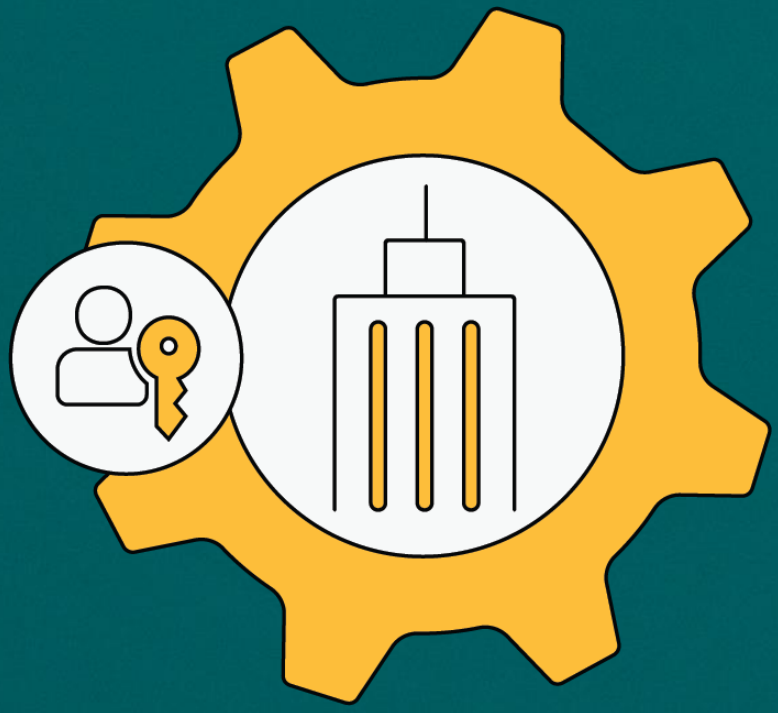
fido ALLIANCE | simpler stronger authentication

The State of Passkey Deployment in the Enterprise



A Snapshot of Passkey Deployments for Employee Sign-ins in the U.S. and UK

www.fidoalliance.org

Executive Summary

Enterprises seeking to strengthen security and move away from phishable forms of authentication such as passwords and SMS OTPs are increasingly showing interest in FIDO authentication-based sign-ins with passkeys for phishing-resistance and usability. But, the state of and methods for deployment are less clear. In 2024, the FIDO Alliance conducted a survey to understand the state of passkey deployments in the US and UK, the methods used to deploy and employees enrolled, and the perceived barriers to deployment.

Research Methodology

The survey was conducted among 400 decision makers who would be / are involved in the deployment of passkeys in companies with 500+ employees across the UK and the US.

The interviews were conducted online by Sapio Research in September 2024 using an email invitation and an online survey.

The survey was produced by the FIDO Alliance Enterprise Deployment Working Group, with underwriting support from:

Respondent demographics summary

Country of residence

200

200

Top 3: Role in passkey deployment

1	IT Service Management	39%
2	Decision Maker	25%
3	Project Manager	19%

Job position

10% were Owners

25% were Directors

19% were C-Level Executives

46% were Managers

Business Size

# of employees	# of respondents
500 to 999	32%
1,00 to 4,999	40%
5,000 to 9,999	12%
10,000+	15%

Top 3: Business Sector

1	IT	27%
2	Finance / Insurance / Accounting	16%
3	Manufacturing	11%

Key findings

1 **Enterprises understand the value of passkeys and the majority are rolling out passkeys for workforce sign-ins:** The majority have either deployed or are in the midst of deploying passkeys with goals tied to improved user experience, enhanced security, and standards/regulatory compliance. Those that are deploying are rolling out a mix of device-bound and synced passkeys.

2 **Enterprises are prioritizing passkey rollouts to users with access to sensitive data and applications**, and are leveraging communication, training and documentation to increase adoption.

3 **Enterprises are reporting significant security and business benefits after rolling out passkeys:** they report positive impacts on user experience, security, cost reduction, productivity and digital transformation goals — and are seeing declines in usage of legacy authentication methods. Interestingly, these benefits directly correlate with what businesses who aren't yet using passkeys dislike most about their current authentication methods: that they can be compromised, are costly, and difficult to use.

4 **Organizations that do not have active passkey projects cite complexity, costs and overall lack of clarity about implementation as reasons**, signaling a need for increased education to enterprises on rollout strategies to reduce concerns.

Key finding 1

Enterprises understand the value of passkeys and the majority are rolling out passkeys for workforce sign-ins.

The majority have either deployed or are in the midst of deploying passkeys with goals tied to improved user experience, enhanced security, and standards/regulatory compliance.

Those that are deploying are rolling out a mix of device-bound and synced passkeys.

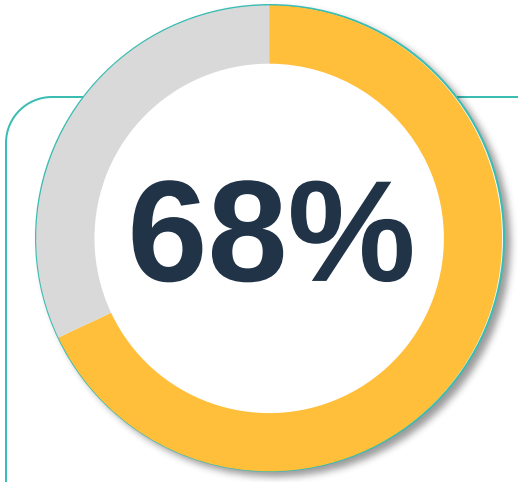
Key finding

1

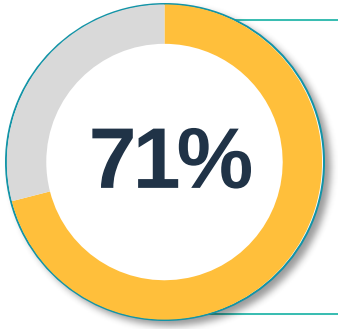
Q1:

At which level of priority is this project positioned in your organization?

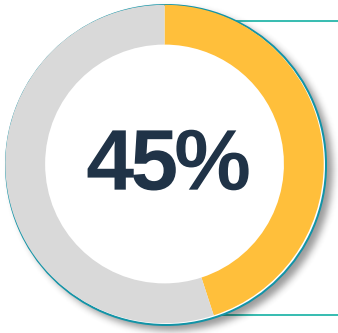
Select One



Two thirds (68%) of all respondents said the deployment of passkeys is a high or critical priority in their organization



of those that have deployed
71% said passkeys are a high or critical priority



of those that have NOT deployed
45% said passkeys are a high or critical priority

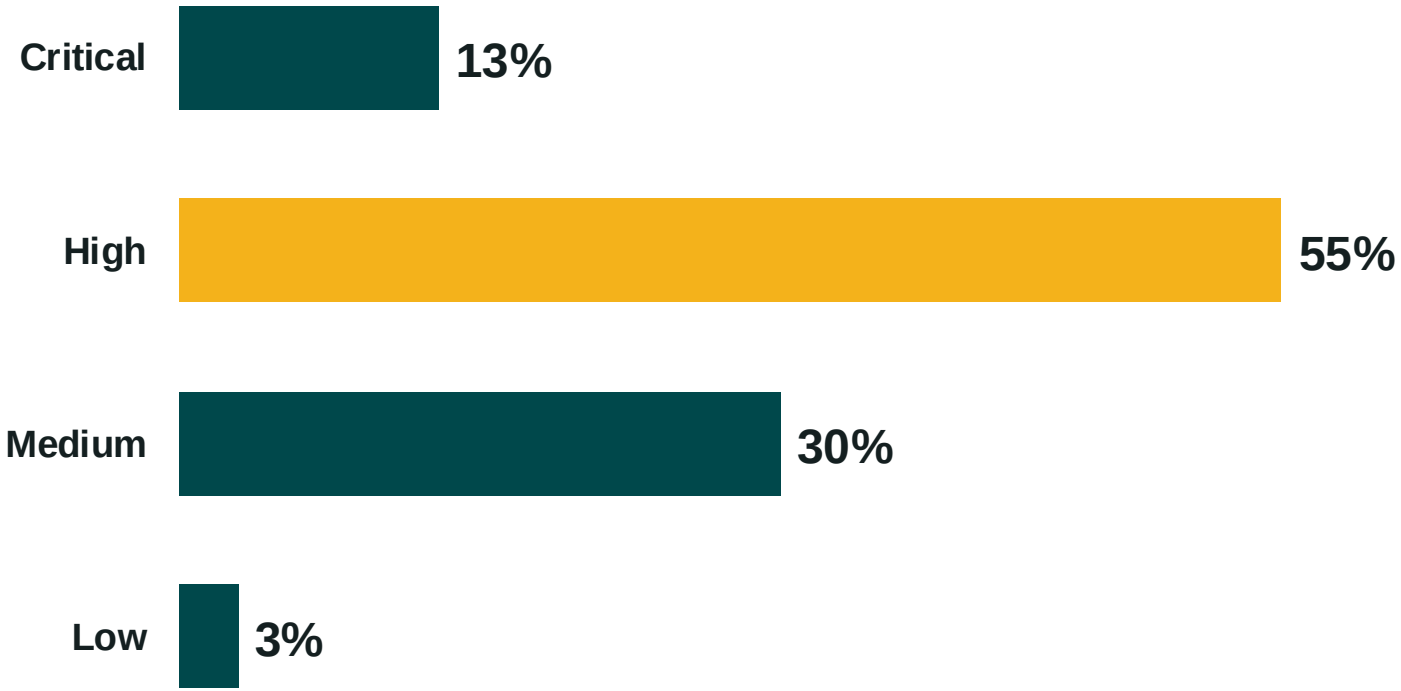
Key finding

1

Q1:

At which level of priority is this project positioned in your organization?

Select One



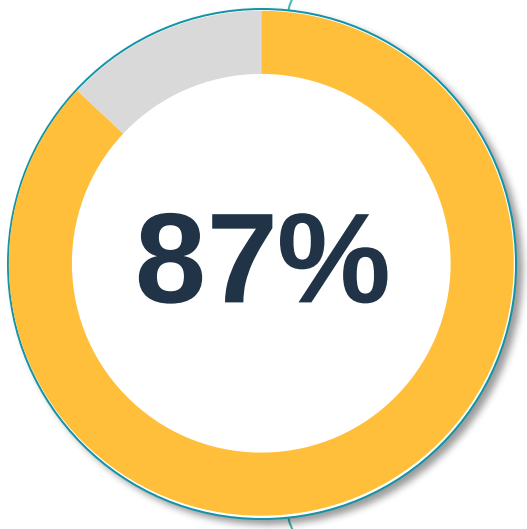
Key finding

1

Q2:

Where does your organization stand in your adoption of passkeys?

Select One



of surveyed organizations have successfully deployed or are deploying passkeys - a growth by 14 percentage points since 2022*

*Compared to data from a 2022 internal FIDO Alliance survey

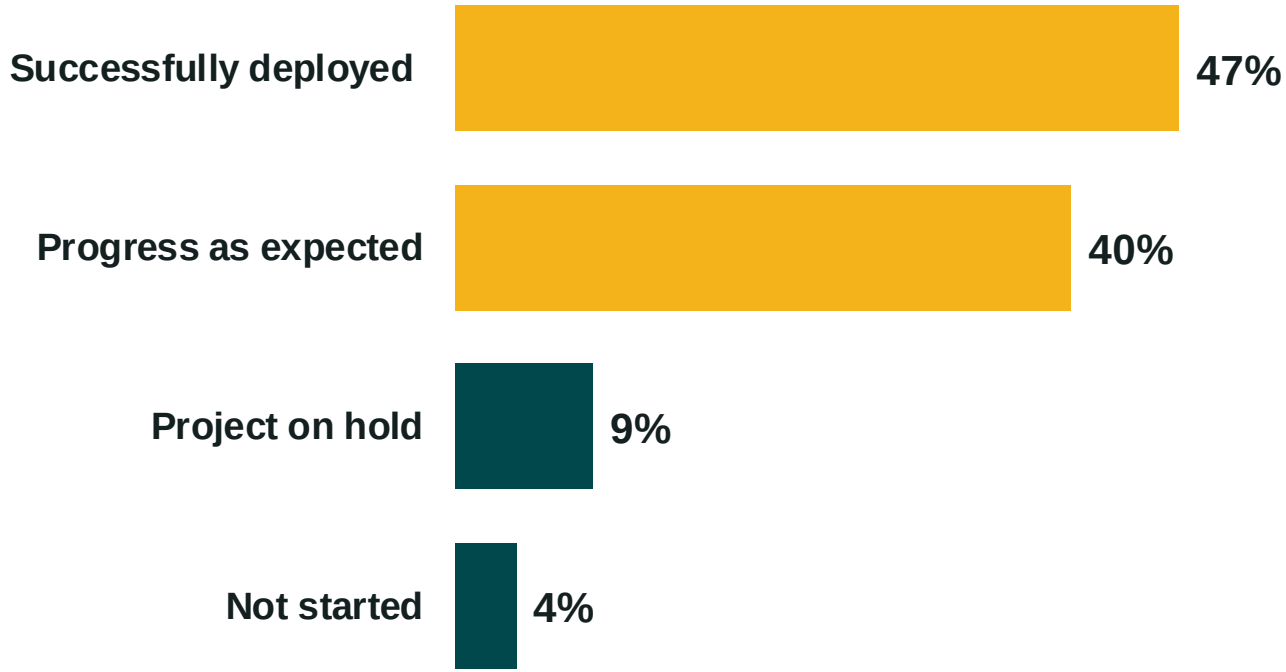
Key finding

1

Q2:

Where does your organization stand in your adoption of passkeys?

Select One



*Compared to data from a 2022 internal FIDO Alliance survey

Key finding

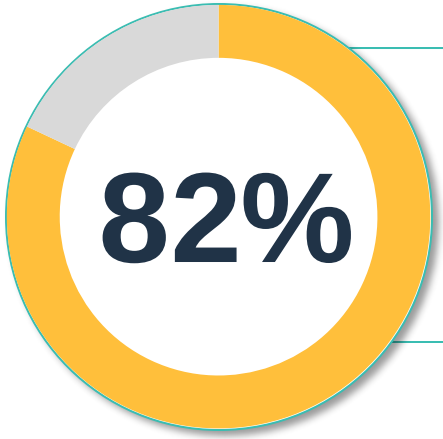
1

Q3:

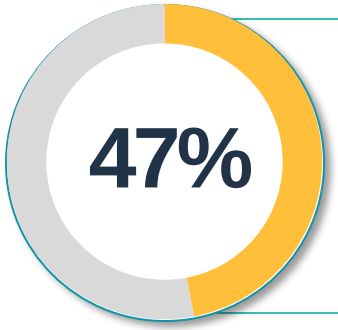
What types of passkeys are you using or considering?

Select all that apply

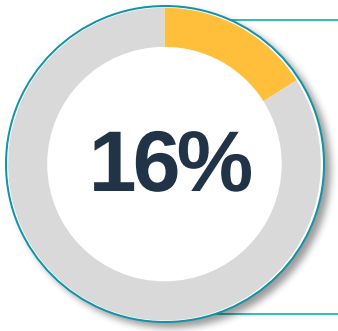
Surveyed companies reported implementing or considering a mix of device-bound and synced passkeys



are deploying device-bound passkeys



are deploying a mix of synced and device bound passkeys



are deploying synced passkeys only

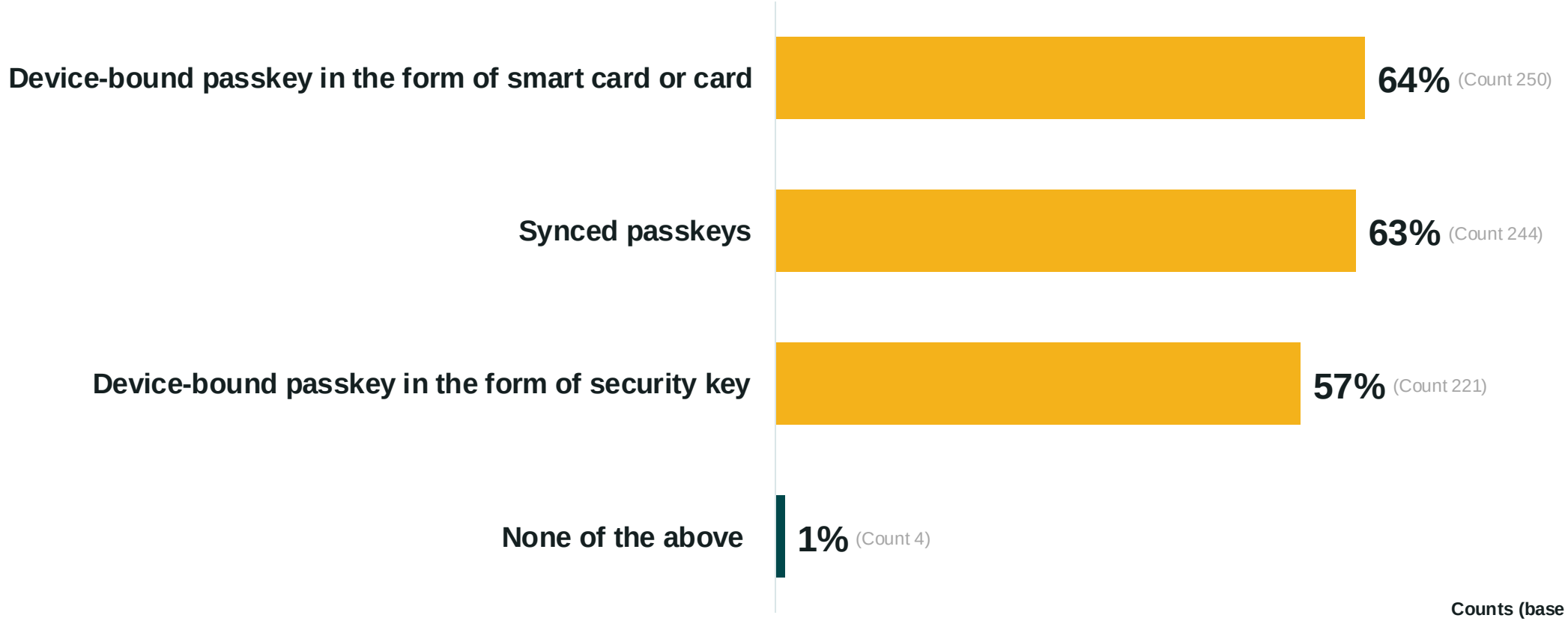
Key finding

1

Q3:

What types of passkeys are you using or considering?

Select all that apply



Counts (base 400)

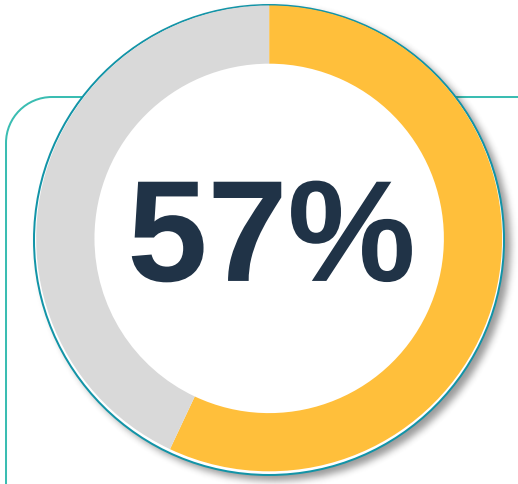
Key finding

1

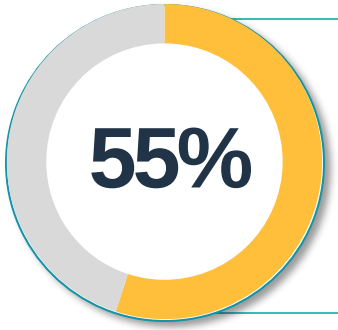
Q4:

What were your organization's main reasons for deploying passkeys?

Select top three



of organizations that have deployed passkeys reported improved user experience as a main reason



reported standards compliance

reported mitigating data breach risks & regulatory compliance

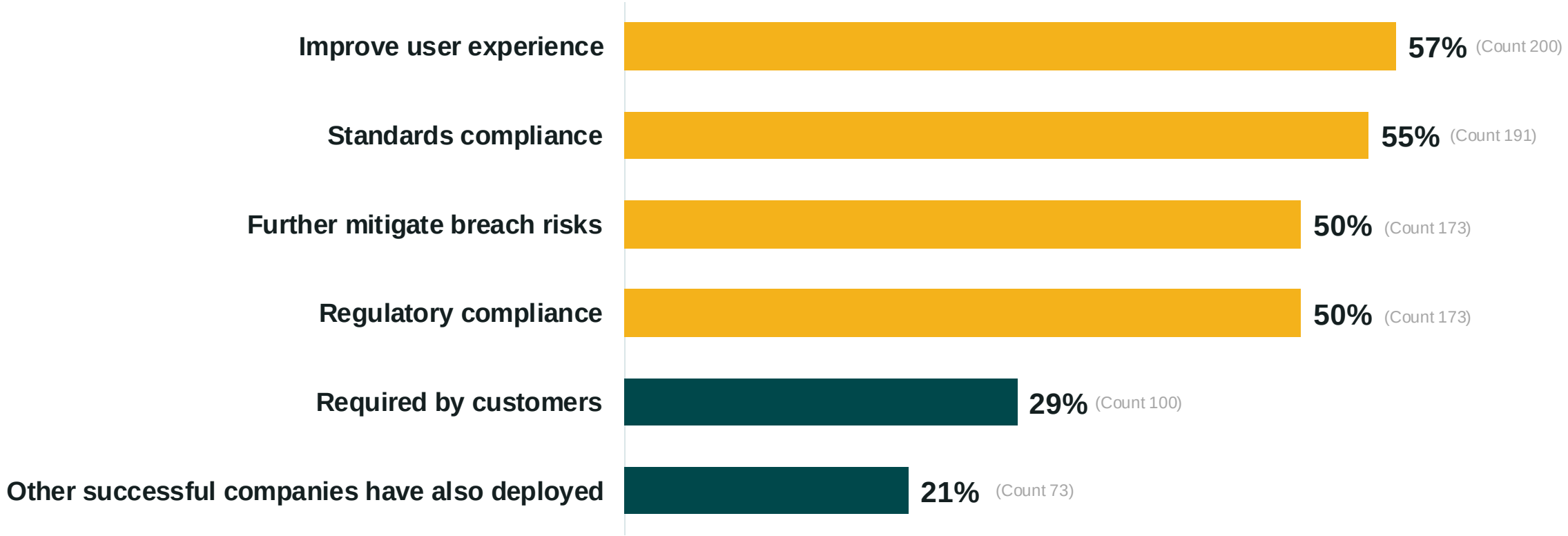
Key finding

1

Q4:

What were your organization's main reasons for deploying passkeys?

Select top three



Counts (base 349)

Key finding 2

Enterprises are prioritizing passkey rollouts to users with access to sensitive data and applications, and are leveraging communication, training and documentation to increase adoption.

Enterprises are prioritizing passkeys with users with access to sensitive data and applications

Key finding

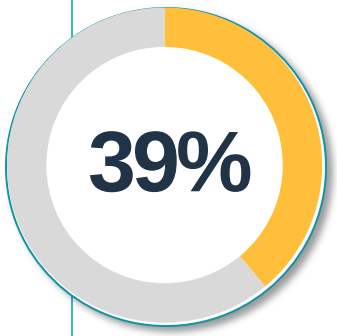
2

Q5:

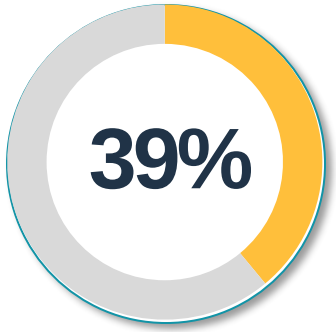
What group of users did you target for your passkey implementation project?

Select all that apply

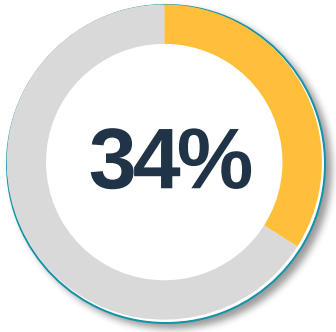
Organizations are prioritizing specific user groups for passkeys, with the top three cited user groups being:



those requiring access to IP



users with admin accounts



users at the executive level

Only 21% said they are targeting all of the users in their organization

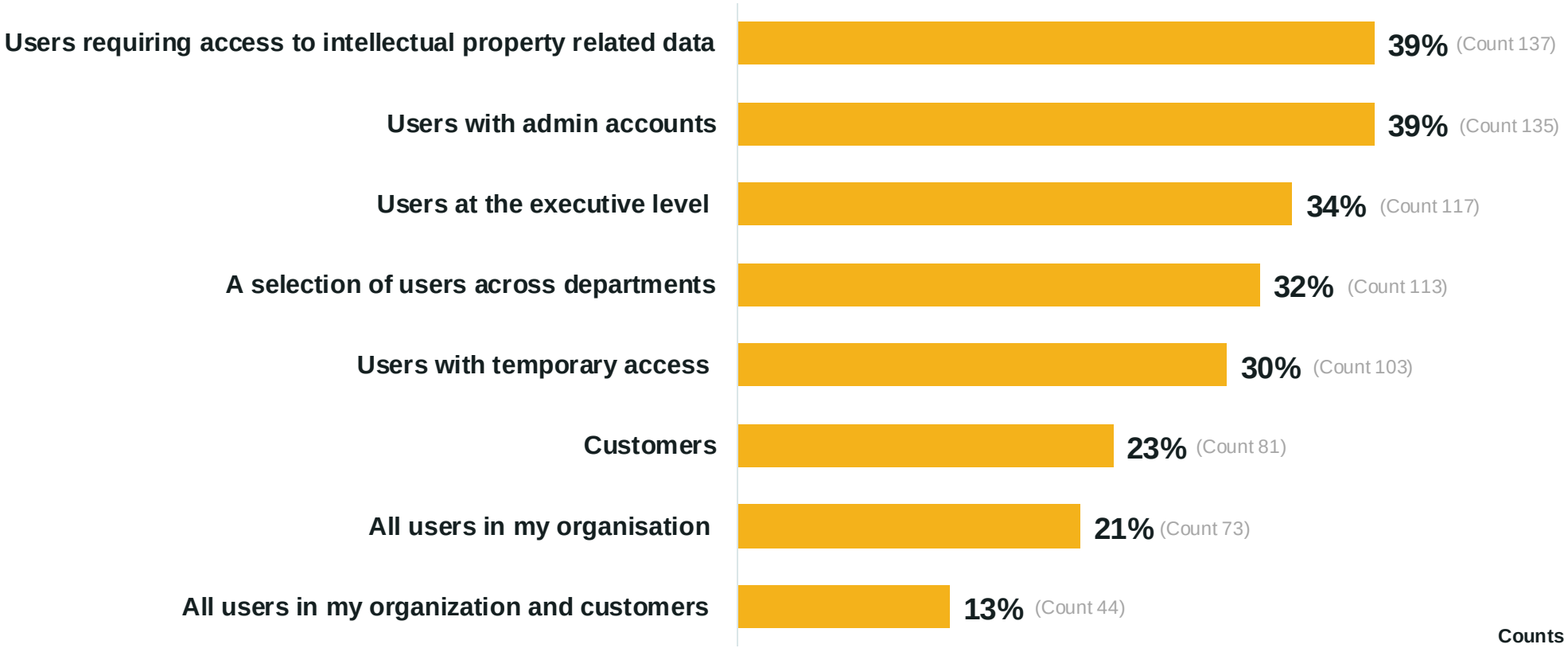
Key finding

2

Q5:

What group of users did you target for your passkey implementation project?

Select all that apply



Counts (base 349)

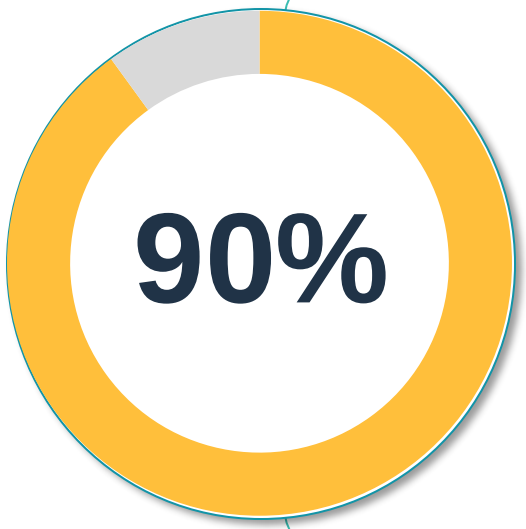
Key finding

2

Q6:

How important is user education in passkey adoption in your organization?

Select one



said that education is important for passkey adoption in their organization

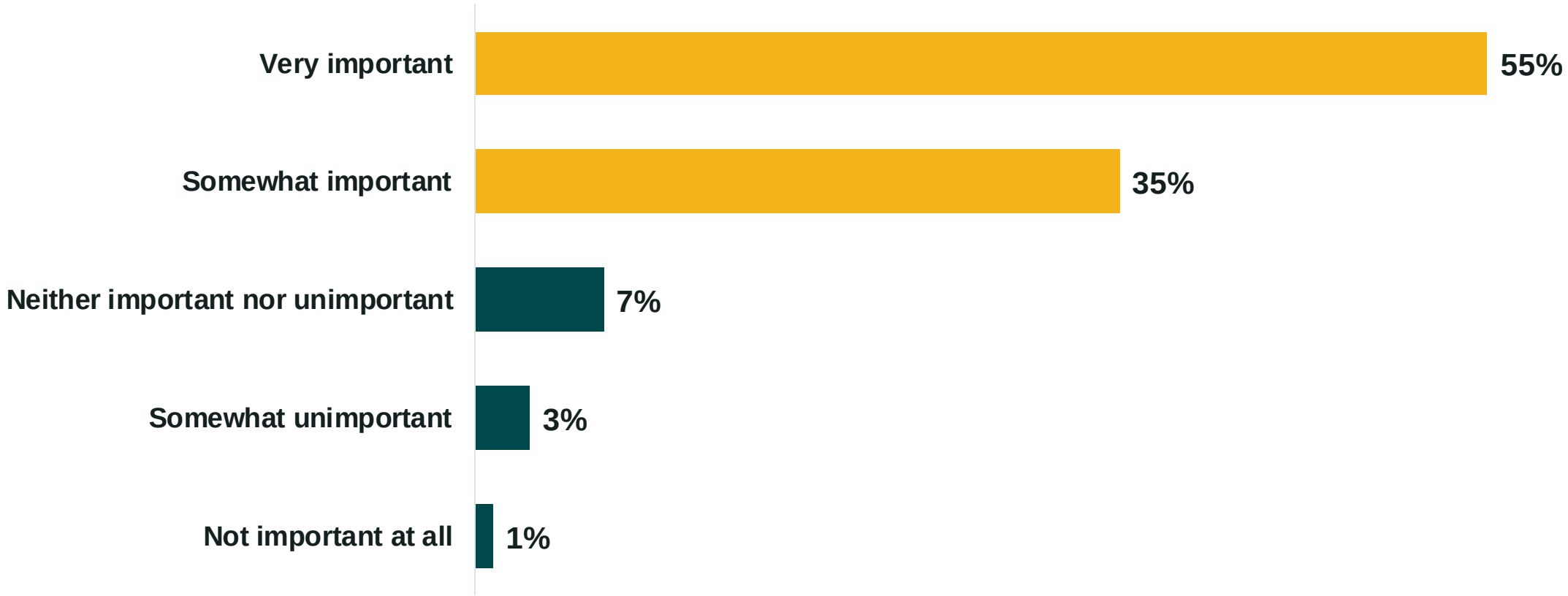
Key finding

2

Q6:

How important is user education in passkey adoption in your organization?

Select one



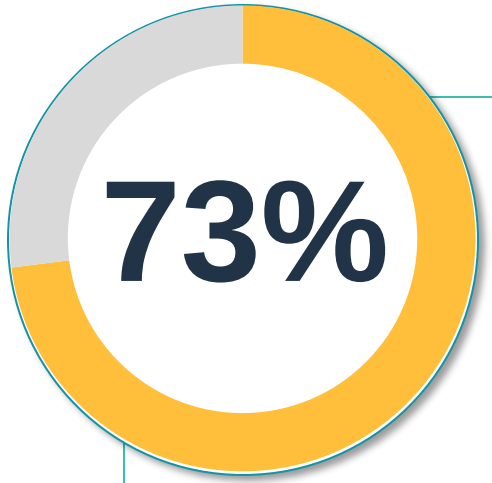
Key finding

2

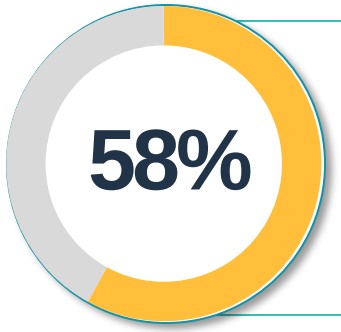
Q7:

What materials are you using for internal user education?

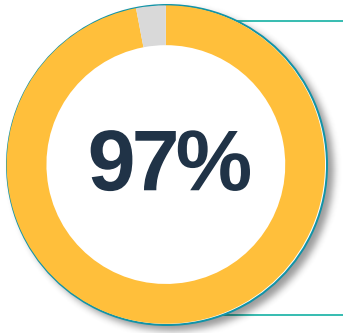
Select one



said they used a combination of materials provided by the FIDO Alliance and some created internally to educate users about passkeys



used both dedicated training session and internal communication tools



provide first use instruction

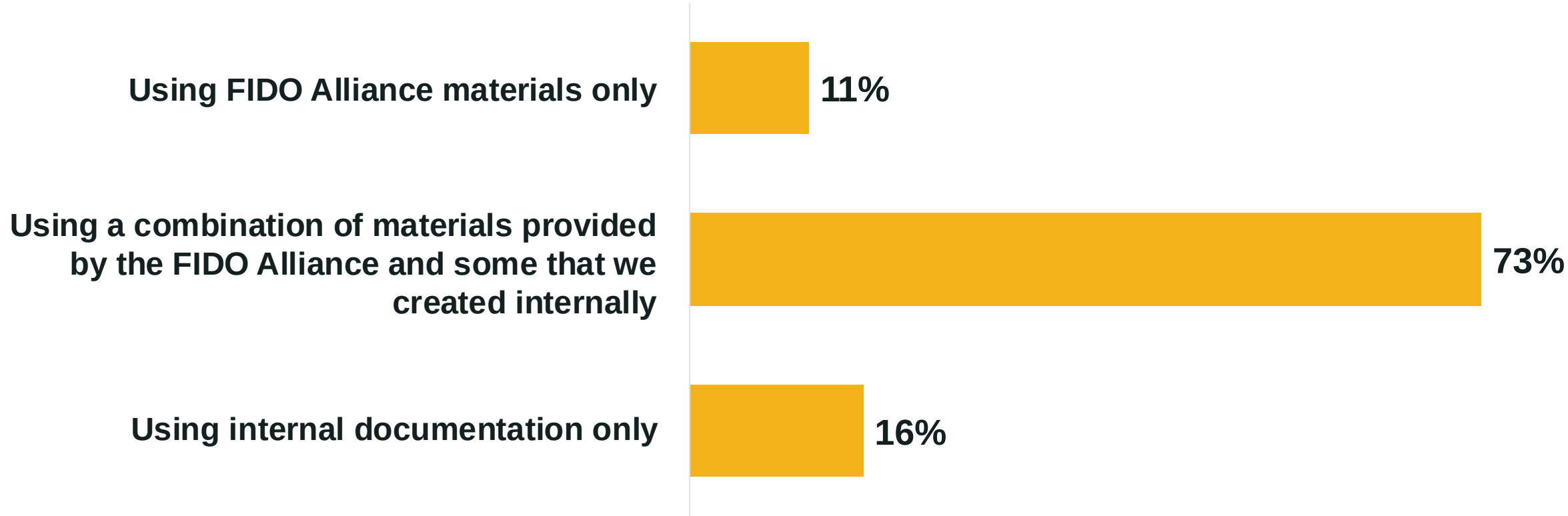
Key finding

2

Q7:

What materials are you using for internal user education?

Select one



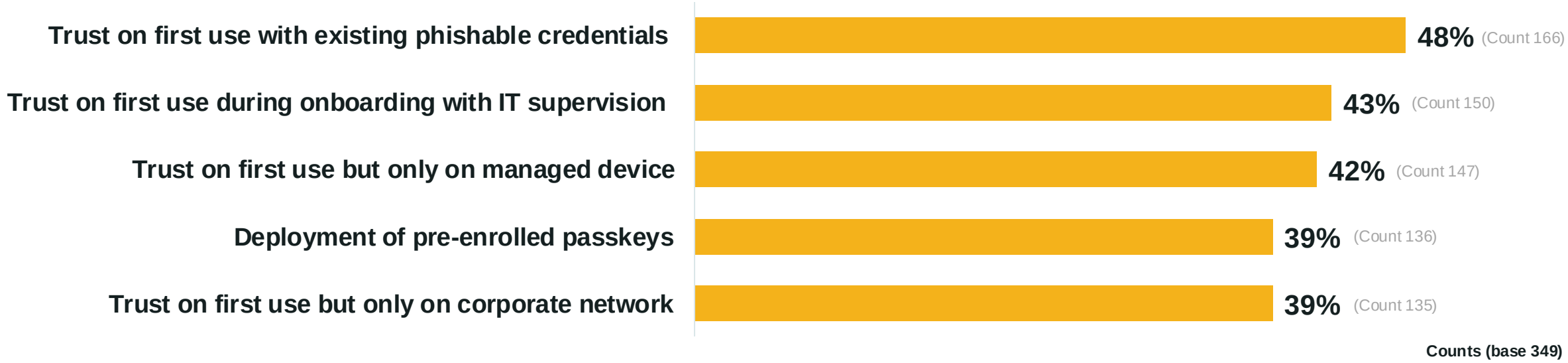
Key finding

2

Q8:

For existing users how did you / do you plan to rollout passkeys?

Select all that apply



Those deploying passkeys are rolling out in a variety of ways – there is no predominant method observed at this time

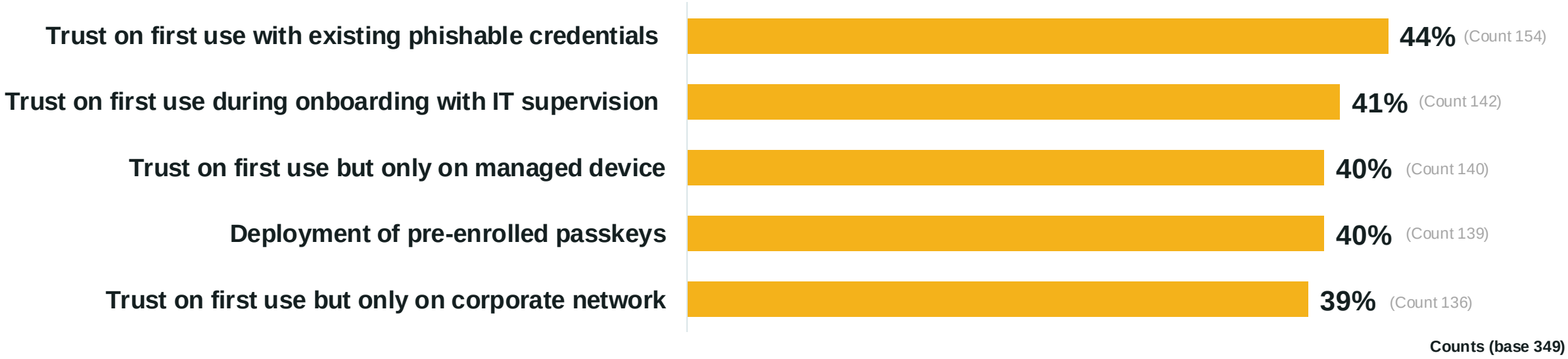
Key finding

2

Q9:

For new users how did you / do you plan to rollout passkeys?

Select all that apply



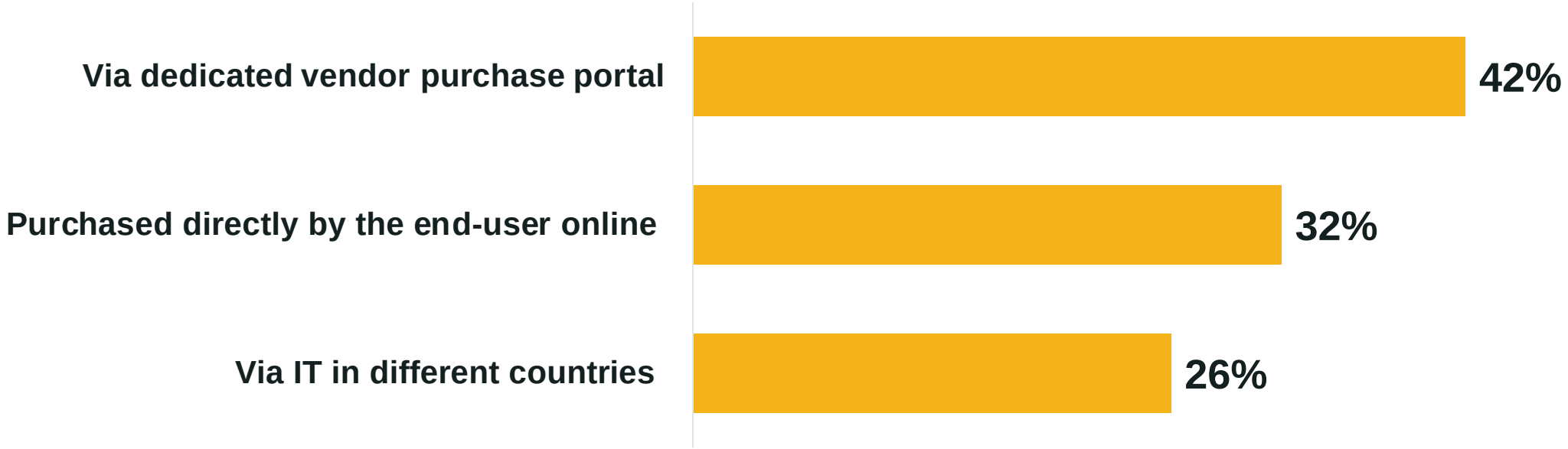
Those deploying passkeys are rolling out in a variety of ways – there is no predominant method observed at this time

Key finding

2

Q10:

If device-bound passkeys in the form of USB security key / smart card were deployed, how would you / did you manage the distribution to the end users? *Select one*



For those deploying device-bound passkeys, the distribution of hardware is mainly managed via online tools

Key finding 3

Enterprises are reporting significant security and business benefits after rolling out passkeys.

They report positive impacts on user experience, security, cost reduction, productivity and digital transformation goals — and are seeing declines in usage of legacy authentication methods.

Interestingly, these benefits directly correlate with what businesses who aren’t yet using passkeys dislike most about their current authentication methods: that they can be compromised, are costly, and difficult to use.

Key finding

3

Q11:

How did / do you measure the passkey deployment and its success?

Select all that apply

Enterprises are measuring progress and success through various metrics – primarily by looking at users' adoption: (% of users who activated passkeys or % of passkey based authentication)

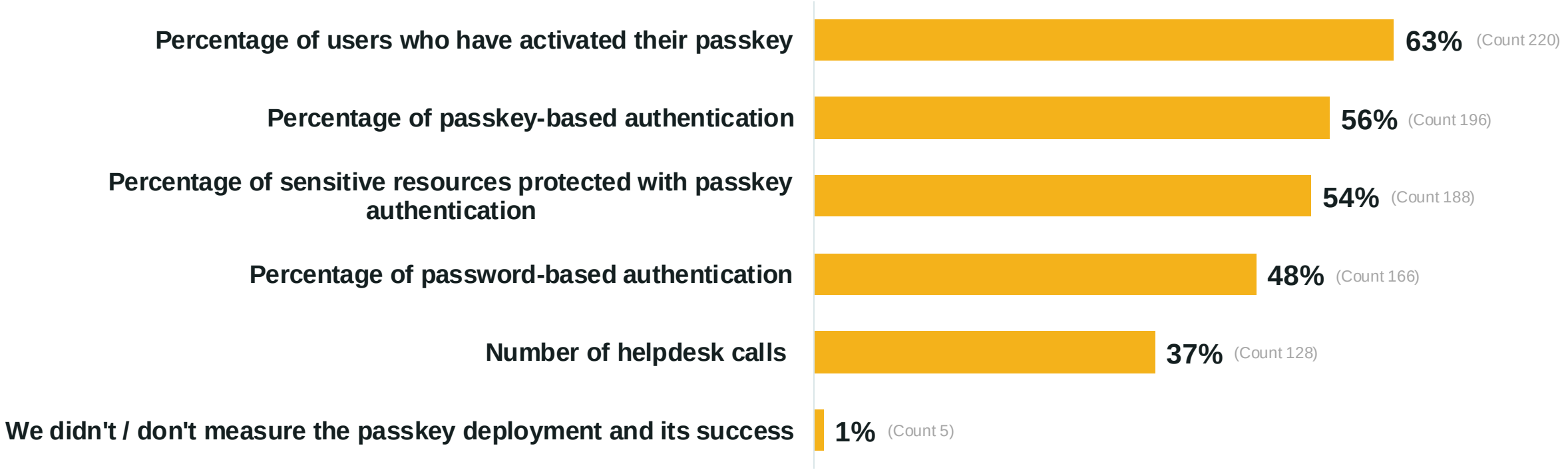
Key finding

3

Q11:

How did / do you measure the passkey deployment and its success?

Select all that apply



Counts (base 349)

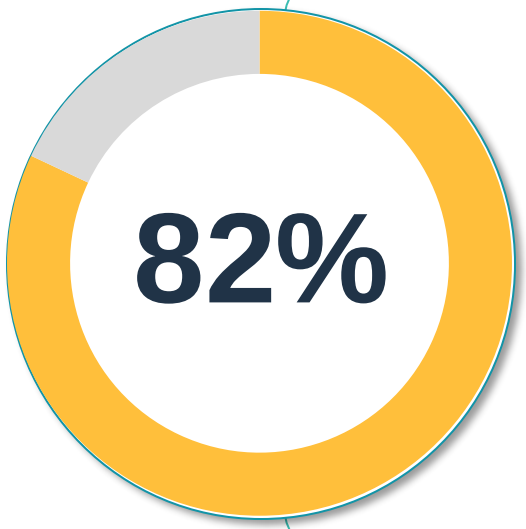
Key finding

3

Q12:

How much of an impact have passkeys made on the following?

User experience for login / authentication



said passkeys are having moderate to strong impacts on user experience

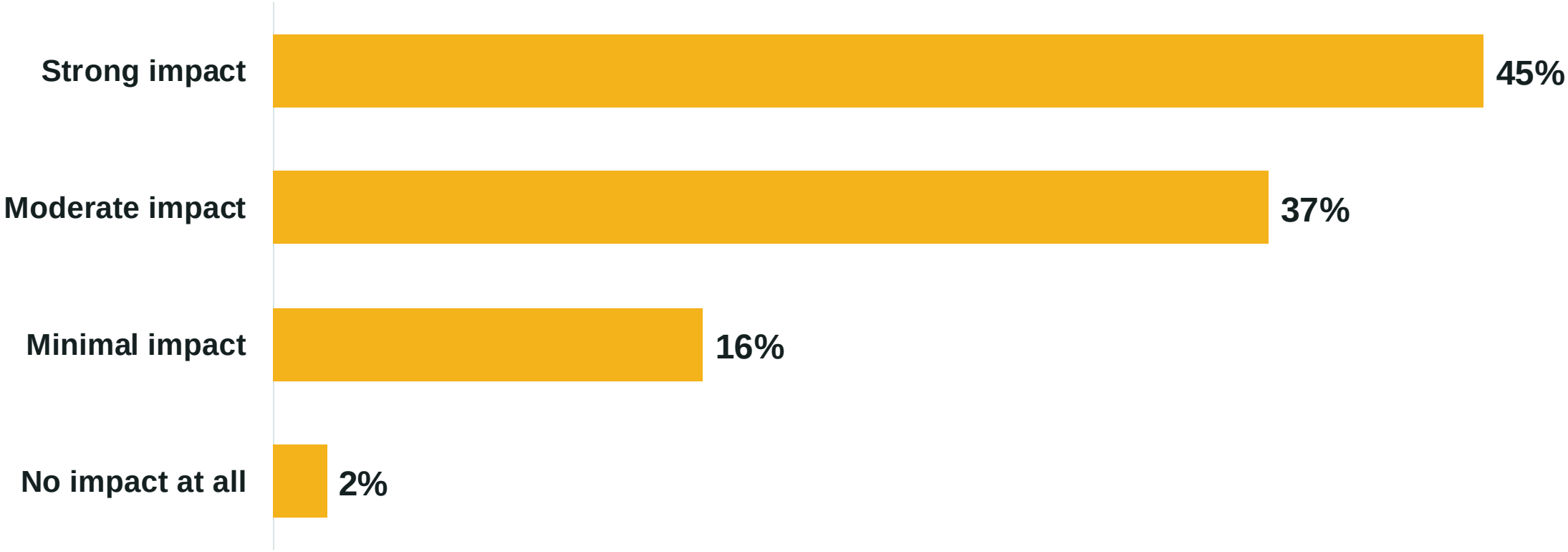
Key finding

3

Q12:

How much of an impact have passkeys made on the following?

User experience for login / authentication



Key finding

3

Q13:

How much of an impact have passkeys made on the following?

Increased security for login / authentication

said passkeys are having moderate to strong impact on increasing security for login/authentication

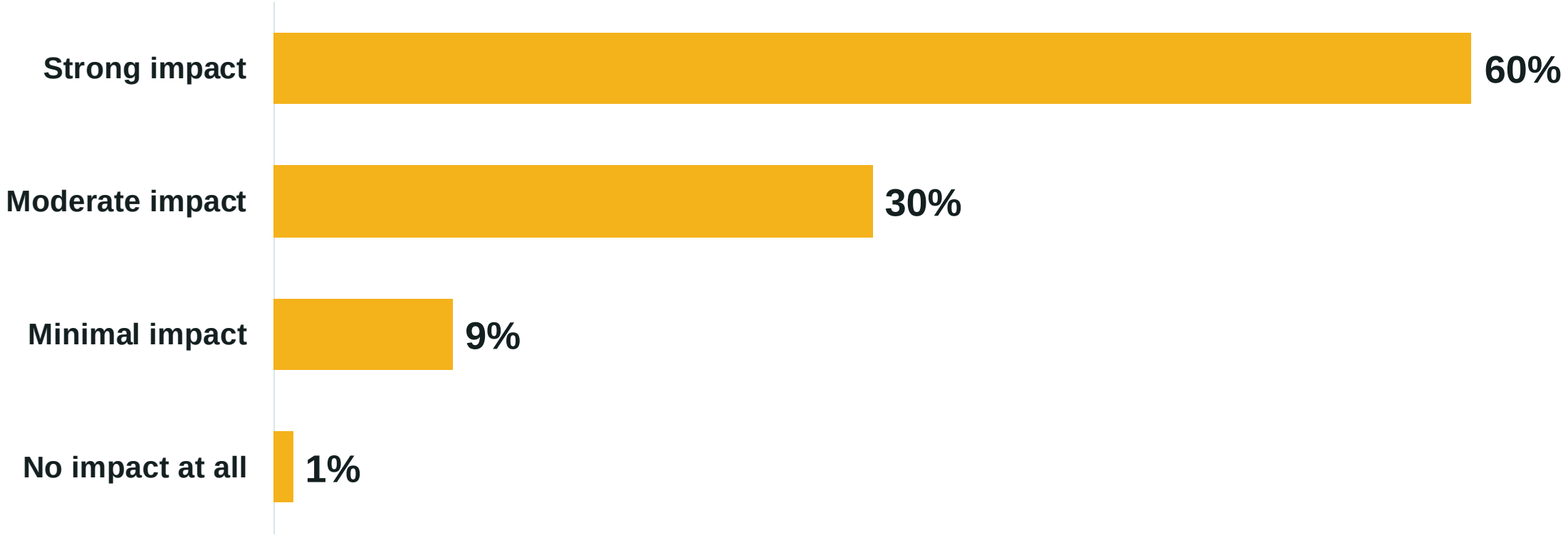
Key finding

3

Q13:

How much of an impact have passkeys made on the following?

Increased security for login / authentication



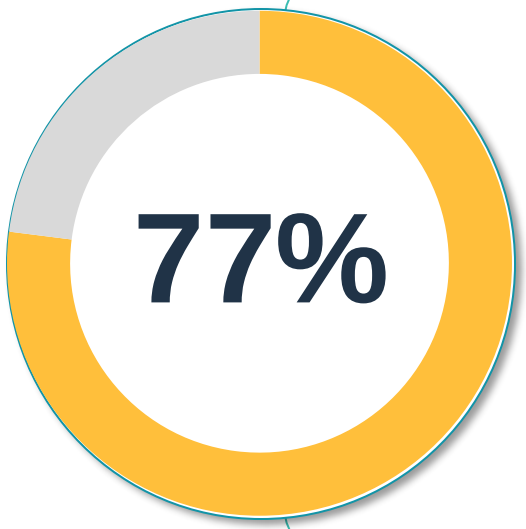
Key finding

3

Q14:

How much of an impact have passkeys made on the following?

Reduction in help desk calls



said passkeys are having moderate to strong impact on reducing help desk calls

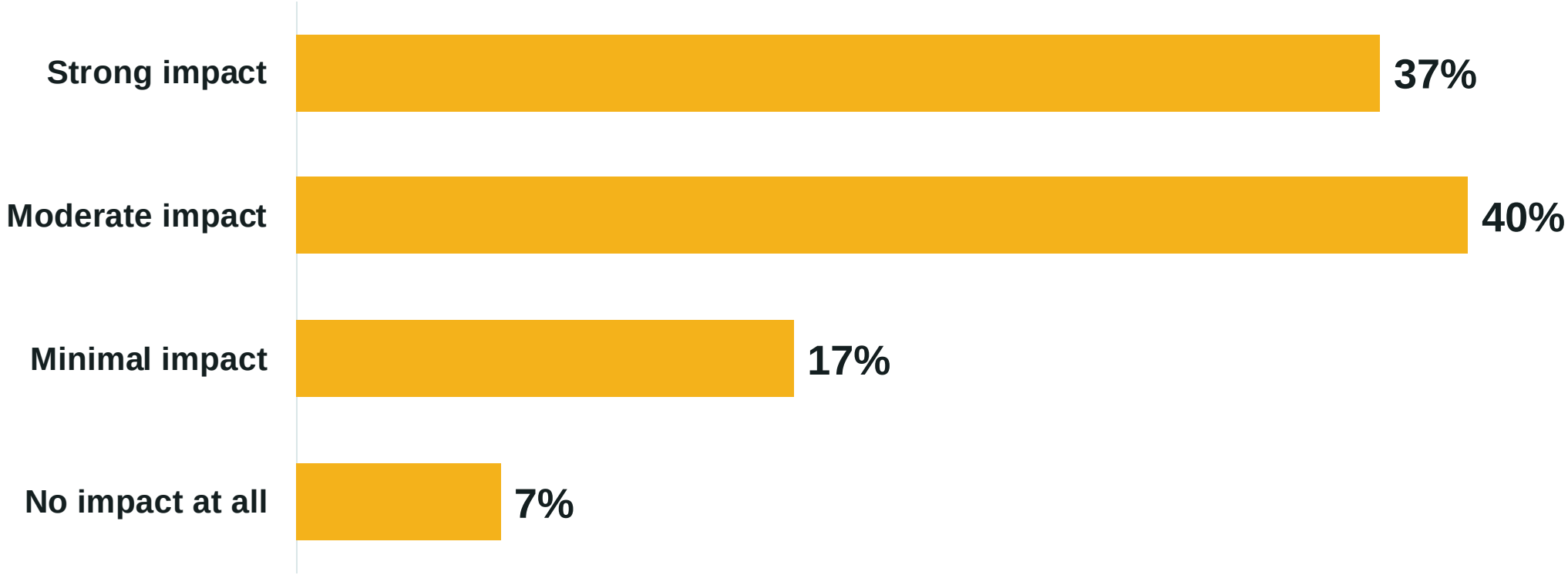
Key finding

3

Q14:

How much of an impact have passkeys made on the following?

Reduction in help desk calls



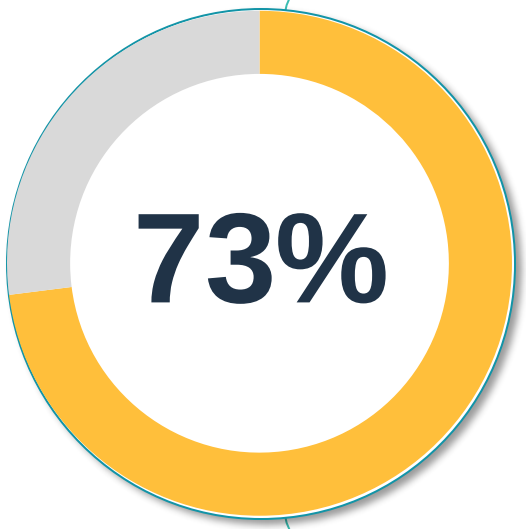
Key finding

3

Q15:

How much of an impact have passkeys made on the following?

Employee productivity



said passkeys are having moderate to strong impact on employee productivity

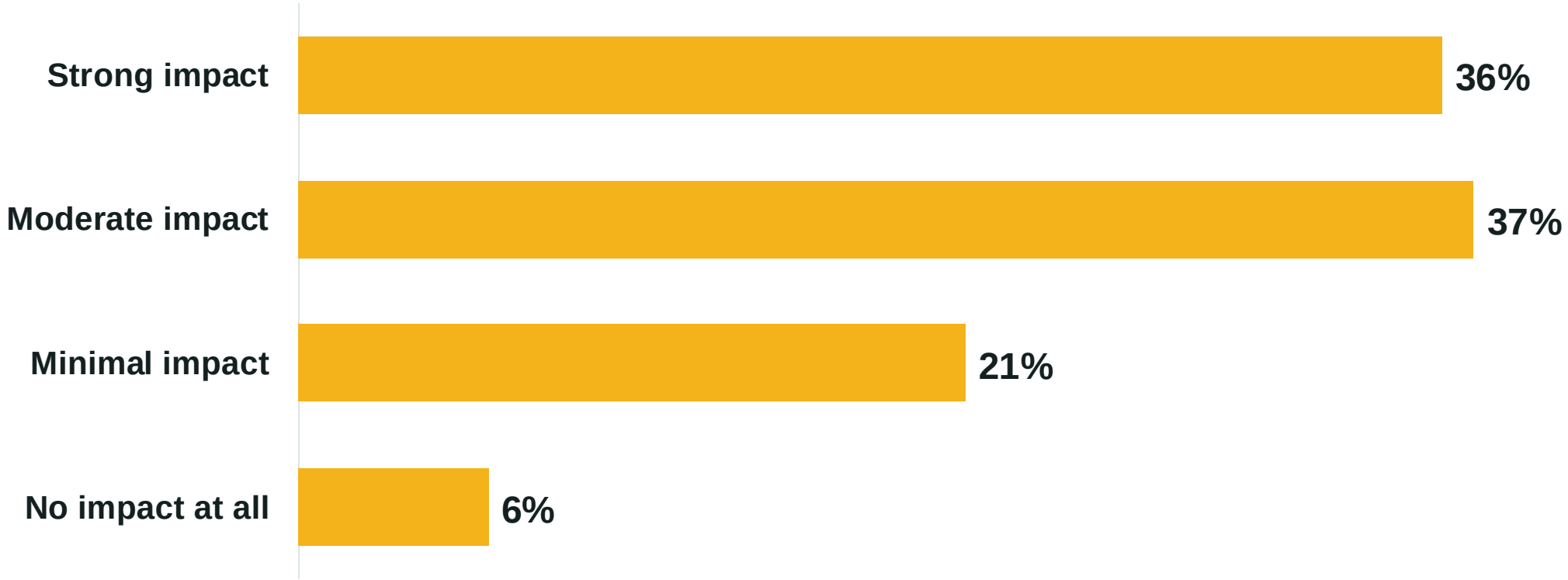
Key finding

3

Q15:

How much of an impact have passkeys made on the following?

Employee productivity



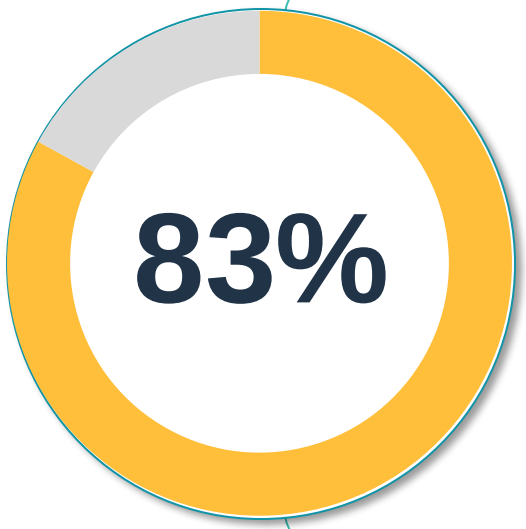
Key finding

3

Q16:

How much of an impact have passkeys made on the following?

Digital transformation goals



said passkeys are having moderate to strong impact on digital transformation goals

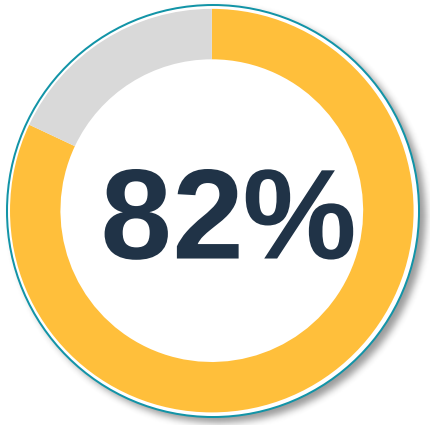
Key finding

3

Summary:

How much of an impact have passkeys made on the following?

User experience for login / authentication

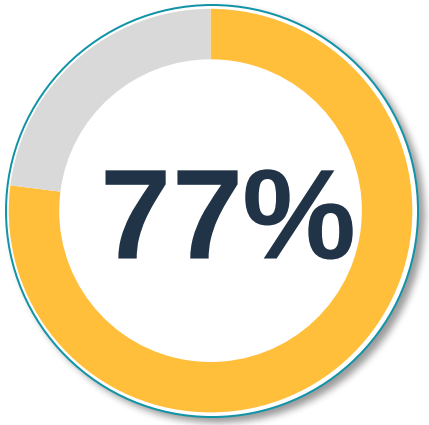


moderate to strong impact

Increased security for login / authentication

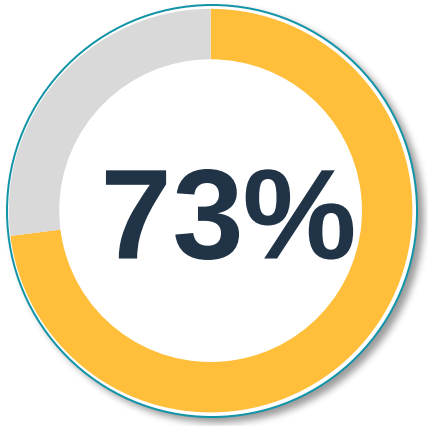
moderate to strong impact

Reduction in help desk calls



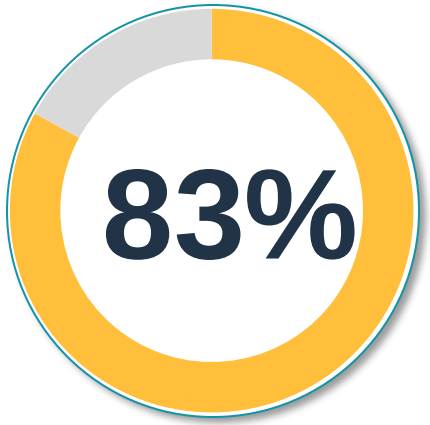
moderate to strong impact

Employee productivity



moderate to strong impact

Digital transformation goals



moderate to strong impact

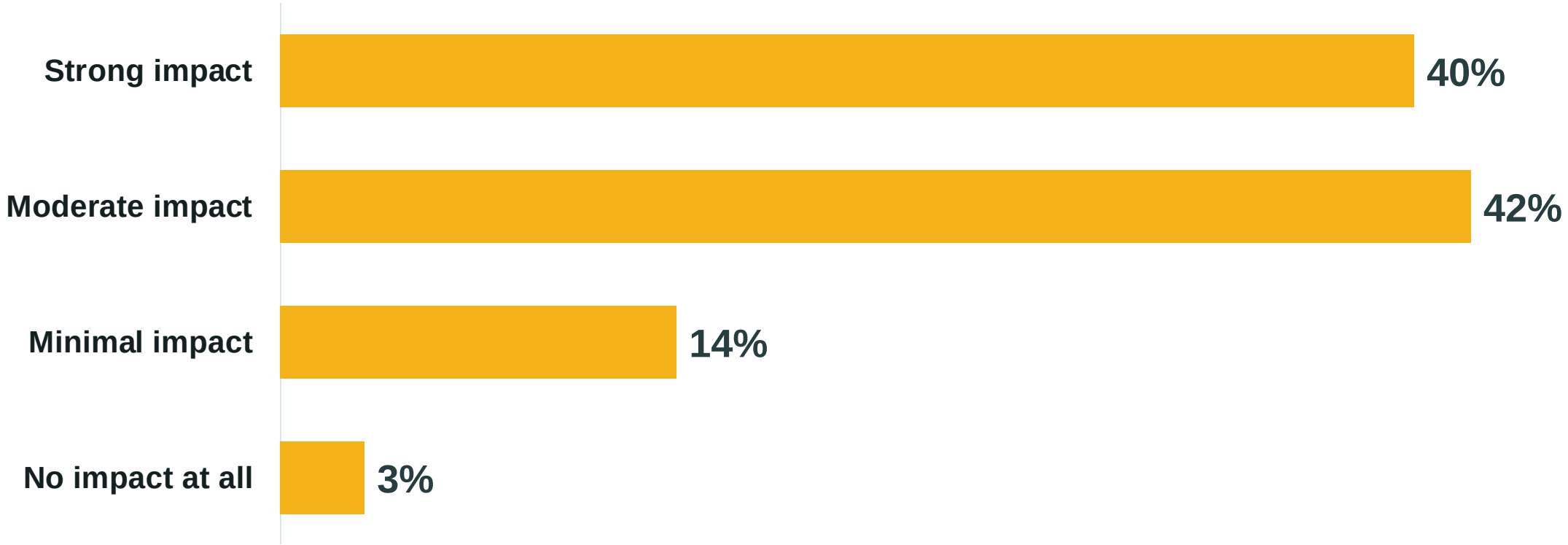
Key finding

3

Q16:

How much of an impact have passkeys made on the following?

Digital transformation goals



Key finding

3

Q17:

What alternative authentication methods were you using before passkeys?
What alternative authentication methods did you keep after deploying passkeys?
Select all that apply

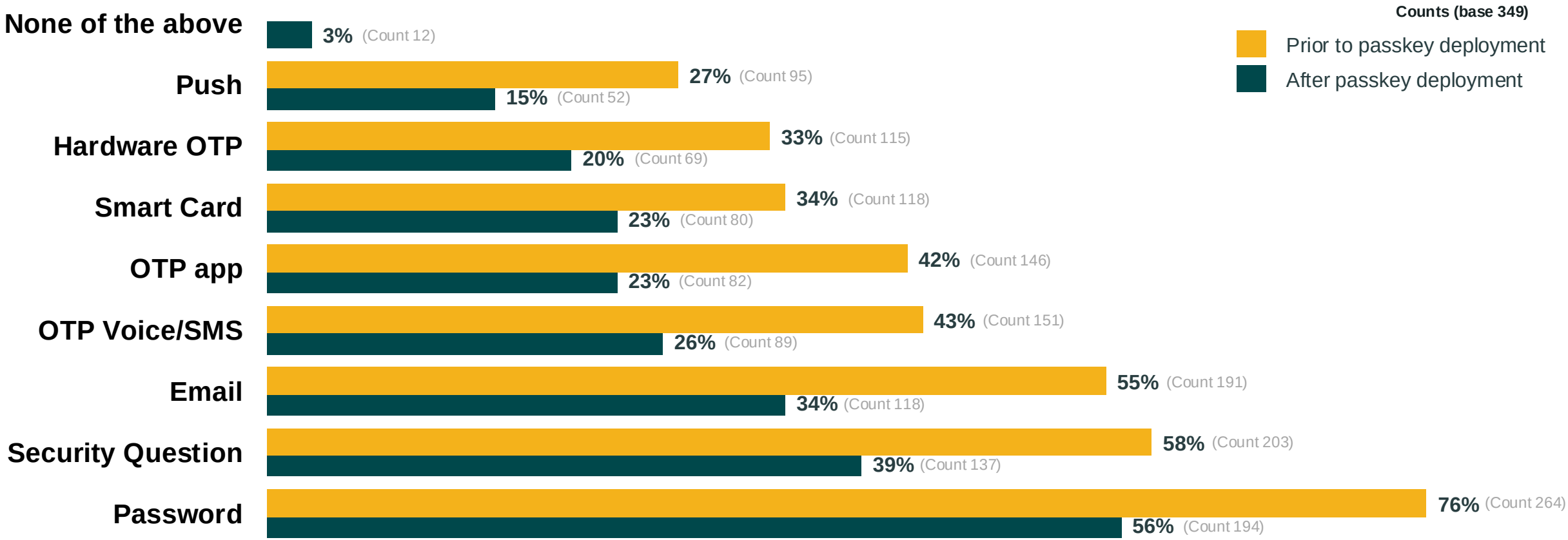
When looking at alternative methods used for authentication before and after passkeys, there are declines in usage across all other methods after passkeys were deployed - particularly usage of phishable forms of authentication such as passwords and SMS/email OTPs

Key finding

3

Q17:

What alternative authentication methods were you using before passkeys?
What alternative authentication methods did you keep after deploying passkeys?
Select all that apply



Key finding 4

Organizations that do not have active passkey projects cite complexity, costs and overall lack of clarity about implementation as reasons, signaling a need for increased education to enterprises on rollout strategies to reduce concerns.

Key finding

4

Q18:

What are the reasons that have delayed or prevented the use of passkeys in your organization?

Select all that apply

Organizations cite various reasons for not adopting passkeys, including complexity, costs and lack of clarity.

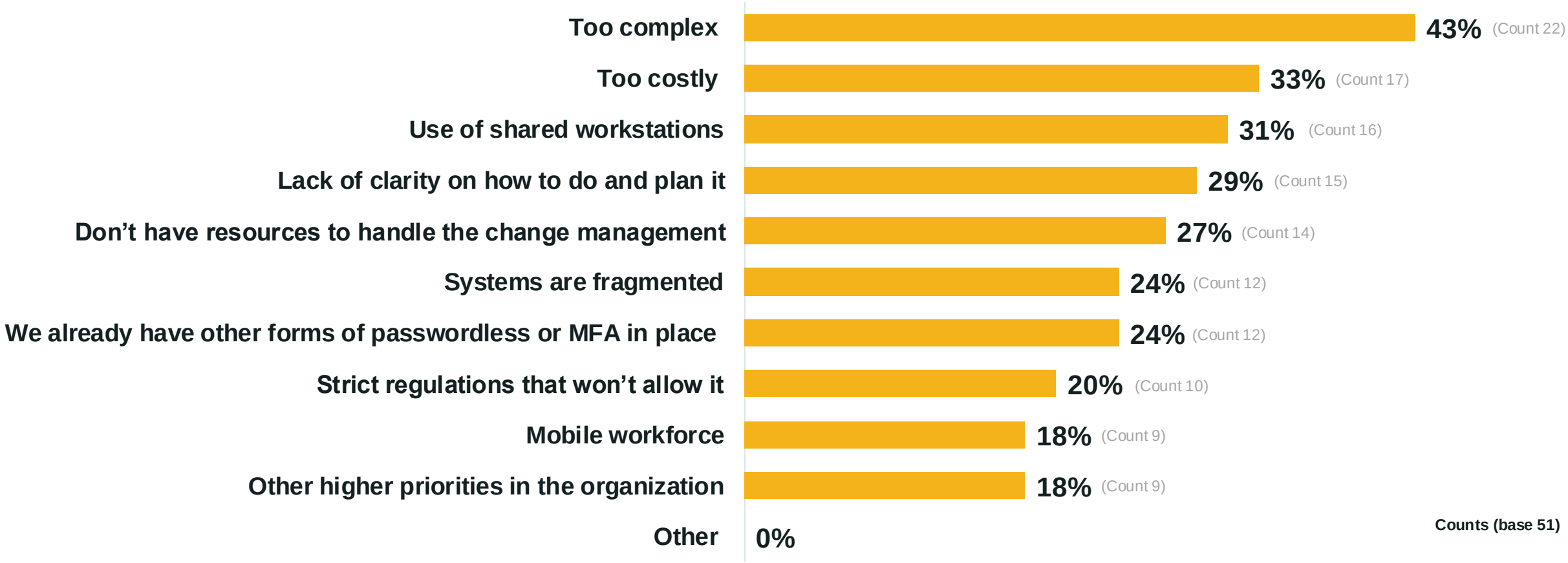
Key finding

4

Q18:

What are the reasons that have delayed or prevented the use of passkeys in your organization?

Select all that apply



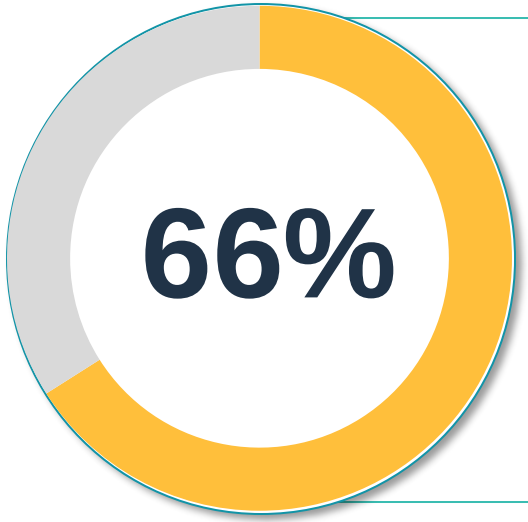
Key finding

4

Q19:

How likely do you believe it is that your organization will continue with the same authentication journey?

Select one



Two thirds believe it's likely their organization will continue with the authentication they have today

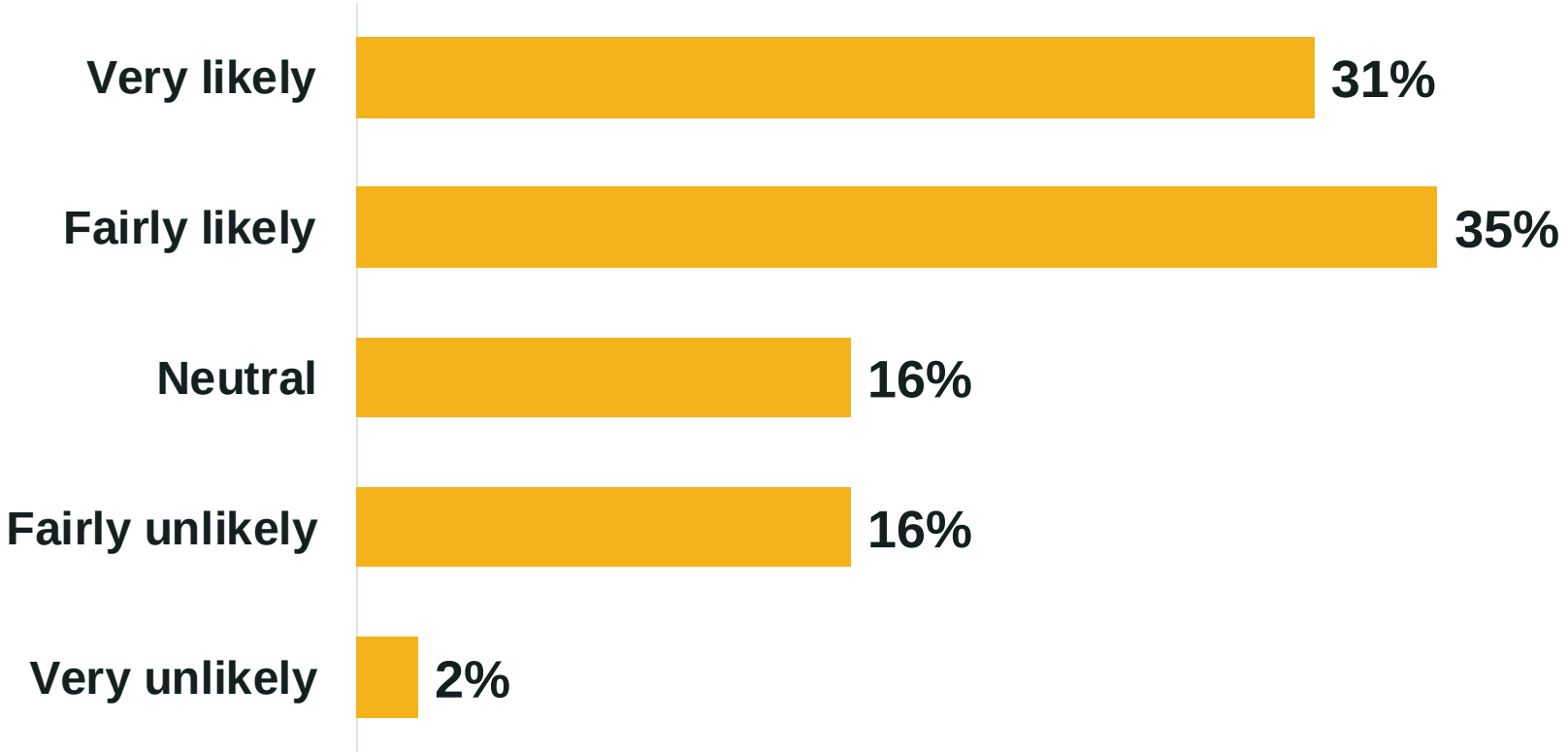
Key finding

4

Q19:

How likely do you believe it is that your organization will continue with the same authentication journey?

Select one



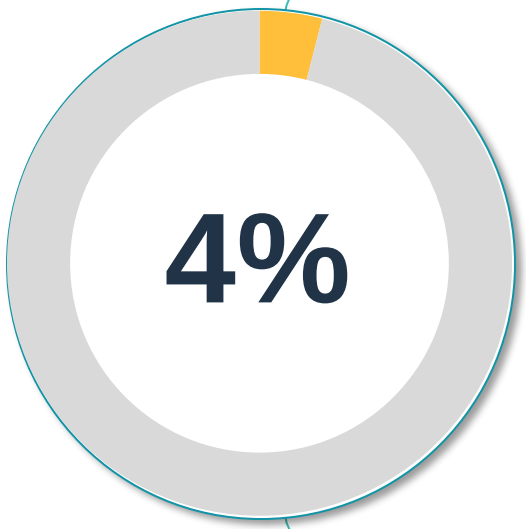
Key finding

4

Q20:

What do you dislike the most about your organization's current authentication journey without passkeys?

Select up to two



Only 4% say they are satisfied with the authentication they have today

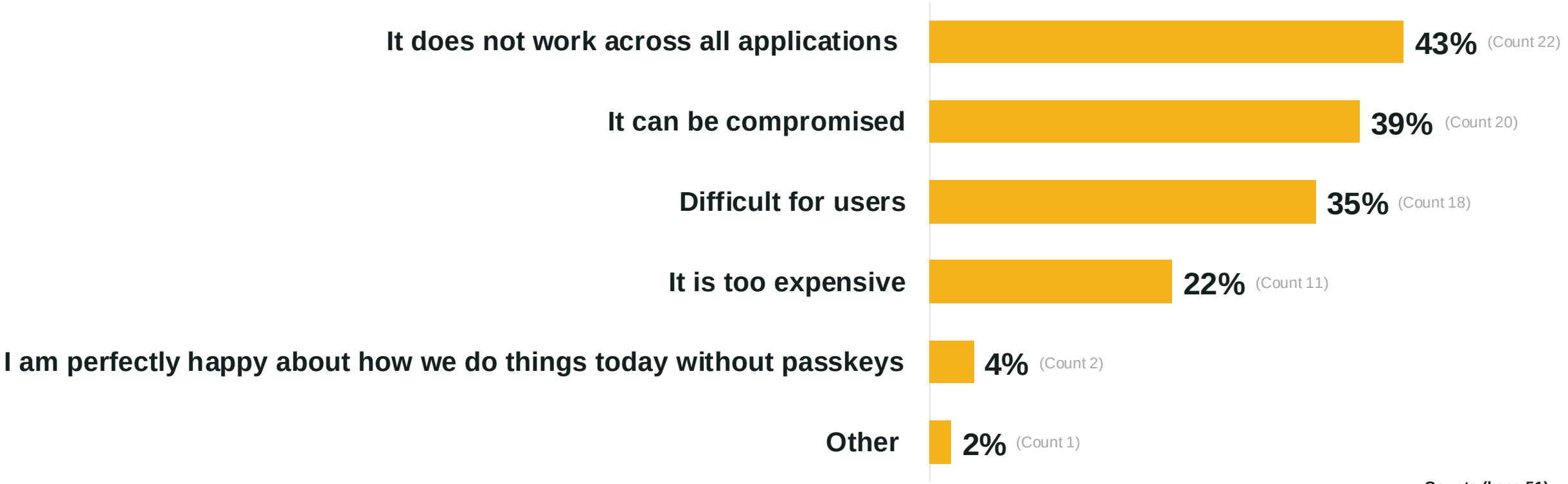
Key finding

4

Q20:

What do you dislike the most about your organization's current authentication journey without passkeys?

Select up to two



Counts (base 51)

Conclusion

As enterprises strive to abandon vulnerable authentication methods like passwords and SMS OTPs, this report highlights the growing consensus on the effectiveness of passkeys in improving usability, security, productivity, and more in workplace environments.

The data also shows how organizations with perceived challenges can shift those into opportunities to drive value and positive impacts, particularly for users handling sensitive information.

As enterprises navigate today's evolving threat landscape, organizations can leverage these insights along with FIDO standards and resources to learn how to deploy phishing resistant authentication for their workforce use cases.

The FIDO Alliance is committed to enabling leaders with actionable research and tools to support passkey adoption in the workforce. Learn more at passkeycentral.org and fidoalliance.org.

Our underwriters

About Axiad

Axiad is an identity security company whose products make authentication and identity risk management simple, effective and real. Our credential management systems make MFA defensible, manageable and usable. Our cutting-edge risk solutions help customers identify and quantify risk and fortify their systems against a barrage of new attacks.

Learn more at www.axiad.com.

About HID

HID powers the trusted identities of the world's people, places and things. We make it possible for people to transact safely, work productively and travel freely. Our trusted identity solutions give people convenient access to physical and digital places and connect things that can be identified, verified and tracked digitally. Millions of people around the world use HID's products and services to navigate their everyday lives, and billions of things are connected through HID's technology. We work with governments, educational institutions, hospitals, financial institutions, industrial businesses and some of the most innovative companies on the planet. Headquartered in Austin, Texas, HID has over 4,500 employees worldwide and operates international offices that support more than 100 countries. HID is an ASSA ABLOY Group brand.

For more information, visit www.hidglobal.com.

About Thales Cybersecurity Products

In today's digital landscape, organizations rely on Thales to protect what matters most - applications, data, identities, and software. Trusted globally, Thales safeguards organizations against cyber threats and secures sensitive information and all paths to it — in the cloud, data centers, and across networks. Thales offers platforms that reduce the risks and complexities of protecting applications, data, identities and software, all aimed at empowering organizations to operate securely in the digital landscape. By leveraging Thales's solutions, businesses can transition to the cloud with confidence, meet compliance requirements, optimize software usage, and deliver exceptional digital experiences to their users worldwide.

More on Thales Cybersecurity Products: www.cpl.thalesgroup.com.

More on Thales Group: www.thalesgroup.com.

fido ALLIANCE | simpler stronger authentication

About FIDO Alliance

The FIDO (Fast IDentity Online) Alliance, www.fidoalliance.org, was formed in July 2012 to address the lack of interoperability among strong authentication technologies, and remedy the problems users face with creating and remembering multiple usernames and passwords.

The FIDO Alliance is changing the nature of authentication with standards for simpler, stronger authentication that define an open, scalable, interoperable set of mechanisms that reduce reliance on passwords. FIDO Authentication is stronger, private, and easier to use when authenticating to online services.