2021 Trends in Securing Digital Identities

A Survey of IT Security and Identity Professionals

dimensional research

Sponsored by IDENTITY DEFINED SECURITY ALLIANCE

Introduction

In 2020, the world experienced a significant shift in how many people work and transact business online. To minimize transmission of the COVID-19 virus, everyone who could stay home did — especially the knowledge workers. Digital identities used to connect remote workers suddenly became an even greater security target for attackers. Almost overnight, workplace trends from the last several years collided to create a new landscape for access and authentication, as cloud adoption, telecommuting, and the use of personal devices all spiked. These changes had to be accommodated by enterprises to provide users with secure connections with the applications and systems they needed to be productive.

Many organizations reacted to their new reality by increasingly focusing on identity as a core element of security to reduce risk, contain costs, and increase productivity. In this report, the Identity Defined Security Alliance (IDSA) examined the impact that the events of 2020 have had on identity and access management in the enterprise and the implementation of identity-focused security strategies.

Sponsored by the IDSA, the report is based on an online survey conducted by Dimensional Research. More than 500 security and identity professionals from the United States who worked at companies with more than 1,000 employees participated in the survey. Some questions were repeated from similar 2020 and 2019 surveys to enable trend analysis.

Key Findings

- **Remote work has significantly impacted identity security**
  - 83% report that remote work due to COVID-19 increased the number of identities
  - 80% say the shift to remote work increased focus on identity security
  - Confidence in the ability to secure employee identities dropped from 49% to 32% in the past year
- **Breaches are still prevalent, but investments in targeted prevention are accelerating**
  - Identity breaches are not increasing, but they are having an impact on organizations
  - At least 70% report they began implementation or planning of identity-related security outcomes in the past two years
  - 97% will make investments in identity-related security outcomes over the next two years
  - 93% believe they might have prevented or minimized security breaches by using identity-related security outcomes
- **Security is taking a broader role in identity and access management, with positive effects**
  - 64% report that they have made changes to better align security and identity functions within the last two years
  - 87% report the CISO has a leadership role when it comes to identity and access management (IAM), a dramatic contrast to 53% that said the same about the security team in 2019
  - Organizations where the CISO has ownership of IAM are more likely to say the security team has an excellent understanding of their identity strategy and implement identity-related security outcomes

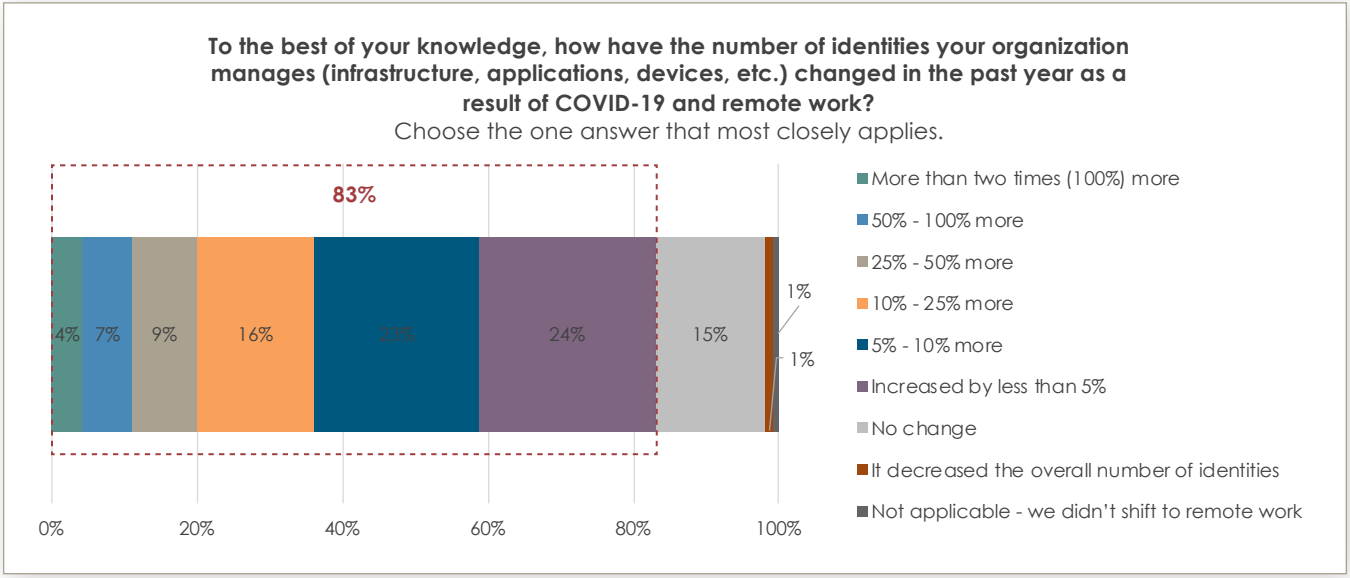
Detailed Findings: Remote work has significantly impacted identity security

COVID-19 and remote work has increased the number of identities

Remote work has been steadily increasing due to more digital communication and collaboration tools that enable staff to do their jobs outside of the physical office. However, in 2020 the number of full-time remote employees rose dramatically as the COVID-19 virus spread around the globe. Many companies went from a small percentage of their workforce being remote to virtually all remote employees to keep their businesses afloat. As a result, there was a significant jump in employees logging in from more devices — including their personally owned smartphones, tablets, and laptops — and from different locations outside the corporate office.

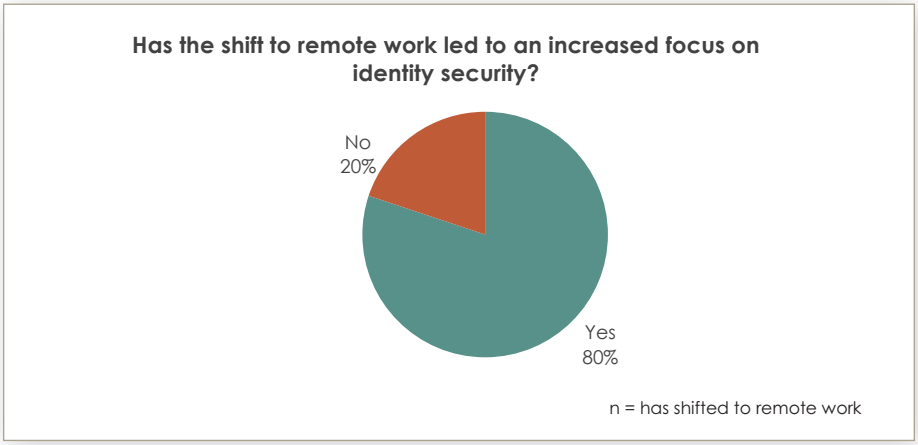
The pandemic not only affected the way we work, but it also changed the way we communicate and transact our daily lives. From education to online shopping, many organizations of all sizes and industries were forced to accelerate digital transformation initiatives to support online services. In addition, this change caused the number of customer identities also to grow, and along with it, required companies to manage and secure significantly more identities.

This research shows that most companies (83%) experienced an increase in the number of identities last year due to COVID-19, including human and machine identities. For some companies, the increase was quite dramatic. One in five (20%) reported that the number of identities they manage increased by more than 25%.



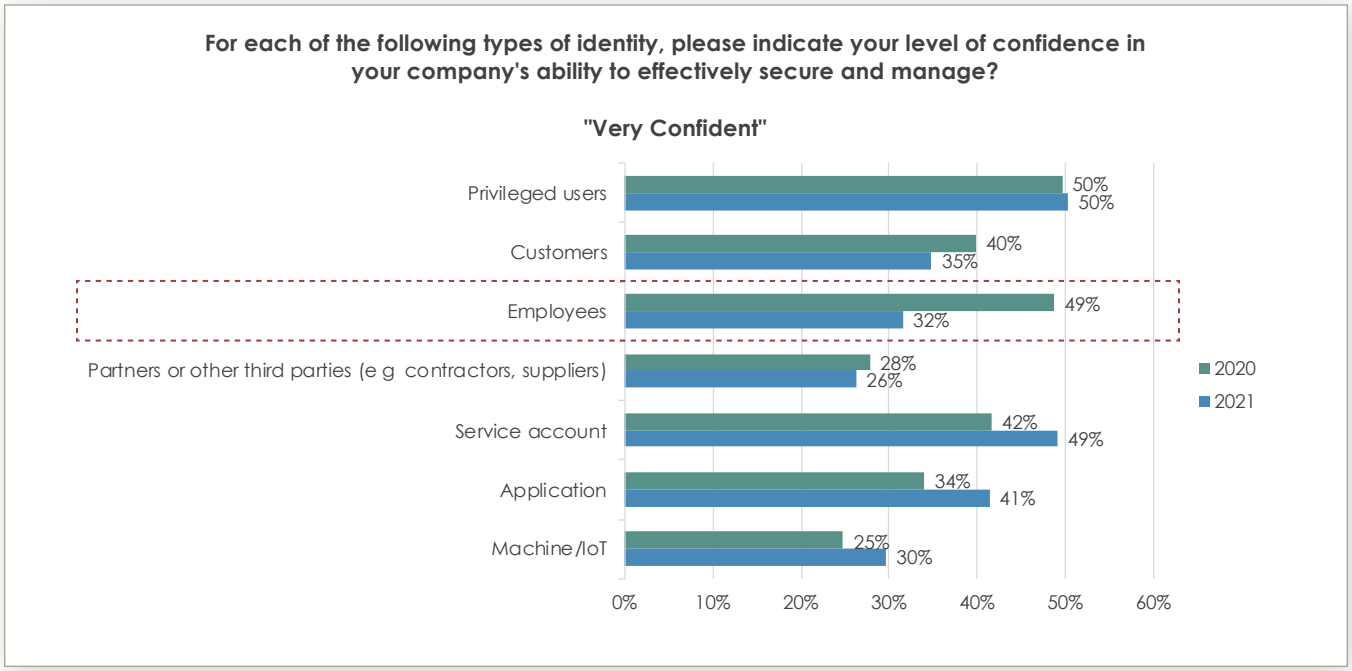
The shift to remote work drove more focus on identity security

With identity serving as the connective tissue between systems, services, and a distributed workforce, many enterprises were forced to reexamine how they could best empower their workforce to connect securely while maintaining consistency across their cloud and on-premises environments. When asked how this shift to remote work changed their team's approach to identity security, the vast majority (80%) of security and identity professionals noted an increased focus on identity security.



Confidence in securing employee identities dropped dramatically in the past year

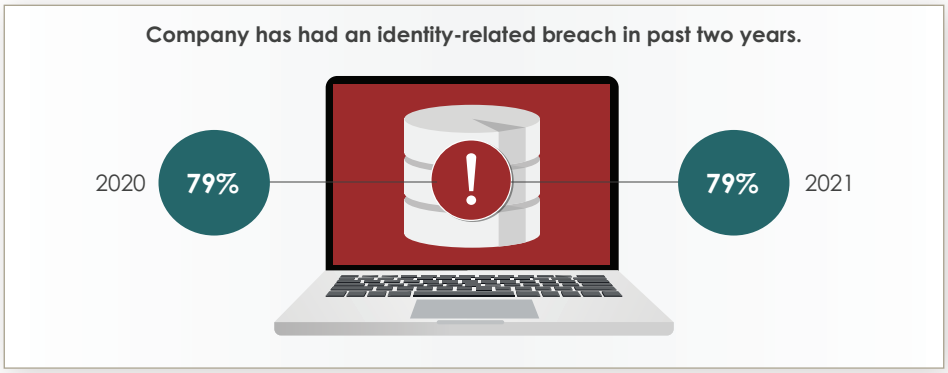
A sharp spike in remote workers will inevitably introduce more risk to the organization as more individuals attempt to interact with sensitive digital assets from unprotected networks and personal devices. As such, it is unsurprising that confidence in securing employee identities dropped dramatically, falling from 49% last year to only 32% this year. This drop in confidence protecting employee identities is particularly notable as other types of identities did not see a similar decline. For example, confidence in the ability to secure other kinds of human identities such as privileged users, customers, and partners stayed flat or saw a minor decline in the past year. In contrast, security and identity stakeholders reported an increase in their confidence in securing machine identities, including service accounts, applications, and machines or IoT (Internet of Things) identities.



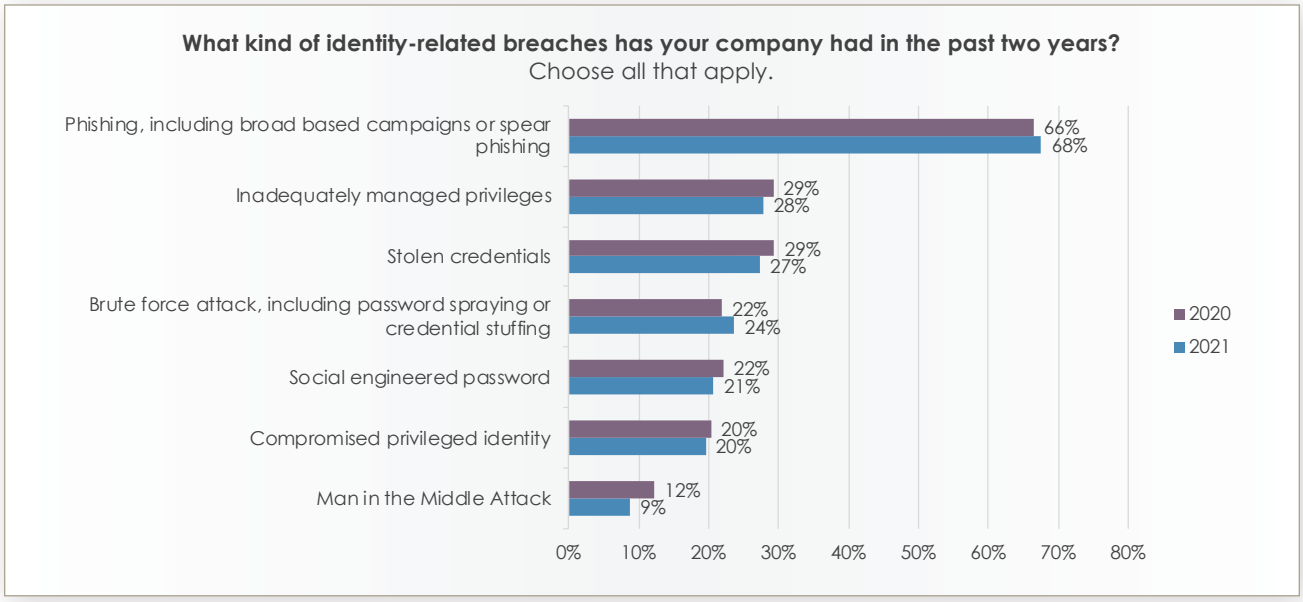
Detailed Findings: Breaches are still prevalent, but investments in identity-related security outcomes are accelerating

Identity-related breaches are not increasing, but they are having an impact

One of the top findings of this survey is that while identity-related security breaches are not increasing, they are also not going away. The data relating to past breaches remained stable during the past year, with 95% of companies acknowledging an identity-related breach at some point in time, which was comparable to 94% in the 2020 study. Similarly, when asked whether or not they experienced an identity-related breach during the past two years, 79% reported breaches equivalent to the number last year.

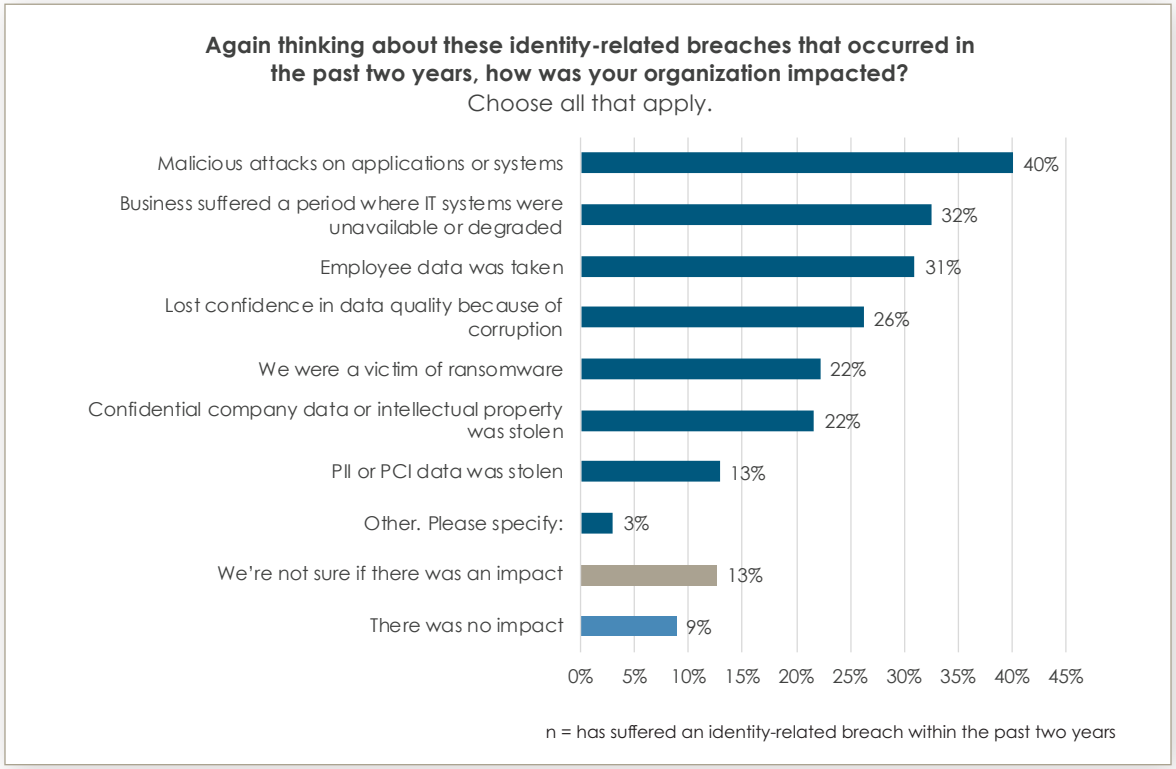


When we further analyzed the types of breaches incurred in the past two years, the number one type of breach cited continued to be phishing (68%), similar to the response given in 2020, with only a slight percentage increase from last year (66%). These comparable responses year-over-year demonstrate attackers' continued emphasis on the easiest path to compromising legitimate credentials for use in penetrating enterprise networks and maintaining persistence after entry.



It is important to stress that these identity-related breaches are much more than an annoyance for security and identity teams; they have a direct business impact. The leading issues reported included malicious attacks on applications and systems (40%), the unavailability of IT systems for a time period (32%), stolen employee data (31%), and lost confidence in data quality because of corruption (26%). Many participants took the time to write in "other" responses, including direct theft of money, loss of revenue, failed audits, anxiety for the security team, and loss of trust in the IT organization.

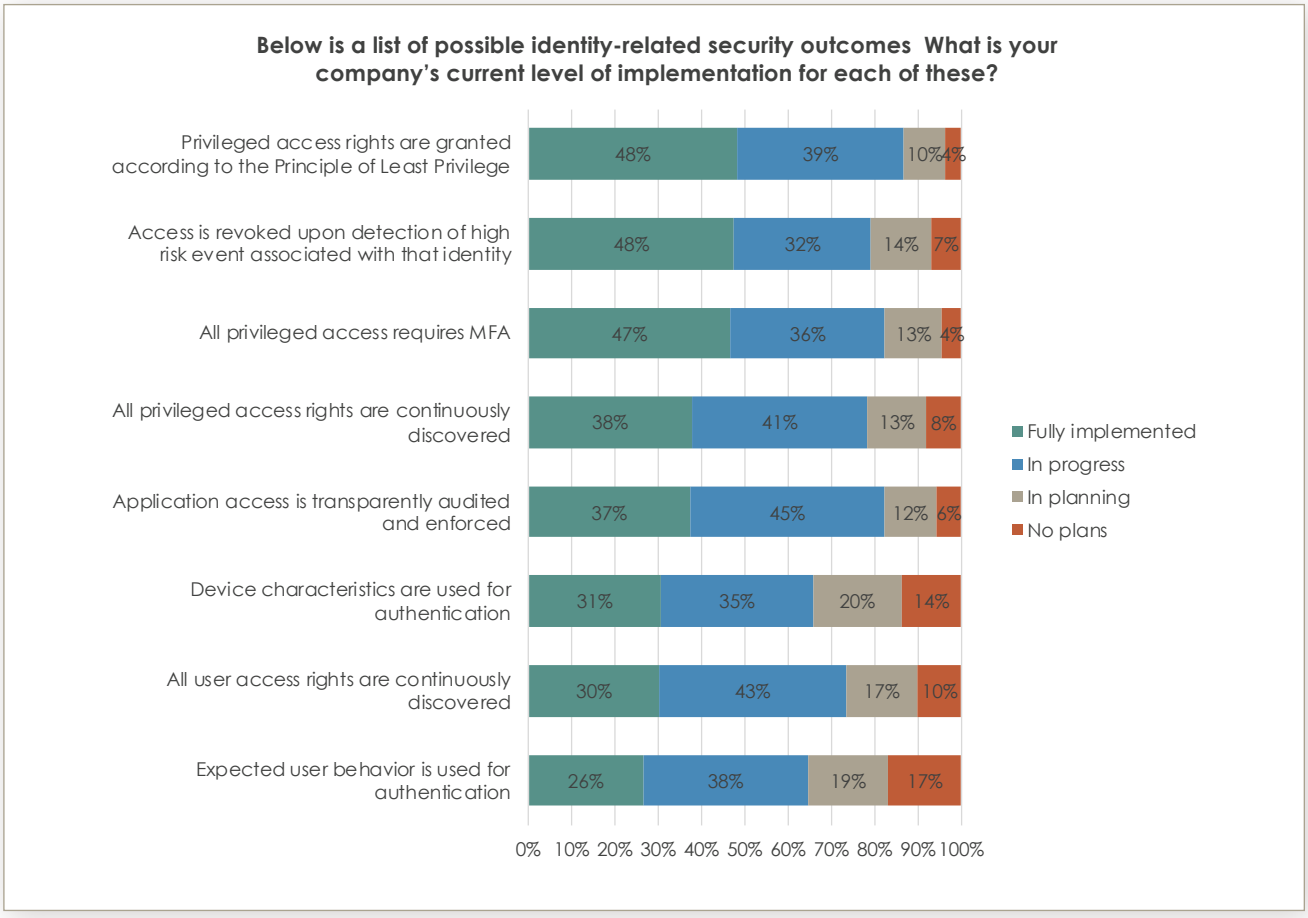
In total, more than three-quarters (78%) say that their organization was impacted by identity-related breaches that occurred in the past two years. But perhaps the most worrisome data point in this question is the 13% who reported that they didn't know for sure if there was an impact, as this group would have been unable to respond effectively to prevent problems in the future.



Implementation of identity-related security outcomes continues to be a work in progress

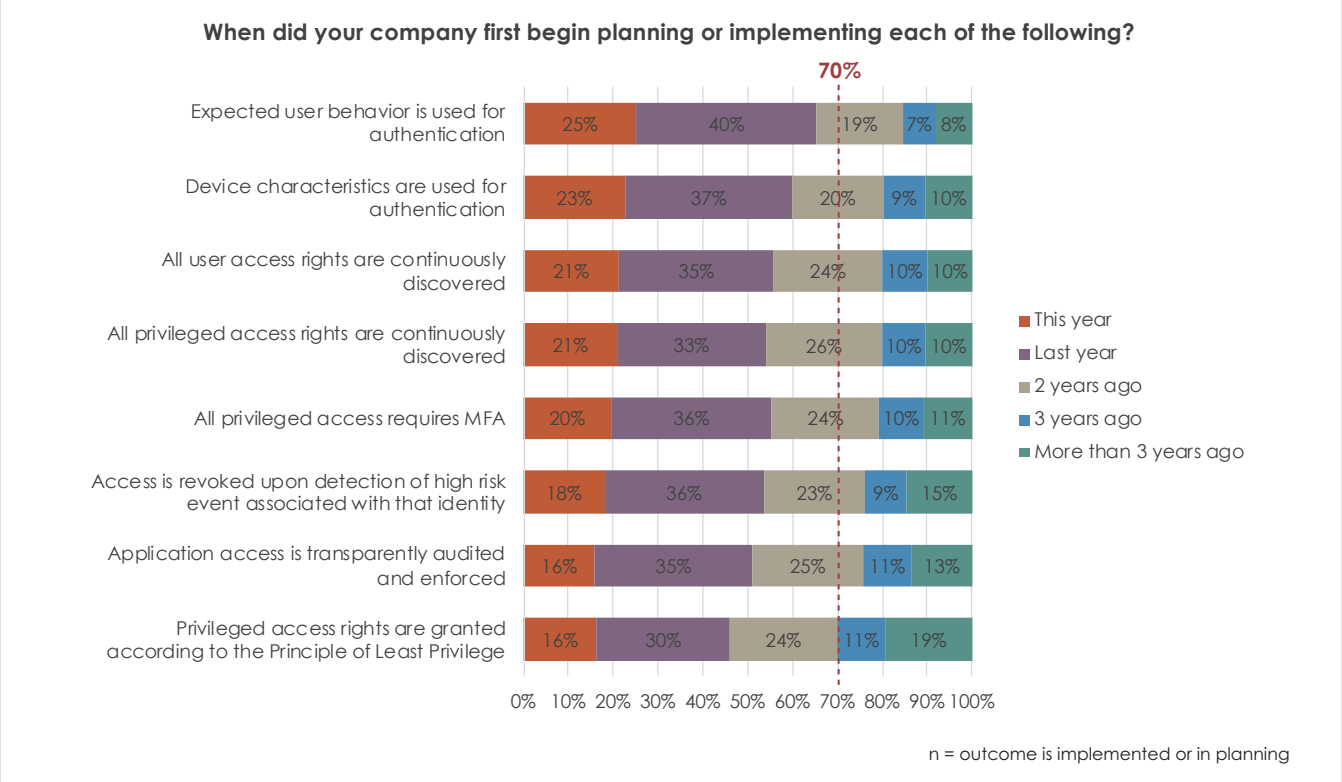
As organizations look for ways to reduce the risk of identity-related security breaches, many will assess their security challenges and define outcomes and approaches relevant to their organization's business needs and priorities. As part of our previous research, Identity Security: A Work in Progress, we assessed the implementation progress of key identity-related security outcomes recommended by the IDSA. *(See https://securityoutcomes.idsalliance.org for more details.)* For our 2021 study, the same question was asked to assess year-over-year progress in implementation and planning and identity movement towards mitigating the risk of identity-related breaches.

Achieving full implementation of these identity-related security outcomes is not complete, as most organizations reveal they are still in the planning or in-progress stages at the time of this survey. There is no single identity-related security outcome that has more than half of companies reporting full implementation, although granting privileged access rights according to the Principle of Least Privilege (48%), revoking access upon detection of a high-risk event (48%), and requiring MFA for privileged access (47%) are getting close to that threshold.



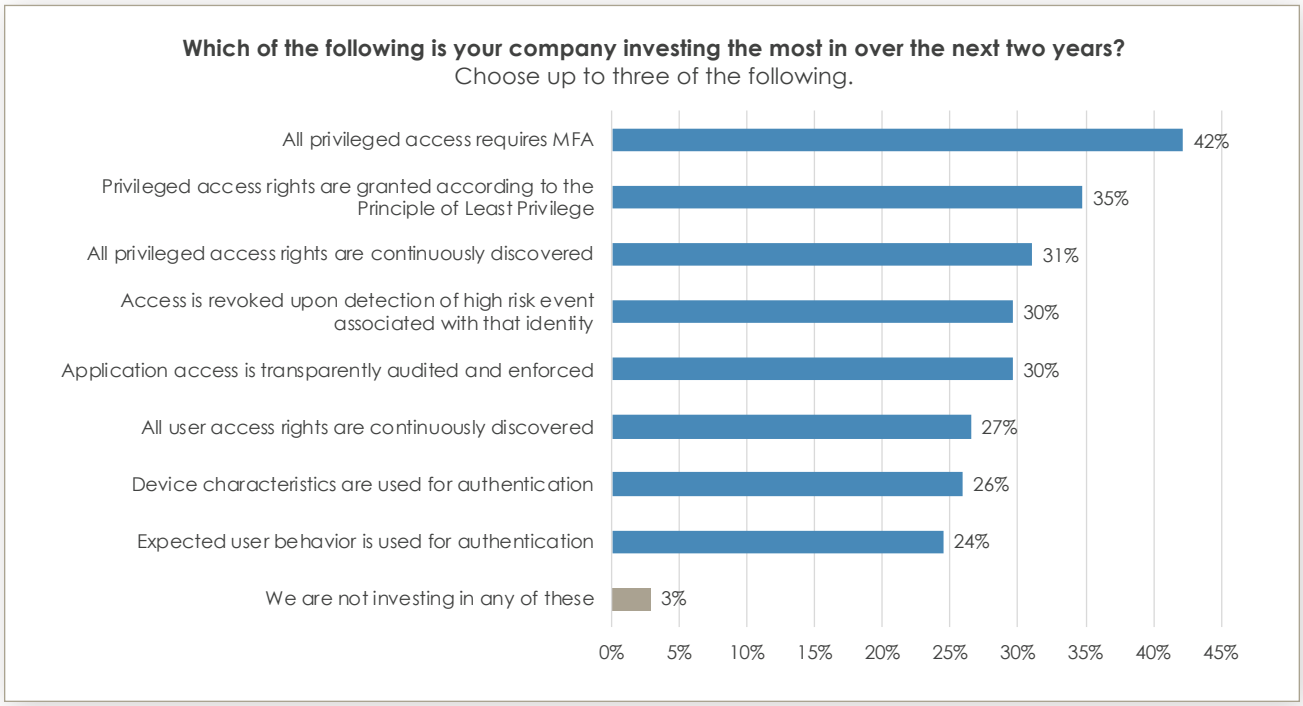
Outcome adoption is relatively new, with most outcomes initiated in the past two years

One of the positive takeaways of this survey is that there is strong momentum in implementing identity-related security outcomes. The past years have shown tremendous progress in all identity-related security outcomes explored, with more than 70% of organizations indicating they first initiated work on each outcome during the past two years.



Companies are planning to invest in identity-related security outcomes over the next two years

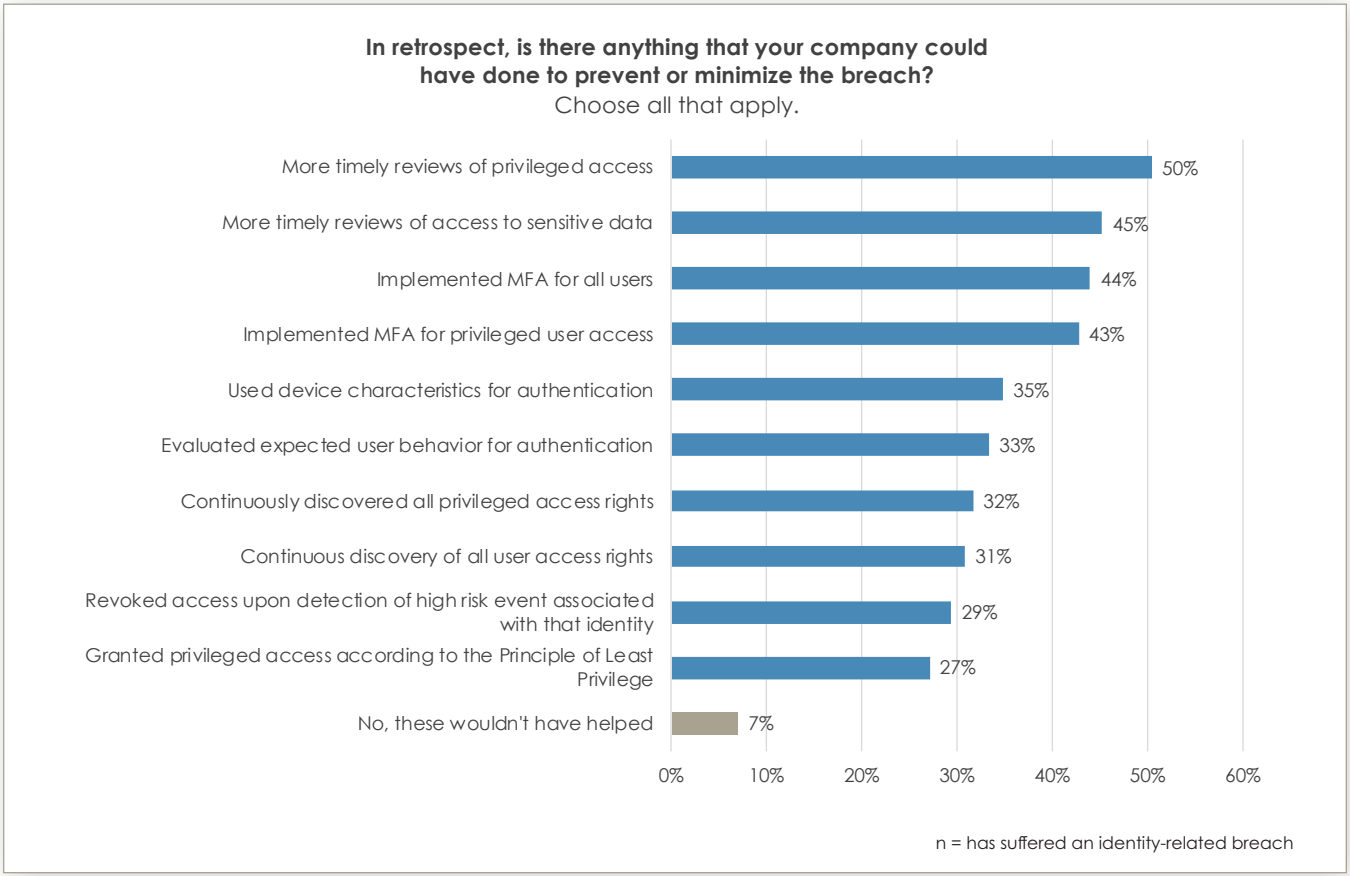
Despite an unprecedented year that for many included reduced IT budgets and strict cost control measures, companies have demonstrated they are willing to invest in identity as a preventative way to reduce their risk and increase productivity. In fact, nearly all IT security and identity professionals (97%) reported making investments across a range of identity-related security outcomes. The top three investment areas for the coming years include requiring multi-factor authentication (MFA) for all privileged access (42%), granting privileged access rights according to the Principle of Least Privileged (35%), and continuously discovering privileged access rights (31%).



Security outcomes expected to have mitigated past breaches

According to IT security and identity experts who have experienced a corporate breach, most (93%) believe that better implementation of security outcomes could have prevented or minimized the breach. The primary security outcome cited is more timely reviews of privileged access (50%) followed by more timely reviews of access to sensitive data (45%), MFA implementation for all users (44%), and MFA implementation for privileged user access (43%).

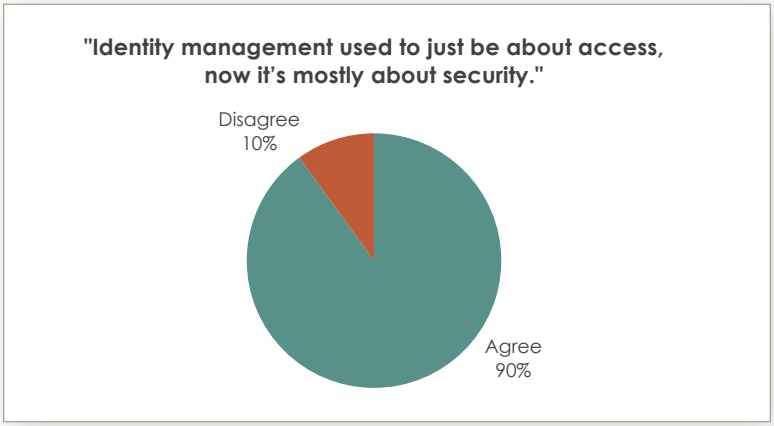
These top four responses indicate that organizations believe that ensuring appropriate access levels and providing additional authentication measures for sensitive data and systems would have prevented or minimized past breaches. These findings track with the more prominent breaches that have occurred in the last several years, including SolarWinds. Given that security and identity professionals strongly expect these outcomes could have helped prevent their past breaches and other high-profile breaches, it is unsurprising that we have seen such a high investment in implementing these outcomes in the past few years. We would expect those investments to begin to pay off moving forward.



Detailed Findings: Security is taking on a broader role in identity and access management, with positive effects

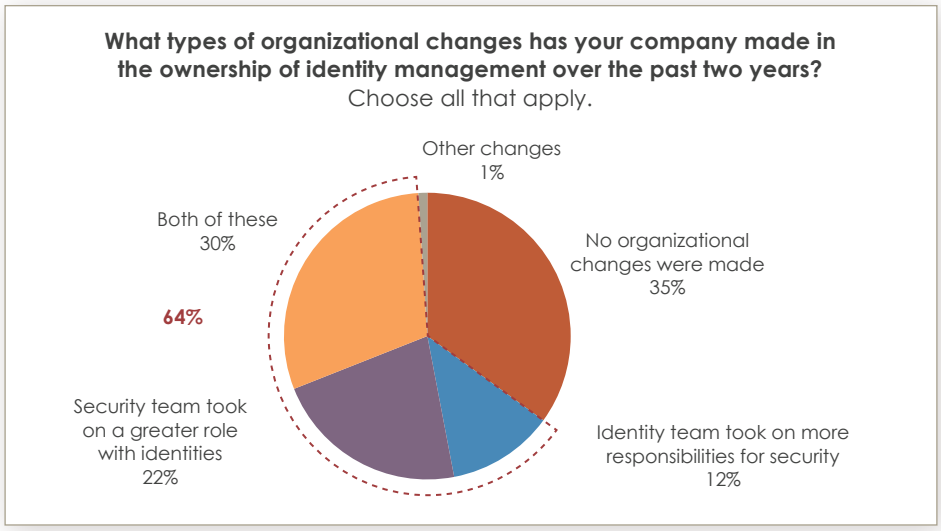
The focus of identity and access management is changing.

Traditionally, identity and access management defined and managed the roles and access privileges of individual users and devices by granting or denying access to enterprise assets, and security was a secondary consideration. Yet, as hackers have aggressively exploited potential weaknesses, identity and access management has assumed greater responsibility for security. According to this research, identity and access management is now considered mostly about security, with 90% of security and identity professionals confirming that they have perceived this change.

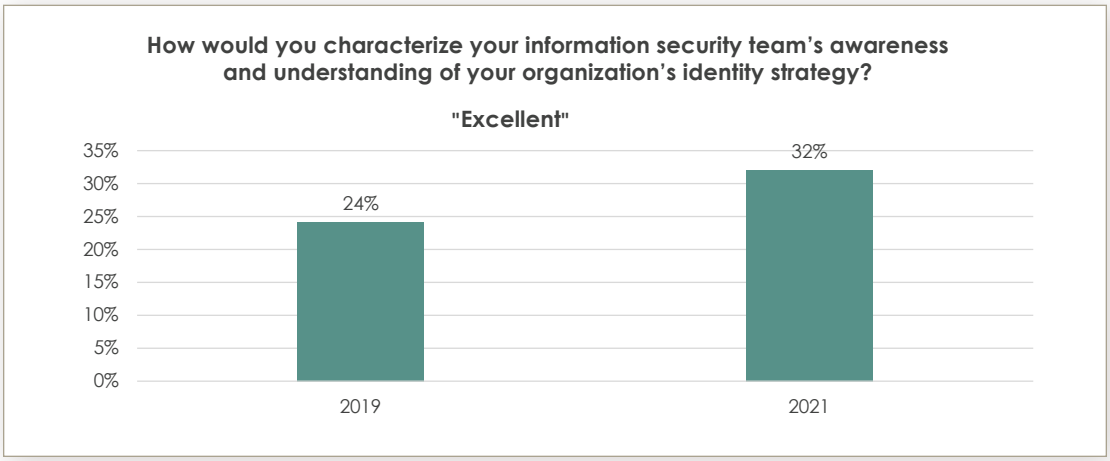


Ownership of identity and access management is evolving

As reported in previous research, Identity and Access Management: The Stakeholder Perspective, IAM is often messy, with departments ranging from HR to line of business units involved in discussions. However, the growing awareness of the importance of identity in enabling and securing everything from DevOps to remote workers has led many organizations to attempt to improve internal collaboration. Two-thirds (64%) of all companies report that they have made changes within the last two years to improve the alignment of security and identity. This number includes 22% where the security team is doing more with identities, 12% where the identity team is doing more with security, and about a third (30%) that says both teams have expanded their traditional responsibilities.



We see a further indication of the evolution towards a security focus around IAM in the increase among security teams' understanding of the overall identity strategy. The number saying that their security team has excellent awareness and understanding of identity strategies is up notably, from 24% in 2019 to 32% this year.



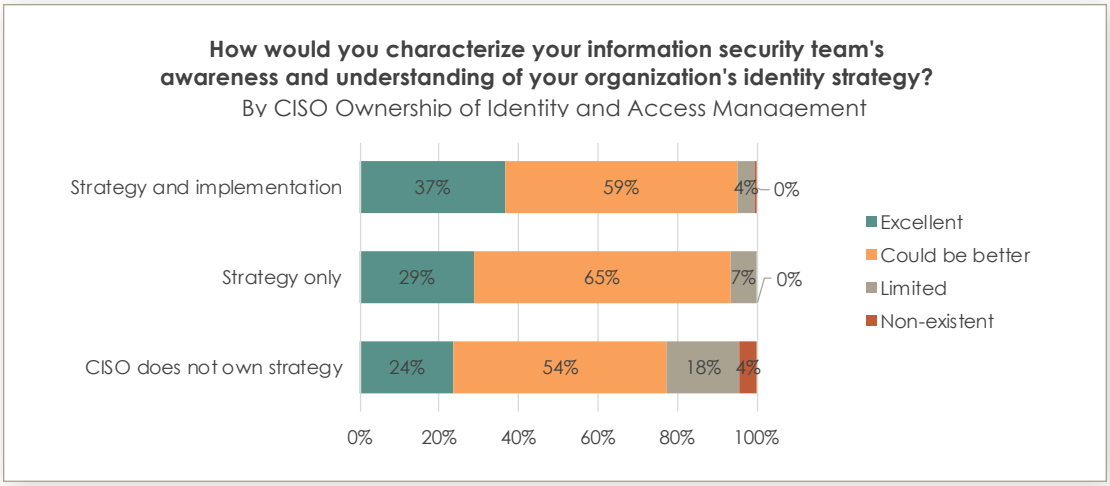
Modern CISOs own identity and access management

Organizations are also making changes in ownership to align security and identity and access management more closely. Specifically, 87% of companies report their chief information security officer (CISO) has an ownership role with identity and access management. And a remarkable 45% own both strategy and implementation for overall identity and access management initiatives.

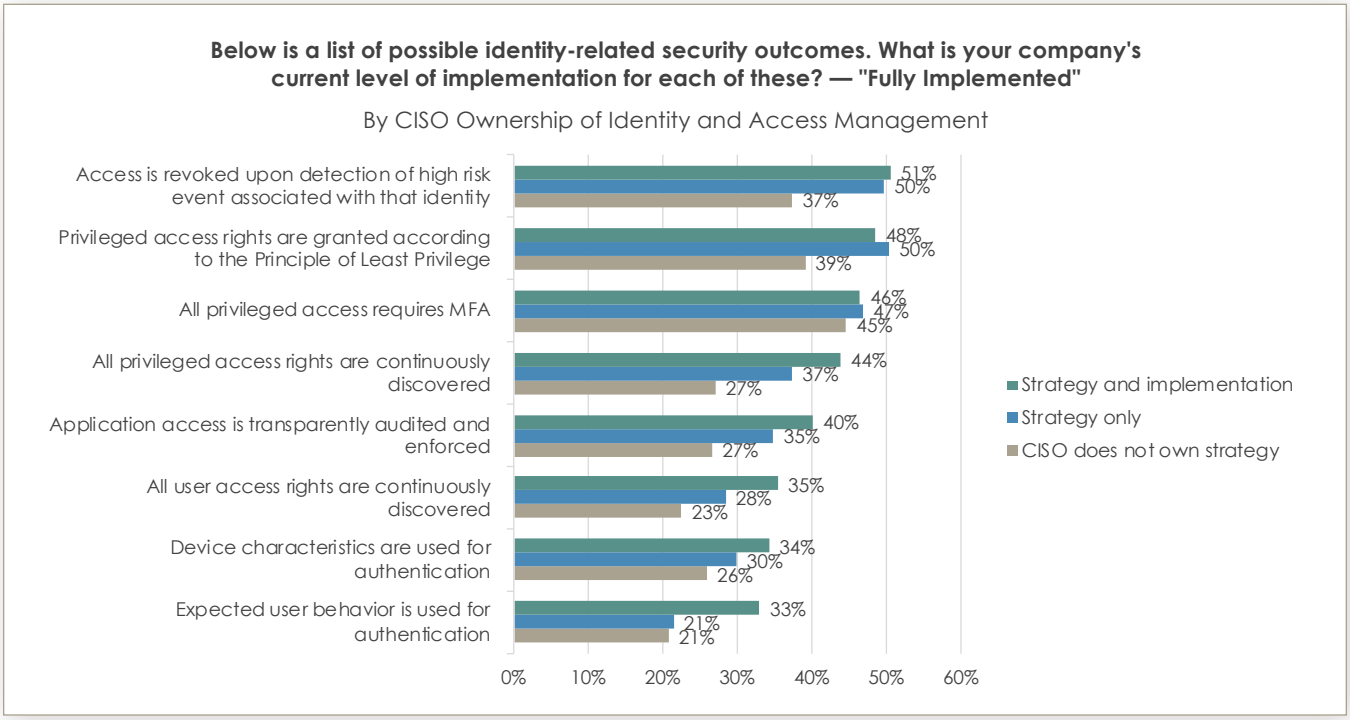
One of the noteworthy revelations of this research is this switch in IAM leadership. While the questions weren't phrased identically in the two surveys, it is informative to notice that in 2019 slightly more than half (53%) reported that security had a leadership role with identity and access management. That is far fewer than the 87% reporting that security executives have a leadership role in 2021.

There are security benefits when the CISO has ownership of identity and access management

The data shows that organizations benefit when the CISO has ownership of identities. We see differences in a few areas. Stakeholders are much more likely to say that the security team has an "excellent" understanding of identity strategy when the CISO has a more significant leadership role.



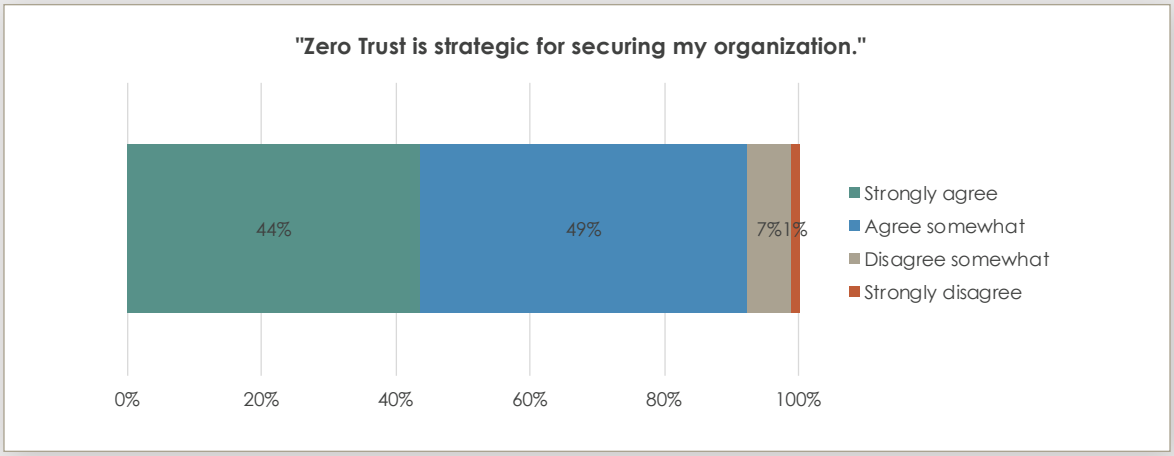
Most importantly, organizations where the CISO has greater ownership of identity and access management have progressed toward fully implementing identity-related security outcomes.



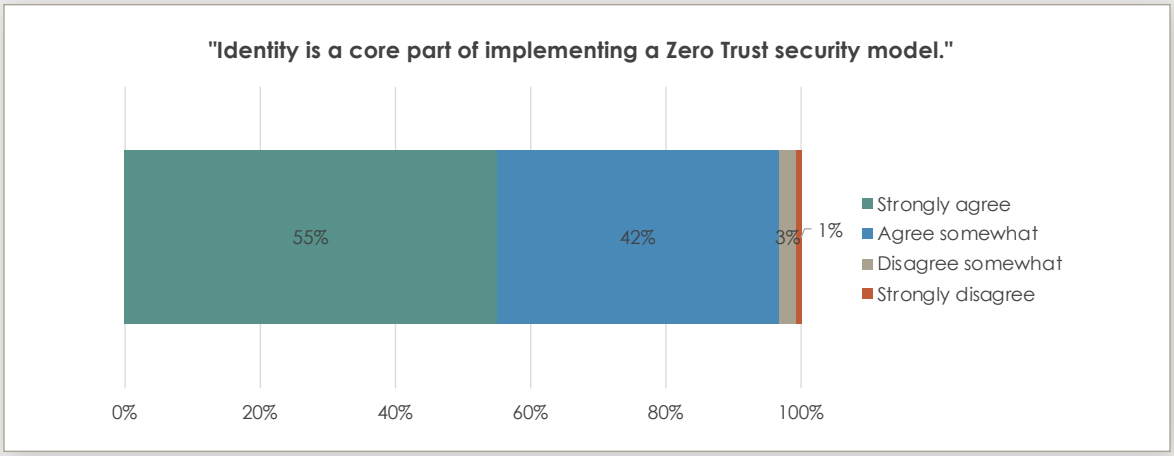
Special Report: Adoption of Zero Trust and the Role of Identity

Organizations are widely adopting Zero Trust and recognize the importance of identity

Zero Trust is a popular approach to security centered on the belief that organizations should not automatically trust anything inside or outside their control and must actively verify everything trying to connect to its systems before granting access. When asked if Zero Trust is strategic to securing their organizations, 93% of IT security experts agreed it was. This number includes 44% who strongly believe Zero Trust approaches are strategic to preventing breaches.

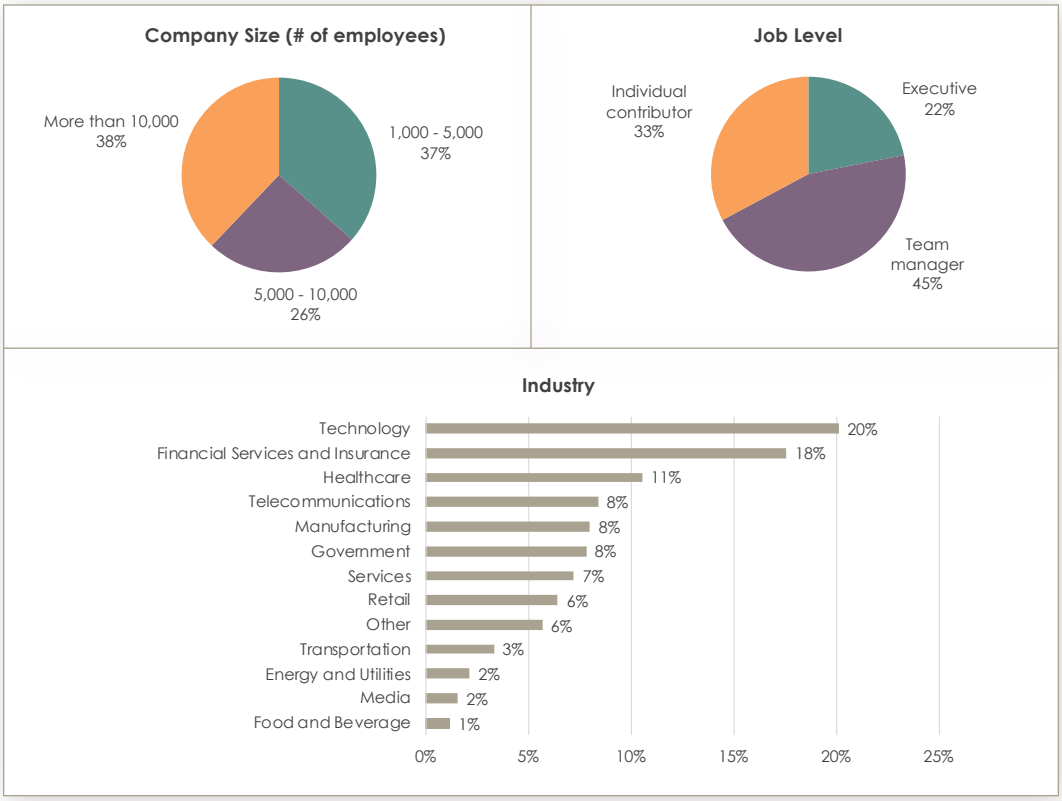


Subsequently, nearly all (97%) agree identity is a foundational component of a Zero Trust security model. This finding suggests that forward-thinking organizations believe they should not implement a Zero Trust architecture without focusing on effective identity and access management.



Survey Methodology and Participant Demographics

An online survey was sent to an independent database of security and identity professionals in the United States. A total of 512 qualified individuals completed the survey. All participants were directly responsible for IT security or IAM at a company with more than 1,000 employees. Each was very knowledgeable about both IT security and identities. Participants included a mix of company sizes, job levels, and industries.



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 nonprofit that facilitates community collaboration to help organizations reduce risk by providing education, best practices, and resources. For more information visit www.idsalliance.org.