fido ALLIANCE | simpler stronger authentication

The State of Passkeys 2026:
Global Consumer and Workforce Report

www.fidoalliance.org

Executive Summary

Passkeys have reached global scale with 5 billion passkeys now in active use. Across both consumer and workforce environments, awareness is now near-universal and adoption has followed: 90% of consumers are familiar with passkeys, and 75% have enabled them on at least some accounts.

In parallel, workforce deployment is approaching mainstream levels, with 68% of organizations deploying, piloting, or rolling out passkeys for employee authentication.

However, passwords remain widely used in parallel.

Among consumers, passwords continue to introduce measurable risk and friction at scale. One-third experienced an account compromise or breach notification in the past year, and nearly half will abandon a sign-in or purchase when they cannot remember a password. In workforce environments, even among organizations that have deployed passkeys, 57% still rely on phishable authentication methods for primary day-to-day sign-in. Deploying passkeys and eliminating passwords are not the same, and many organizations are still bridging that gap.

Despite this, the direction of travel is clear. Organizations further along in deployment report tangible results: 47% improved security posture, 45% faster login times, and 35% reductions in helpdesk costs. These outcomes directly validate the core drivers behind adoption: stronger phishing resistance, improved user experience, and operational efficiency.

The remaining barriers are increasingly well understood. Legacy system compatibility, budget constraints, and concerns around account recovery continue to slow workforce progress, though many are proving manageable in practice. Of organizations that identified user behavior as a barrier, 53% describe it as a minor factor requiring some training — though in the US this rises, with 43% reporting active resistance and 15% saying it has directly delayed their rollout. On recovery specifically, 89% of organizations report confidence in their ability to restore access when passkeys are lost.

The State of Passkeys 2026 data marks a clear inflection point. Passkeys are established; the focus now shifts from enabling availability to driving primary usage and, ultimately, reducing reliance on passwords. For organizations, the priority is moving beyond partial deployment to operational adoption. For service providers, it is reducing remaining friction and increasing user preference for passkeys. Across the industry, continued alignment on standards, user experience, and real-world deployment will determine how quickly the transition is completed.

Research Methodology

Consumer survey

The consumer survey was conducted among 11,000 adults who regularly log in to websites, apps, or online services across the United States, United Kingdom, France, Germany, Australia, Singapore, Japan, South Korea, China, and India. Interviews were conducted online by Sapio Research in April 2026. The margin of error is ±0.9 percentage points at a 95% confidence level.

Workforce survey

The workforce survey was conducted among 1,400 decision-makers involved in decisions about employee sign-in, authentication, or passkey deployment in organizations with 500 or more employees across the same ten countries. Interviews were conducted online by Sapio Research in April 2026. The margin of error is ±2.6 percentage points at a 95% confidence level.

Regional groupings used throughout this report

- **US:** United States (enterprise n=200; consumer n=2,000)
- **Europe:** United Kingdom, France, Germany (enterprise n=600; consumer n=3,000)
- **APAC:** Australia, China, India, Japan, Singapore, South Korea (enterprise n=600; consumer n=6,000)

Respondent demographics summary

Consumer survey

11,000 respondents across 10 Countries


2,000


1,000


1,000


1,000


1,000


1,000


1,000


1,000


1,000


1,000

Login Frequency

71%	Multiple times daily
15%	Once a day
14%	Occasionally

Employment Status

49%	Full-time employed
10%	Part-time
6%	Self-employed
14%	Retired

Respondent demographics summary

Enterprise survey

1,400 respondents across 10 countries


200


100


100


100


100


100


100


100


100


100

Organization Size

# of employees	# of respondents
500 to 999	24%
1,00 to 4,999	37%
5,000 to 9,999	20%
10,000+	19%

Seniority

39% Manager / team manager

30% Senior manager / head of department

16% Director

11% C-suite / executive leadership

4% Vice President

Decision-making involvement

51% are the primary decision-maker

30% share decision-making responsibility

13% influence or recommend decisions

6% are involved in implementation or execution

Primary job function

40% IT / Information Technology

12% Operations

11% HR / People Operations

9% Cybersecurity / Information Security

6% Identity and Access Management

Key findings

1. The Awareness Battle Is Being Won, and It Is Translating Into Adoption
2. Yet Passwords Are Still Causing Real, Measurable Harm
3. Workplace Deployment Is Approaching Mainstream Levels
4. Deploying Passkeys and Eliminating Passwords Are Not the Same Thing
5. Organizations Leading the Way Are Seeing ROI
6. There Remain Barriers to Overcome

Key finding 1

The Awareness Battle Is Being Won, and It Is Translating Into Adoption

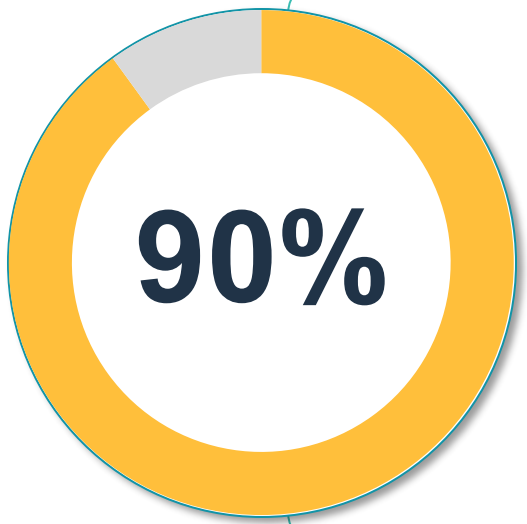
Consumer survey (base: 11,000)

Key finding

1

Q1:

Which of the following best describes your use of passkeys for apps and online accounts?



of global consumers are now aware of passkeys

Awareness and active use of passkeys have reached scale. **Ninety percent of global consumers are now aware of passkeys** - only 7% say they are not familiar with them at all, with a further 3% unsure. More importantly, awareness is converting into action at high rates.

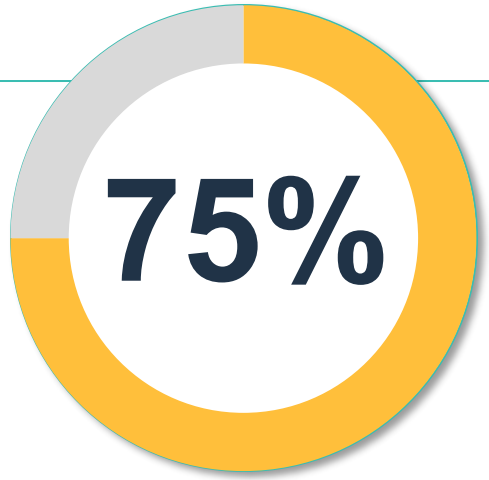
*Consumer survey (base: 11,000)

Key finding

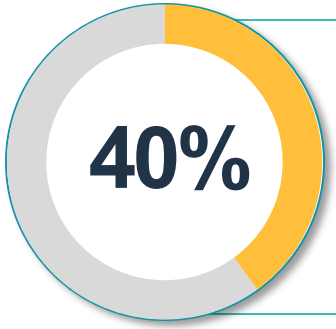
1

Q1:

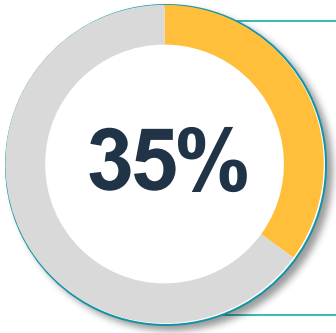
Which of the following best describes your use of passkeys for apps and online accounts?



have enabled passkeys on at least some accounts



have enabled passkeys on most of their apps and accounts



have enabled passkeys on a few apps or accounts

*Consumer survey (base: 11,000)

Key finding

1

Q1:

Which of the following best describes your use of passkeys for apps and online accounts?

Regional breakdown:
passkeys enabled on at least some accounts

APAC leads on adoption, driven by very high rates in China and India (both 88%). Within Europe, the UK (77%) is ahead of France (64%) and Germany (70%). The US sits mid-range globally.

*Consumer survey (base: 11,000)

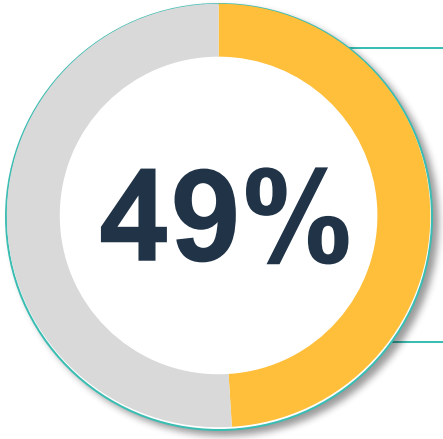
Key finding

1

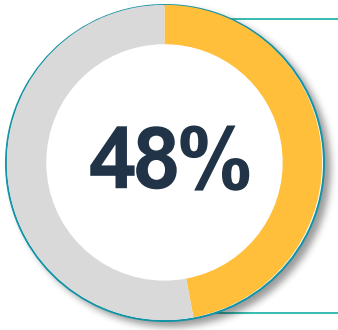
Q2:

How frequently do the following statements describe your attitude or behavior regarding passkeys?

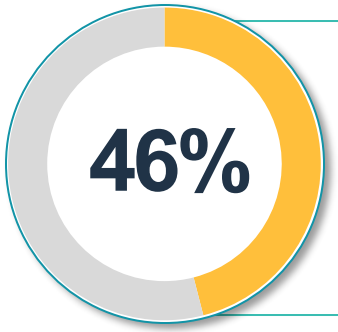
Passkey use is becoming habitual. Among all consumers - not just those who have enabled them - nearly half report using passkeys proactively and consistently.



49% use passkeys to access apps and online services “whenever possible” or “most of the time”



48% prefer passkeys over passwords “whenever possible” or “most of the time”



46% choose to set up or opt in to passkeys when prompted at that frequency

Key finding

1

Q2:

How frequently do the following statements describe your attitude or behavior regarding passkeys?

Regional breakdown:
habitual passkey use (use passkeys “whenever possible” or “most of the time”)

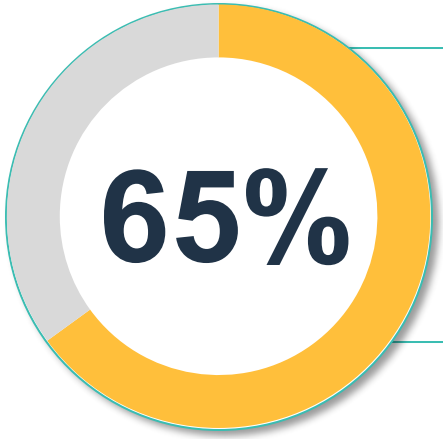
Key finding

1

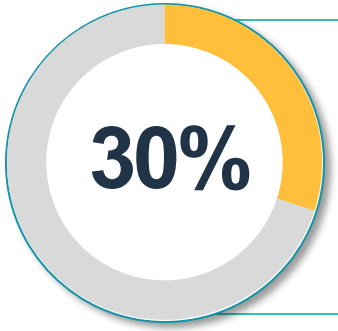
Q3:

Has your employer deployed or discussed using passkeys in the past year?

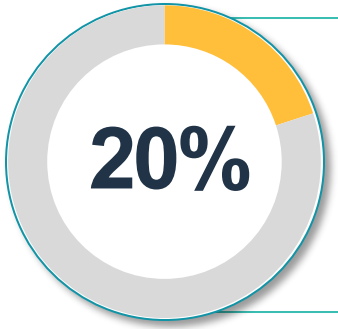
Consumer experience of passkeys at work is reinforcing broader adoption patterns. Among those who are employed:



65% report some form of passkey activity at their employer



30% say their employer has fully deployed passkeys for employee access



20% say they are currently piloting or rolling out passkeys

Among employed respondents only, base: 6,481

Key finding

1

Q3:

Has your employer deployed or discussed using passkeys in the past year?

Regional breakdown:
employer passkey activity (deployed, rolling out, or discussed)

Among employed respondents only, base: 6,481

Key finding **2**

Yet Passwords Are Still Causing Real, Measurable Harm

Consumer survey (base: 11,000)

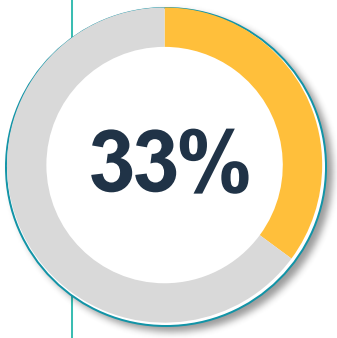
Key finding

2

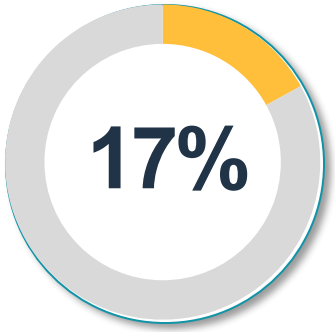
Q4:

Have you had your password stolen and/or any account compromised in the past year?

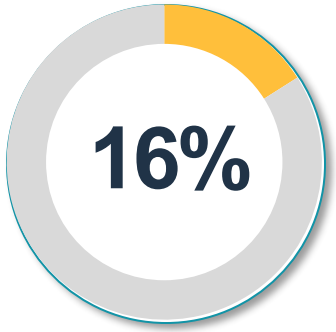
Despite increased passkey availability and use, password-related security failures continue at scale.



had a confirmed compromise or received a breach notification in the past year



know for certain that at least one account was compromised



received a notification that their password or data was exposed

Only 48% are confident no account was compromised

Key finding

2

Q4:

Have you had your password stolen and/or any account compromised in the past year?

Regional breakdown: confirmed compromise or breach notification

The US stands out significantly, with 41% of consumers having confirmed a compromise or received a breach notification - ten percentage points above both Europe and APAC. Within APAC, India is the outlier at 49%; Japan is the lowest globally at 14%.

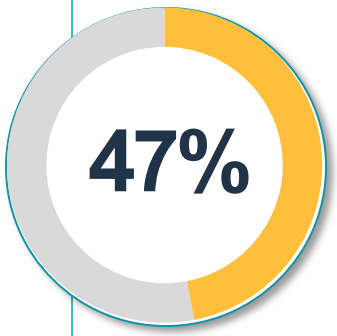
Key finding

2

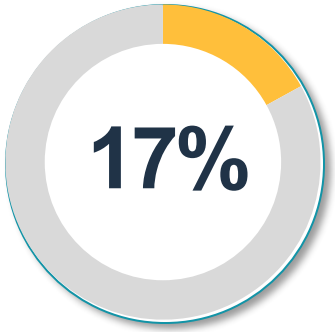
Q5:

How likely are you to abandon a purchase or account sign-in due to a forgotten password?

The friction caused by passwords is translating into measurable commercial and engagement loss.



are likely to abandon a purchase or sign-in when they cannot remember their password



are highly likely to do so

are somewhat likely

Only 48% are confident no account was compromised

Key finding

2

Q5:

How likely are you to abandon a purchase or account sign-in due to a forgotten password?

Regional breakdown: likely to abandon due to forgotten password

The US and Europe are closely aligned, with around half of consumers at risk of dropping out of a transaction. The lower APAC figure masks significant within-region variation: India (64%) is the highest globally, while Japan (25%) and South Korea (36%) pull the regional average down.

Key finding 3

Workplace Deployment Is Approaching Mainstream Levels

Enterprise survey (base: 1,400)

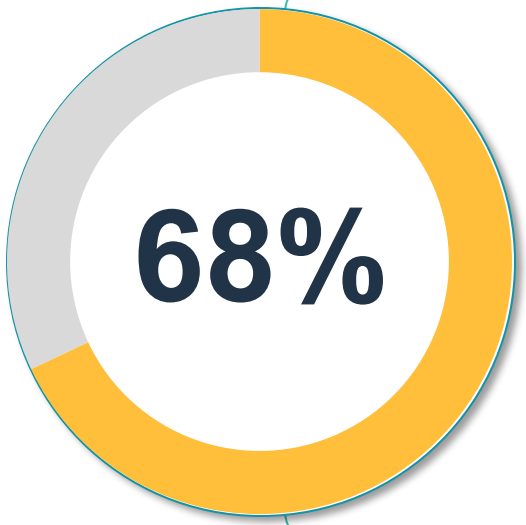
Key finding

3

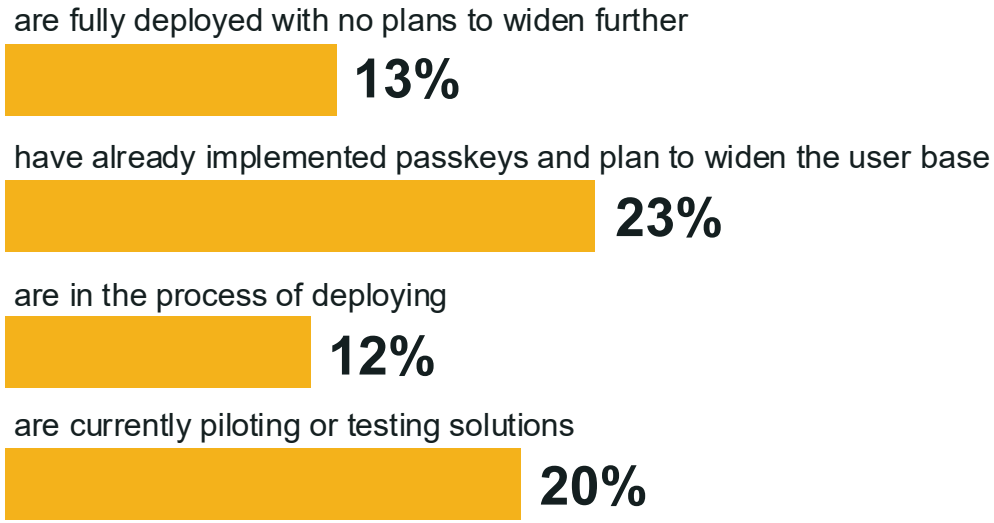
Q6:

What is your organization's current progress with implementing passkeys for your workforce?

For the majority of organizations, passkey deployment for the workforce is no longer aspirational - it is operational.



have deployed, are deploying, or are actively piloting passkeys



Key finding

3

Q6:

What is your organization's current progress with implementing passkeys for your workforce?

Regional breakdown: deployed, deploying, or piloting

The US leads on active deployment, with Europe behind by eight percentage points.
Within APAC, India (76%) and China (78%) show the highest rates; Japan (65%) and South Korea (60%) are lower.

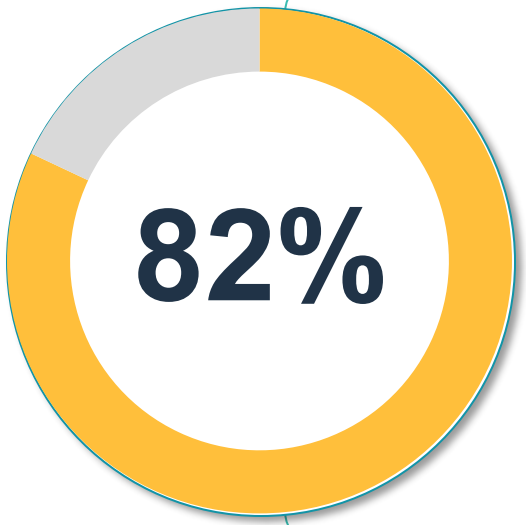
Key finding

3

Q7:

How would you describe your organization's ambition to become fully passwordless for the workforce?

Deployment intent goes beyond current activity. The direction of travel toward full passwordless authentication is near-universal at the strategic level.



say implementing fully passwordless authentication is a goal they have either reached or are actively pursuing

say fully passwordless is already in place across most of the workforce	28%
say fully passwordless is a short-term goal (next 6–12 months)	29%
say it is a longer-term goal (next 1–3 years)	25%

Key finding

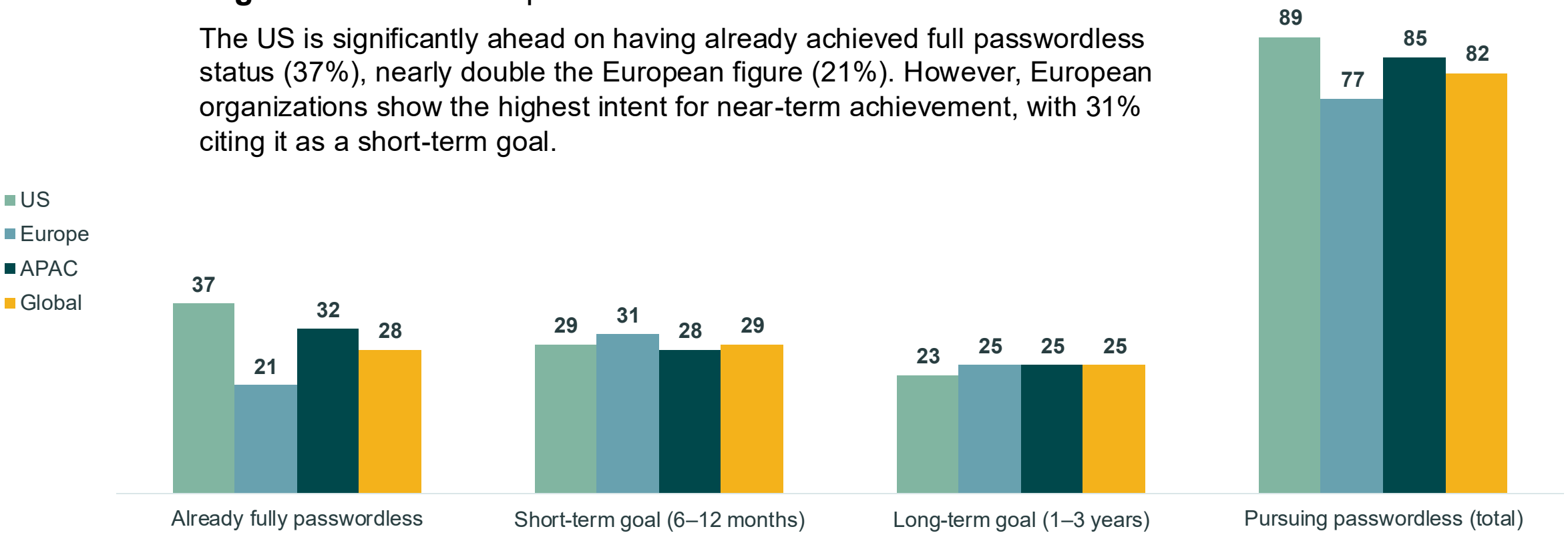
3

Q7:

How would you describe your organization's ambition to become fully passwordless for the workforce?

Regional breakdown: passwordless ambition

The US is significantly ahead on having already achieved full passwordless status (37%), nearly double the European figure (21%). However, European organizations show the highest intent for near-term achievement, with 31% citing it as a short-term goal.

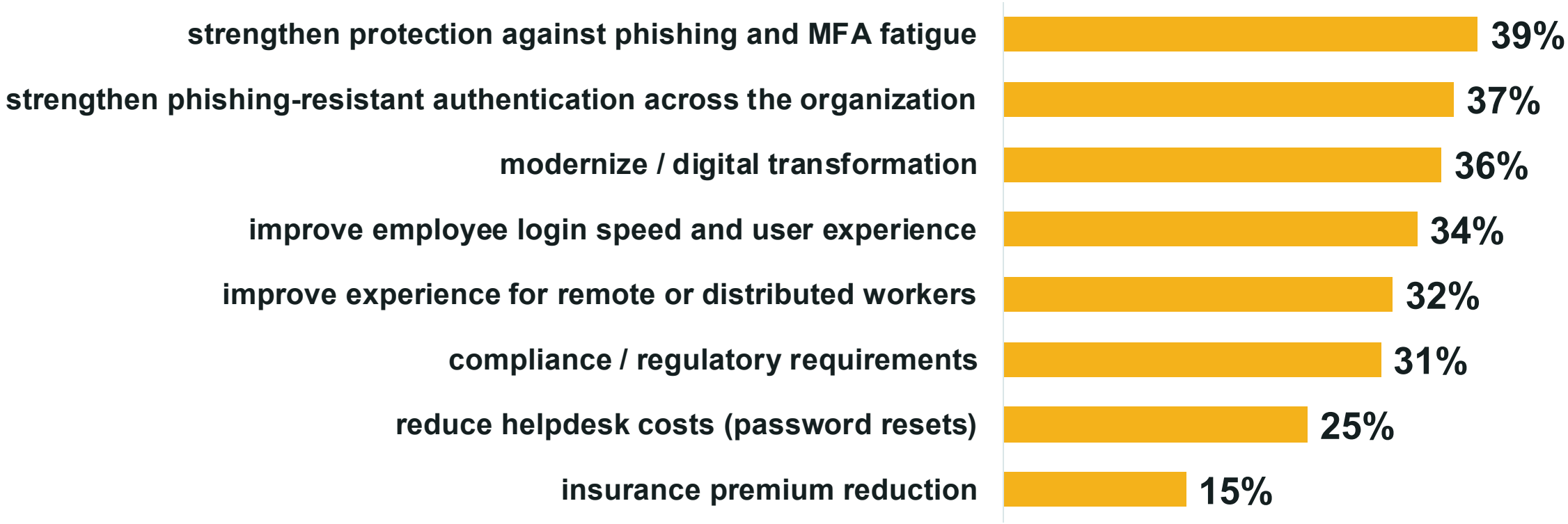


Key finding

3

Q8:

What are or were the main drivers for considering or implementing passkeys? *(Select top 3)*



Base: 1,202 - those with active passkey consideration or adoption

Key finding

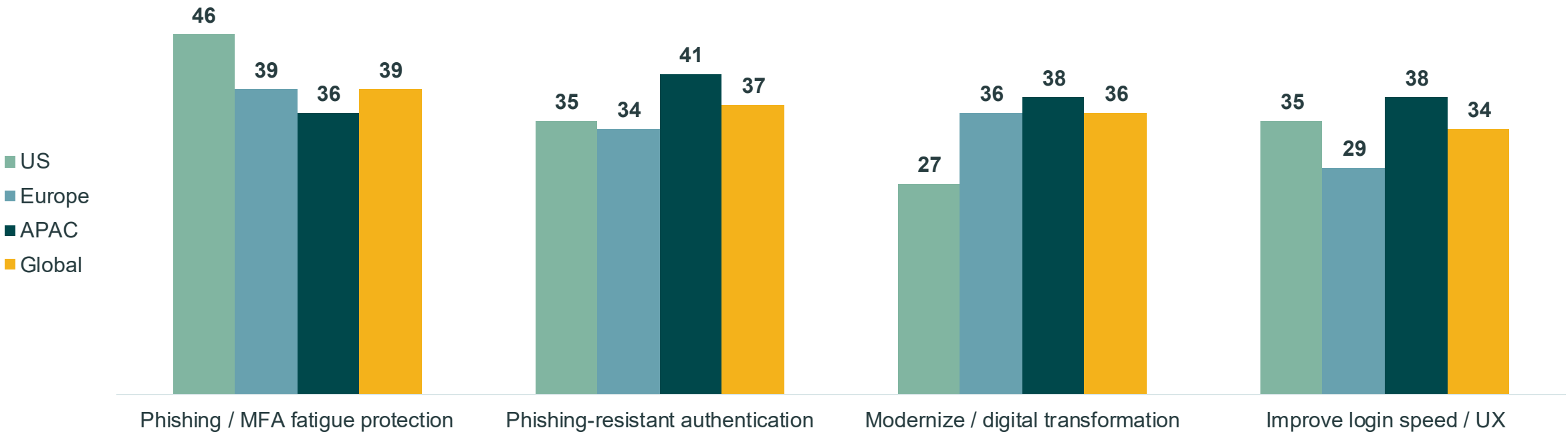
3

Q8:

What are or were the main drivers for considering or implementing passkeys? *(Select top 3)*

Regional breakdown: top drivers

Phishing protection is the top driver in the US (46%) and globally. Digital modernization and UX are more prominent motivators in APAC. Europe sits closest to the global average across all four leading drivers.



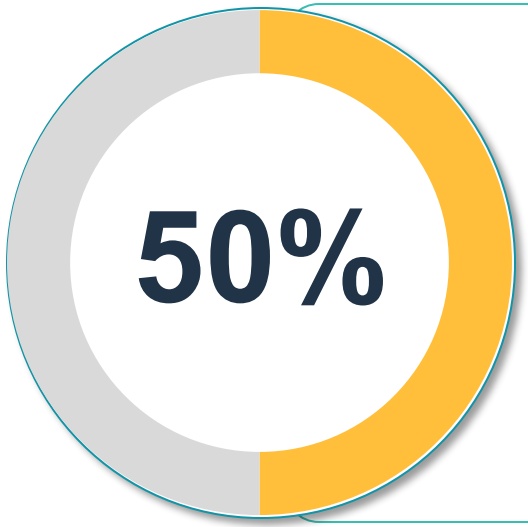
Key finding

3

Q9:

Which type of passkey approach is your organization currently using?

Deployment approaches are maturing. Half of all deploying organizations are using a combined strategy rather than a single-type approach



are using a mix of device-bound and synced passkeys

are primarily using synced passkeys	23%
are primarily using device-bound passkeys	22%
4% say it is too early to determine their approach	

Deployment approaches vary by region. Globally, half of organizations use a mix of device-bound and synced passkeys, and this holds broadly across the US (53%) and APAC (56%). Europe is the exception, splitting almost evenly between synced-only (26%) and device-bound-only (26%), with fewer organizations taking the mixed approach (44%).

Base: 945 - those using passkeys

Key finding **4**

Deploying Passkeys and Eliminating Passwords Are Not the Same Thing

Enterprise survey (base: 1,400)

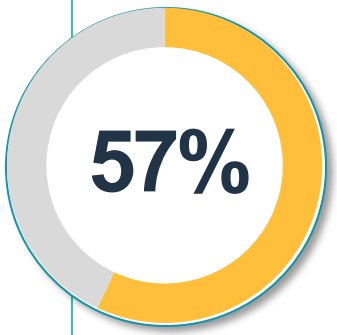
Key finding

4

Q10:

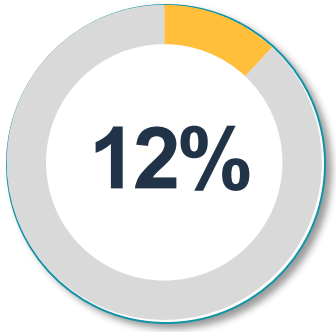
Which sign-in method do employees use most often today?

Despite strong passkey deployment figures, passwords remain the dominant day-to-day authentication method for the majority of the workforce.



of organizations report a phishable authentication method as the primary day-to-day sign-in for employees

report a passkey-based method as primary



smart card or certificate-based login

28% password plus authenticator app (push notification or TOTP)
18% password plus SMS or email one-time code
11% password only

Key finding

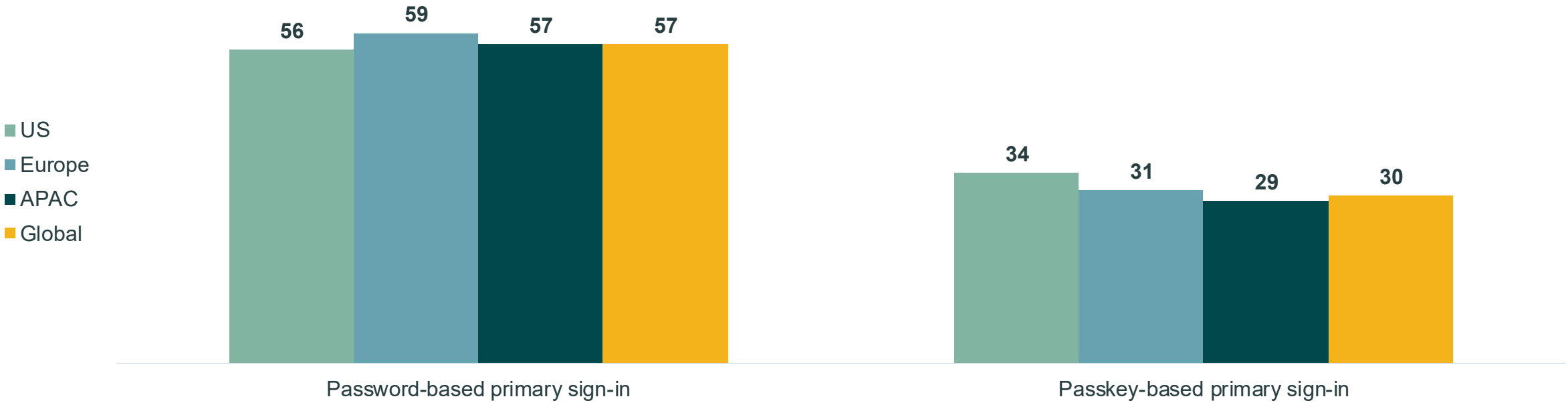
4

Q10:

Which sign-in method do employees use most often today?

Regional breakdown: primary sign-in method today

Password dependency is consistent across all three regions. The US has the highest rate of passkey-based primary sign-in (34%), but even there, more than half of organizations still authenticate the workforce primarily via passwords.



Key finding

4

Q11:

What is the main reason your organization has not yet moved to a fully passwordless workforce environment?

Base: 1,011 - those not yet fully passwordless

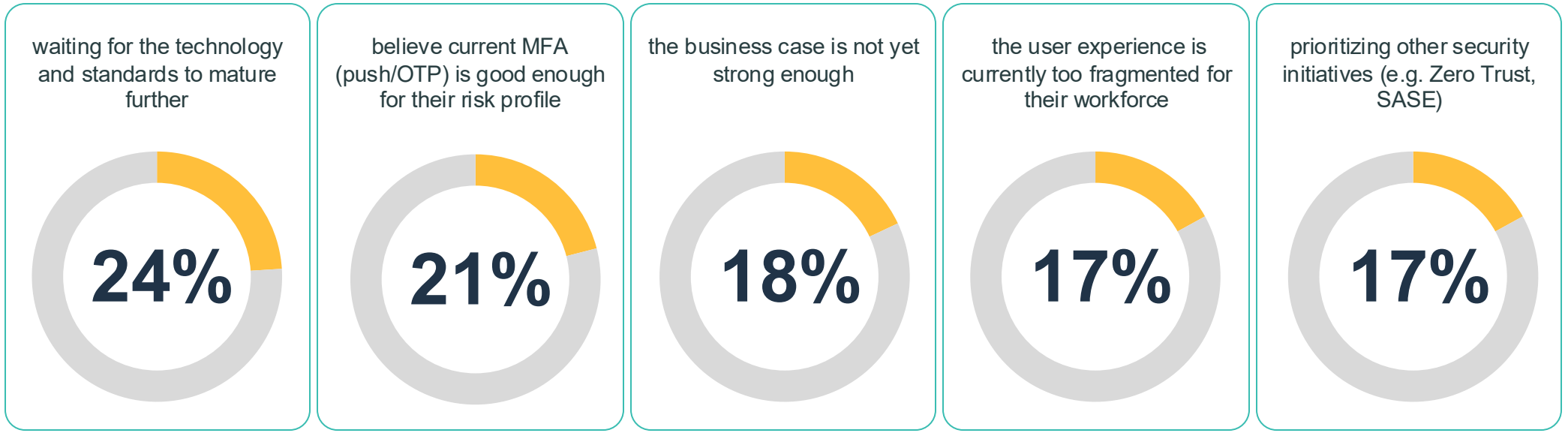
Key finding

4

Q12:

If your organization is NOT planning to roll out passkeys in the next 24 months, what is the primary reason?

Among those without near-term passkey plans:



In an environment where phishing remains the dominant attack vector, a significant number of organizations are holding ground with authentication methods that remain vulnerable. The perception that "current MFA is good enough" represents a risk that the data on ongoing account compromise does not support.

Base: 455 - those not currently deploying

Key finding **5**

Organizations Leading the Way Are Seeing ROI

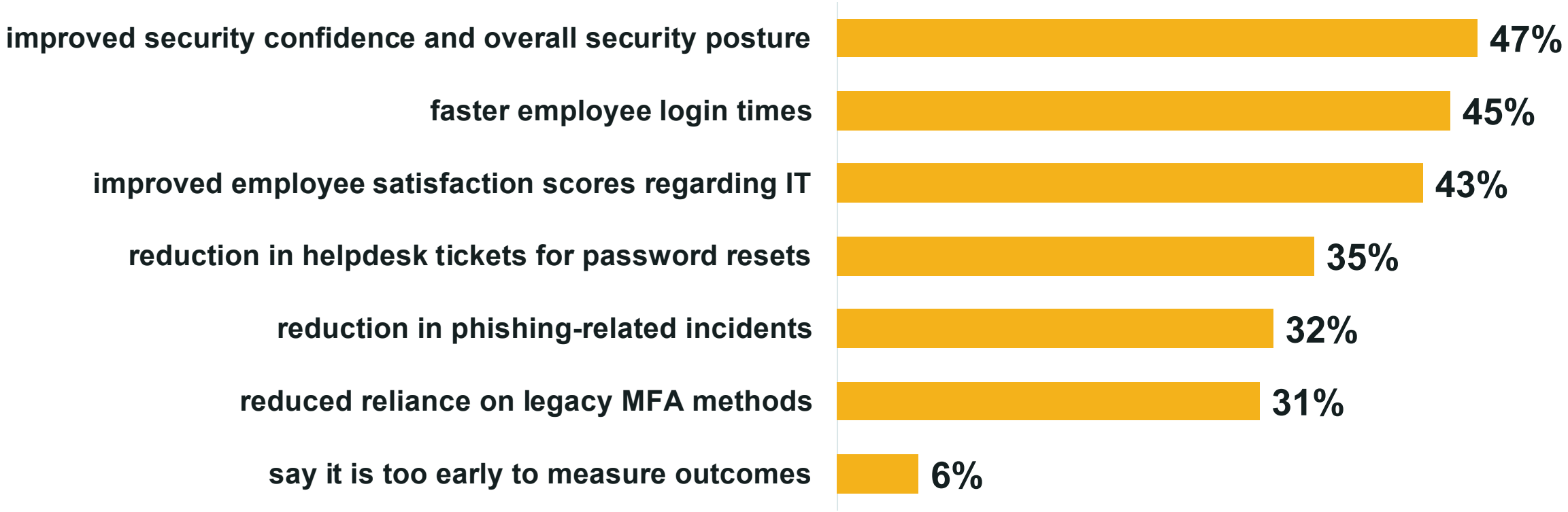
Enterprise survey (base: 945 - organizations that have begun rollout)

Key finding

5

Q13:

For those who have begun rollout, what measurable outcomes have you observed so far?



Key finding

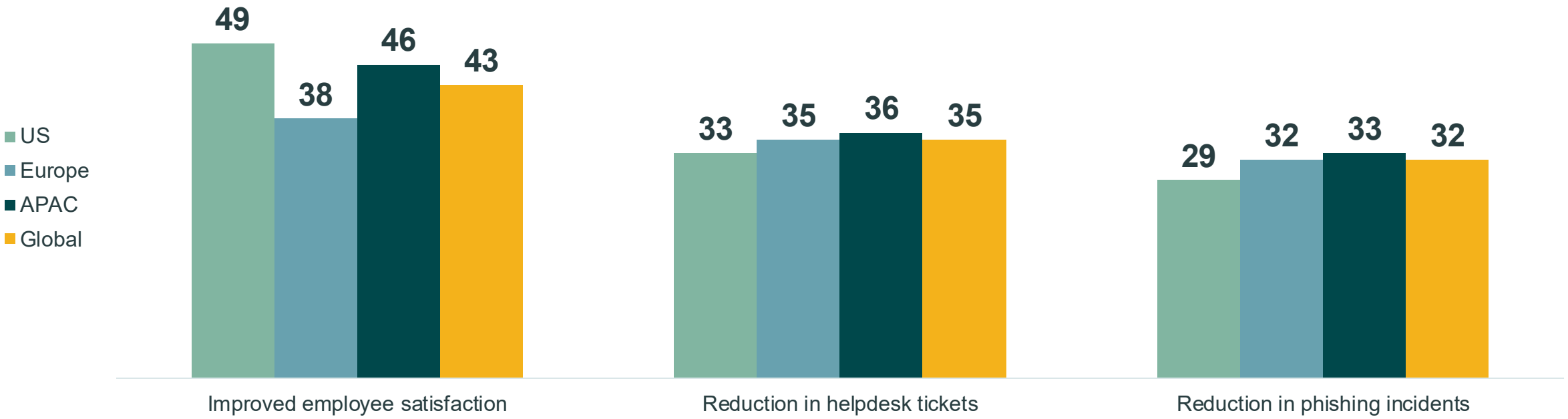
5

Q13:

For those who have begun rollout, what measurable outcomes have you observed so far?

Regional breakdown: measurable outcomes

APAC organizations report the highest rate of improved security confidence (52%). The US and APAC are closely aligned on faster login times (both ~50%), while Europe lags at 37%. Helpdesk ticket reduction and phishing incident reduction are consistent across all three regions.



Key finding

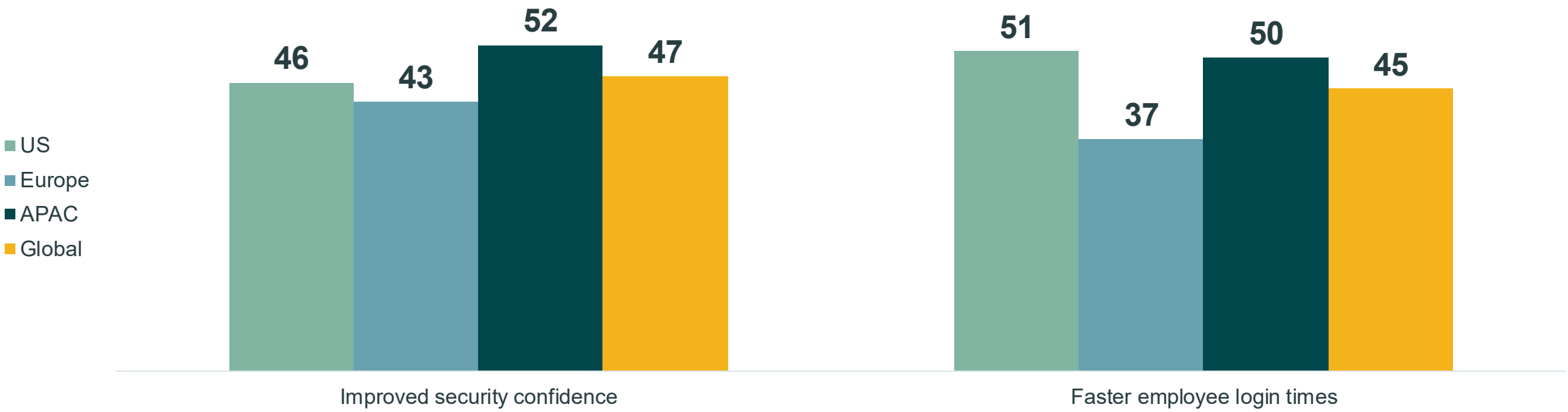
5

Q13:

For those who have begun rollout, what measurable outcomes have you observed so far?

Regional breakdown: measurable outcomes

The investment is being validated on exactly the terms on which it was made. The top driver for deployment was phishing protection; the most widely reported outcome is improved security posture. The second most cited driver was improving login UX; faster login times and improved employee satisfaction score at 45% and 43% respectively.



Key finding 6

There Remain Barriers to Overcome

Enterprise survey (base: 1,400)

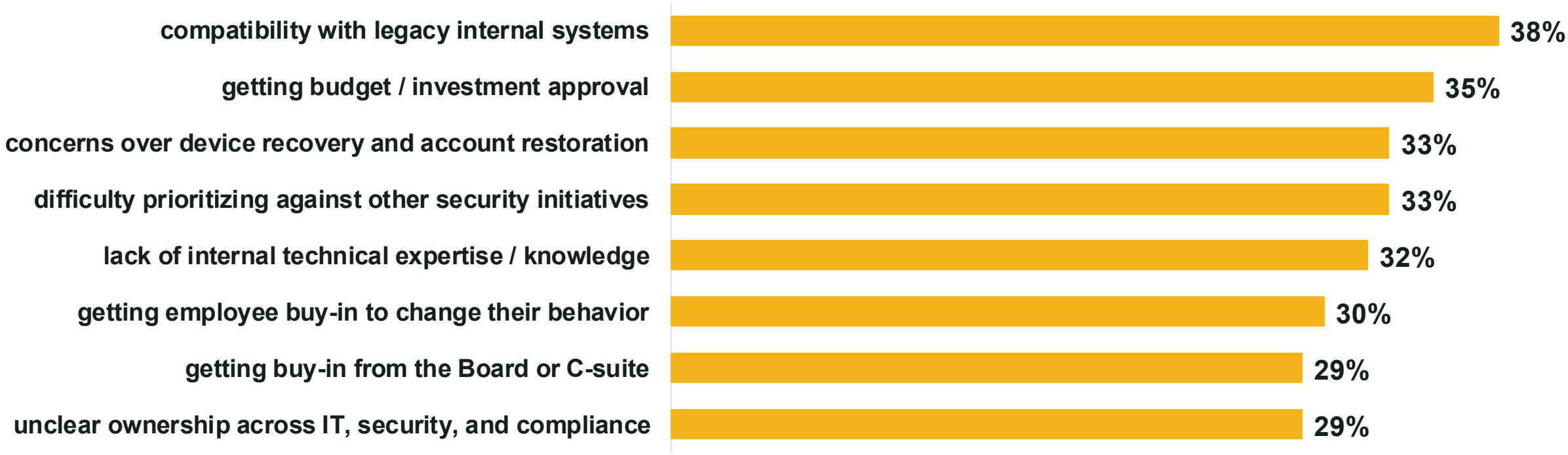
Key finding

6

Q14:

How would you rate the following organizational barriers in your passkey rollout or decision to delay?

The primary blockers are concentrated in three areas:
legacy system compatibility, **budget**, and **account recovery concerns.**



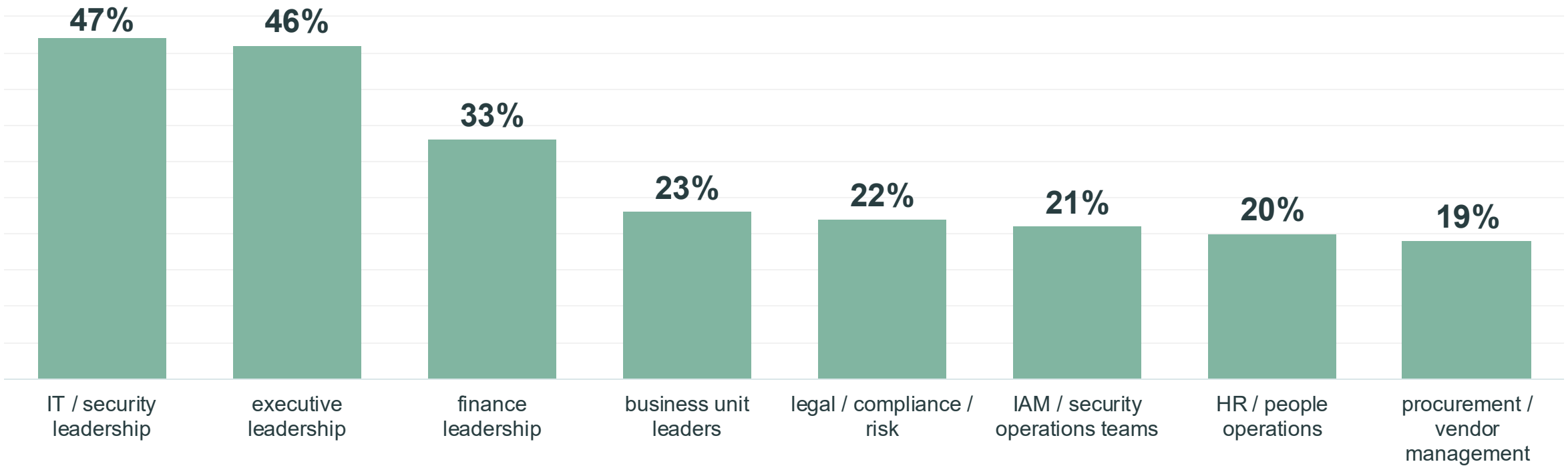
Key finding

6

Q15:

Who do you need to secure budget and/or buy-in from?

For those facing budget or buy-in challenges, approvals span multiple stakeholders:



Base: 1,162 - those facing budget or C-suite barriers

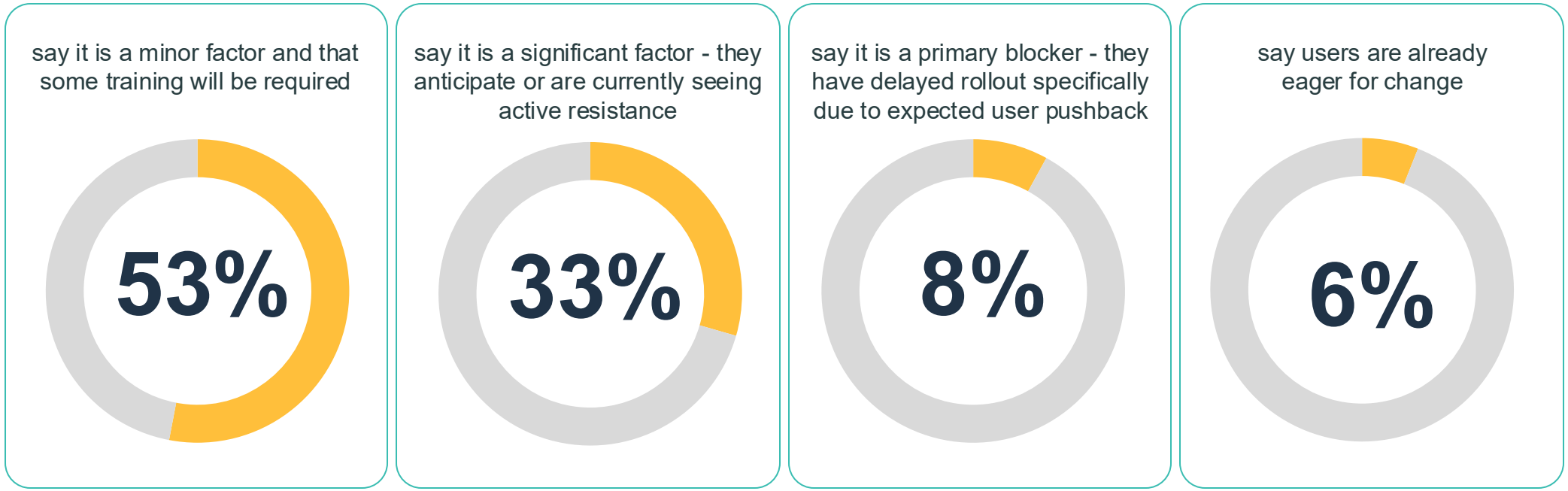
Key finding

6

Q16:

To what extent is user behavior or unwillingness to change a factor in your deployment strategy?

Employee behavior change is a real but manageable factor. Among those who identified employee buy-in as a barrier:



Base: 996 - those identifying employee buy-in as a barrier

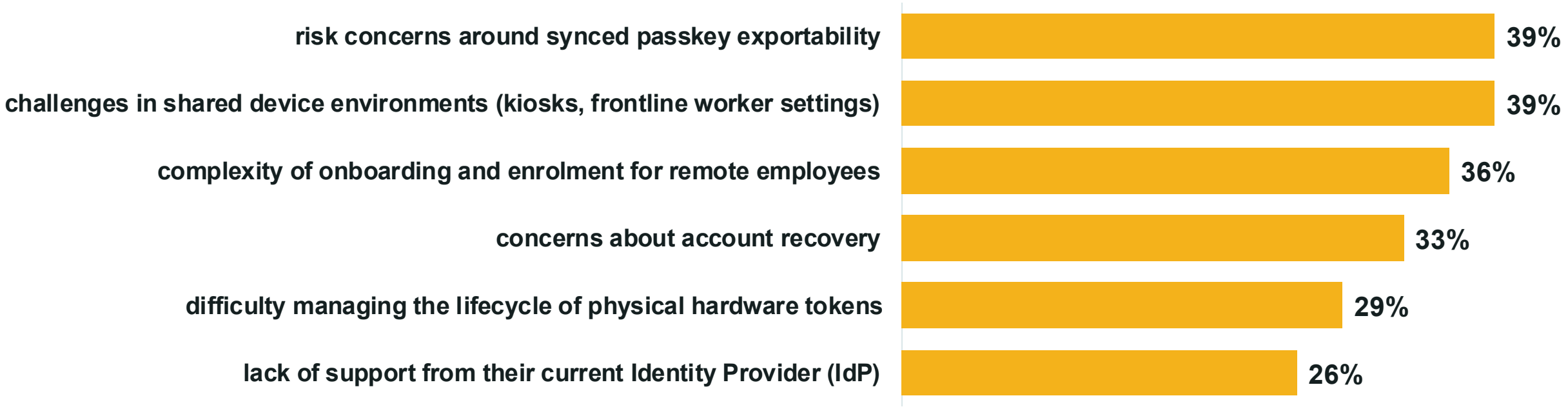
Key finding

6

Q17:

What are the primary technical or security concerns preventing adoption?

Among organizations that identified technical barriers:



Base: 1,258 - those identifying technical, legacy, or recovery barriers

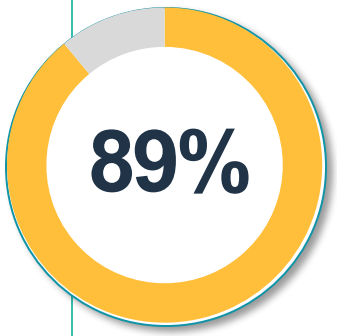
Key finding

6

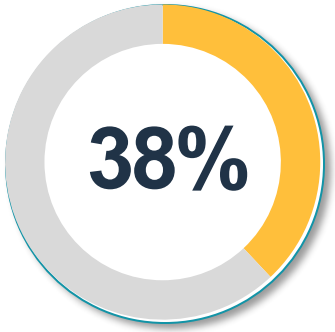
Q18:

How confident is your organization in its ability to recover employee access if a passkey is lost or unavailable?

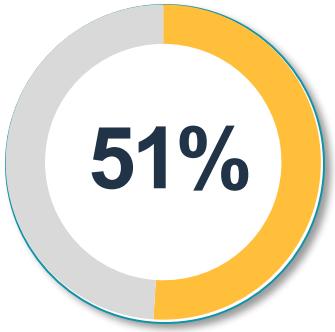
Credential recovery, often cited as a pre-deployment concern, is proving manageable in practice.



express confidence in their ability to restore access if a passkey is lost



are very confident



are fairly confident

Key finding

6

Q18:

How confident is your organization in its ability to recover employee access if a passkey is lost or unavailable?

Regional breakdown: confidence in recovery

Key finding

6

Q19:

Which approaches give you confidence in recovery?

Base: 1,243 - those confident in recovery

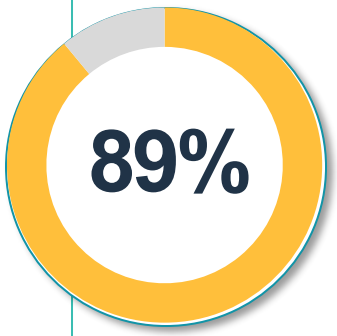
Key finding

6

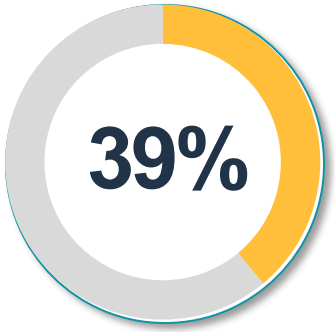
Q20:

If a trusted, interoperable standard existed to link a passkey to a verified digital identity (such as a National Digital ID), how much would this increase your organization's confidence in moving to a fully passwordless workforce?

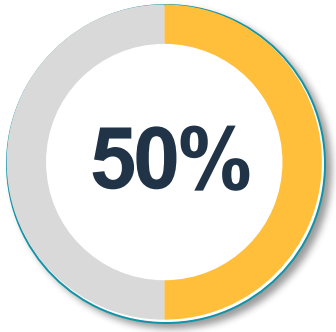
Confidence in deployment would increase significantly if robust identity-linking standards existed.



89% **say such a standard would increase their confidence**



39% say they would move to a passwordless policy immediately



50% say it would help them expand passkeys to more high-risk user groups

Base: 1,351 - those with active passkey plans

Conclusion

The 2026 data paints a picture of a technology that has achieved genuine scale. Passkeys are now part of the authentication landscape for the majority of consumers and a growing majority of enterprises. The outcomes for early movers are validated and compelling, and the direction of travel is clear.

The work ahead lies in closing the gap between having passkeys as an option and making passwords obsolete. The data shows that the gap is real, that the barriers are identifiable, and that a significant number of organizations have already closed it.

For enterprises yet to begin, the findings of those who have gone first offer a reliable guide. For service providers, the data identifies where friction remains - in shared device environments, in identity recovery, and in user behavior.

fido ALLIANCE | simpler stronger authentication

About FIDO Alliance

The FIDO Alliance (www.fidoalliance.org) enables identity technologies that put trust and simplicity at the center of interactions among people, services, and devices. The Alliance provides a member-driven forum that publishes open technical specifications, certifies secure and interoperable products, and operates global market enablement programs.