



IDENTITY DEFINED
SECURITY ALLIANCE

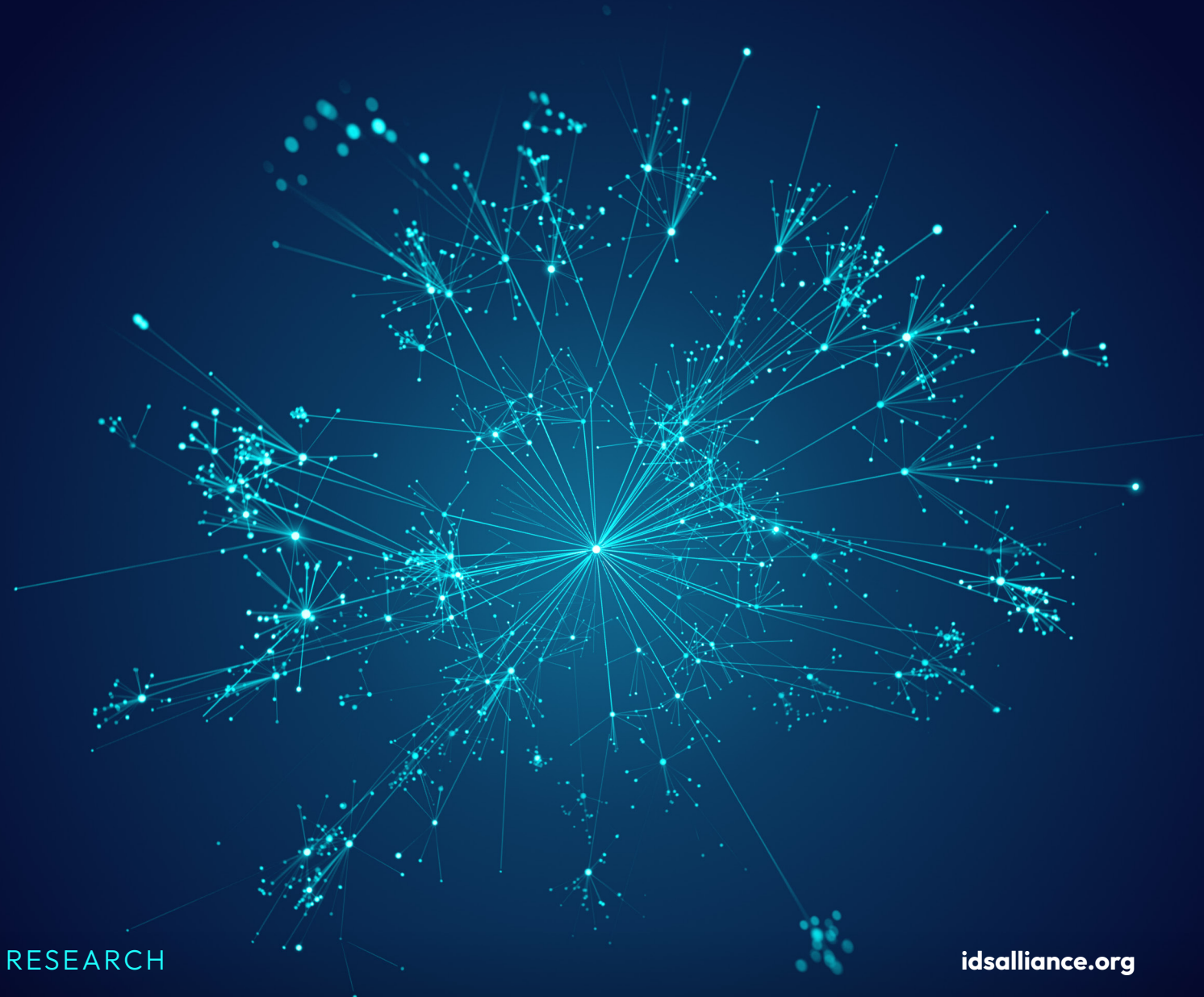


dimensional
research

2025

Trends in Identity Security

A Survey of IT Security
and Identity Professionals



RESEARCH

idsalliance.org

Table of Contents

03	Introduction
04	The State of Identity and Security in 2025
06	Artificial Intelligence
08	Non Human Identities/Machine Identities
09	Zero Trust
10	Digital Wallets
11	Ongoing Challenges of Identity Security
14	Prioritize Securing Identities With IDSA
15	Goals & Methodology

Introduction

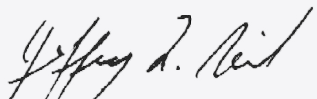
2025 opens a new world to identity management and security professionals. That has a direct effect on identity vendors, corporations, and consumers. Last year, in this report, we wrote of increasing complexity and scope in the identity space. The quantum leap in this year's increase is fueled by agentic artificial intelligence and non-human identities (NHIs). Peer research shows that NHIs outnumber human identities on the internet by much more than eight to one.

On the good news front, the number of identity-related incidents reported has plateaued and, in some cases, dropped. The efforts of the identity and security professional, as well as consumers, are paying off.

This year, we commissioned a study with Dimensional Research again 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 other relevant topics. 512 qualified individuals completed the survey. All were directly responsible for IT security and/or identity at a company with more than 1,000 employees and were knowledgeable about both IT security and identity.

These annual research reports are often cited, and we greatly appreciate that. On the following pages, I invite you to explore the state of identity and security.

My identity is,



Jeff Reich, CISSP, CRISC

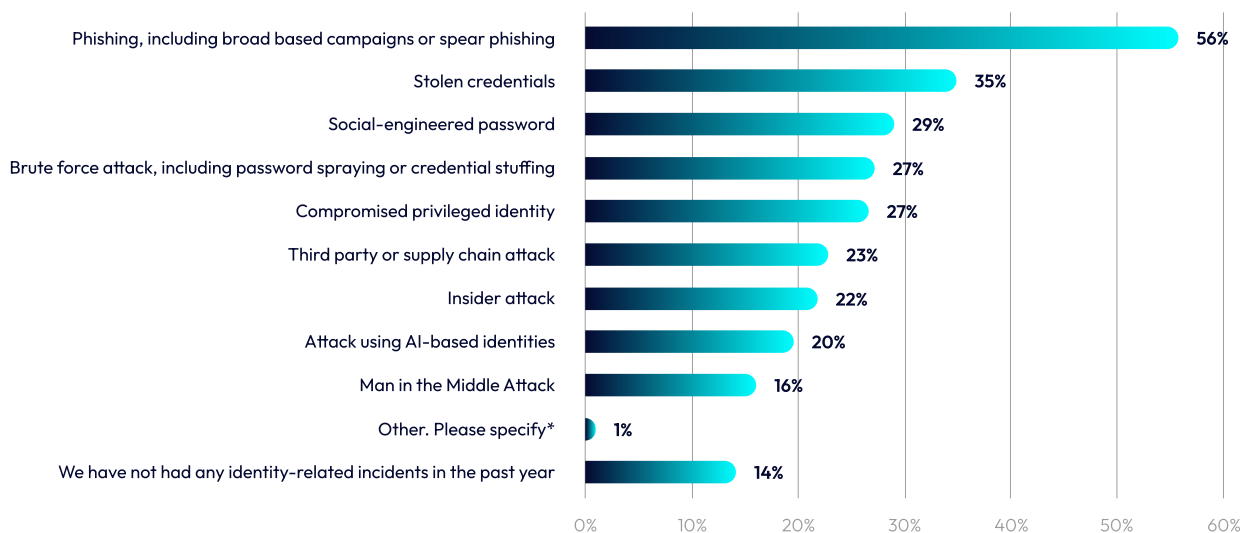
Executive Director, Identity Defined Security Alliance

The State of Identity and Security in 2025

This year's report contains some good news. Many metrics on identity security are improving. Of the organizations responding, 14% indicated having no identity-related attacks in the past year. Phishing remains the highest volume identity-related threat by a large margin.

Looking at the other threats, Not many of you should be surprised that artificial intelligence entered the picture this year, and we will cover that later in this document.

What kind of identity-related incident has your company had in the past year?

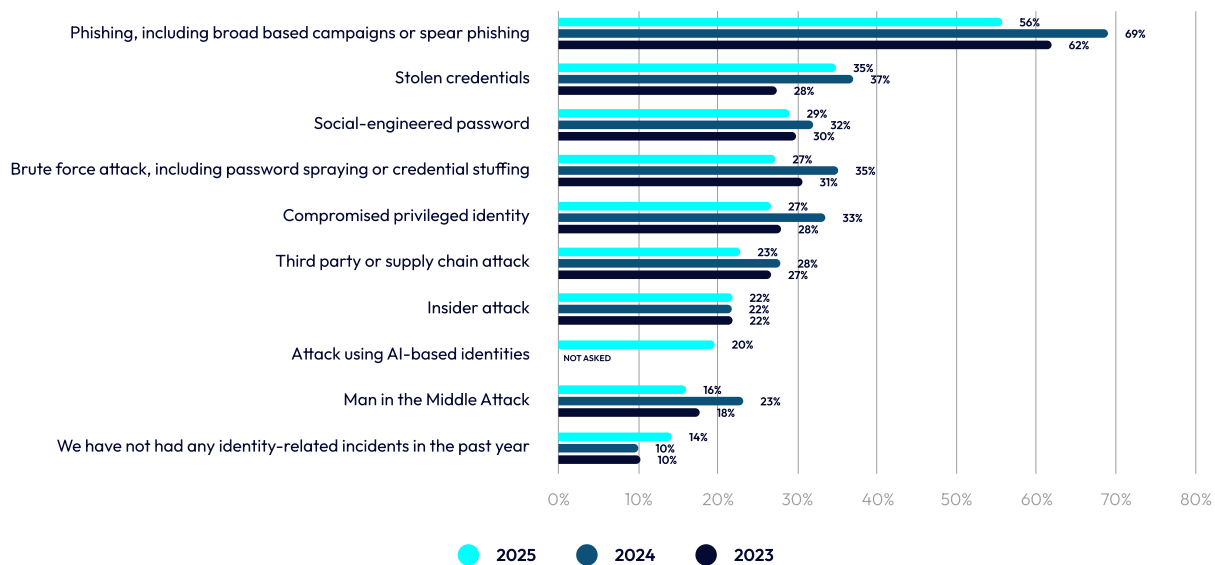


*Other: Credential stuffing; Privilege escalation

This chart can let us know where to spend more effort and resources. Although we are seeing improvement, with the proliferation of anti-phishing education and phishing tests in many organizations, perhaps we need to shift more resources to providers and internal organizations to help stem the tide of phishing.

As mentioned, phishing dropped from over two-thirds of companies reporting in 2024 to a bit over half in 2025. Stolen credentials, brute force attacks, and social engineering also decreased substantially. Less common incidents, such as insider threats and supply chain compromises, fell into the mid-to-low teens. Importantly, the number of companies reporting no identity-related incidents nearly doubled; your security investments and education efforts are beginning to pay off.

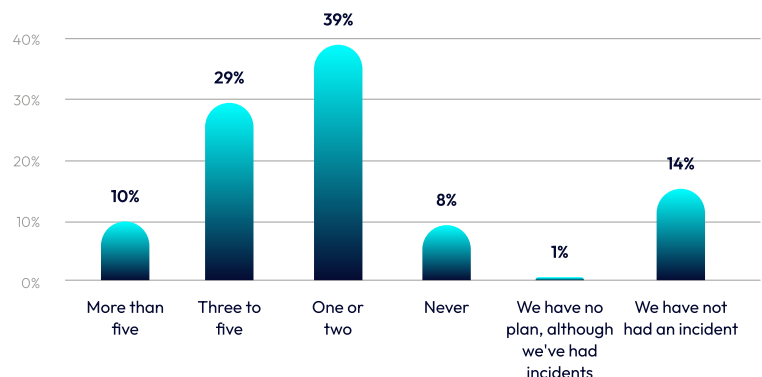
What kind of identity-related incident has your company had in the past year?



Let's look at the number of incidents reported. In 2025, organizations reported a significant decline in nearly all types of identity-related security incidents compared to 2024, which had seen a sharp rise. Time will tell whether this becomes an ongoing trend or is an outlier.

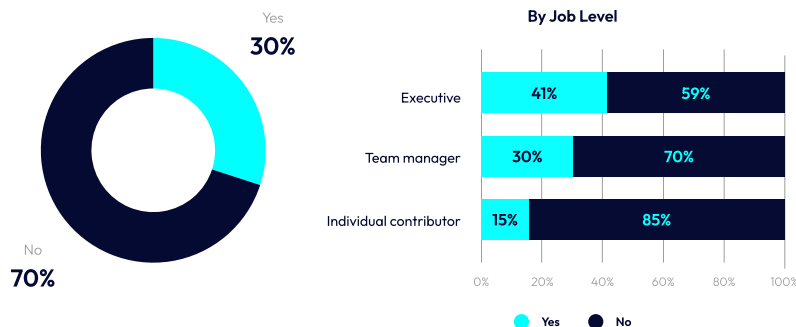
As one would expect, the drop in the number of incidents correlates with the number of times that an incident response plan was invoked.

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



Artificial Intelligence

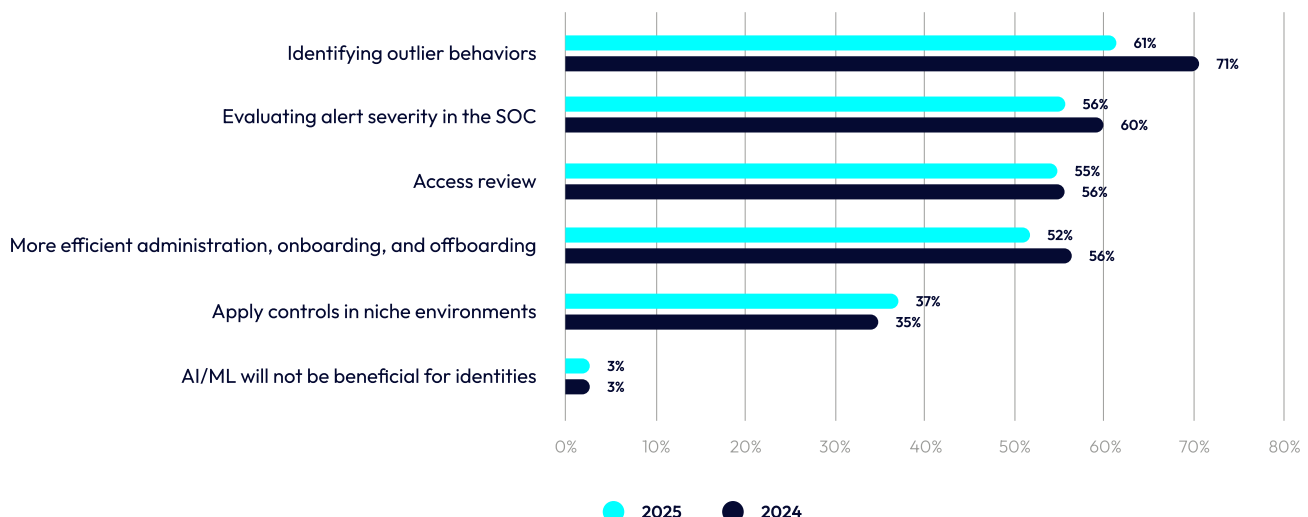
To the best of your knowledge, has your company experienced an identity-related incident that was generated using AI?



C'mon, did you really think we could conduct a research survey in 2025 without touching AI?

30% of respondents have experienced an AI-generated incident. A few years ago, when asking about security perceptions, you could see a visible gap between the executives, managers, and individual contributors. That gap had been shrinking, however, not on this topic. Executives reported one-third more incidents than managers and almost three times more than individual contributors. This is a data point that we will use in our 2026 work, so that we can all drive to close this gap.

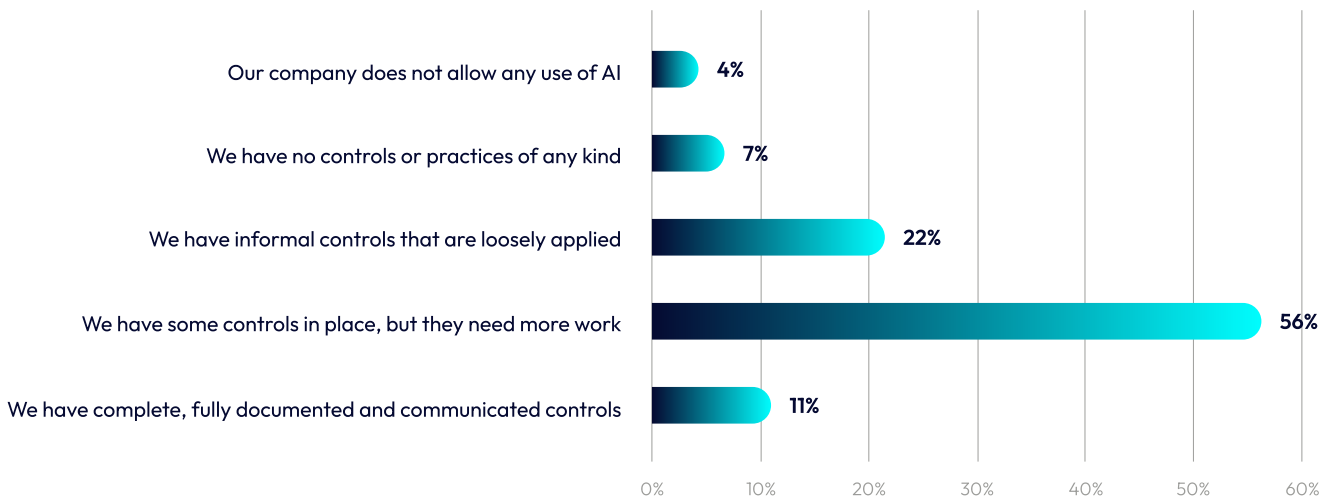
In your opinion, what types of identity-related use cases would benefit from artificial intelligence or machine learning (AI/ML) capabilities?



It's interesting to note that with the exception of niche environments, respondents see less benefit using AI for identity-related use cases. With the explosive growth in the use of AI, it would seem that we are using a tool much more in standard business use cases and faith in the technology has lost ground with identity experts.

The AI news is not all negative. Look at the progress in the chart below. Over half of the respondents have some controls in place for AI. A majority of those need work. An amazing 11% say they have all of the right controls in place. The bell curve is complete with the 11% that either have no controls or believe they have no AI use.

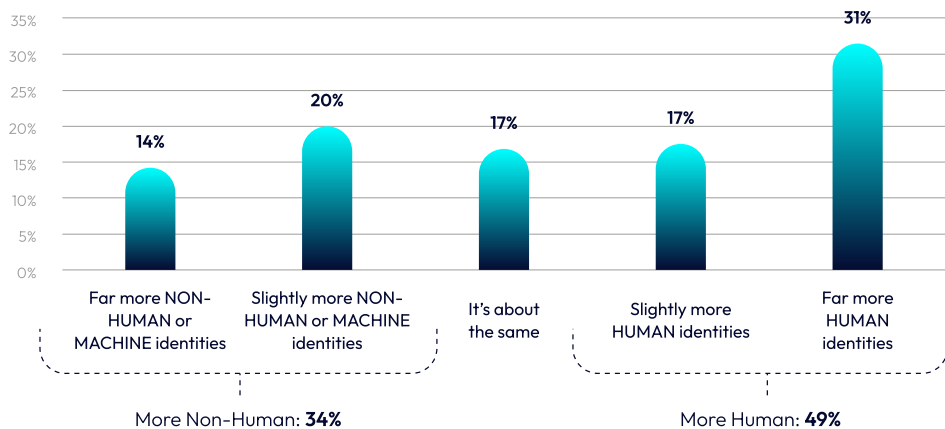
What controls has your company introduced around use of AI?



Non Human Identities/Machine Identities

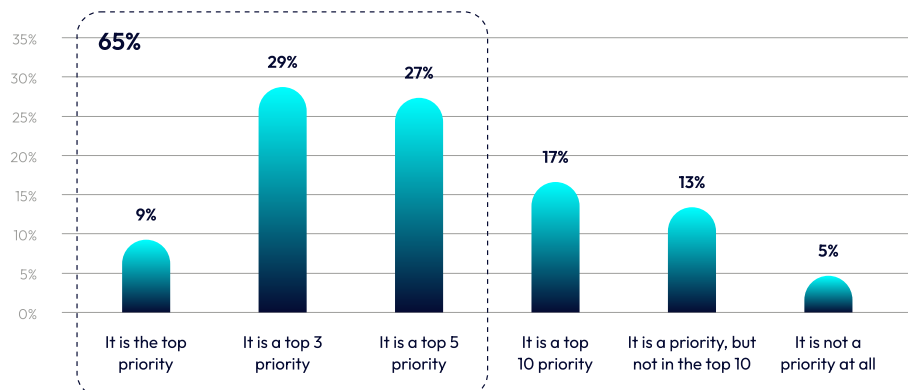
In general, NHIs outnumber human identities on the internet. I still don't think the robot overlords are about to rule us, you can breathe easy. NHIs can provide a wonderful lever in our systems so we can accomplish more than before.

To the best of your knowledge, how does the number of human identities at your company compare to the number of non-human or machine identities?



Tightly coupled with AI, NHIs drive Artificial Intelligence. Two-thirds of respondents see this and have made NHI management a top 5 priority in their plans. This is the beginning of a new era in identity management.

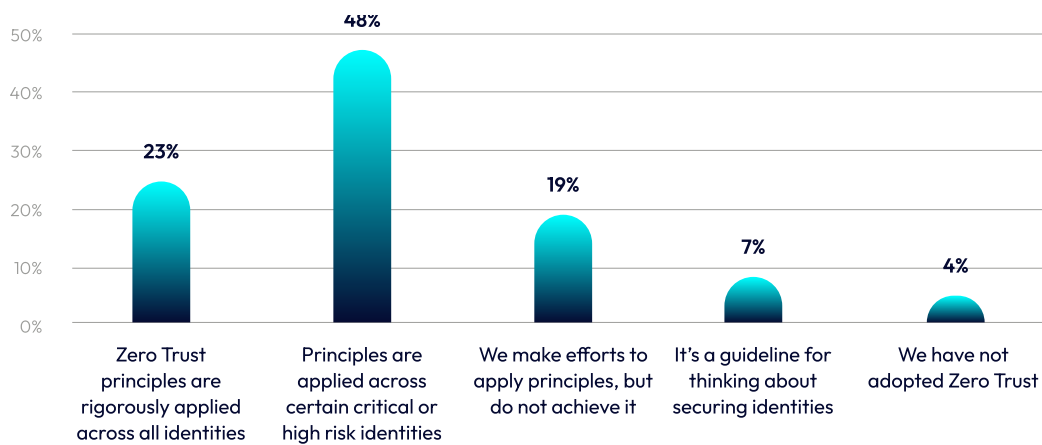
Where does managing non-human Identities (NHIs) or machine identities fit into your organization's priorities?



Zero Trust

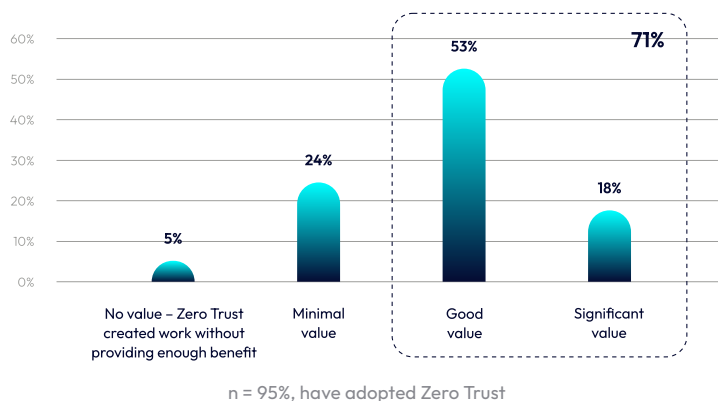
Zero Trust is now recognized as mainstream. The research outlines the prioritized approach to implementing Zero Trust so critical, high-risk identities can be better isolated and protected.

How extensively has your organization adopted the Zero Trust security framework for identities?

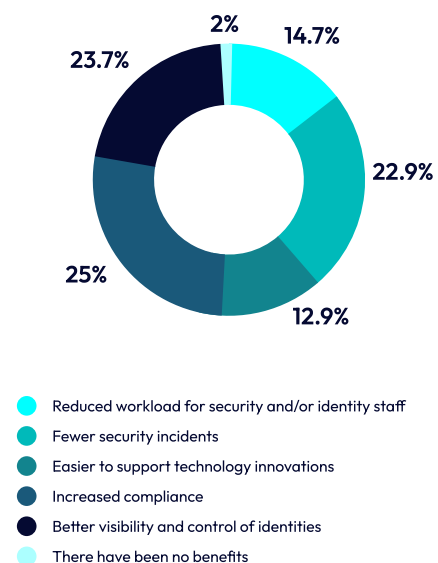


The obvious benefits of Zero Trust are being realized. This makes sense to most, and we will continue to track the acceptance of this framework.

In your opinion, what has been the ROI (Return-on-Investment) or business value achieved by investing in Zero Trust?



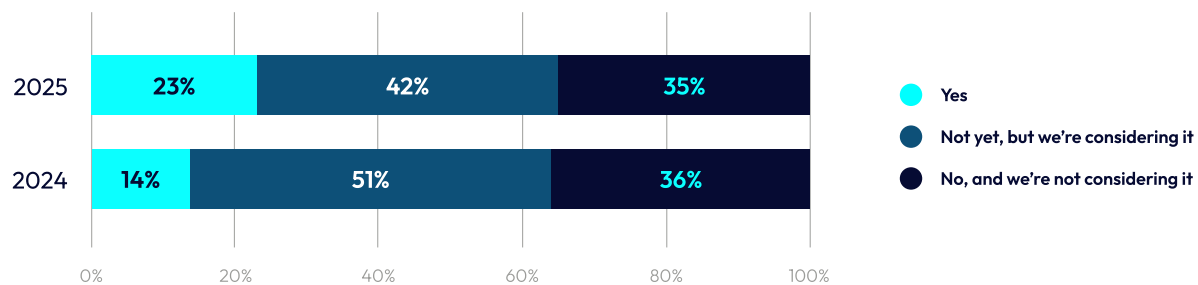
What benefits has your company achieved by investment in Zero Trust?



Digital Wallets

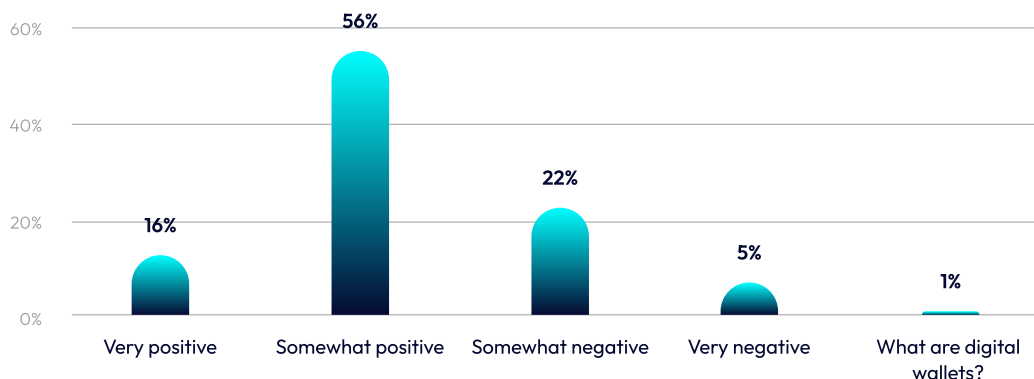
Digital wallets provide local control and access to digital identities. The survey shows us small growth in use. They are being used for some payments and government identities. Some cross-border identification is related to digital wallets.

Is your company investing in digital wallet technology or processes?



We don't often ask for personal opinions. We took this opportunity to gauge the individual interest in digital wallets. This will likely have an influence on organizational decisions in the long run. Close to three-quarters of the respondents feel positive about digital wallets.

What is your personal opinion of digital wallets issued by a neutral third-party such as a government or non-governmental organization (NGO) (i.e. passports, driver's licenses, payment services, or insurance cards delivered as digital credentials)?



Ongoing Challenges of Identity Security

Even with the good news, our research found that 91% of businesses still face barriers to identity security. Complexity leads the batch of barriers, with respondents continuing to cite complex environments (44%) at the top of the list, up slightly from last year (38%). This is often categorized as technical debt. Many of us operate in deficit.

What barriers prevent your company from doing more to secure identities?



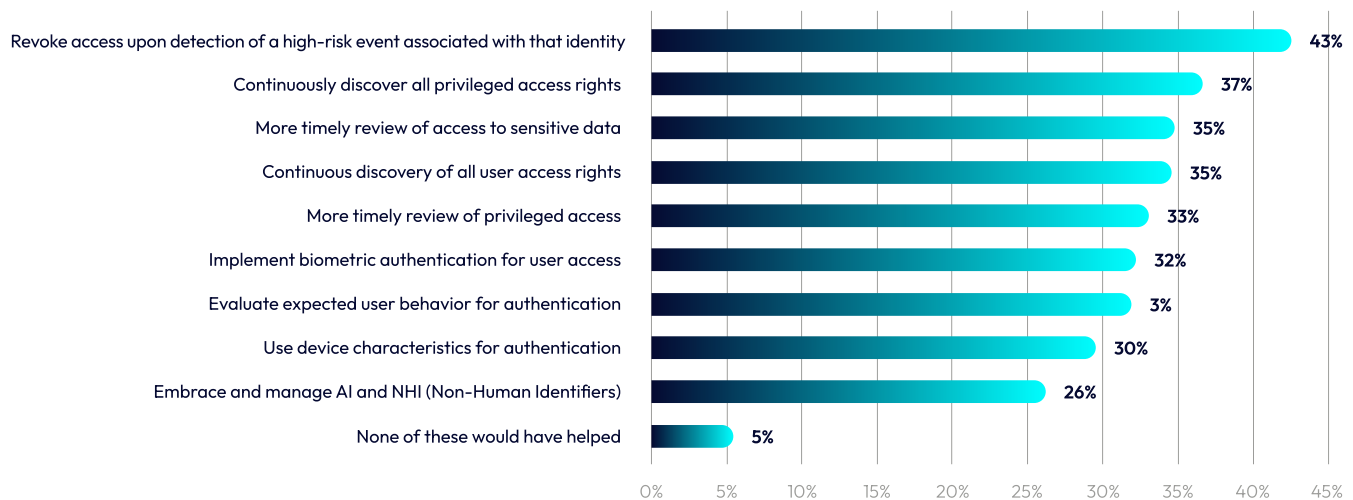
*Other: Merger & Acquisitions; Skilled personnel; Access for partners with unclear inflow and outflow of employees; Business prioritizes convenience over security; Determining the priority for remediation; Strict compliance rules

In the same vein and running a close second is the complexity surrounding identity frameworks (40%), significantly up from 2024 (30%). Ever-present budget shortfalls (32%) round out the top three, cited less often than in 2024 (38%). Next year's report might let us know if that is a result of the general economy or greater emphasis on security budgets.

Those saying that nothing prevents them from doing more to secure identities, because they have what they need, increased by 50% over 2024.

Based on the incidents reported, respondents continue to report that the foundational practice of revoking access upon detection of a high-risk event could be the most influential preventive measure.

Think back to the identity security incidents your company has experienced in the past year. Which of the following could have prevented those incidents if they had been more fully implemented?



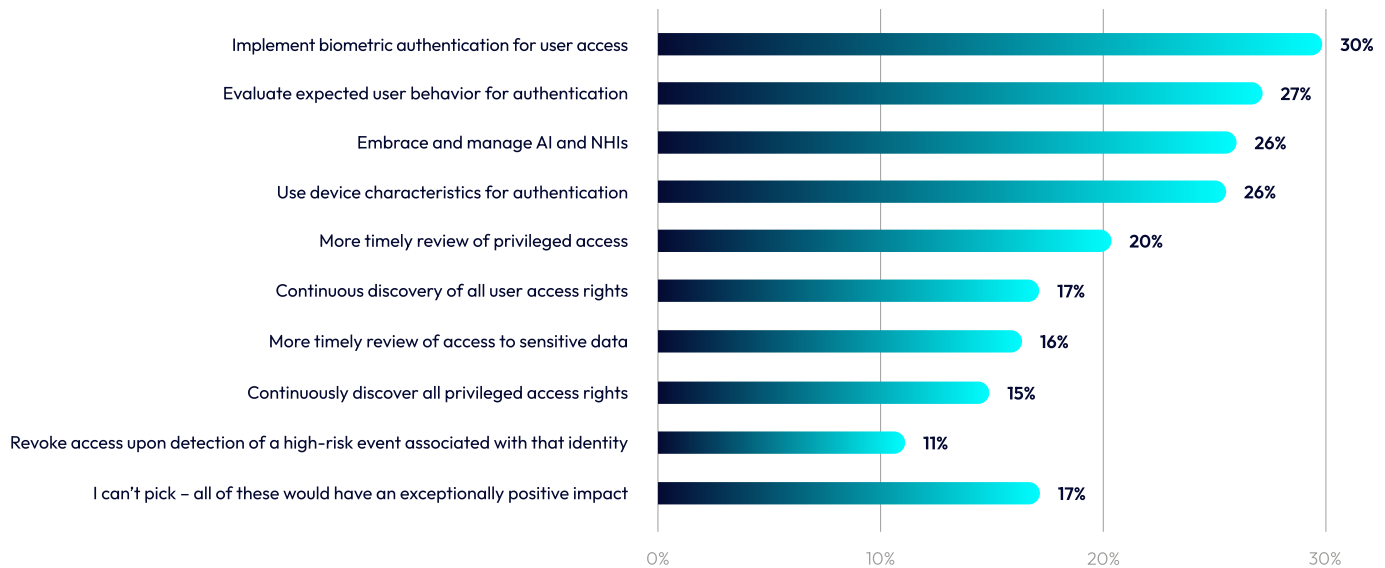
n = 86, have had an identity-related incident in the past year.

That is not to minimize the protective measures that focus on access reviews, whether specific, continuous, or just timely. Access control dominates the top six categories of measures that respondents believed could have prevented a security incident.

The percentage of general respondents identifying the steps that could have prevented an incident is slowly dropping every year, and that is more good news.

In 2026, IDSA will be looking at how vendors and their customers can work together to prevent more, continued incidents. The chart below gives us an idea of where to start that journey.

In your opinion, which of the following identity-related security outcomes would have the LEAST impact on identity security at your company in the coming 2–3 years?



Prioritize Securing Identities With IDSA

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

Continued involvement and investment from leadership teams continues to be required to help businesses address these threats. Companies must address the complexity of their systems and technology architectures and gain access to security expertise and standards to help them better manage their risk. The risk management needs to be embedded in all business processes. To do that, security teams need to ensure they have the right processes, tools, technologies, and communication to discover and respond to identity security threats in close to real time.

Find out more about the
trends in identity security.

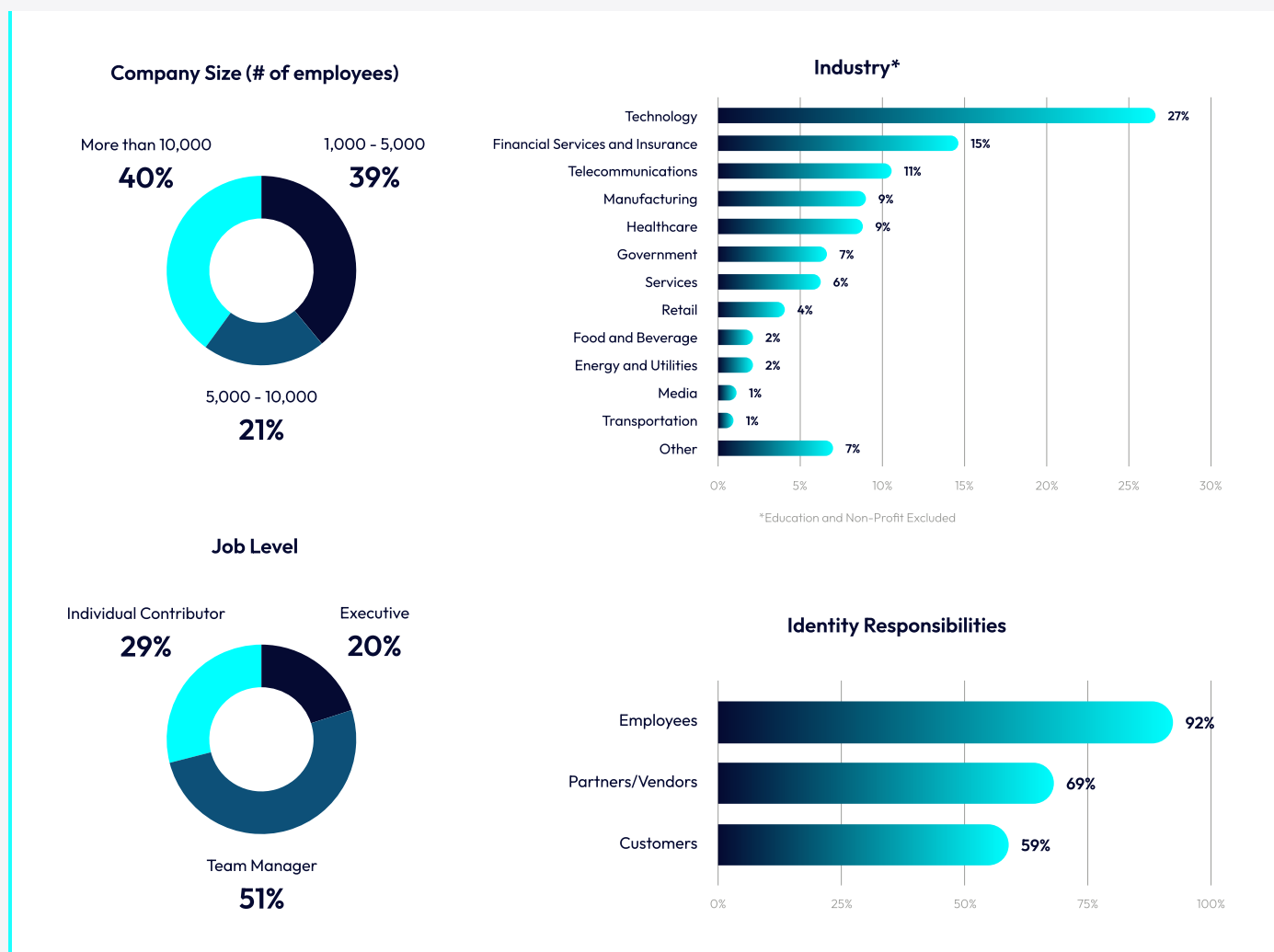
visit www.idsalliance.org

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 **512 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.



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.

Distribution is limited for use 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.