RSA

RSA.com

2026 RSA ID IQ Report

The RSA Identity Security Pulse Check

Table of Contents.

Executive summary.

The 2026 RSA ID IQ Report asked more than 2,000 global experts to detail how often identity security failed them, how much they lost when it did, and the vulnerabilities they dread the most.

What they told us was alarming: identity failed more organizations than last year, doing even more financial damage. Unless leaders act, the risks their organizations face will become more severe—and the consequences of those risks will cost them even more.

The data shows us a growing identity security gap, with most organizations still using old solutions that fail to adequately address new challenges. Most users still rely on passwords for authentication; their organizations report more frequent breaches and higher losses. At the same time, they are stymied in moving toward passwordless by complex operating environments and challenging use cases.

Organizations lack the capabilities they need to defend against social engineering and bypass attacks on their IT help desks, even as that tactic becomes a more alarming risk. And while organizations are monitoring human, machine, and service identities, it's clear from the rate of data breaches that they aren't using that information to proactively or effectively reduce risks.

Perhaps because of those growing risks, experts report that they're all in on AI for cybersecurity. Across sectors, more users believe that AI will do more to help cybersecurity than enable cybercrime, with more organizations than ever reporting plans to integrate some form of AI into their cybersecurity stack. Organizations also report by a large margin that agentic AI for cybersecurity will be the top capability they prioritize.

I'll let the findings speak for themselves. And while this information on its own is useful, it's essential that leaders act on it by prioritizing passwordless authentication, implementing modern methods to defend against help desk scams, proactively finding and resolving their identity risks before they become breaches, and using AI as a force multiplier to automate faster decision-making.

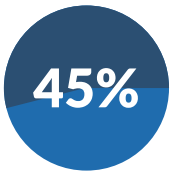
The first step in addressing any problem is admitting that there is one. The 2026 RSA ID IQ Report makes it clear that there are major concerns with most organizations' identity security. Identity simply fails too many organizations too often. The likelihood of a breach—and the cost of inaction—are simply too high to maintain the status quo.

Greg Nelson, CEO, RSA

2026 RSA ID IQ Report key findings

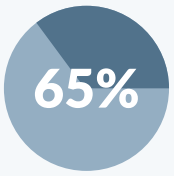
The 2026 RSA ID IQ Report shares information from 2,120 experts working in cybersecurity, identity and access management (IAM), IT, or other fields. Key findings include:

of organizations reported an identity-related breach in the last three years, a 27-percentage-point increase from 2025

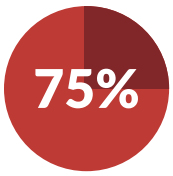


of organizations said that identity-related data breaches cost them more than the average data breach

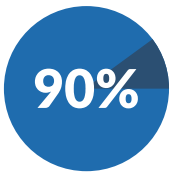
of organizations said that identity breaches caused them significant harm



of organizations said they were seriously concerned that their IT help desk or service desk would fail to stop a social engineering attack

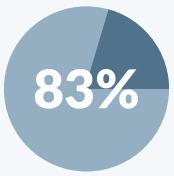


of organizations are operating in hybrid environments, a 5-percentage-point increase from 2025

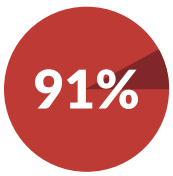


of organizations reported challenges in moving toward passwordless authentication

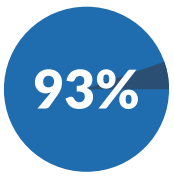
of organizations continue to use passwords as their primary method of authentication



of organizations believe AI will do more to help cybersecurity than cybercrime, a 3-percentage-point increase since 2025



of organizations plan to implement some form of AI into their tech stack over the next year, a 12-percentage-point increase since 2025



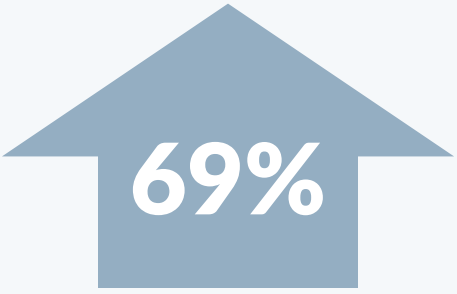
of organizations have not reached optimal Zero Trust maturity

More identity breaches caused even more damage this year

Analysis of the survey responses found that organizations suffered more breaches resulting from identity security failures this year: 69% of organizations reported a breach in the last three years, a 27-percentage-point increase since the 2025 RSA ID IQ Report.

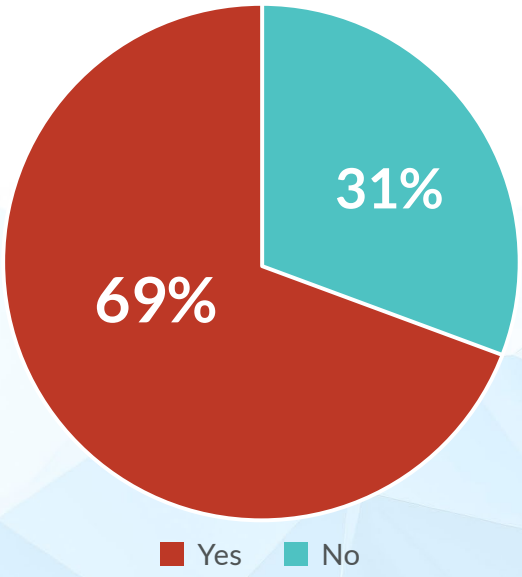
In addition to occurring more frequently, those breaches did greater damage and had higher costs. More than a fifth (21%) of all respondents reported that a breach caused by identity cost them between $5-10 million, while nearly a quarter (24%) reported that the cost of an identity breach exceeded $10 million. Breaches costing more than $10 million rose by three percentage points as compared to last year's report.

Those are alarming numbers by any measure. They're particularly concerning when compared with the global average cost for a data breach resulting from any attack vector: the IBM Cost of a Data Breach Report 2025 found that an average breach costs $4.44M. When identity fails, it costs organizations considerably. It's no wonder that 70% of all respondents rated the severity of a breach as a four or five out of a five-point scale.



of organizations reported experiencing an identity-related breach in the last 3 years, a **27-percentage-point increase from 2025**

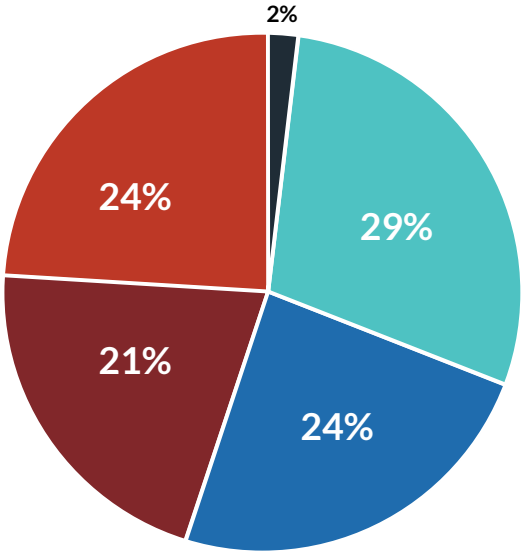
Did your organization experience an identity-related **breach in the last three years?**



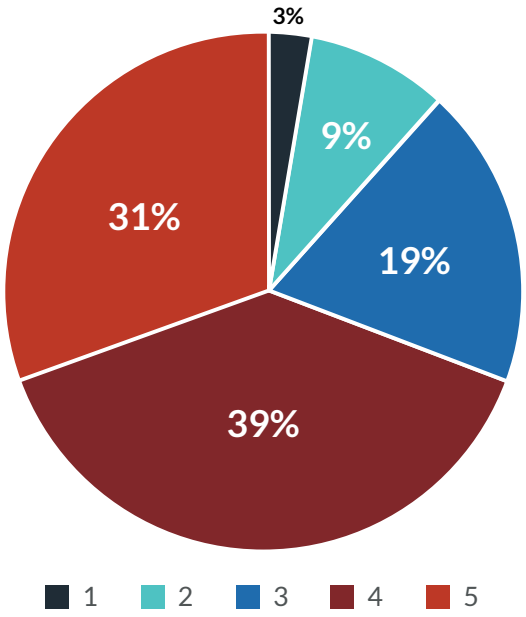
24%

of organizations experiencing an identity-related breach said the breach cost **$10M+, a 3-percentage-point increase from 2025**

How much money do you believe your organization lost because of identity-related data breaches over the last three years?



If you experienced an identity-related breach within the last three years, rate the severity of its effect on your organization from 1 to 5.



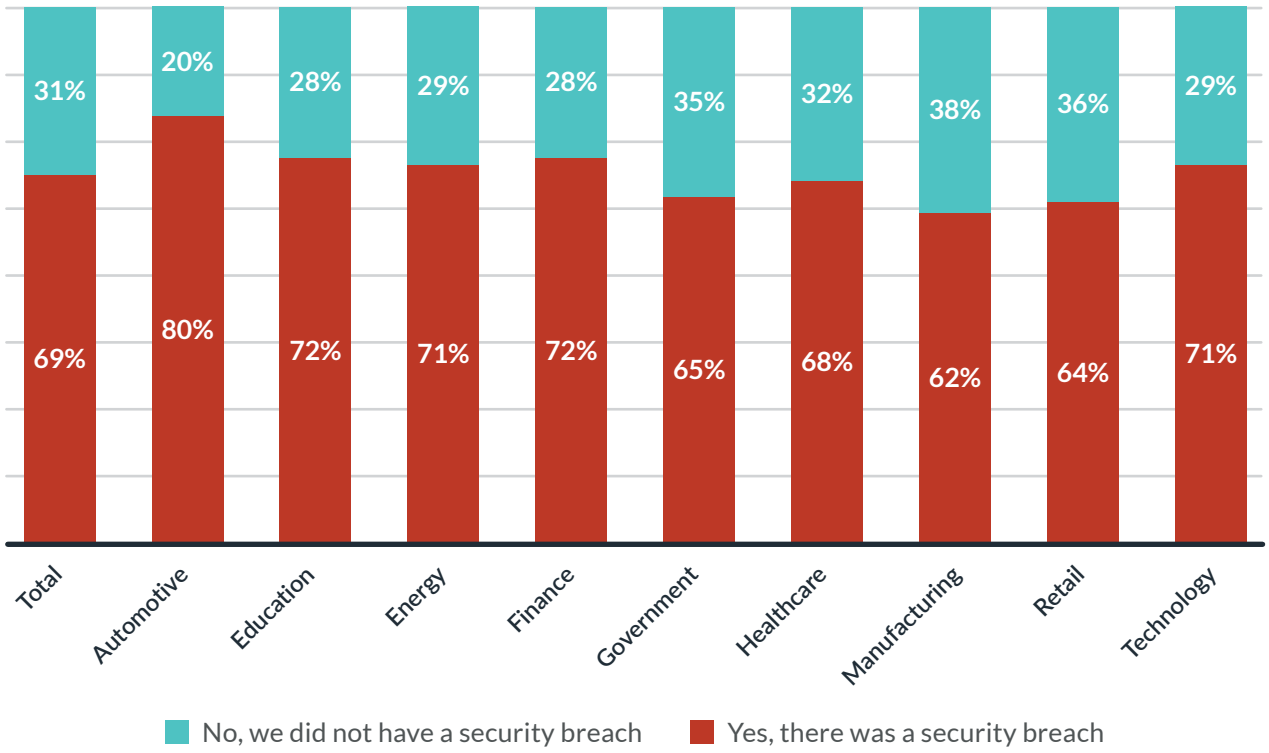
$4.44 Million

Global average for cost of all data breaches, per the **IBM Cost of a Data Breach Report 2025**

Security breaches by sector

Examining the rates of data breaches by sector, the automotive industry (80%), finance (72%), energy and utilities (71%), and technology (71%) reported the highest frequency of data breaches. Retail (64%) and manufacturing (62%) represent the least attacked sectors by industry.

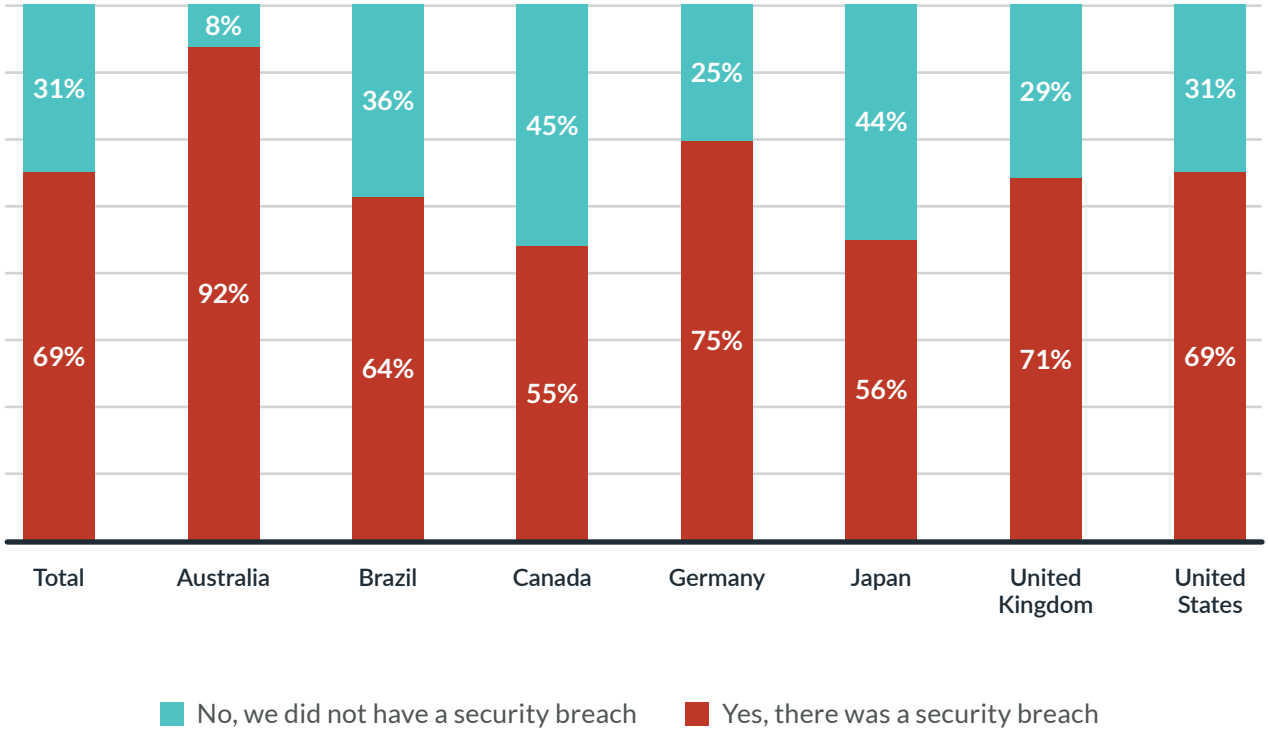
By sector: Did your organization experience an identity-related breach in the last three years?



Security breaches by country

By country, Australia (92%), Germany (75%), the United Kingdom (71%), and the United States (69%) reported the most frequent identity-related breaches in the last three years, while Japan (56%) and Canada (55%) reported the fewest instances. We explain later in the report how certain practices correlate with the frequency and impact of these breaches.

By country: Did your organization experience an identity-related breach in the last three years?



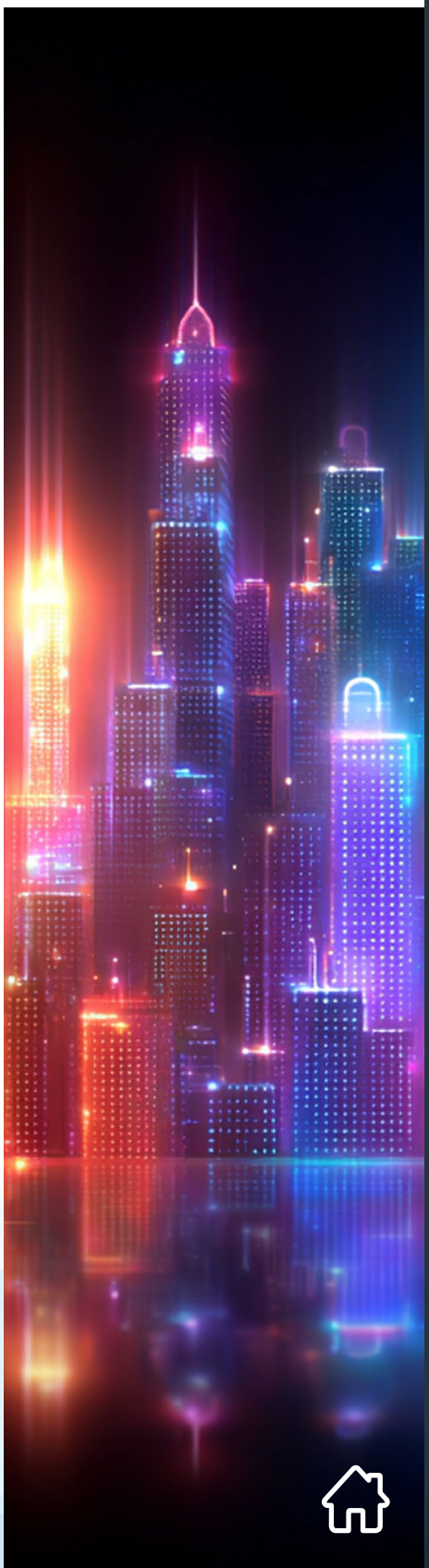
Zero Trust “progress”

While only 7% of organizations report that they have reached optimal Zero Trust maturity for identity as defined by CISA, the majority—57%—believe that they’ve reached the “Advanced” Zero Trust stage, which includes:

- Phishing-resistant MFA
- Consolidation and secure integration of identity stores
- Automated identity risk assessments
- Need/session-based access

That confidence is contradicted by the fact that **69% of organizations were breached**, and **70% reported that those breaches were severe.**

That’s not to dissuade organizations from trying to mature their Zero Trust stance—quite the contrary. Instead, the gap between where organizations think they are on their Zero Trust journey and the frequency with which they’re breached should be a warning to security leaders to do more to protect themselves.



The cybersecurity risks that keep experts up at night

Respondents selected phishing as the threat vector that poses the most significant cybersecurity risk for their organization. And there's good reason to prioritize phishing: year to year, phishing (which leads to stolen credentials) and the use of stolen credentials remain among the most frequent and highest-impact attacks. One of the best ways to avoid phishing is to remove the credentials that phishers attempt to steal: rather than use shared secrets, organizations should strive to implement phishing-resistant, passwordless authentication.

192 days

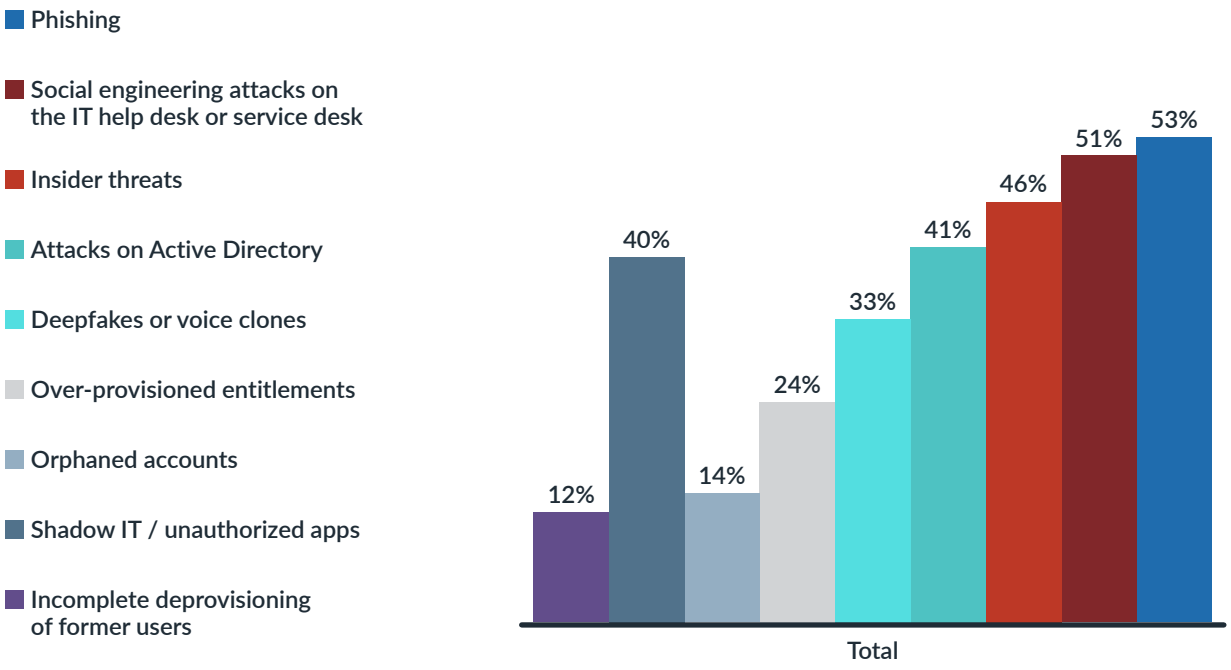
Average time it takes organizations to identify and contain a breach originating from phishing

$4.8 Million

Average cost of data breaches originating from phishing

IBM Cost of a Data Breach Report 2025

While phishing is a perennial cybersecurity risk, emerging cybersecurity risks are quickly gaining ground as significant risks. 51% of respondents said that social engineering attacks on the IT help desk or service desk were the most significant risk for their organization.



Your help desk needs help

Given the headline-grabbing help desk attacks on MGM Resorts, Ceasars Entertainment Group, Marks & Spencer, Co-op, and House of Dior, there's good reason to prioritize this risk. As Scattered Spider and other cybercriminal groups have shown, there's significant risk when cybercriminals attempt to bypass multi-factor authentication (MFA) by calling an IT Help Desk or service desk posing as a legitimate user, and asking the help desk to create new accounts, suspend MFA, or enroll new users or devices. In fact, cybersecurity experts specifically ranked social engineering attacks on IT help desks as the top risk facing their organization.

Compounding this risk is that organizations simply aren't using newer, phishing-resistant methods to assure users' identities. Most organizations use older methods to authenticate users: 58% of organizations use passwords, 50% use OTP, and 46% use shared secrets. Comparatively, only 36% reported using bi-directional authentication, which allows both parties to verify one another, and only a quarter (25%) reported using risk-based solutions to help them prioritize users and use cases.

Older methods for assuring users' identities

58% of organizations use passwords

50% use OTP

Newer methods for assuring users' identities

36% use bi-directional identity assurance

25% use risk-based solutions

Who's calling?

Since 2023, BlackCat, ALPHV, Scattered Spider, and other cybercriminal groups have socially engineered organizations' IT help desk personnel to launch MFA bypass attacks, causing significant damages and losses:

MGM Resorts: $145M

Caesars Entertainment: $15M

Marks & Spencer: £300M

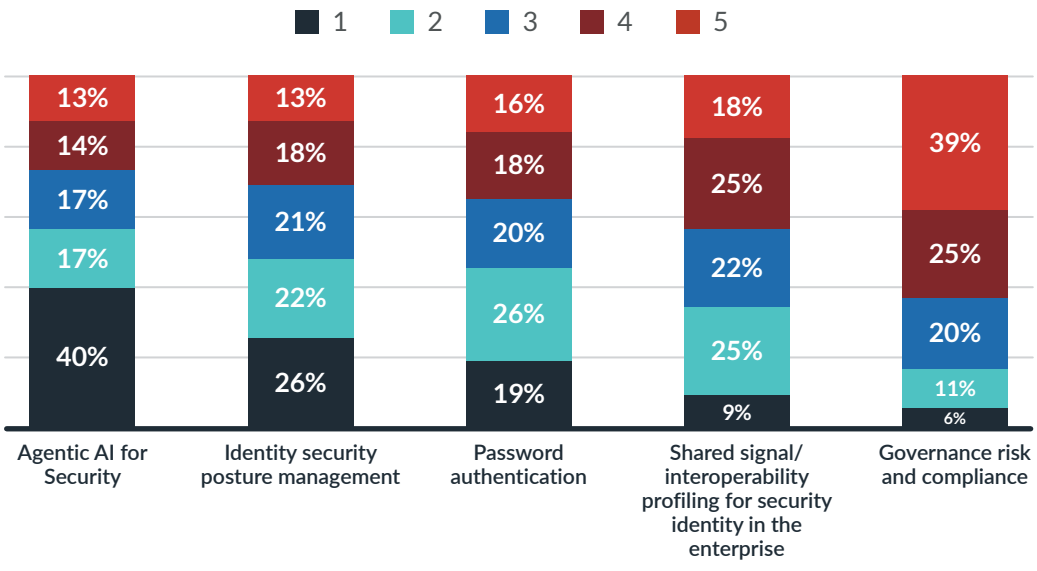
One-third (33%) of users said new techniques like deepfakes or voice clones posed the greatest risk to their organization. Those tactics may prove more effective without modern methods of preventing MFA bypass attacks.

Some of the other risks experts fear the most cluster around identity lifecycle stages and entitlement creep. Insider threats (46%), shadow IT and unprovisioned apps (40%), and over-provisioned entitlements (24%) stand out as priority risks among users. These issues can be exacerbated by inadequate visibility into identity risk, manual identity lifecycle processes, and retroactive risk mitigation.

The cybersecurity capabilities users prioritize

Agentic AI for security was the top choice among users by a wide margin, with 40% of respondents placing it as their number-one priority. Identity security posture management (ISPM)—a new cybersecurity framework that enables organizations to manage risk, enforce policy, and strengthen compliance across increasingly complex environments—was listed as the second most critical capability, ranking as the top choice among 26% of respondents.

Rank the following cybersecurity capabilities from 1 to 5.



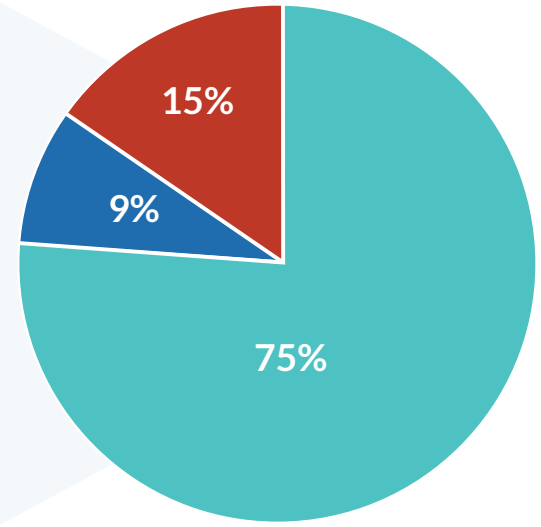
Operating environments

Most organizations operate in hybrid environments, using a mixture of both cloud and on-premises resources. Businesses must ensure that all users, devices, entitlements, and environments are adequately secured.

In which of the following environments do you support applications and users?

75%

of organizations operate in hybrid environments, **a 5-percentage-point increase since last year**



Hybrid (cloud and on-premises) Cloud only On-premises only

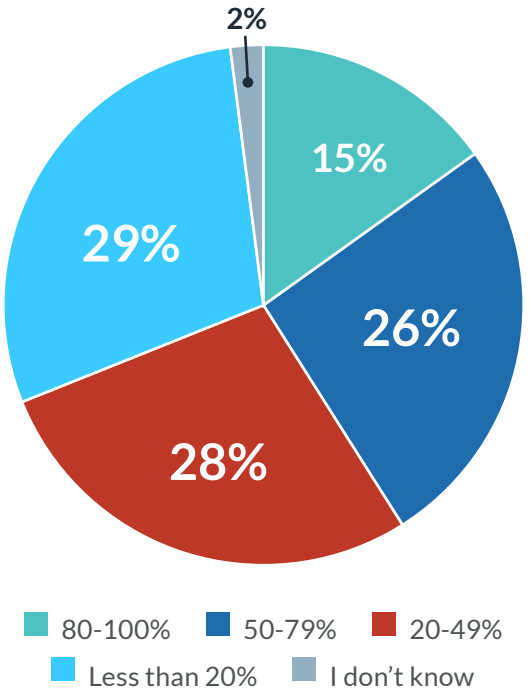
Passwords—and password risks—persist

Most organizations do not use passwordless as their primary authentication method. That's great news for cybercriminals: year to year, the use of stolen credentials is the leading cause of data breaches.

Complex environments and mixed-use cases and user groups make it a challenge for organizations to deploy comprehensive passwordless.

The persistence of password-based authentication correlates with more frequent and more costly data breaches. Australian organizations reported one of the lowest rates of passwordless adoption by country with 50% still in the earliest stage of adoption. Australian organizations also suffer the highest rate of identity-related data breaches by country (92% of organizations reported a breach in the last three years), the most severe consequences (47% said the breach caused major harm), and the most financial losses (44% reported a breach cost them more than $10 million).

What percentage of your users primarily use passwordless form factors to complete authentication?



Contrast those findings with Japan, which reported the highest instance of using passwordless as the primary authentication method (37% of organizations said they used it at least 80% of the time). Japan also reports one of the lowest rates of identity-related data breaches (56% of organizations) and less severe outcomes.

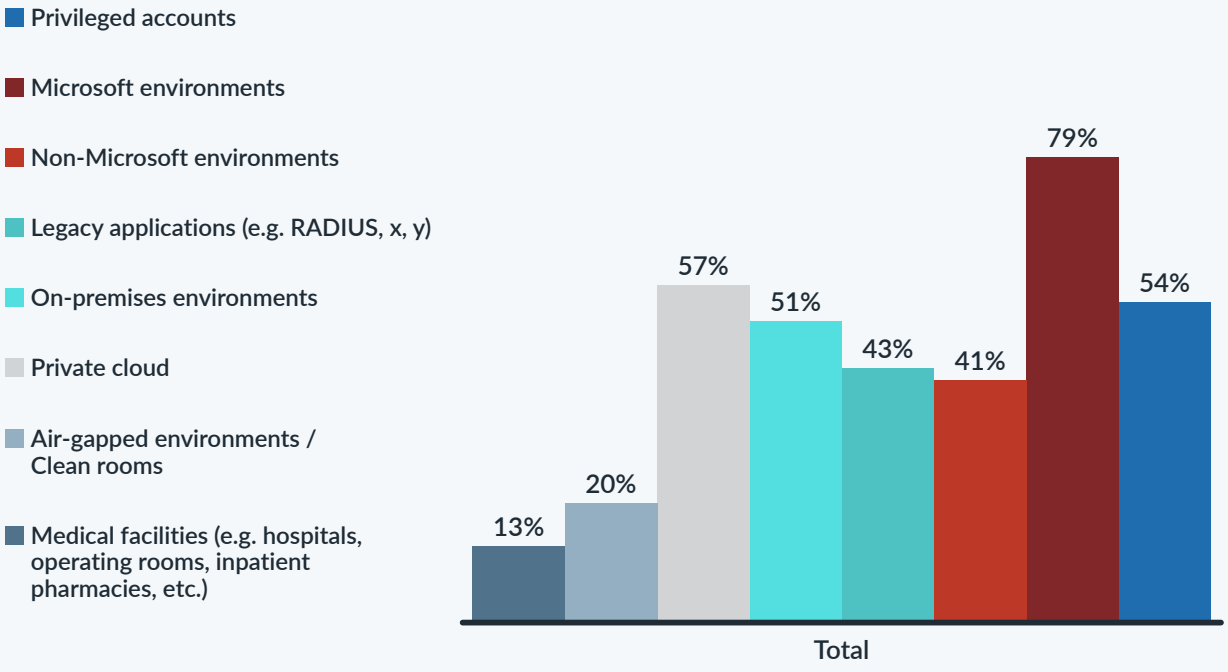
	Australian organizations	Japanese organizations
Ranking in overall passwordless use, by country	#5	#1
Percentage of users who use passwordless as their primary form of authentication	10%	37%
Reported a breach	92%	56%
Percentage who reported the breach as causing major harm (5 out of 5)	47%	44%
Percentage of breaches that cost more than $10M	24%	28%

> **"Complex environments and mixed-use cases and user groups make it a challenge for organizations to deploy comprehensive passwordless."**

What's slowing passwordless down?

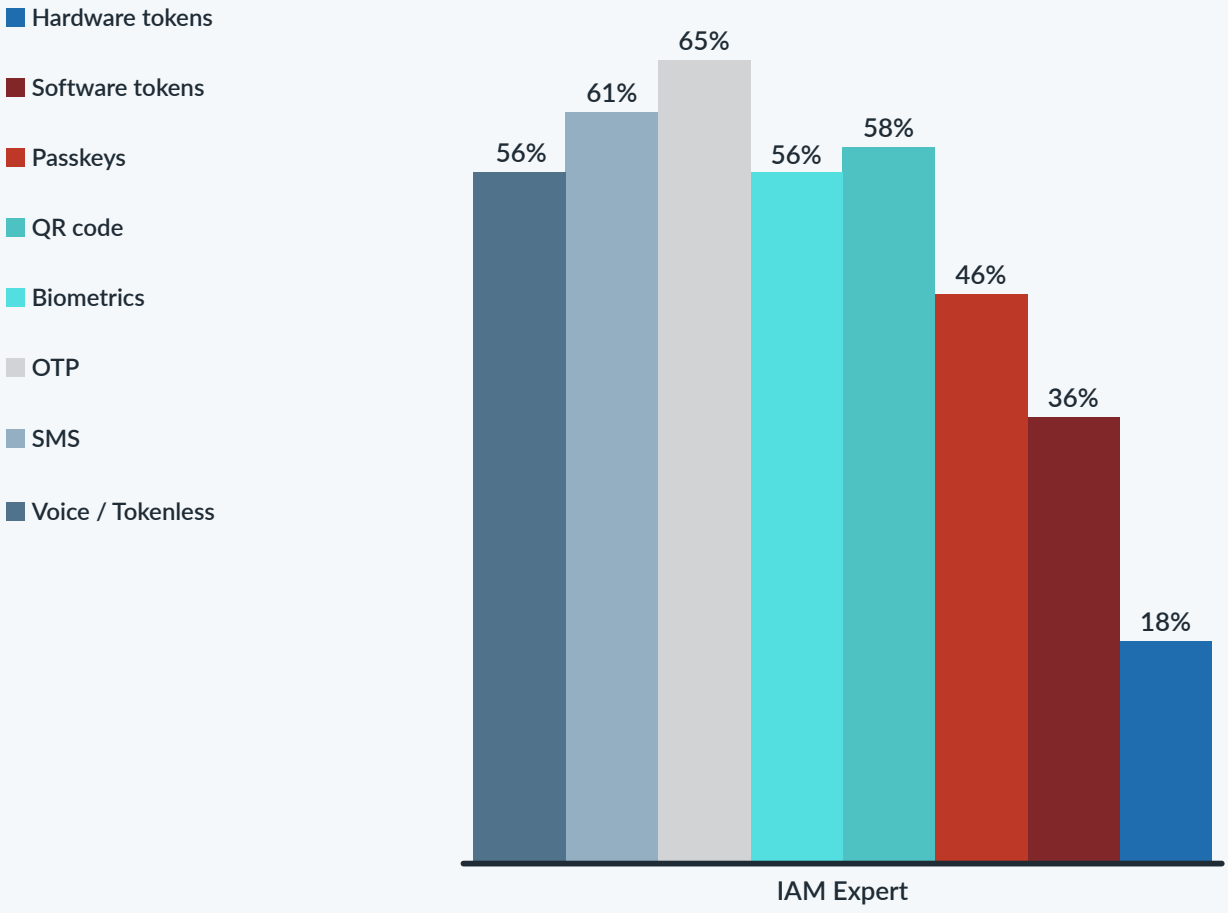
When it comes to deploying passwordless, most organizations must account for a wide range of users and use cases. We believe that this is proving to be a significant challenge for organizations, as passwordless still lags.

Which of the following environments, user groups, or use cases does your organization support?



Because most organizations operate in hybrid environments and must support diverse users and use cases, identity specialists are preparing to use a diverse range of form factors to provide every user with passwordless authentication.

Which of the following form factors do you intend to use to implement passwordless solutions?



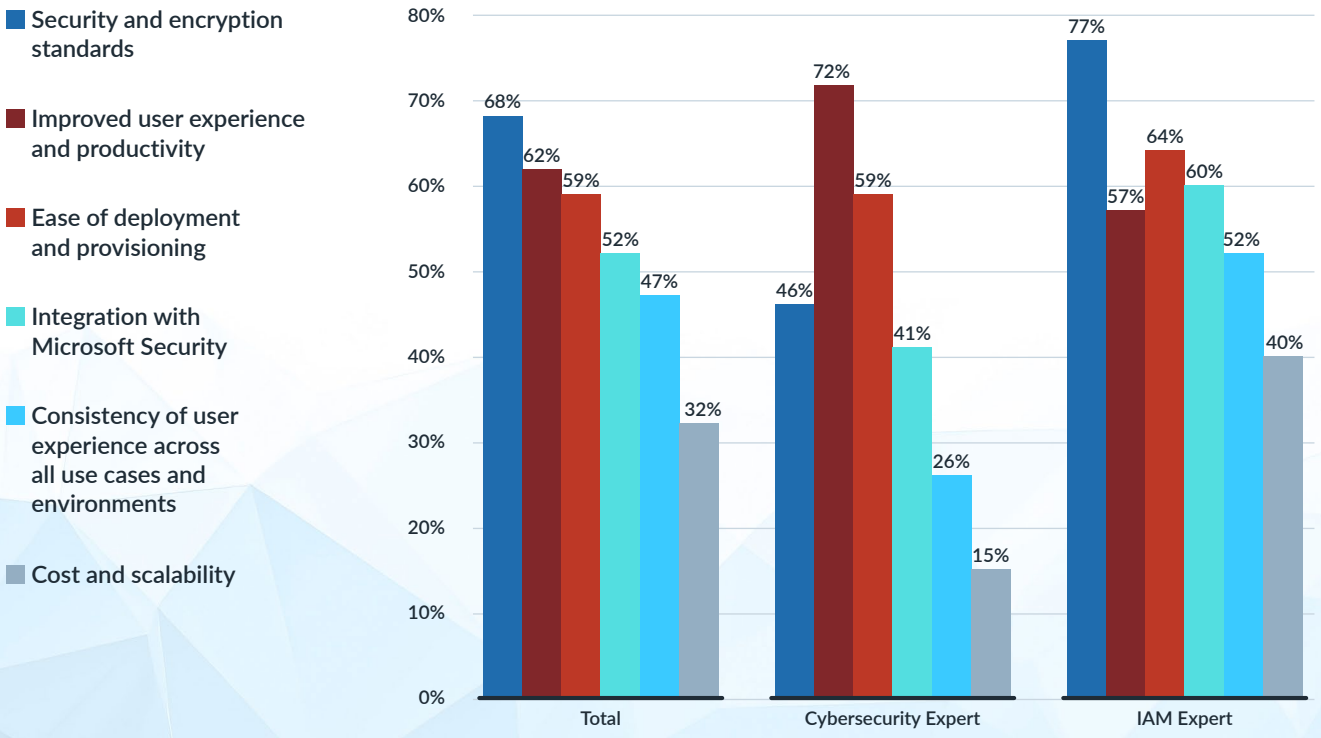
The struggle for passwordless

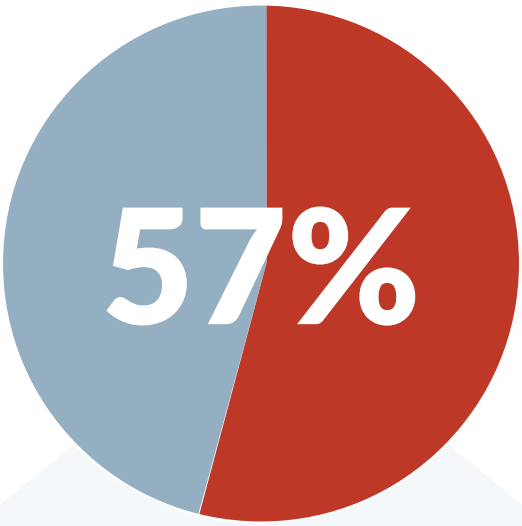
Nearly all (90%) of respondents said there was some challenge slowing them down in deploying passwordless solutions. But for these users, there's not one specific challenge that they must address. Instead, there are three: 57% of respondents said security concerns were slowing passwordless, 56% cited concerns about user experience, and 52% said a lack of complete platform support (including legacy apps and third-party systems) was the main challenge in preventing them from rolling out passwordless.

These are all vital concerns that organizations must overcome to implement passwordless effectively. Interestingly, more practical constraints are much less of an issue: only 47% of users said they didn't have the money to deploy passwordless.

There's no one clear challenge that organizations should address. To address experts' different passwordless priorities (and to overcome the challenges preventing them from deploying passwordless), businesses must balance security and encryption standards, improved UX, and ease of use.

What factors are most important to you in selecting a passwordless solution?





Of organizations do not use passwordless as their primary means of authentication

New year, same problem

Year to year, passwords are a leading cause of data breaches:

2025 Verizon Data Breach Investigations Report: Credential abuse "is still the most common vector."

2024 Verizon Data Breach Data Breach Investigations Report: "Over the past 10 years, stolen credentials have appeared in almost one-third (31%) of breaches."

2023 Verizon Data Breach Investigations Report: "Credentials have really gained ground over the past five years, as the use of stolen credentials became the most popular entry point for breaches."

2022 Verizon Data Breach Investigations Report noted that poor password practices were "one of the leading causes of data breaches" every year for the past fifteen years.

Identity risk monitoring and management

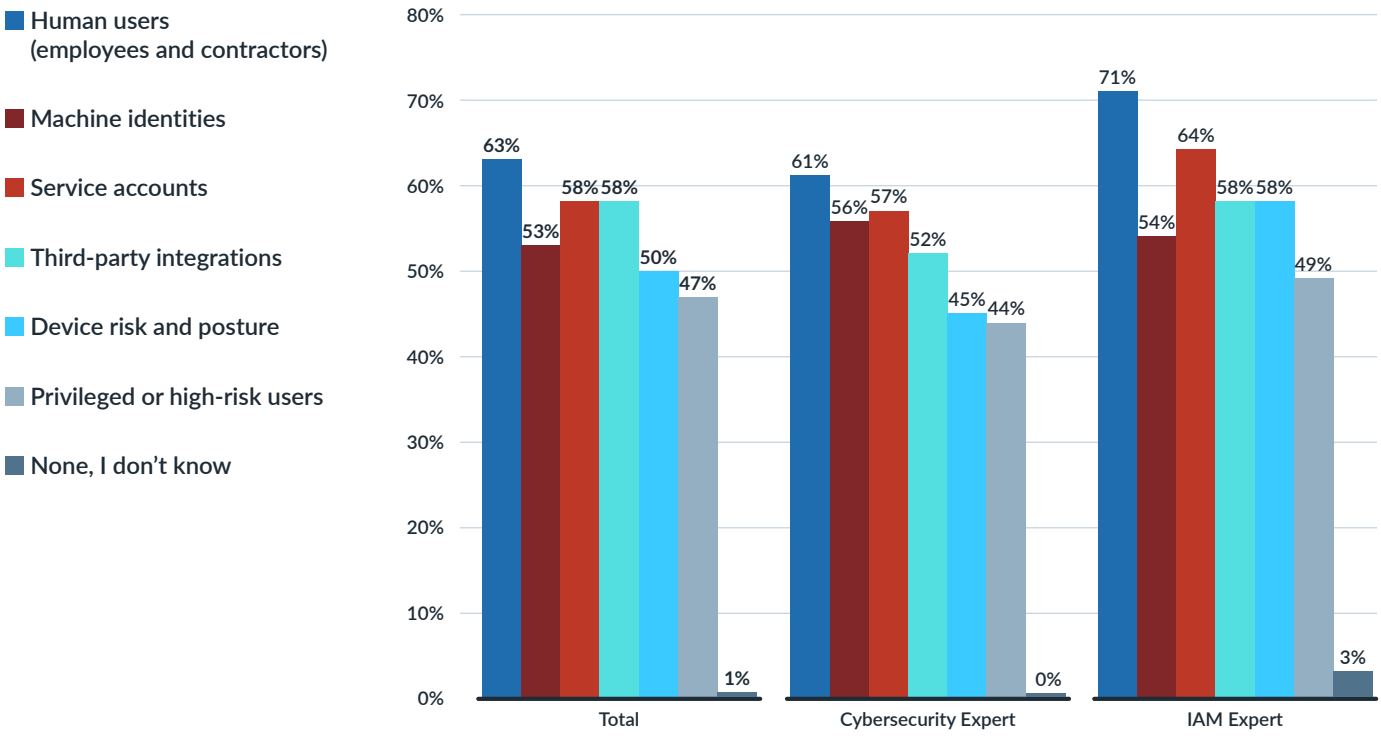
Organizations show a high rate of monitoring for identity risk across users and types, with most respondents saying that they monitor human users, machine accounts, service accounts, and third-party integrations, and half saying they also monitor device risk and posture. IAM experts are more likely to monitor these accounts for identity risk than their cybersecurity peers are.

It's encouraging that organizations are addressing the breadth of their identity attack surface. But integrating all that information—and using it effectively—will be a challenge. With thousands of entitlements per account, there's a considerable amount of noise that security teams will need to parse to find risks and prioritize actions.

That enormous dataset may be driving respondents' cybersecurity investment priorities: more than a quarter (26%) of respondents said that ISPM was their top priority. ISPM can help organizations assess their access exposure and prioritize actions to limit risks.

One example of why organizations need ISPM to find the signal in the noise and reduce risk is machine identities. Organizations that monitor for machine identities reported the most frequent breaches with the greatest impact and losses. Nearly three quarters (72%) of organizations that monitor machine identities reported an identity-related breach in the last year. Those organizations also reported the most harm from those breaches, with 34% saying the breaches did significant harm, and the most catastrophic losses, with 27% reporting losses of more than $10 million.

Which areas are you actively monitoring or scoring for identity risk?

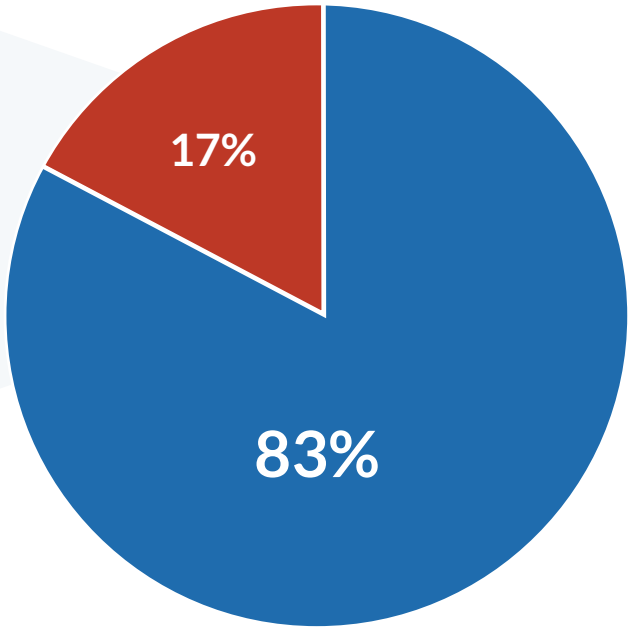


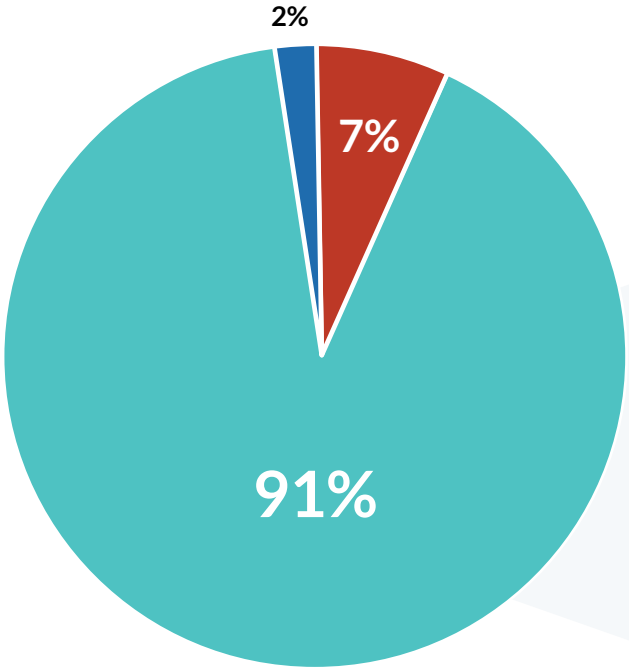
AI for cybersecurity

There is growing acceptance that AI will do more to help security than empower cybercrime, with 83% of users saying that the technology represents more of an asset to organizational defense than to adversaries. Likewise, 91% of respondents said they planned to implement AI in their tech stack over the next year, a 12-percentage-point increase since last year's survey.

These responses align with what users said would be their priority among cybersecurity capabilities: 40% of respondents put agentic AI for security as their top choice, the most of any feature.

Over the next five years, do you expect AI to do more to help organizations with cybersecurity or to enable threat actors?



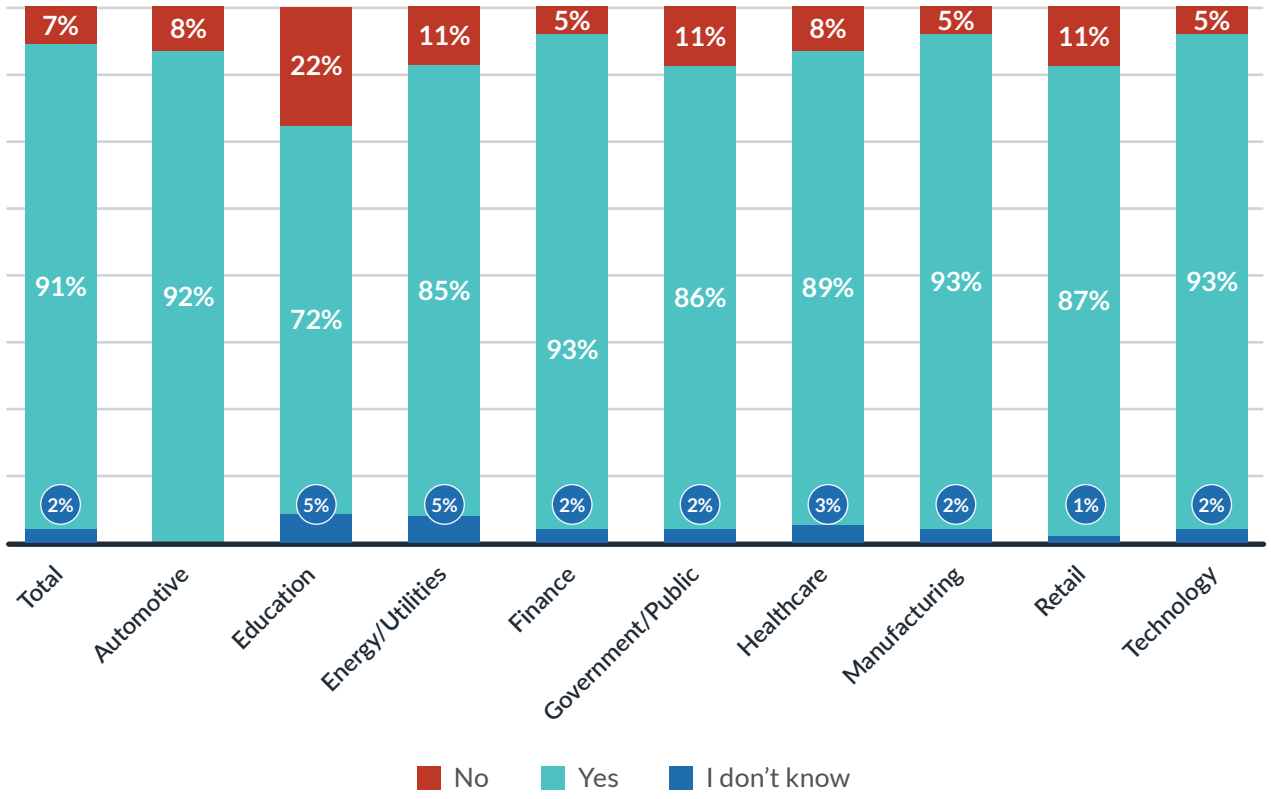


Does your organization have plans to implement automation, machine learning, or other forms of AI as part of its cybersecurity stack in the next year?

No Yes I don't know

By sector, nearly every industry reports a high likelihood of implementing some form of AI into their tech stack over the next year. Finance (93%), manufacturing (93%), technology (93%), and the automotive industry (92%) all reported high levels of integrating AI in their tech stack. Education (72%) reports the lowest levels of implementing AI.

By sector: Does your organization have plans to implement automation, machine learning, or other forms of AI as part of its cybersecurity stack in the next year?



Methodology and sample

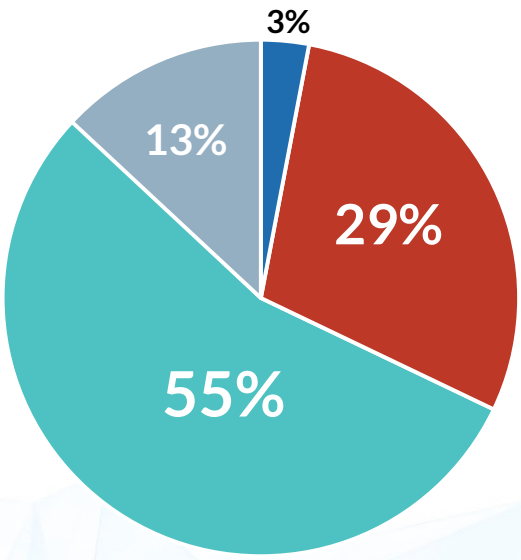
RSA shared the 2026 RSA ID IQ Survey from July 20, 2025 to August 15, 2025, asking users to respond to 26 questions about their cybersecurity priorities, the risks their organizations face, the frequency and impact of identity-related data breaches, and other factors in the identity space. In that time, we received 2,120 responses from Australia, Brazil, Canada, Germany, Japan, the United Kingdom, and the United States.

Respondents were asked to identify their role in their organization, the sector in which they worked, and the size of their organization.

RSA reviewed all responses, correlating some answers with others to see if there were any relationships between answers.

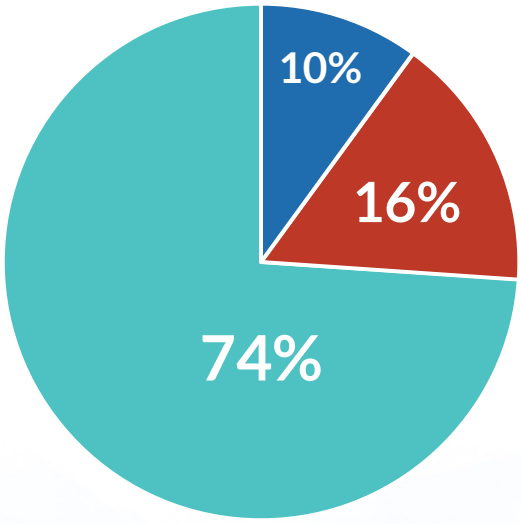
2026 RSA ID IQ demographics

Role in organization

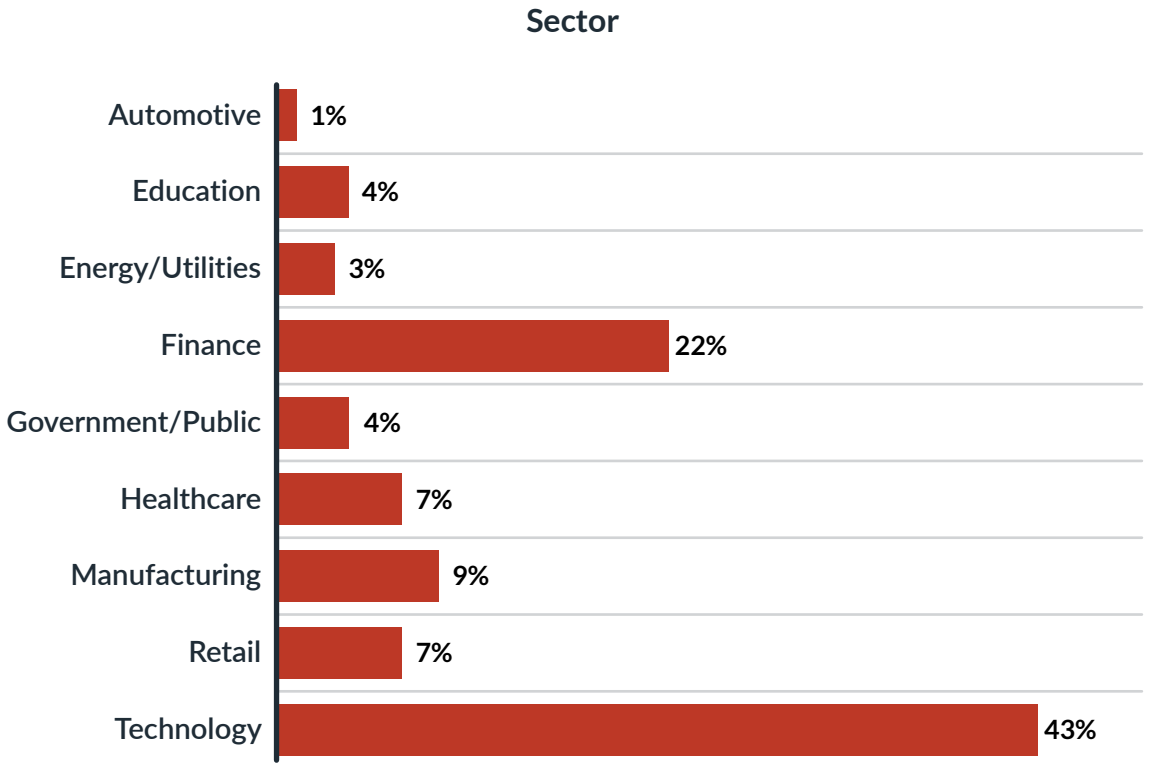


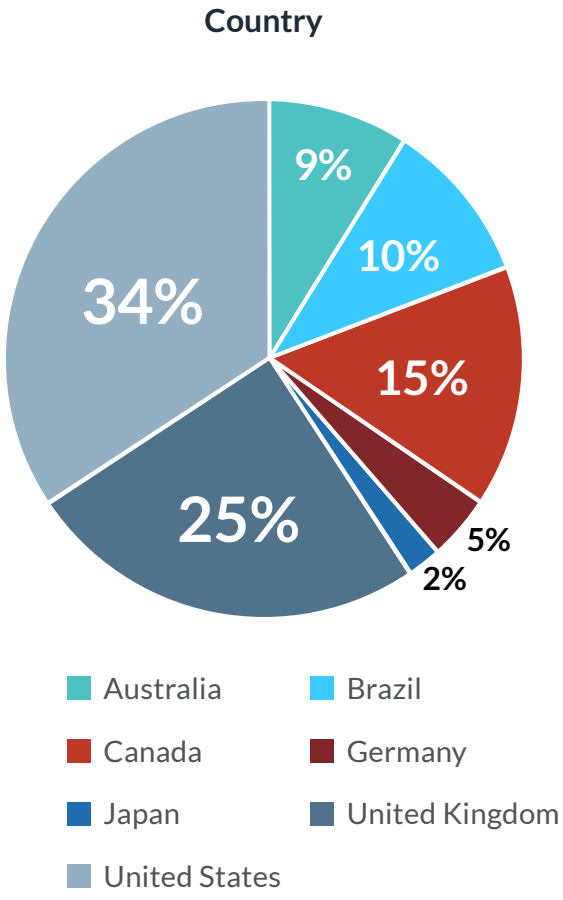
- Compliance or Risk Officer
- Cybersecurity Expert
- IT Decision Maker or Architect
- IAM or Identity Expert

Organization Size



- 2,500 - 4,999
- 5K - 9,999
- 10K+


Sector
Automotive
1%
Education
4%
Energy/Utilities
3%
Finance
22%
Government/Public
4%
Healthcare
7%
Manufacturing
9%
Retail
7%
Technology
43%


Country
9%
10%
15%
5%
2%
25%
34%
Australia
Brazil
Canada
Germany
Japan
United Kingdom
United States

From information to action

The first step in fixing any problem is admitting there is one. The 2026 RSA ID IQ Report demonstrates that identity is a significant problem for many organizations that leads to high-cost, high-impact data breaches.

Organizations should prioritize the capabilities that can keep them secure, including:

- Passwordless authentication that works for every user, in every environment, every time
- ISPM to find risks and recommend action
- Cross-environment support capable of protecting cloud, hybrid, and on-premises users
- Bi-directional identity verification to defend the IT help desk and users from MFA bypass attacks and social engineering
- Automated identity intelligence to dynamically assess risk and automate responses

Contact RSA to demo these capabilities. Or see why the world's most secure organizations are secured by RSA: start your free, 45-day trial of RSA ID Plus now.

About RSA

RSA provides mission-critical cybersecurity solutions that protect the world's most security-sensitive organizations. The RSA Unified Identity Platform provides true passwordless identity security, risk-based access, automated identity intelligence, and comprehensive identity governance across cloud, hybrid, and on-premises environments. More than 9,000 high-security organizations trust RSA to manage more than 60 million identities, detect threats, secure access, and enable compliance.

For additional information, visit our website to contact sales, find a partner, or learn more about RSA.