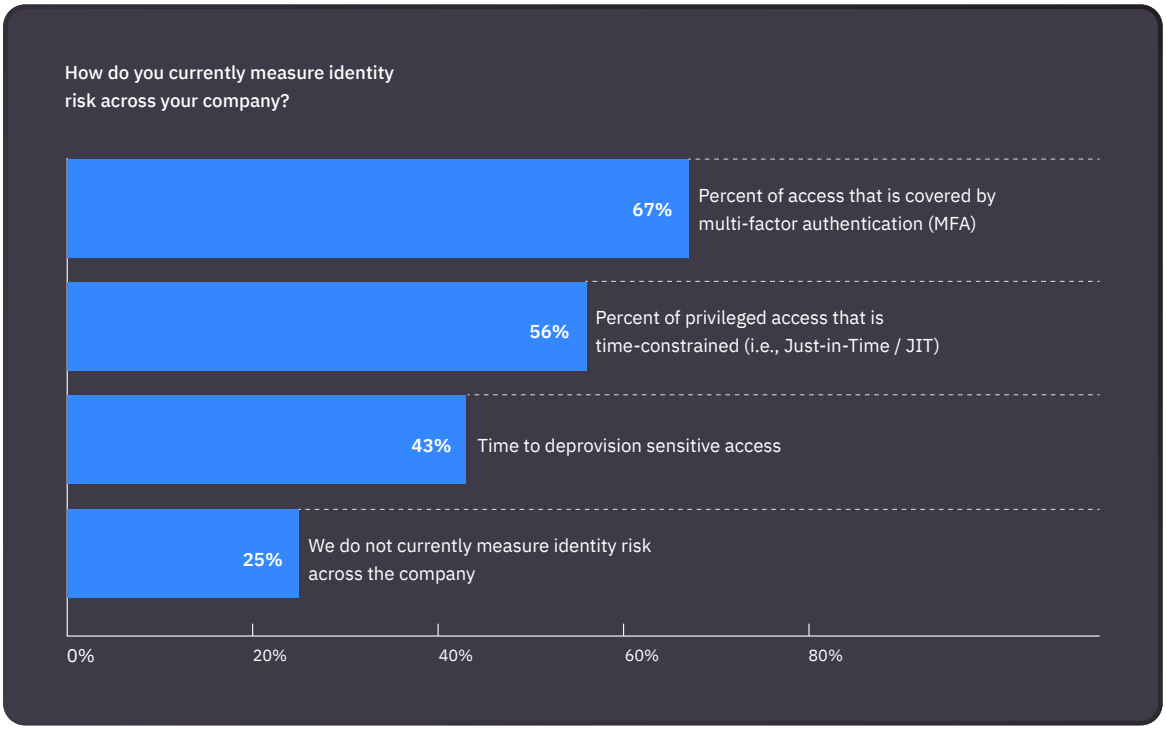
When asked about their process to identify and deactivate unused or orphaned accounts, 64% of respondents said they have an automated process in place. 29% of respondents said their process is still manual, while 6% either don't have a process or are still developing one.



Measuring Identity Risk

Despite advances in technology and processes, measuring identity risk still remains a challenge for many organizations today. In fact, one in four respondents (25%) stated they are not currently measuring identity risk across their company.

The top metrics currently used to measure company-wide identity risk include the percent of access that is covered by multifactor authentication (67%), percent of privileged access that is time-constrained or just-in-time access (56%), and time to deprovision sensitive access (43%).

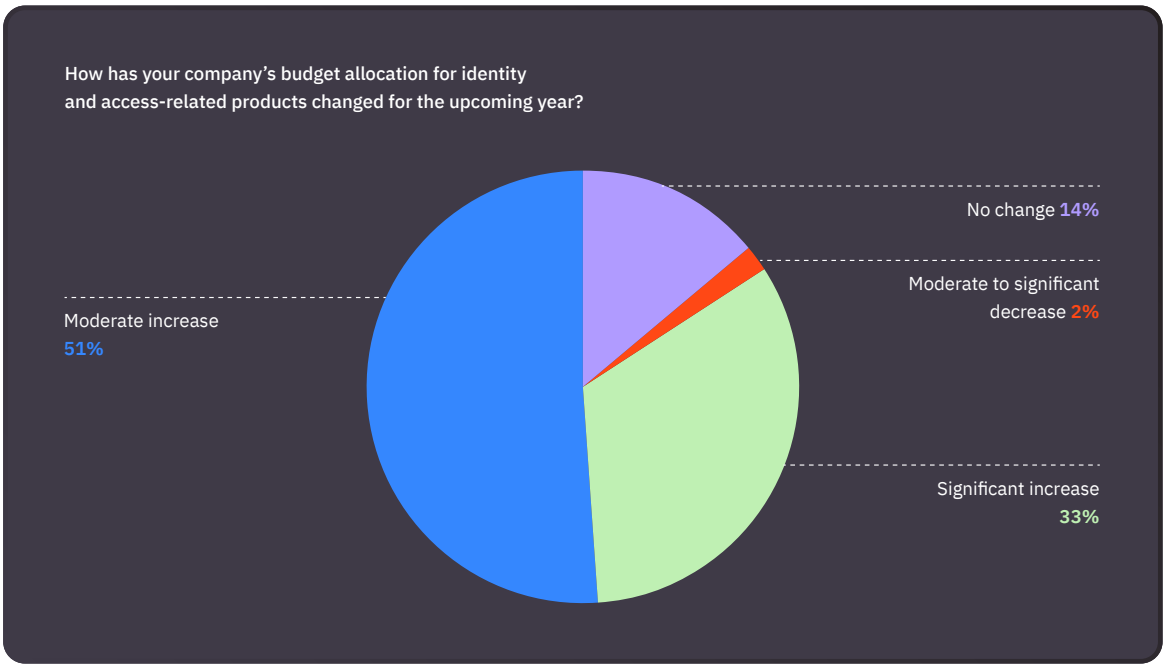


Of the respondents who experienced multiple instances of cyberattacks or breaches due to improper access or overprivileged users in the past 12 months, 36% do not currently measure identity risk.

Budgets Increase to Meet Identity and Access Needs

Amid the reality of economic uncertainty, there's been an open question about how security budgets could be impacted. However, smart organizations understand that security is one area that cannot be trimmed or scaled back. In today's environment, the reputation and viability of a business is predicated upon its ability to maintain operations and keep sensitive information safe.

With this in mind, it's encouraging to see that the majority (84%) of survey respondents reported either a moderate or significant increase in their company's budget allocation for identity and access-related products this year.



Smaller organizations with 250-500 employees were more likely to see a significant increase (50%; compared to the broader survey group at 33%), whereas larger organizations with 5,001-10,000 employees were more likely to see no change (27%; compared to the broader survey group at 14%).

Respondents who experienced multiple instances of attacks or breaches due to improper access were far more likely to see an increase in budget allocation for the upcoming year (92%) compared to those who did not experience any instances of attacks or breaches (69%).

Nearly all respondents (95%) said their budget allocations for identity and access-related products are adequate; however, only 38% said their budget allocations are *completely* adequate.

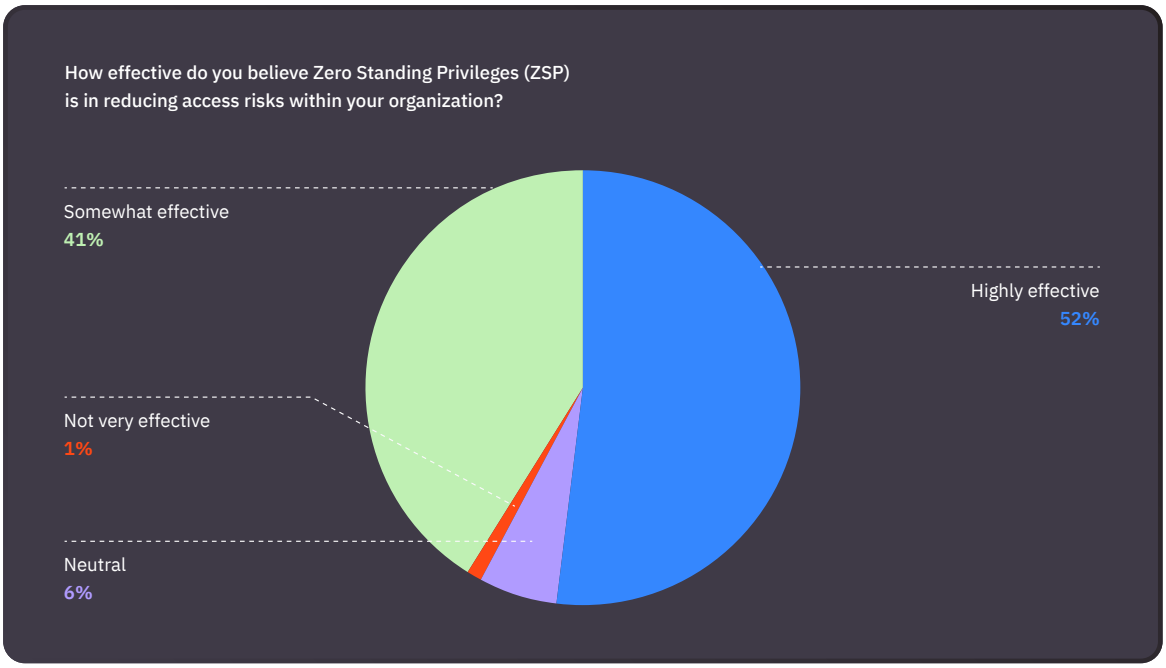
Despite increasing budgets and respondents self-reporting that their allocations are adequate, 73% of respondents still find themselves *frequently or very frequently* negotiating higher security budgets due to increasing security risks and responsibilities.

Zero Standing Privileges Holds Promise to Reduce Risk

The concept of zero standing privileges (ZSP) is gaining traction among security leaders as a means of improving identity security and reducing risk.

In an enterprise with ZSP in place, a user is only granted the minimum levels of access and privilege needed to complete a task, and only for a limited amount of time. This means that should an attacker gain entry to a user's account, there is far less potential for them to access sensitive data and systems.

According to the *Identity Security Outlook Report*, 93% of security leaders stated they believe ZSP is effective at reducing access risks within their organization, with 52% saying it's *highly effective*.

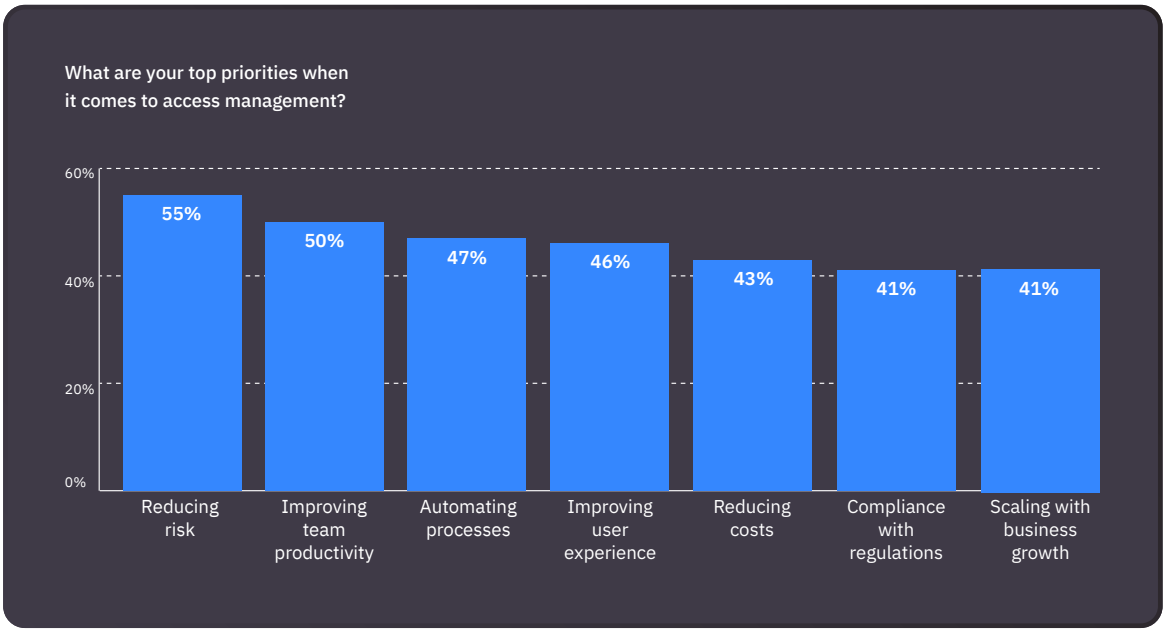


Furthermore, the vast majority of respondents (91%) reported that ZSP is currently being enforced across at least some of their company's systems. Only 8% of respondents are not yet enforcing ZSP at all.

Top Identity and Access Management Priorities

As security leaders face greater complexity across their organizations' systems and escalating attacks from adversaries, it's no surprise that risk reduction was cited as respondents' top priority for identity and access management (55%).

This was followed by improving team productivity (50%), automating processes (47%), and improving user experience (46%). Additional priorities include reducing costs (43%), compliance with regulations (41%), and scaling with business growth (41%).



Interestingly, improving user experience was cited as the top priority among respondents who experienced multiple instances of attacks or breaches due to improper access in the last year. This group also identified their top identity challenges to be executive and employee resistance to change, which may indicate that greater friction within the organization may be leading to an increased risk factor.

Conclusion

The results of the *2024 Identity Security Outlook Report* send a clear message: identity is messy. That's because identity uniquely sits at the intersection of human behavior, technology, legal frameworks, and cybercriminal activity. As technology systems become increasingly complex, heterogeneous, and interconnected, the "messiness" of identity only becomes more apparent.

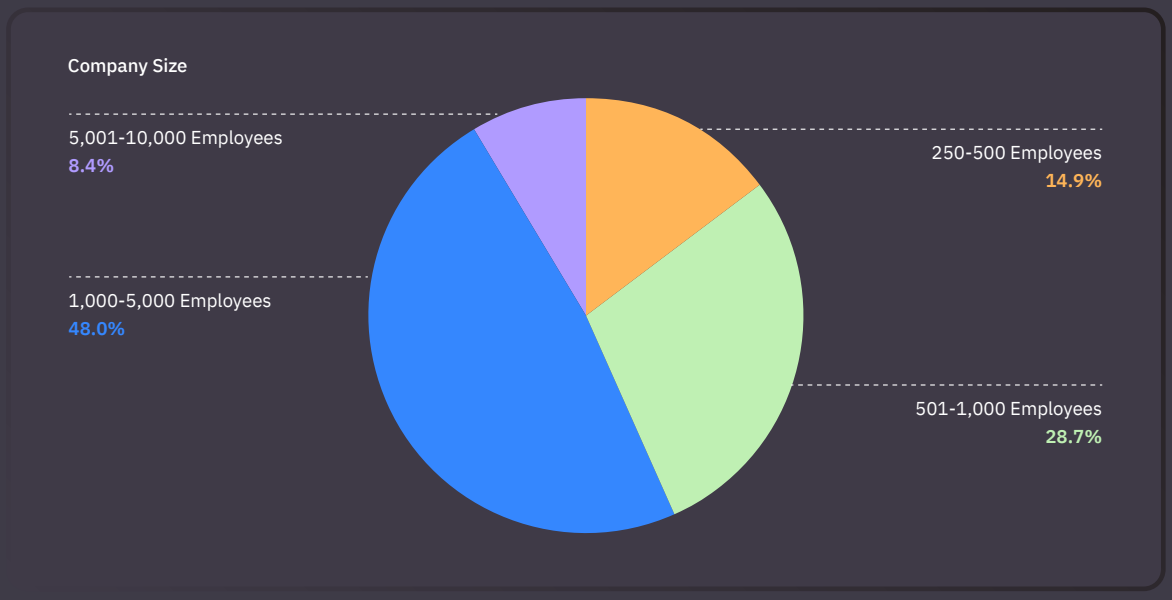
Poor identity and access practices can hinder team productivity and result in a negative employee experience. More importantly, however, identity has now become a prime target for attackers. With more than three-fourths of security leaders citing an identity-related breach or attack in the last year alone, we're now squarely in a new world order, one in which identity and access must be viewed and managed as a high-priority security risk.

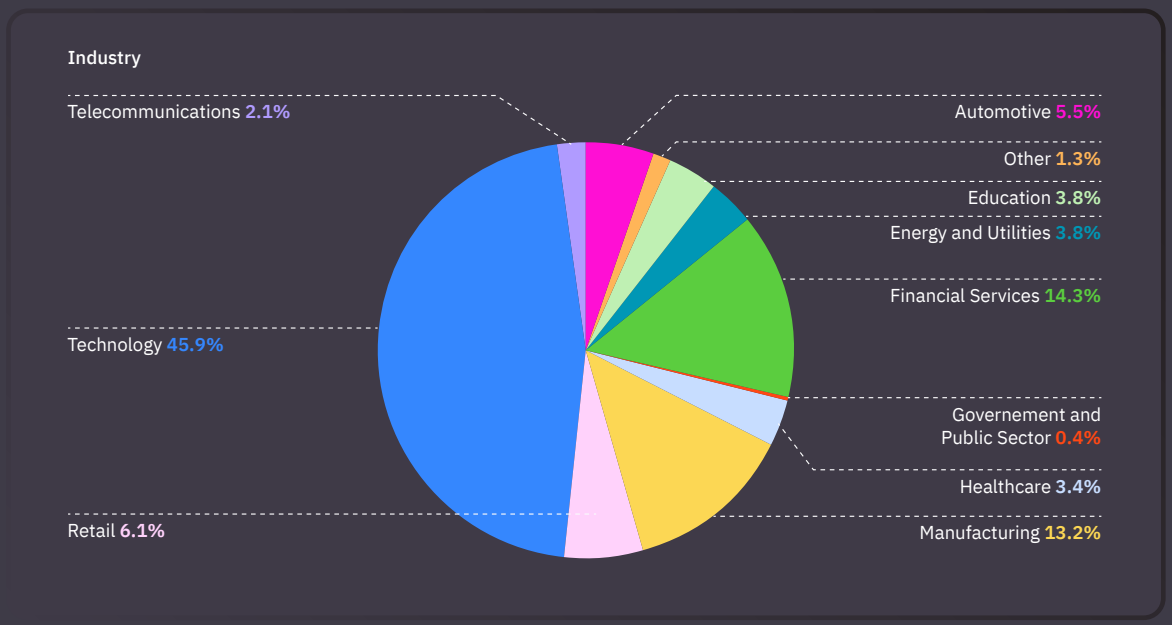
Fortunately, there are several glimmers of hope. First, many security leaders are leaning into automation to ease the burden on their teams and improve efficiency. The majority are also benefiting from increased budget allocations for identity security, with most citing their new budgets as adequate. Finally, most security leaders recognize just how effective zero standing privileges can be for reducing risk.

In the days ahead, security leaders will continue to prioritize risk reduction while also making efforts to boost team productivity, automate processes, and improve the user experience. With a more holistic, security-minded approach, businesses can finally bring identity chaos to order.

Demographics and Methodology

Demographics





Methodology

The *2024 Identity Security Outlook Report* findings are based on the results of an online survey conducted in February 2024 that examined the opinions of 523 US-based IT professionals, director level and higher at companies of 250 to 10,000 employees, whose roles involve information security.

ConductorOne

2024 Identity Security Outlook Report

ConductorOne

About ConductorOne

ConductorOne helps organizations secure their workforce identities through modern access controls and governance. Security and IT teams use ConductorOne to unify access visibility, move to just-in-time (JIT) access, remove inappropriate access, and automate access reviews. Modern enterprises like DigitalOcean, Ramp, Instacart, Panther, and DeepWatch trust ConductorOne to achieve zero standing privileges and ensure compliance.

For more information, please visit: www.conductorone.com