



IDENTITY DEFINED
SECURITY ALLIANCE



dimensional
research

2024

Trends in Identity Security

A Survey of IT Security and Identity Professionals

Table of Contents

- 03** Introduction
- 04** The State of Identity and Security in 2024
- 07** Ongoing Challenges of Identity Security
- 09** How 2024 Trends Are Impacting Identity
- 11** Security Outcomes Remain A Work In Progress
- 14** Prioritize Securing Identities With IDSA
- 15** Goals & Methodology

Introduction

Our job of protecting digital identities continues to grow in complexity and scope as the number of identity-related incidents rises in every category. With issues like identity sprawl, and system complexity, CISOs and organizations at large need to find effective ways to protect the identity information of their employees, vendors, partners, and customers.

To explore the current state of cybersecurity, we commissioned a study with Dimensional Research to understand the approaches large companies are taking toward security and identity. The study invited independent security and identity professionals across the United States, who were asked questions focused on their current plans, identity and security history, and more. 521 qualified individuals completed the survey. All had deep knowledge of IT security and identity from an organization with over 1,000 employees.

The research finds that as the number of identities increases (identity sprawl), more businesses are suffering identity-related incidents and are identifying securing them as a top priority. We continue to see that securing these identities remains a significant challenge, and security outcomes remain a large work in progress.

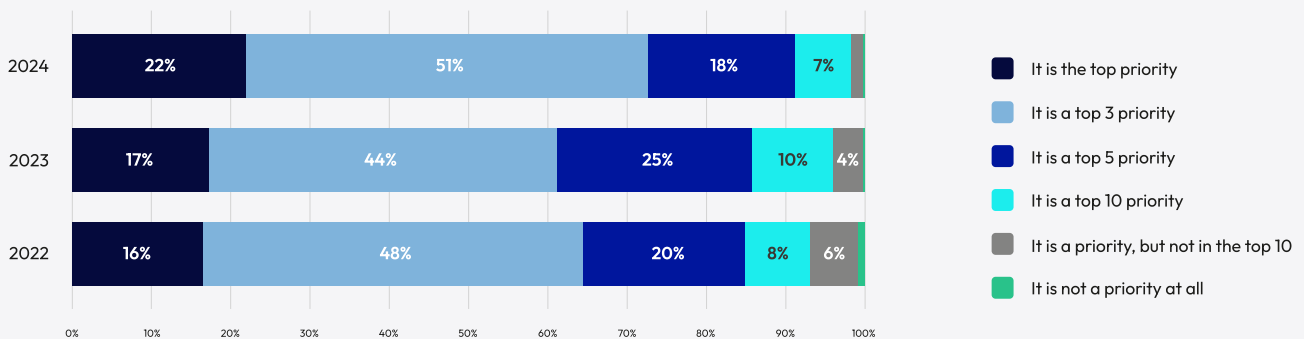
Let's start by exploring the state of identity and security and then dig into some security challenges and necessary outcomes.



The State of Identity and Security in 2024

Our research found that 22% of businesses see managing and securing digital identities as the number one priority of their security program, up from 17% in 2023. More than half of respondents (51%) said they now see it as a top three priority, and another 18% see security digital identity as a top five priority. Only 2% of businesses don't see securing identities as a top 10 priority. This trend of increasing priority is a positive sign of the recognition of the importance of identity.

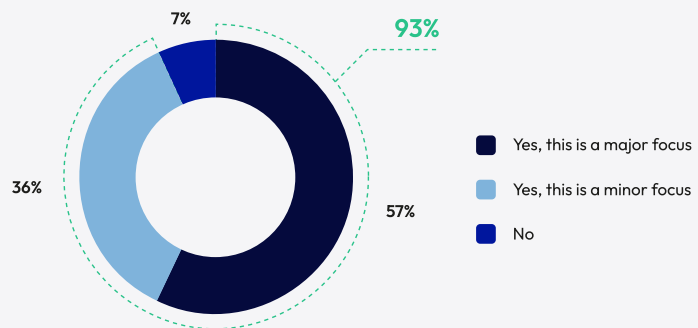
How would you characterize the importance of effectively managing and securing digital identities within your company's security program? Choose the one answer that most closely applies.



The increased focus on security digital identities is not surprising given the emergence of identity sprawl. Over half (57%) of the respondents consider managing identity sprawl a major focus.

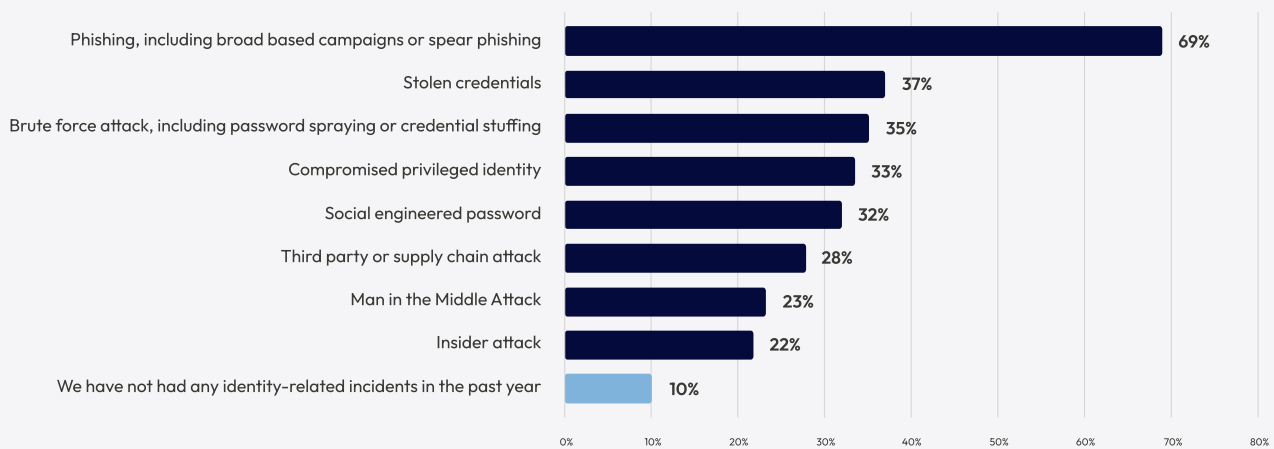
This increase in digital identities comes with the cost of increases in cyber-attacks targeting them.

Is your company taking any steps to manage identity sprawl?
(i.e. minimizing the number of identities for each employee or customer)



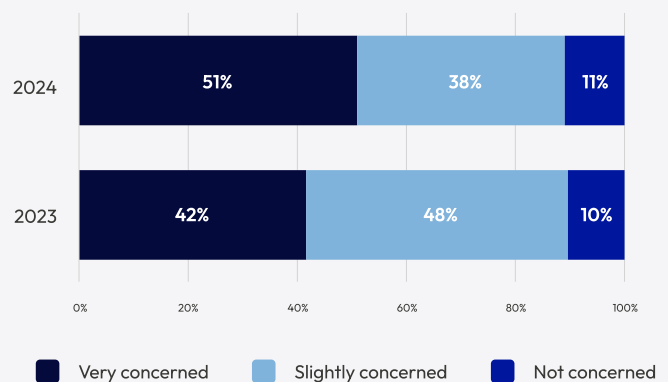
The most significant reason behind this increase was phishing at 69%, up from 62% in 2023. Coming in at a distant second was stolen credentials, also increased from 2023. As indicated in the chart below, a large variety of attacks accounted for around one-quarter to one-third of incidents experienced.

What kind of identity-related incidents has your company had in the past year?
Choose all that apply.



Employee behavior continues to affect identity-related incidents. Most organizations are concerned about employees using corporate credentials for social media.

How concerned are you about the risk of employees using corporate credentials (i.e. Office365) for social media accounts (i.e. Facebook)?

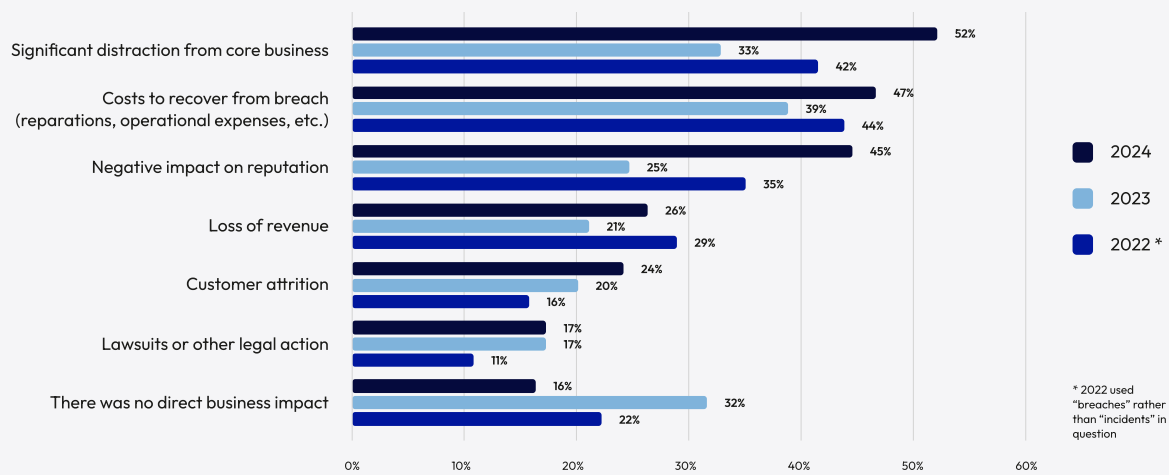


84% of identity stakeholders said incidents directly impacted their business. This is a notable increase from 68% in 2023. The most significant impact, seeing a measurable rise this year, was distracting from core business (52%), followed by the cost of recovering from the breach.

This dropped from number one last year yet increased from 33% to 47%. Close behind and keeping third place is the negative impact on the company’s reputation with a whopping increase from 25% to 45%. We should not ignore the creeping increase in customer attrition from identity-related incidents, up to 24%.

What direct impact to business results did your company have as a result of identity-related incidents in the past year? Choose all that apply.

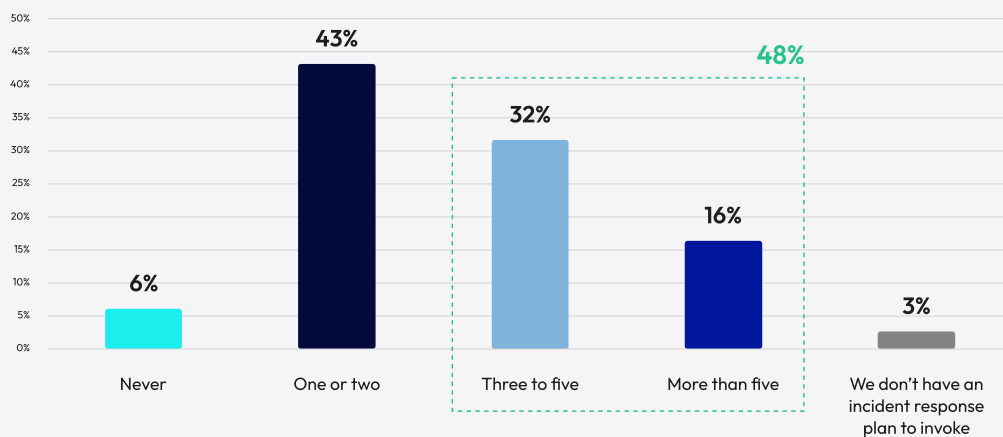
n = have had an identity related incident in the past year



The surprising increase in the number of times an organization invoked its incident response plans tells us that the number almost doubled this year to 91%. 48% invoked their plans more than once and 3% remained without any plan.

How many times did your company invoke incident response plans for an identity-related incident in the past year?

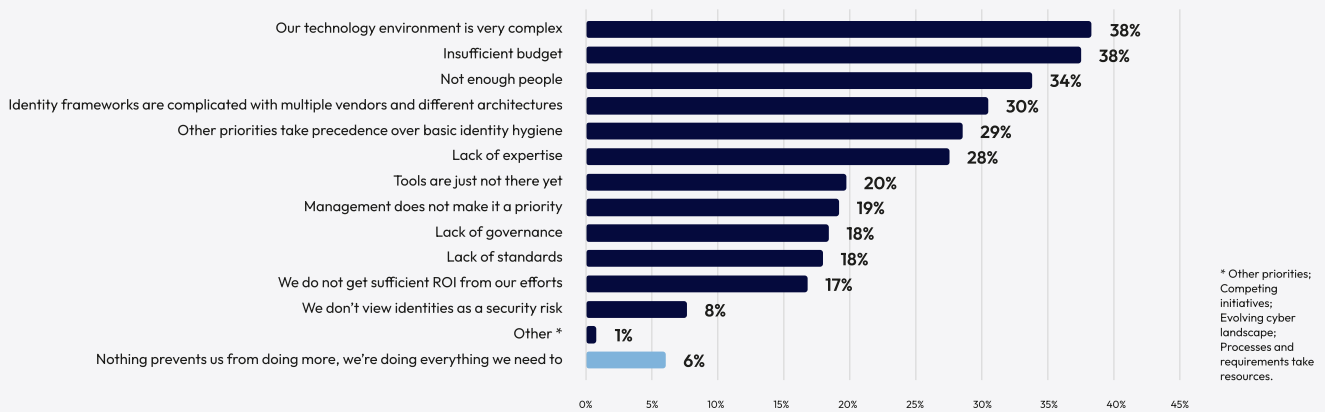
n = have had an identity related incident in the past year



Ongoing Challenges of Identity Security

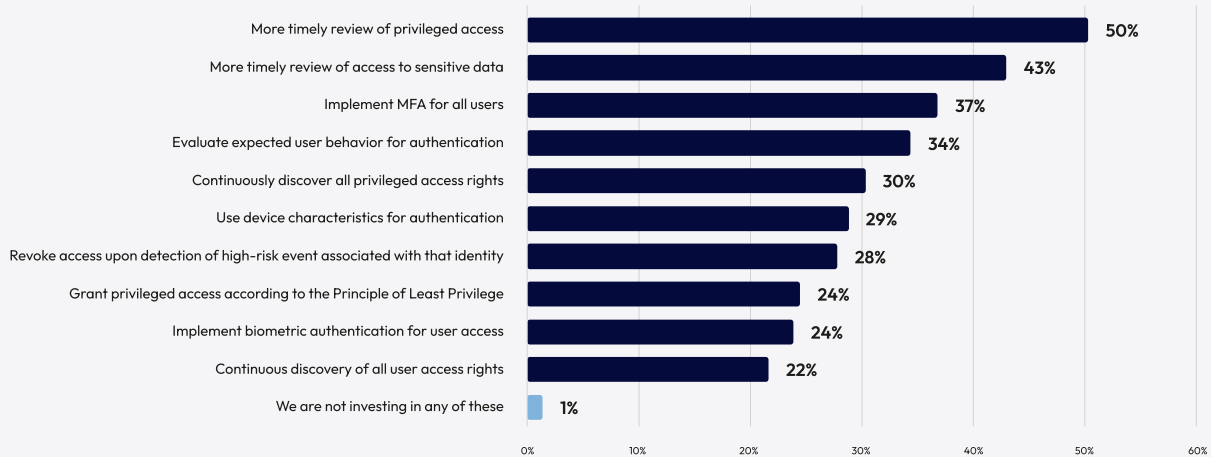
Our research found that one of the biggest challenges for security teams was the sheer number of barriers they now face. This year, the top two reasons at 38% were complex technology environments and insufficient budget (up from 30%). Respondents also identified people at 34%, up from 25% last year.

What barriers prevent your company from doing more to secure identities?
Choose all that apply.



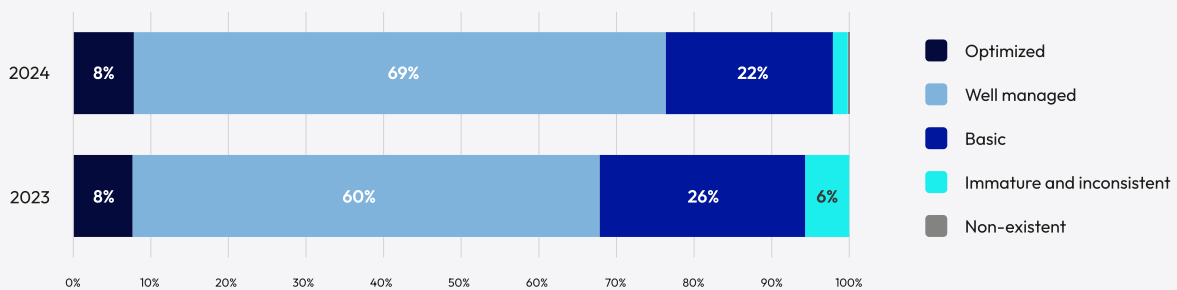
Tied to the 34% of respondents that indicate “not enough people,” the top two planned investments focus on more timely access reviews. Implementation of MFA comes in next. Looking at user behavior and device characteristics provides the opportunity for innovation, while many of the other planned investments form the foundation for zero trust, whether or not that is the plan.

Which of the following is your company investing the MOST in over the coming year?
Choose up to three of the following.



An increased majority of identity stakeholders (69%) said their company’s security identity capabilities were well managed, and 8% continue to say they were optimal. Less than one quarter (22%) only believe their company has basic security identity capabilities.

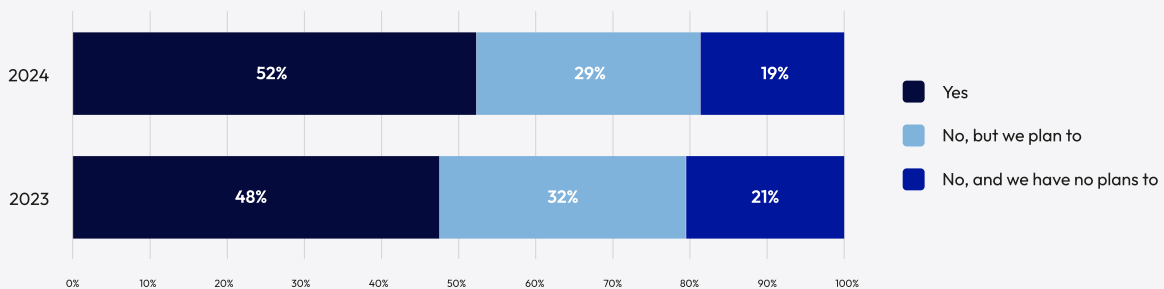
How would you characterize your company’s capabilities for securing identities?
Choose the one answer that most closely applies.



How 2024 Trends Are Impacting Identity Security

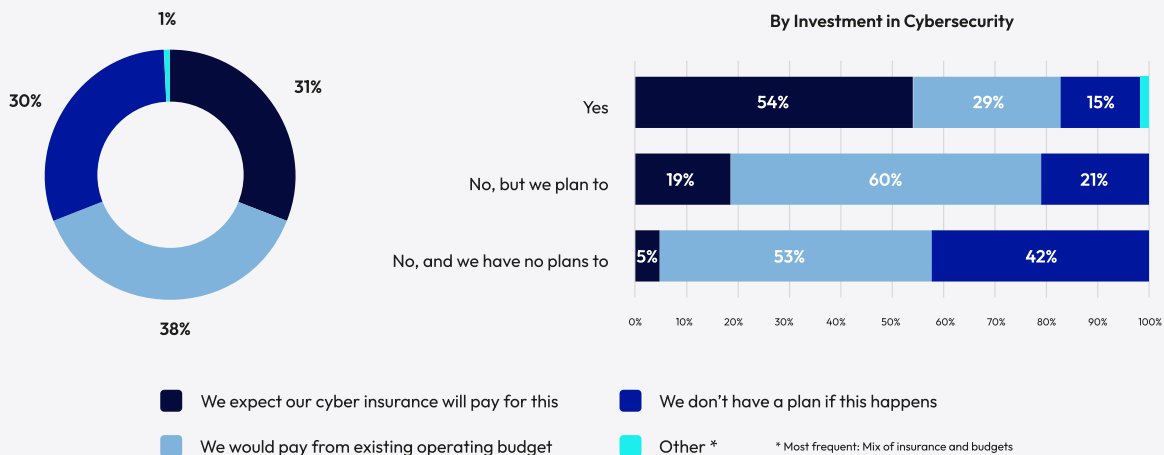
The study found that the majority of businesses (89%) are somewhat or very concerned that new privacy regulations will impact their identity security. This is consistent with last year and may be why cyber insurance for identity-related incidents remains consistent, with 52% of businesses having already invested and 29% planning to, similar to last year.

Has your company invested in cyber insurance for identity-related incidents?



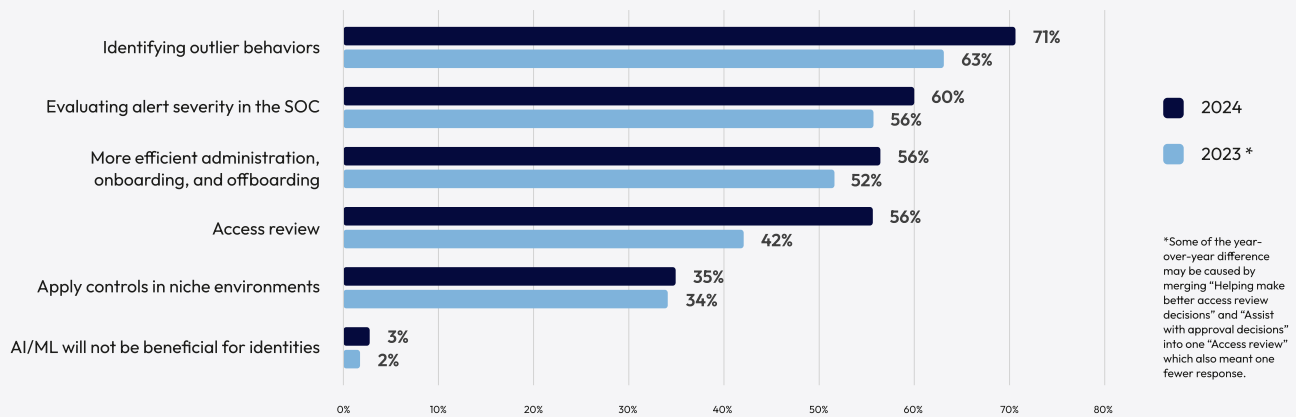
One reason these numbers are holding steady may be that only 31% of those surveyed expect cyber insurance to cover the cost of breach remedies.

What is your company's plan to pay for breach remedies if needed?
(i.e. offer credit monitoring or compensation to customers impacted by a breach)

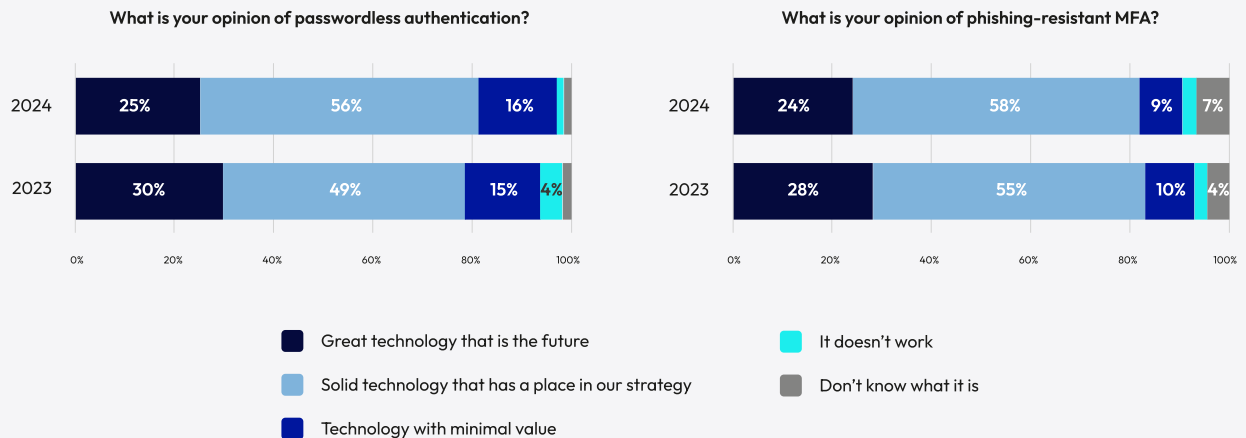


The research also explored the technologies required to address identity security challenges. For example, respondents were asked about the use cases they perceived as having the most benefit from artificial intelligence and machine learning. Identity and security stakeholders consistently (96%, down slightly) report AI/ML will be beneficial. The number one use case was identifying outlier behaviors (71% up from 63%), followed by evaluating the severity of alerts (60% up from 56%), and making administrative tasks more efficient (56% up from 52%).

In your opinion, what types of identity-related use cases would benefit from artificial intelligence or machine learning (AI/ML) capabilities? Choose all that apply.



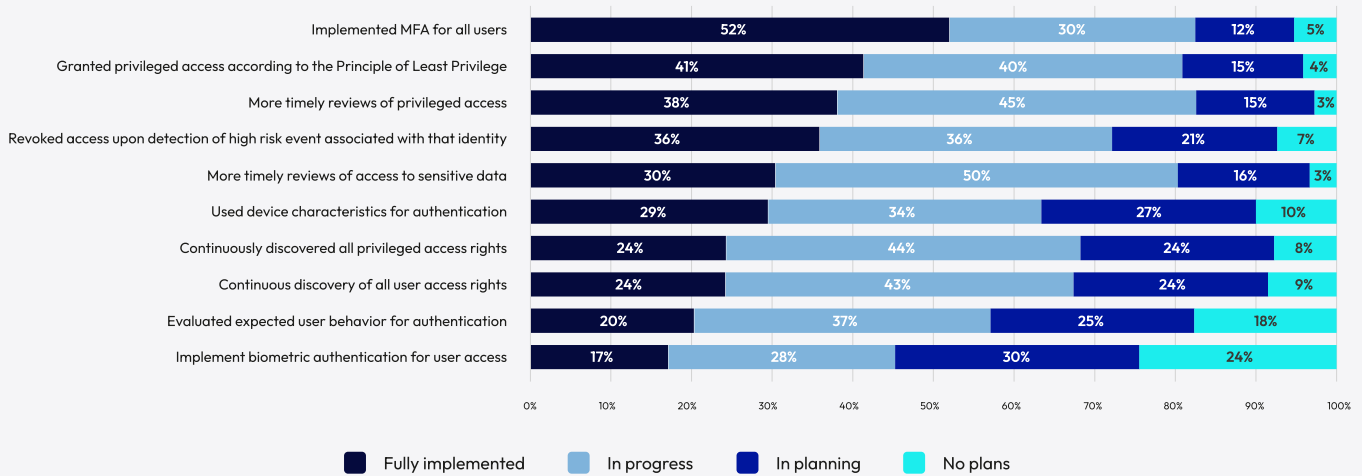
Identity stakeholders continue to see passwordless authentication as a tool in addressing identity issues, with 81% saying it's a great or solid technology. Respondents were also consistent in their answers about phishing-resistant multi-factor authentication (MFA), with 82% saying it's a great or solid technology for the future.



Security Outcomes Remain A Work In Progress

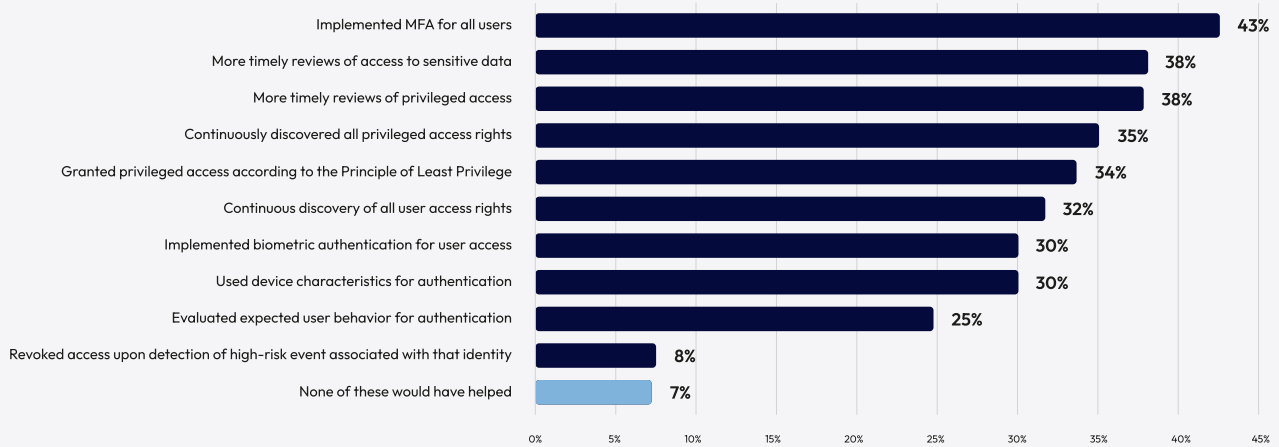
Identity stakeholders also provided insight into their company’s level of implementation of identity-related security outcomes. The most advanced outcome was the implementation of MFA for all users, a common theme throughout the research at 52% fully implemented. Granting access according to the principle of least privilege was at 41% fully implemented. Many of the outcomes are in progress.

Below is a list of possible identity-related security outcomes. What is your company’s current level of implementation for each of these?



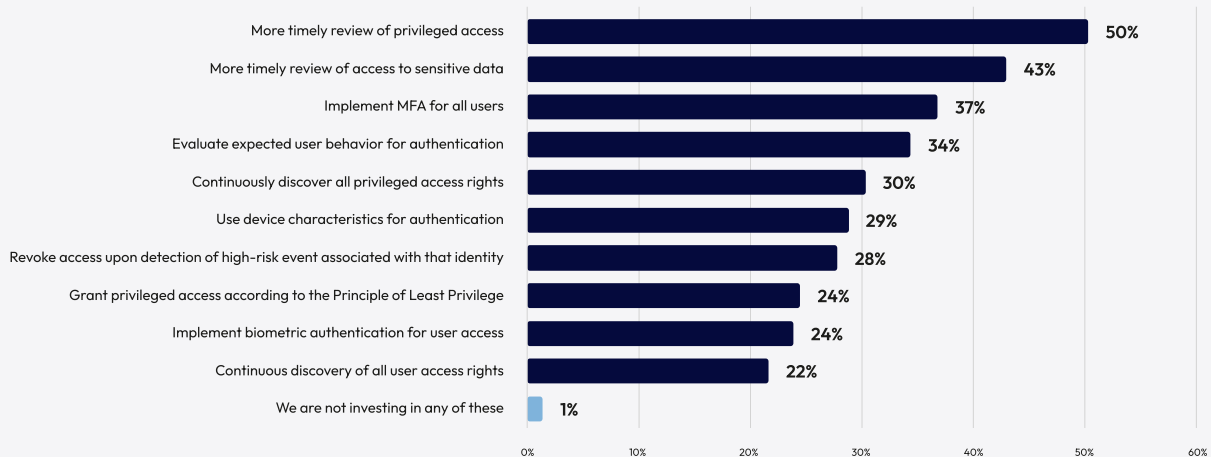
Looking back at the identity-related incidents encountered, 93% of identity stakeholders said security outcomes could have lessened the business impact of incidents. That number is down slightly this year, although remains strong. As it was last year, implementing Multi-Factor Authentication (MFA) for all users is reported to have the greatest chance to minimize the business impact of an incident. Going back to basics with routine, timely access reviews are solidly in second and third place.

In retrospect, could any of the following have prevented or minimized the business impact of the incident? Choose all that apply.



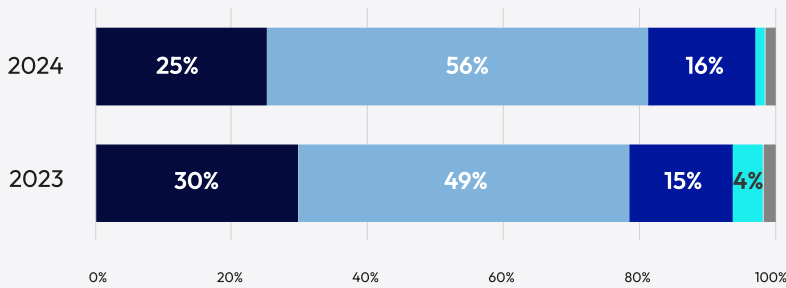
99% of businesses, the highest percentage in the history of our research, plan to further invest in security outcomes in the next 12 months. Top of the list is ensuring more timely reviews of privileged access (50%) and access to sensitive data (43%). Businesses also continue to increase investment in MFA for all users (37%).

Which of the following is your company investing the MOST in over the coming year? Choose up to three of the following.

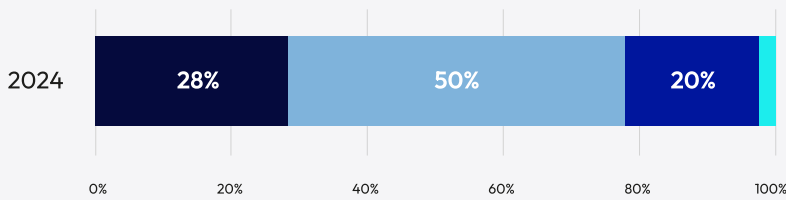


Looking at some more current technologies, respondents felt similarly about passwordless authentication, biometric authentication, and phishing-resistant MFA with 78%-82% saying that the technology is solid or great.

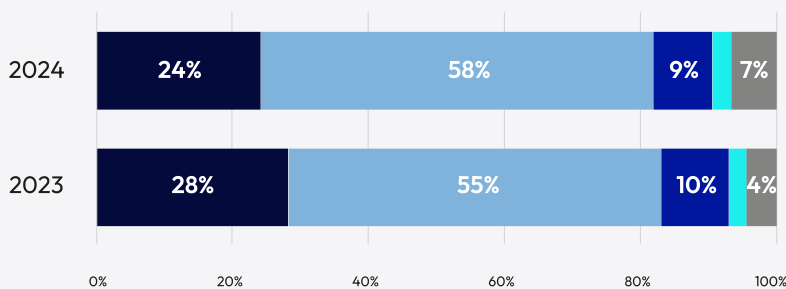
What is your opinion of passwordless authentication?



What is your opinion of biometric authentication (facial recognition, fingerprint, etc.)?



What is your opinion of phishing-resistant MFA?




- Great technology that is the future
- Solid technology that has a place in our strategy
- Technology with minimal value
- It doesn't work
- Don't know what it is

Prioritize Securing Identities With IDSA

Securing digital identities is a critical priority for organizations across all sectors in the fight against ever-evolving and increasingly sophisticated cyber threats. Our research finds that businesses increasingly recognize the risk of identity-related incidents and prioritize the dangers in their security programs.

More involvement and investment from senior leadership teams continue to be required to help businesses address these threats. Companies must also address the complexity of their systems and technology architectures and gain access to security expertise and standards to help them better manage their risk. To do that, security teams need to ensure they have the right processes, tools, technologies, and communication to discover and mitigate identity security threats as quickly as possible.



Find out more about the
trends in identity security.

visit www.idsalliance.org

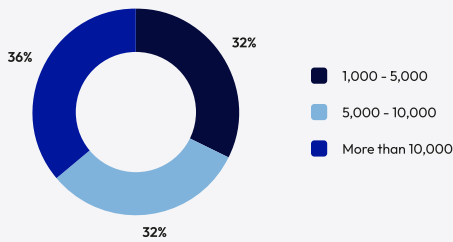
Goals & Methodology

The primary research goal is to identify the experiences and approaches toward security and identities at large companies.

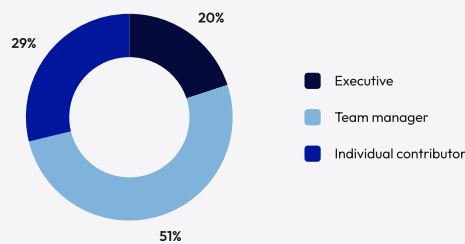
Independent sources of security and identity professionals in the United States were invited to participate in an online survey. A variety of questions were asked on history with identities and security, current plans, and other topics. Certain questions were repeated from similar surveys conducted over the previous four years to enable trend analysis.

A total of **521 qualified individuals** completed the survey. All were directly responsible for IT security or identities at a company with more than 1,000 employees and were very knowledgeable about both IT security and identities.

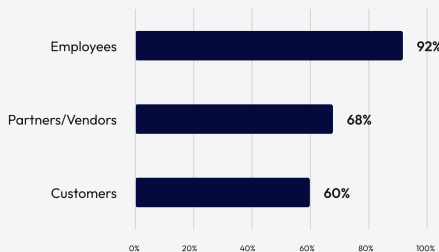
Company Size (# of employees)



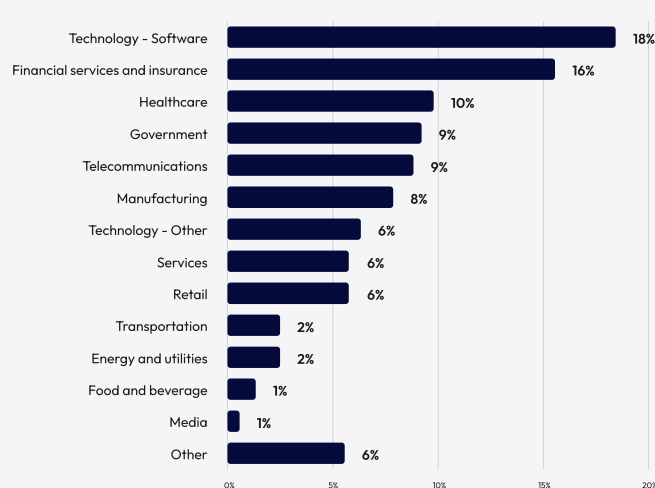
Job Level



Identity Responsibilities



Industry
(Education and Non-Profit Excluded)



About Dimensional Research

Dimensional Research® provides practical market research to help technology companies make their customers more successful. Our researchers are experts in the people, processes, and technology of corporate IT. We understand how technology organizations operate to meet the needs of their business stakeholders. We partner with our clients to deliver actionable information that reduces risks, increases customer satisfaction, and grows the business.

For more information, visit dimensionalresearch.com.

About IDSA

The IDSA is a group of identity and security vendors, solution providers, and practitioners that acts as an independent source of thought leadership, expertise, and practical guidance on identity-centric approaches to security for technology professionals. The IDSA is a non-profit that facilitates community collaboration to help organizations reduce risk by providing education, best practices, and resources.

For more information on the Identity Security Alliance and how to become a member, visit www.idsalliance.org.

Limited for distribution by Identity Defined Security Alliance members only.

Portions of this document may be reproduced with the following attribution: Identity Defined Security Alliance, www.idsalliance.org.