

# Password decisions survey

2023

 **bit**warden

# Demographics

**43%**

C-level Executive

**85%**

Sole decision maker

**99%**

Full-time employee

**34%**

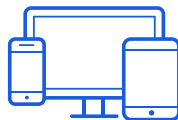
Director

**46%**

Age 35-44

**73%**

Bachelors or  
masters degree



**36%** Information Technology



**15%** Manufacturing and Construction



**9%** Finance/Accounting



**8%** Science/Programming/Software



**5%** Health Care

# About the survey

In Fall 2022, Bitwarden partnered with Propeller Insights to poll 800 independent IT decision makers across a wide range of industries who play a key role in enterprise purchasing decisions for the third iteration of this survey.

This year's findings show that passwordless technology has made inroads with businesses enthusiastic about its perceived security benefits and improved user experience (UX).

The survey also demonstrates a continued desire for C-suite-driven security leadership and underscores how security concerns are influencing business decisions.

# Password habits at work



# Strategies for managing passwords at work

Password management software remains popular – but so do risky practices such as writing down passwords or saving them on spreadsheets

84%

Password management software

54%

Document on my computer

45%

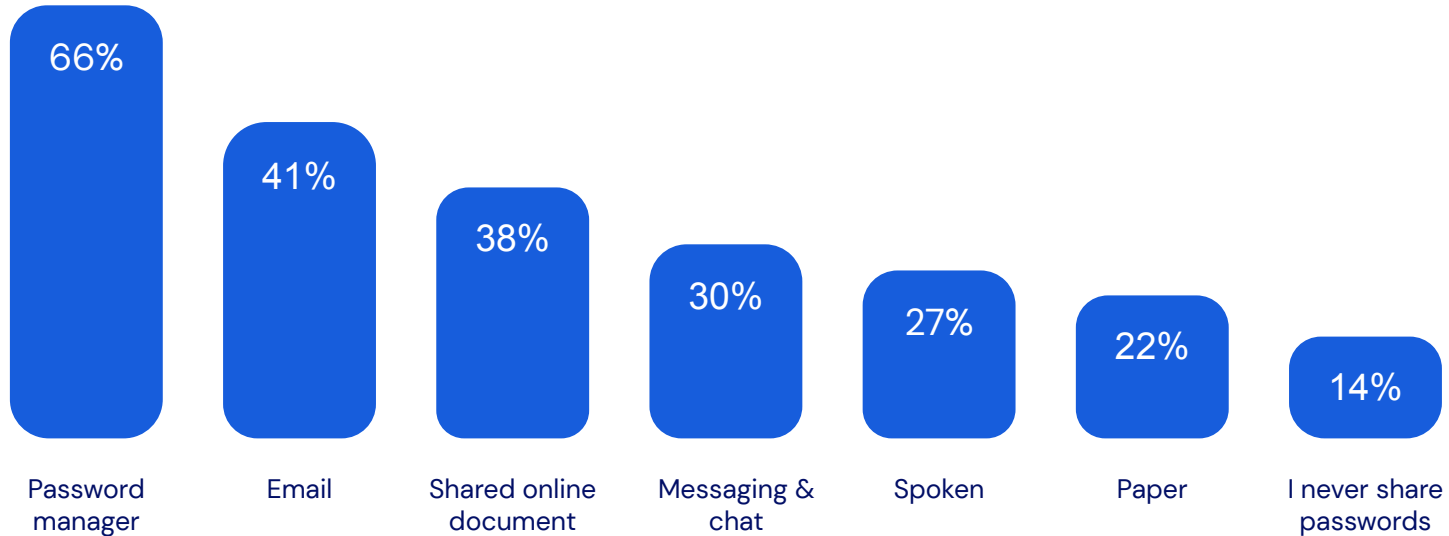
My memory

29%

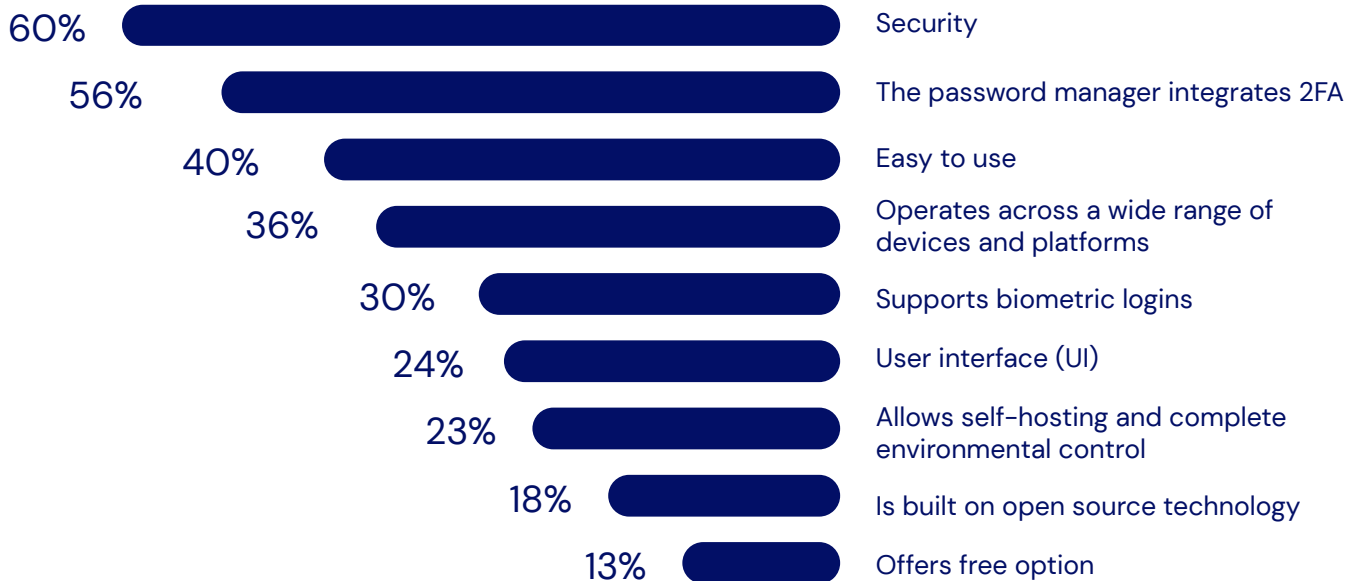
Pen and paper

# Password sharing methods

Most (66%) of IT decision makers share passwords through a password manager but a sizable number also share via email and online documents



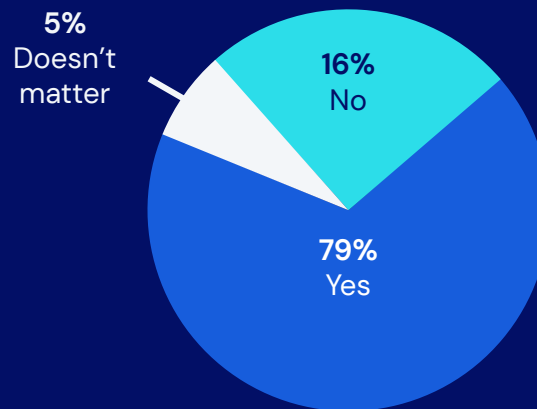
# Most important attributes for a good password manager



# Enterprise-wide password manager

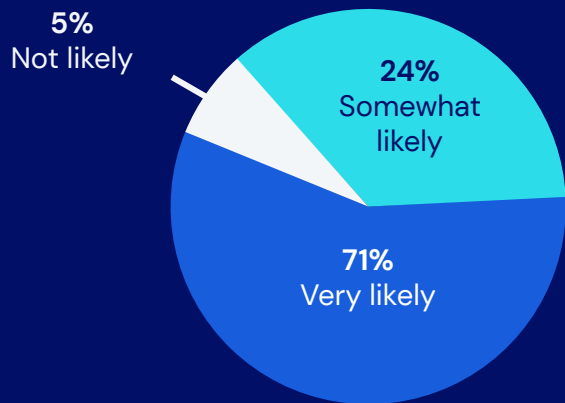
A large majority (79%) want their employer to require employees to use the same password manager across the organization

Would you like your employer to require employees to use the same enterprise-wide password manager across the organization?





If your company used a password manager and provided a complementary family account for personal use, how likely would you be to use it at home with your family?



## Complementary family account

If offered, 71% said they'd also be very likely to use a password manager at home

# Password reuse

Almost all (90%) reuse passwords

11%

More than 15 sites

24%

10-15 sites

36%

5-10 sites

19%

1-5 sites

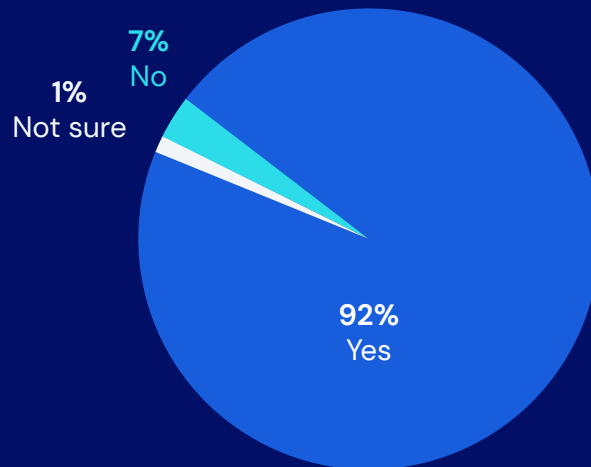
10%

Never reuse

## 2FA is wildly popular

92% use it in the workplace, up from 88% last year

Do you use two-factor authentication in the workplace?



Why do you think people may be reluctant to utilize two-factor authentication technology at work or for personal use?

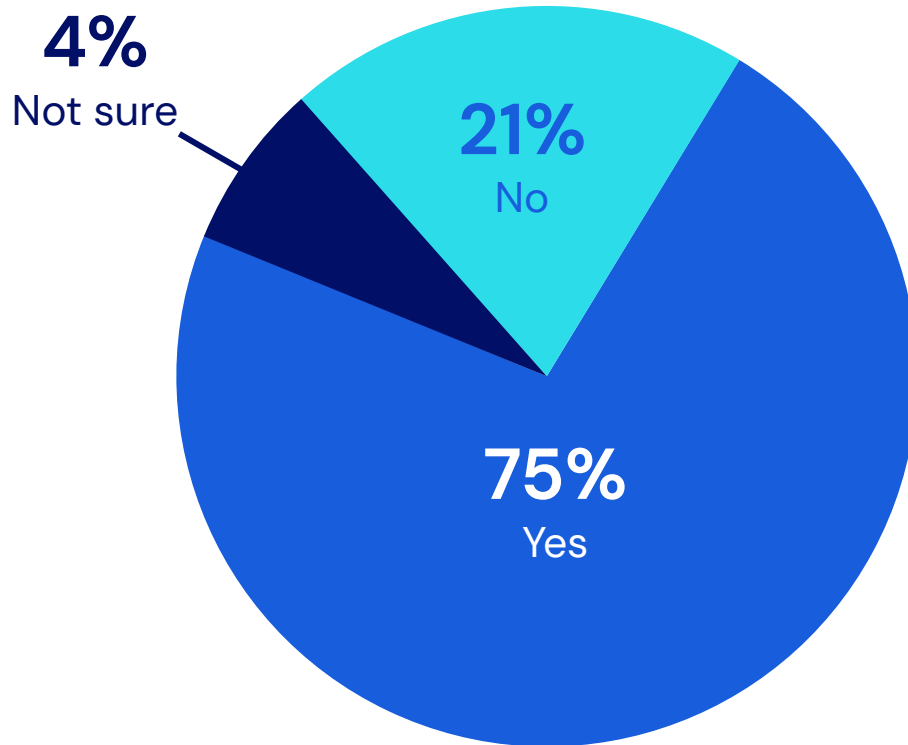


## Ignorance is not bliss

Almost half (48%) believe people who are reluctant to use 2FA are not aware of the benefits

# Does your organization have cyber insurance?

Almost three-fourths (75%) say their organization has cyber insurance



# Cyber insurance requirements

Show your work: 65% were required to demonstrate they offered cyber awareness training to employees when they applied for cyber insurance. 64% had to show use of MFA. 61% had to demonstrate use of a password manager



# Security risks & cyber attacks



# Which entity are phishing attacks most often pretending to be?

Close to half (41%) of phishing attacks come from fake financial institutions

41%

My financial institution

22%

My boss or exec

21%

Government entity

8%

Family member or friend

6%

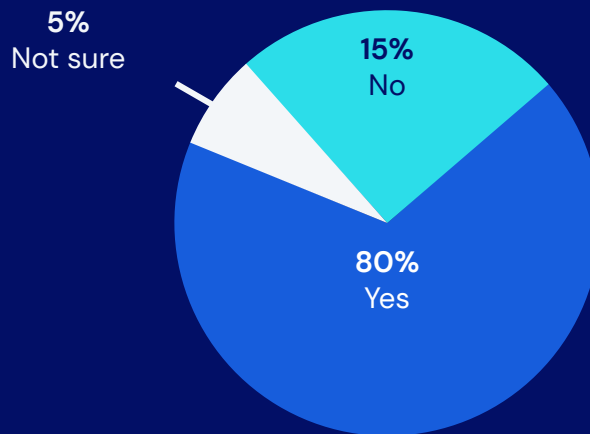
Healthcare organization



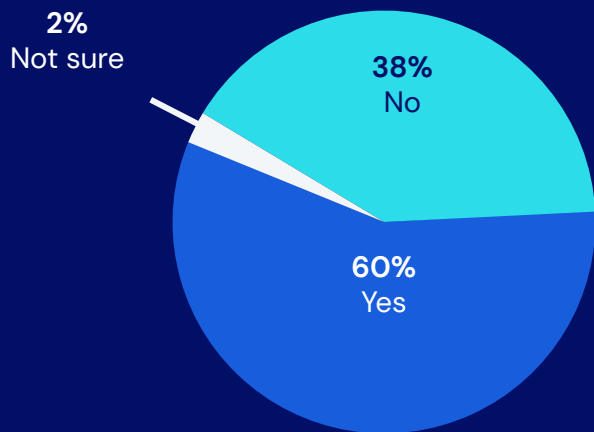
# Ransomware migration strategy

Up from 75% last year, 80% report having a ransomware mitigation strategy in place

Does your organization have a ransomware mitigation strategy?



Has your organization ever experienced a cyberattack?



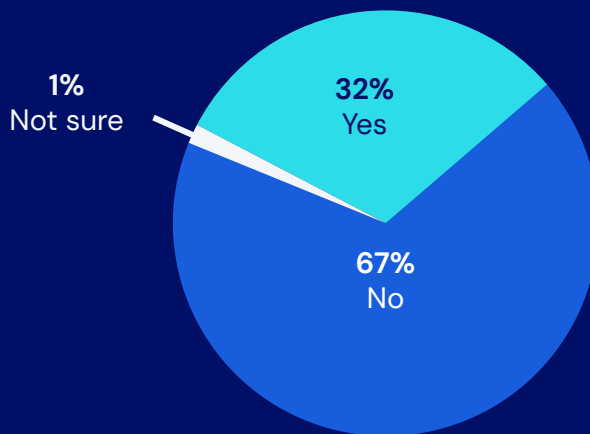
## Cyberattack experiences

The percentage reporting cyberattacks is up: 60% this year, compared to 54% last year

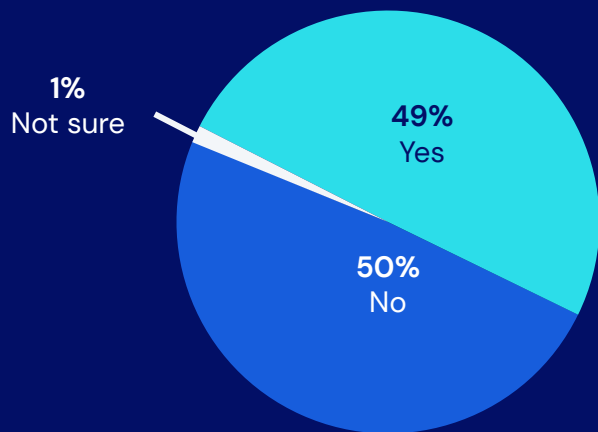
# Shadow IT Engagement

Almost one-third (32%) of IT decision makers and 49% of employees engage in 'shadow IT'

Have you ever used unauthorized devices or software without IT's approval?



Has your organization struggled with employees using unauthorized devices or software without IT's approval?



## Shadow IT Struggles

Almost half (49%) report employees engage in 'shadow IT'

# Why do you think employees within your organization use unauthorized devices or software without IT's approval?

Most believe employees do it because they think it makes them more efficient

73%



They believe it helps make their day-to-day 'on the job' activities faster and more efficient

52%



Lack of authorization for certain applications or software they want to use

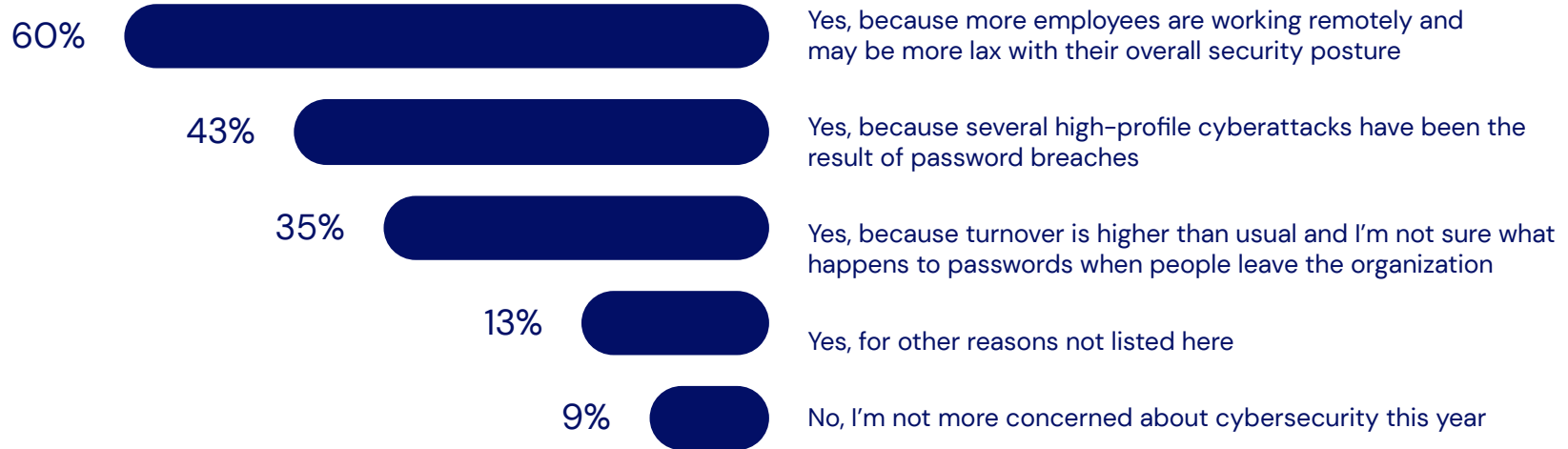
50%



Slow response times to IT-related issues involving company-issued devices and software

# The persistence of remote work continues to drive cybersecurity concerns

Have you become more concerned about cybersecurity in the past year?

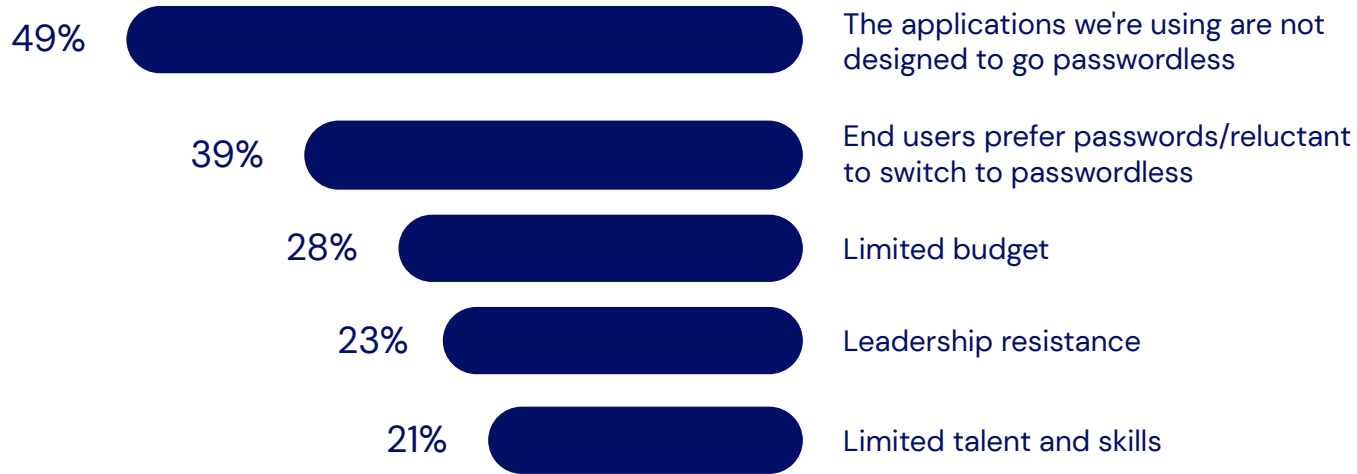


# Passwordless revolution



# Why has your organization not deployed passwordless?

Of the IT decision makers that have not gone passwordless, half cite the inability of applications in use to make the transition

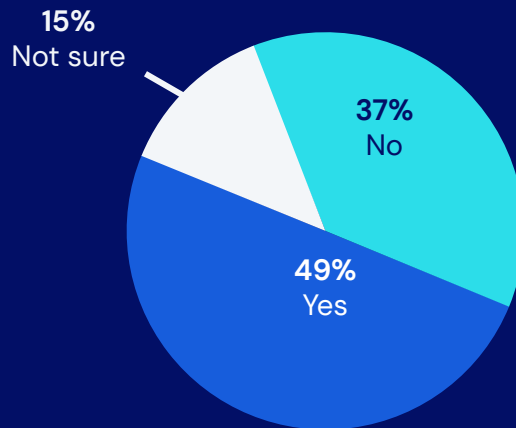




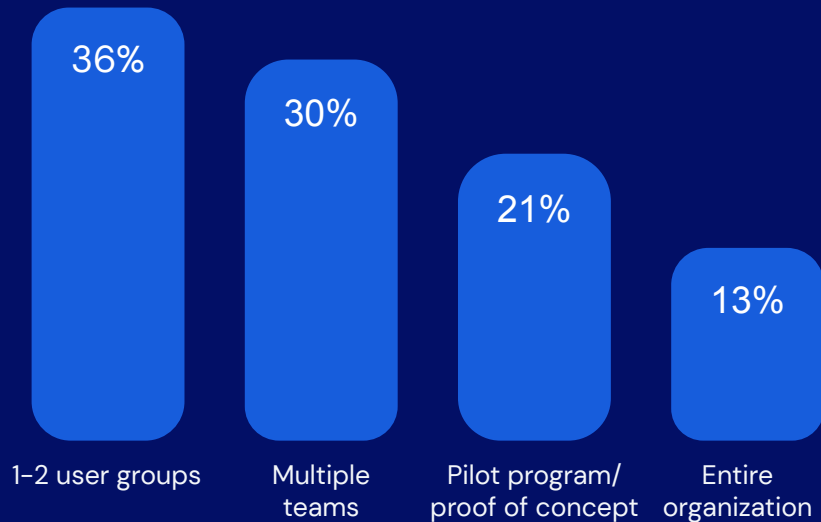
# Deploying passwordless

Around half (49%) are deploying or have plans to deploy passwordless tech

Do you currently deploy, or have future plans to deploy, passwordless?



How far along are you in your deployment?

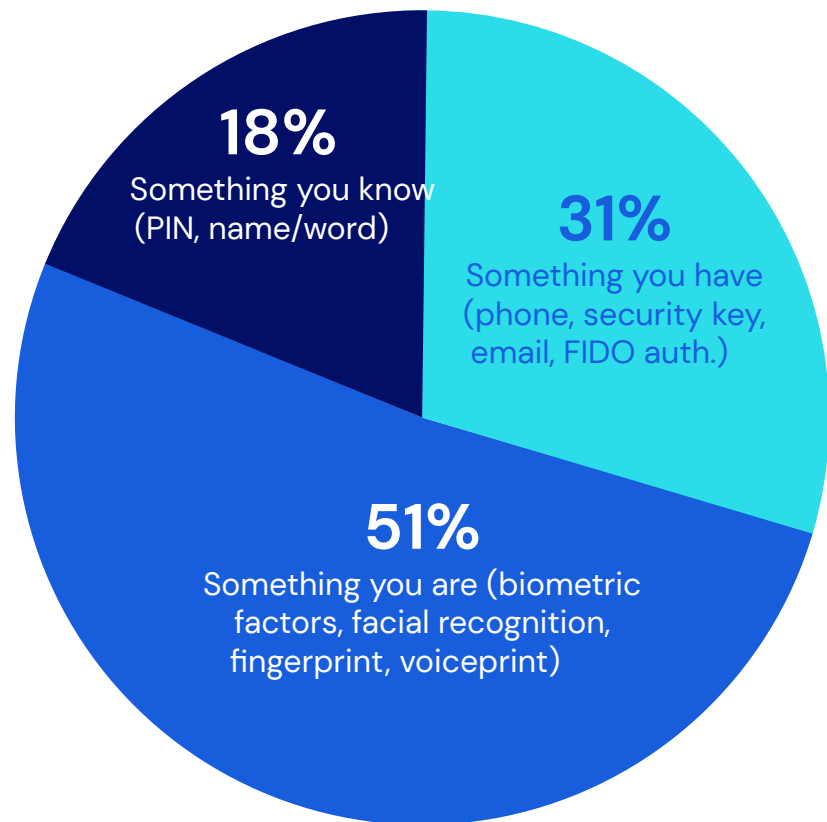


## Deploying passwordless

Two-thirds (66%) have 1-2 users groups or multiple teams going passwordless

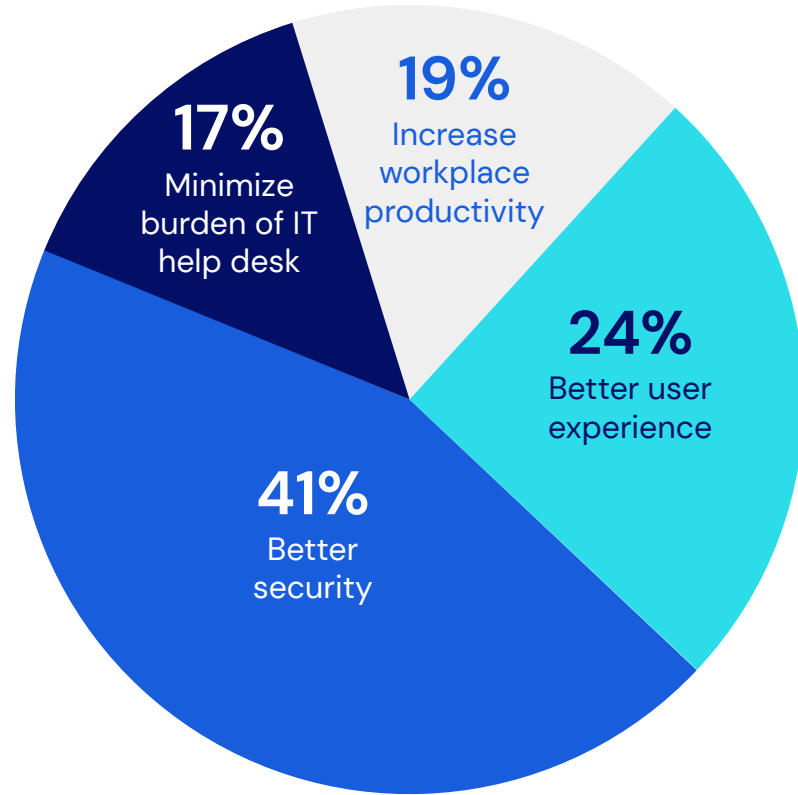
# Passwordless authentication

A majority (51%) are relying on the 'something you are' form of passwordless authentication



# The primary reason to deploy passwordless?

Better security, say 41%



# FIDO2 Gaining

47% say FIDO2 is an 'important aspect' of their passwordless adoption

