LastPass •••|

fido ALLIANCE | simpler stronger authentication

The 2023 Workforce Authentication Report:

Embracing the Passwordless Future

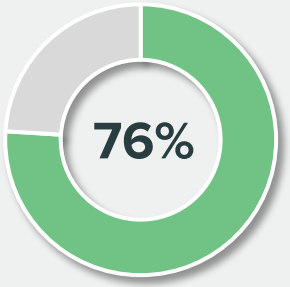
Research was conducted by Sapio Research through an online survey of 1,005 IT decision makers in the United States, Germany, Australia, United Kingdom, and France.

Executive summary

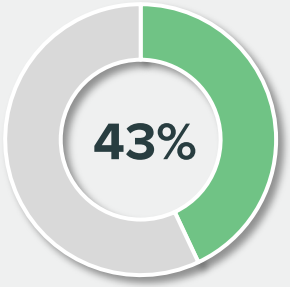
- 92% of businesses have or plan to move to passwordless technology with 95% of businesses currently using a passwordless experience at their organization. 89% of IT leaders expect passwords will represent less than a quarter of their organization's logins in 5 years or less.
- The main barrier to passwordless adoption is education: 55% of IT leaders feel they need more education on how the technology works and/or how to deploy it.
- A majority of businesses are still using phishable authentication methods, such as passwords (76%) and MFA (43%) when it comes to authenticating users within their organization.
- 92% of IT leaders believe passkeys will benefit their overall security posture; and 93% of IT leaders agree that passkeys will eventually help reduce the volume of unofficial (Shadow IT) applications.
- A majority of IT leaders (50%) believe that passwordless authentication will reduce the need for non-passwordless MFA offerings; 56% believe it will also result in a reduction in IT help desk requests.

Businesses are still relying on a plethora of layered phishable authentication methods.

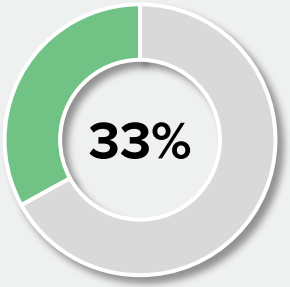
What are the current methods of authentication used within your organization?



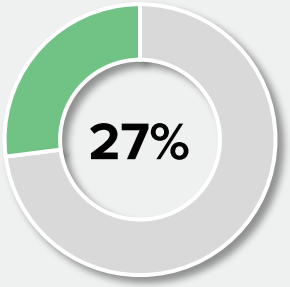
Passwords
(including all entry methods)



Multi-Factor Authentication
(MFA)

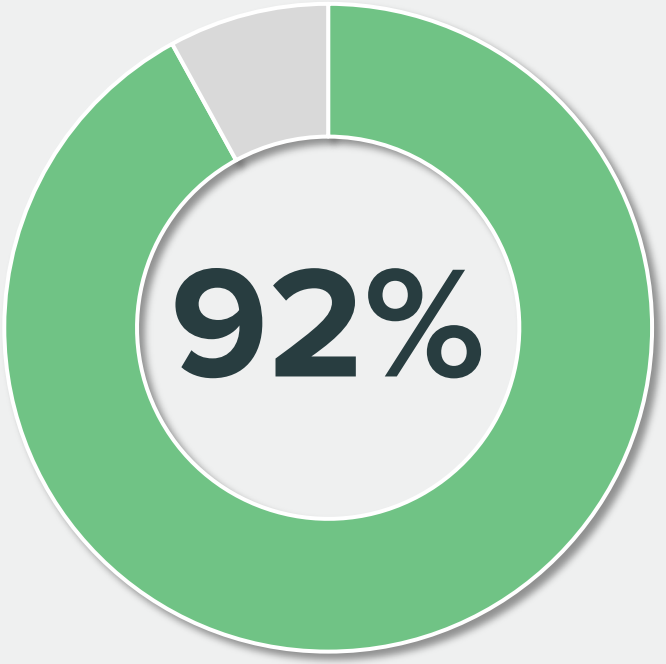


One-Time Passcodes
(OTPs)



Single Sign-On
(SSO)

With security top of mind, businesses have rapidly become aware of passkeys and passwordless authentication – and their impact on securing their data.



84% of IT leaders are familiar with passkeys **while 92% said passkeys will benefit their overall security posture.**

Businesses want to choose where they store passkeys, with **69% of IT leaders anticipating storing them in a third-party password manager** while 30% would store them in a browser-based password manager.

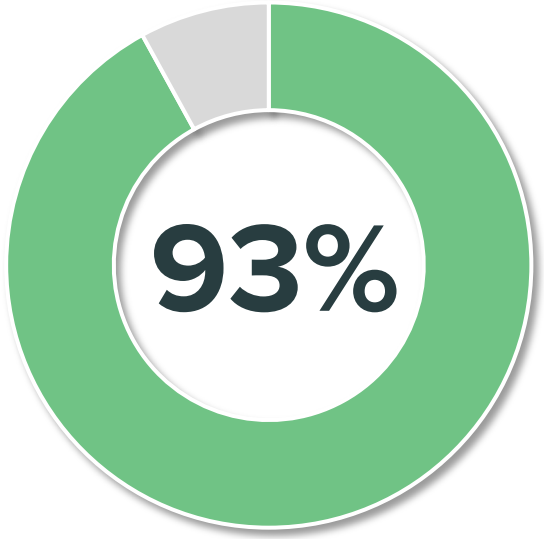
Businesses see a wide range of benefits to implementing passwordless authentication – including improving security posture, consolidating their tech stack, lessening strain on IT resources, and making the employee user experience more seamless.

Which of the following effects do you expect passwordless authentication to have on your business?

- **50%** Reducing the need for non-passwordless MFA offerings
- **48%** Reducing the need for SSO
- **47%** Reduction in support desk tickets
- **46%** Reducing the need for privileged access management
- **42%** Streamline onboarding / offboarding employees

What do you believe the main benefits of passwordless authentication will be?

- **59%** Improved security posture
- **56%** Reduction in IT help desk requests
- **50%** Improved user experience
- **36%** Regulatory compliance
- **33%** Cost savings



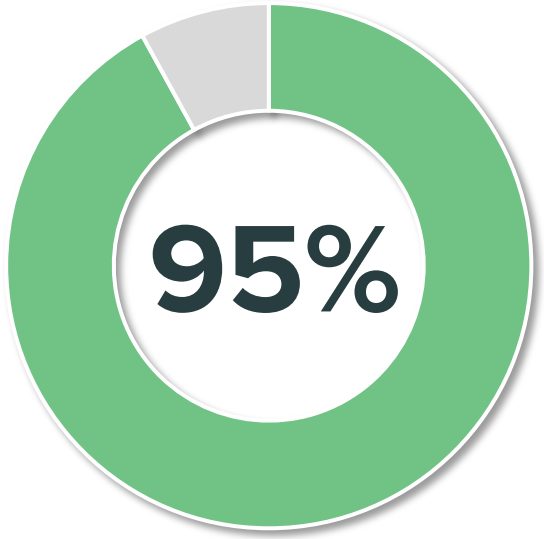
93% of IT leaders agree that passkeys will eventually help reduce the volume of unofficial (Shadow IT) applications.

Which makes sense since most businesses would use a password manager to store passkeys, making these apps more visible on the admin level.

As with any emerging technology, businesses have taken stock of potential barriers to adoption, primarily highlighting a need for education around security and implementation of the new technology.

What are your main barriers to adoption of passwordless authentication?

- **55%** Feel they need more education on how the technology works and/or how to deploy
- **31%** Fitting with existing infrastructure
- **28%** Resistance to change by end users / using new technology
- **26%** Solution not fully mature and will require change management
- **23%** Unproven technology / not yet adopted market-wide



The way we talk about passwordless – solution vs. experience – must evolve too, when **95% of businesses are using a passwordless experience** (no longer typing or entering a password) rather than a solution (completely removing the password).

Even so, 92% of businesses already have or plan to move to passwordless technology. And 89% of IT leaders expect passwords will represent less than a quarter of their organization's logins in 5 years or less.

Respondents identified these as the main drivers to invest in passwordless authentication:

- **18%** Security concerns with existing authentication solution (e.g., traditional MFA)
- **17%** Increasing employee productivity
- **17%** Securing the hybrid work environment
- **14%** Preventing breaches / remote attacks
- **9%** Standards compliance
- **8%** Workstation login
- **8%** Existing solution not user friendly
- **6%** Other successful companies / peers have also deployed

While passwordless is on the horizon for many businesses, **it will be a marathon not a sprint** to reach a fully passwordless environment.

LastPass •••|®

About LastPass:

LastPass is an award-winning password manager which helps millions of registered users organize and protect their online lives. For more than 100,000 businesses of all sizes, LastPass provides password and identity management solutions that are convenient, easy to manage and effortless to use. From enterprise password management and single sign-on to adaptive multi-factor authentication, LastPass for Business gives superior control to IT and frictionless access to users.

www.lastpass.com

fido ALLIANCE | simpler stronger authentication

About the FIDO Alliance:

The FIDO Alliance was formed 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.

www.fidoalliance.org