Deloitte.

Moving beyond passwords with digital authentication systems

In 2016, Deloitte published an article on the challenges around passwords that were creating the conditions for disruption, the potential of passwordless authentication as a solution, the emerging technologies that could support adoption and what was likely to evolve in the future. It proved to be prescient.

The password problem

Weak, reused, and compromised passwords were common problems for users and those responsible for security in 2016. Seven years later, little has changed, and passwords still pose a significant security risk. Fortunately, many technologies that were emerging then are now mainstream, offering more options and flexibility for organizations that want to do away with passwords yet still maintain—and in many cases may improve—not just security, but also the user experience.

While the use of passwords may protect a user's identity and personal data, in today's digitally connected world, 100% security is simply not possible if you are online. Unfortunately, for customers, business associates, frontline employees, and executives, having to remember and enter ever more complicated passwords to complete a task does not provide a good user experience. And in terms of security, passwords still represent one of the weakest links.

A 2023 survey by password management company NordPass found the average person has 100 passwords.[1] Interestingly, this represents a 25 percent increase over a similar poll taken between 2019 and 2020 by the same company.

> "In 2023, the average person has 100 passwords." [1]

With the number of passwords increasing, users often fall back on poor practices to make their lives easier—and that's a problem. According to password management software provider LastPass, 50 percent of people in 2023 are still using the same password on all their accounts,[2] while cybersecurity provider Dataprot found that 51% of people share passwords for work and personal accounts.[3] And in many cases, the choice of passwords still leaves a lot to be desired. Even today, the most popular passwords are still "123456," "123456789," "qwerty," and "password." [4]

Not surprisingly, passwords are a favorite target for hackers. According to WebsteBuilder.org,[2] hacking attacks that use scripts to guess usernames and passwords happen every 39 seconds, globally. Furthermore, Verizon's Data Breach Investigations Report[5] found that "an estimated 81% of data breaches are due to poor password security." As demonstrated through various use cases, corporate cyber breaches often have significant costs associated with technology, legal, and public relations expenses—not to mention less tangible but more damaging hits to reputation or credit ratings, loss of contracts, and other costs.

Biometrics and the evolution of fast identity online (FIDO)

In 2016, when Deloitte authored its first article on the possibilities of a world without passwords, the idea was just beginning to gain traction at the corporate level. At that time, a multitude of newer authentication methods and technologies had become available, each of which are in use today:

Multi-factor authentication (MFA)

Starting in the early 2000s, the use of two-factor authentication became widely adopted.[6] In this case, the user receives a one-time code sent to their mobile phones to enter, in addition to the traditional password entered onto the user's laptop screen. Enhanced security comes from authentication taking place over two devices possessed by the user.

Biometric technologies

Around 2013 [7], primarily based on the popularity of the newest smartphone models, the use of biometric authentication went mainstream. These technologies require no memorization of complex combinations of letters, numbers, and symbols because they leverage distinct characteristics of "you"—your fingerprint, voice, face, heartbeat, and even common movements. Biometrics captured by smartphone cameras and voice recorders are the most prevalent,[8] including fingerprint, iris, voice, and face recognition. These approaches fall under the umbrella of "what you are" (see Figure 1).

Checking your biometric data against a trusted device that only you own—as opposed to a central repository—has become the preferred approach. For example, a user could scan their retina via the camera on a laptop or smartphone, using biometric identification as a first step to gain access to their online bank account. In a second step, the bank could then send a challenge via text message to the user's mobile phone, requiring them to reply with a text message to finish the authentication.

> "The advantage of Passwordless authentication lies in its ability to bridge the gap between usability and security. In particular standards based, interoperable solutions such as FIDO2 and WebAuthN give users a phishing resistant authentication capability that uses familiar platform-based authenticators to provide security in an easy and convenient manner."
>
> – **Ryan Galluzzo,** Identity Program Lead - Applied Cybersecurity Division at the National Institute of Standards and Technology

Other authentication practices

A separate set of authentication methods fall under the umbrella of "what you have"—not only smartphones, but perhaps security tokens carried by individuals, software-enabled tokens, or even an adaptation of blockchain databases used by bitcoin. Hardware USB keys enable workers to log in by entering their username and password, followed by a random passcode generated by the fob at set intervals of time. Software tokens operate similarly, with a smartphone app, for example, generating the codes. Distributed blockchain technology, as well as risk-based authorization that grants a user access by verifying their location, usage times, or access patterns, are some other technologies that are now widely available.

Mature passwordless options

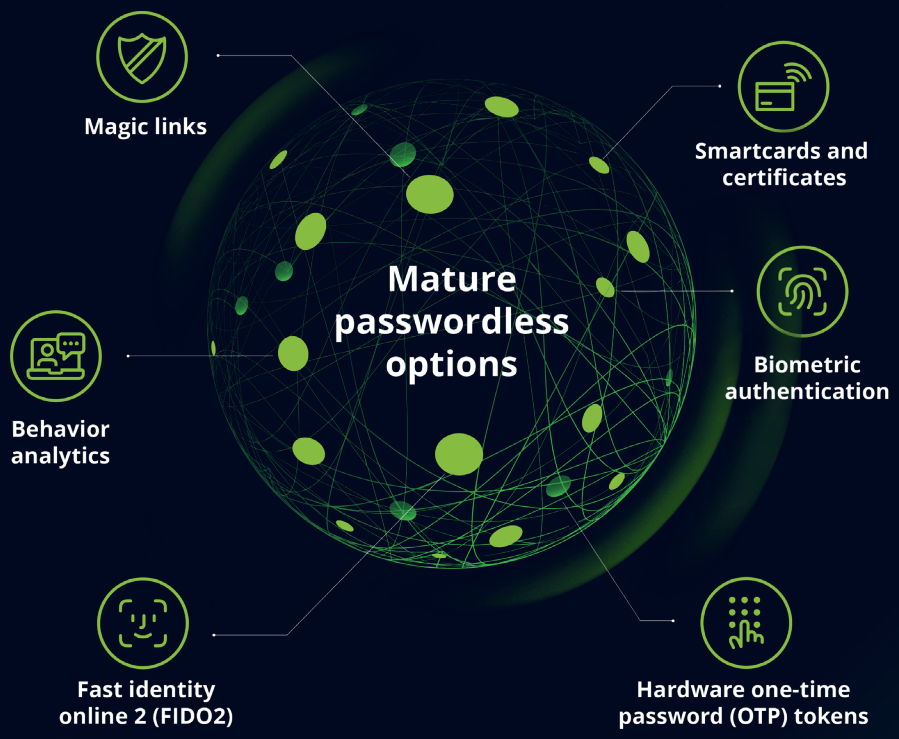


Figure 1: *Different passwordless authentication technologies may be used as part of a multi-factor strategy to decrease risk and enhance the experience for different types of users.*

Regardless of which authentication methods are selected, the benefits are essentially the same. With multiple devices or "gatekeepers" involved in the MFA process, the risk of a security incident stemming from a compromised password is significantly reduced.

One development in the move toward passwordless authentication was the foundation of FIDO by several leading technology vendors in 2012. This significantly advanced technical standards for new open, interoperable, and scalable online authentication systems without passwords.

And now, a decade after the alliance was founded, the FIDO security standard has continued to expand and has been adopted by many companies.[9] The latest iteration, known as FIDO2, leverages two-factor authentication as well as security keys (FIDO2 keys) and hardware tokens.

Current adoption levels

The adoption of passwordless methods in the workforce and customer authentication transactions is on the rise. Despite the many benefits, the rate of adoption has been slower than expected.

A June 2022 Ping/Yubico report[10] that surveyed 600 IT leaders across five markets shows that despite 91 percent of those surveyed being "very or somewhat worried" about passwords being stolen at their organization, 99 percent have yet to adopt passwordless authentication, even though all those surveyed saw its benefits.

Although, based on what Deloitte has seen with many of its clients recently, the increasing interest and adoption of passwordless authentication is real. So, what's driving this growth?

Five key adoption drivers

There are five main drivers accelerating the adoption of passwordless authentication:

1

Consumer expectation for a seamless, user-friendly experience.

These days, it's not just about security. User expectations are continually rising for consumers, so user-friendliness is critical. Through passwordless authentication using biometrics or a token, for example, login and access become more seamless while remaining secure.

2

Workers remain remote postpandemic.

While remote working was forced on many businesses due to the coronavirus pandemic, many organizations still see its advantages as part of their digital transformation and modernization strategies. According to a January 2023 **Survey of Working Arrangements and Attitudes (SWAA),** 13 percent of full-time employees are fully remote, and 28 percent are in a hybrid arrangement. While the number of paid full-time days worked remotely was down from 2020 to 2021 levels, they still totaled 27 percent. As such, many organizations are focused on how to make authentication and access easier for remote workers while still maintaining high-quality levels of enterprise security.

3

The concept of zero trust and its adoption.

Zero trust isn't just a methodology. It's also a mindset that assumes there is no defensible perimeter that may effectively protect today's modern organization. Instead, zero trust operates on a "never trust, always verify" principle. Passwordless authentication has a significant role to play in zero trust as it helps secure the enterprise, but in a way that does not degrade the user experience.

4

Large hacks leveraging compromised credentials.

As mentioned, more than 80 percent[11] of data breaches are caused by weak, reused, or compromised passwords. Many of the attacks over the last two years have been highly publicized, highlighting the need for improved security practices. By using biometrics or other forms of authentication that are not passwords, it's possible to reduce the source of risk entirely.

5

Increased number of technology vendors adopting FIDO standards.

FIDO standards are now widely adopted, with many companies participating. Over 90 percent of today's browsers now support FIDO authentication.[12]

"Eighty percent of data breaches are caused by weak, reused, or compromised passwords." [11]

Strategies for reducing risk

For organizations considering dropping the use of passwords as their main method of authentication, there are many options available. What is right for your organization depends on what you are trying to achieve and specific use cases. The table below provides an overview.

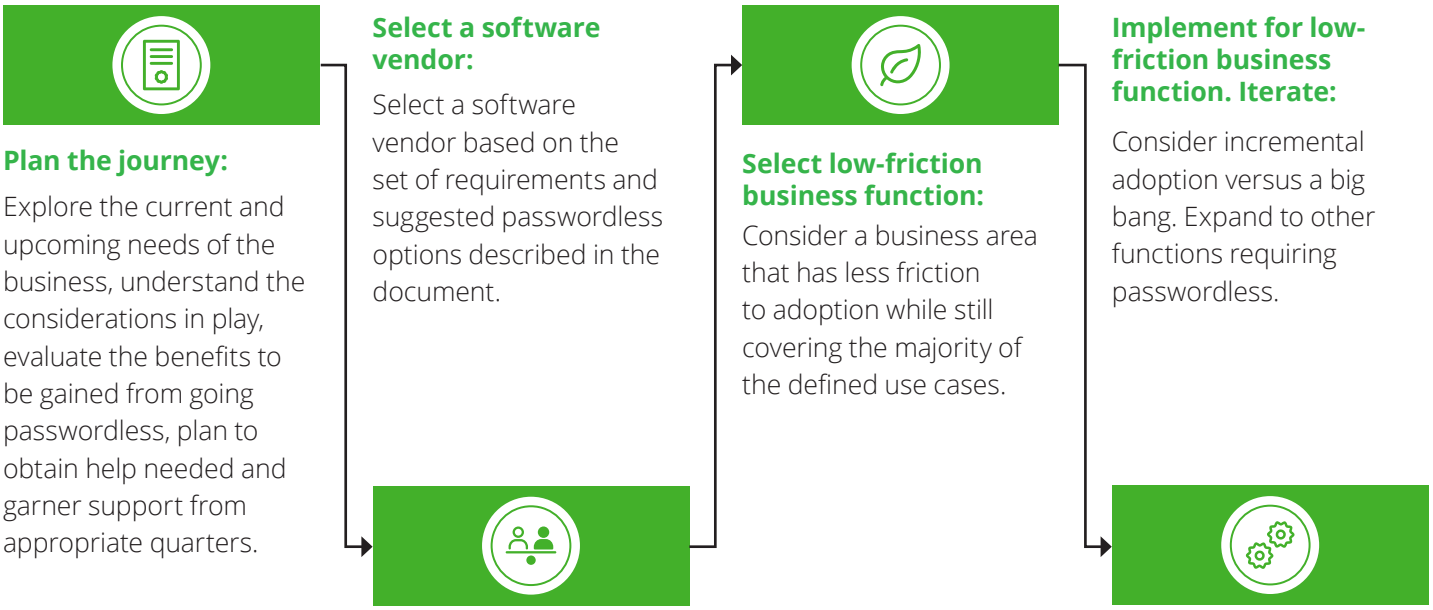
Key considerations for passwordless adoption

Category	Key considerations
Account recovery features	• In case of primary authentication failure, multiple methods of account recovery can be supported by passwordless authentication. Out-of-band one-time passwords, PINs, bypass codes, registering a driver's license and presenting it (via a camera), or user biometrics can be used as a backup authenticator. Organizations may need to consider specific account recovery needs when determining an appropriate passwordless option.
Support for application programming interfaces (APIs)	• To leverage passwordless authentication, applications must support universal login, or the API must be embedded with the passwordless authentication login flow, such as cloud portals, Kerberos web single-sign-on (SSO) applications, etc. Organizations should assess whether the selected passwordless option is compatible with their application environment.
Devices support	• Device types supporting passwordless authentication include tablets, mobiles, and computers. Organizations should assess whether the selected passwordless option is compatible with the devices in their environment.
Change management	• Adopting passwordless authentication can be achieved by using software-as-a-service (SaaS) solutions and understanding identity protocols such as OpenID connect and Security assertion markup language (SAML) that integrate well with MFA platforms. • Effective and detailed change management and training plans are required as users may be skeptical or hesitant to adopt new methods, set up new devices, program biometrics, etc. • The registration period can be time-consuming – an appropriate process for enrollment should be crafted and rolled out to help facilitate a smooth and streamlined rollout.
Identity proofing	• For high-value transactions, removing passwords for Identity-proofing and replacing them with passwordless authentication requires industries to comply with National institute of standards and technology (NIST) and FIDO2 specifications. This allows users to leverage the passwordless authentication features of their devices. High-level identity assurance and authentication are achieved with the use of passwordless authentication. Organizations may need to consider identity-proofing requirements when determining an appropriate passwordless option.
Fraud detection	• Transaction-based security, an airtight fraud policy set forth with minimum standards regarding end-to-end fraud prevention, can prevent fraudulent use cases to a great degree. Organizations may need to consider fraud detection requirements when determining an appropriate passwordless option.
FIDO2 and other open standards ability	• Web and SaaS applications are well supported through identity federation and the Web authentication API. Bridge technologies that enable passwordless authentication are required to satisfy some use cases. Organizations may need to consider relevant open standards when determining an appropriate passwordless option.
Inconvenience of carrying physical devices	• Device-bound user certificates with keys stored in software or an embedded secure element offer a compelling passwordless authentication mechanism. Carrying a device is inconvenient and can be lost. Organizations may need to consider the user experience when determining an appropriate passwordless option.
Co-existence strategy (to include a password with passwordless technology) for faster adoption	• The speed of passwordless adoption will depend to a large degree on application providers. Applications that can externalize authentication by supporting SSO, authentication plugins, or authentication proxies will benefit from passwordless technologies promptly. • Acquiring passwordless authentication platforms can provide integration options and support additional authentication methods, leading the way to passwordless authentication adoption. Organizations may need to consider their specific architecture, infrastructure and environment when determining an appropriate passwordless option.
Skillset and Experience	• Organizations should assess whether they have the appropriate resources, with the required subject matter knowledge and skill set, to support a transition to passwordless and what external support they may need.
Cost	• Given the number of considerations to evaluate to determine the applicable fit for the organization, the subsequent rollout related efforts of the selection solution and effort to be put into streamlining adoption and the associated pressure to make optimal decisions for the organization to gain the productivity and cost benefits, it is possible to get stunned into slow, expensive and time consuming cycles that delay the time to value and return on investment (ROI). Organizations may need to consider the cost, benefits and ROI as they balance the technical, functional and human aspects of this initiative.

Figure 2: *Pros and cons of popular passwordless authentication methods*

Next steps for password-based organization

A passwordless world is rewarding on multiple levels and the journey to get there needs to be undertaken by being thoughtful towards the different considerations for successful and optimal navigation. An executive summary of the path is provided in Figure 3 (below).



Conclusion

Passwords are a dated solution that is fast moving towards obsolescence in the modern world – they do not offer the smooth experience and security that today's users and organizations have increasingly come to demand and expect. This inevitably leads to poor password hygiene, such as sharing passwords across accounts.

Today, passwords are still the root cause of the vast majority of security incidents.[12] With remote work now "business as usual," organizations should begin planning now to gradually shift to a world without insecure, cumbersome, and hard-to-remember passwords.

Businesses that hesitate could be jeopardizing security, stalling employee productivity, and losing revenue. Organizations that have begun passwordless implementation understand the timely importance, business benefits, and employee buy-in that may come with such a move.

To learn more about how Deloitte supports enterprise passwordless authentication, please visit **Cyber Risk Services | Deloitte US.**

Connect with us:

Mike Wyatt
Principal
Deloitte & Touche LLP
miwyatt@deloitte.com

David Mapgaonkar
Principal
Deloitte & Touche LLP
dmapgaonkar@deloitte.com

Raj Radhakrishnan
Managing Director
Deloitte & Touche LLP
rajradhakrishnan@deloitte.com

Endnotes

1. "Study reveals average person has 100 passwords", Adam Rowe, March 21, 2023, accessed September 18, 2023, https://tech.co/password-managers/how-many-passwords-average-person#:~:text=According%20to%20one%20NordPass%20study%2C%20the%20average%20person,the%20passwords%20and%20other%20login%20information%20for%20them.
2. "55 important password statistics you should know: 2023 breaches & reuse data", Jenny Chang, 2023-09-17, accessed September 18, 2023, 55 Important Password Statistics You Should Know: 2023 Breaches & Reuse Data - Financesonline.com
3. "Password statistics in 2023 – how to save & protect your data", Georgie Peru, February 25, 2023, accessed September 18, 2023, 59+ Password Statistics in 2023 That Are Important To Know (webhostingprof.com)
4. "Most common passwords: latest 2023 statistics", Paulius Masiliauskas, Kristina Jarusevičiūtė, April 20, 2023, accessed September 18, 2023, Most Common Passwords 2023 - Is Yours on the List? | CyberNews
5. "21 Must-Know Weak Password Statistics for Utmost Security", Jovan, March 30,2022, accessed September 18, 2023, 21 Must-Know Weak Password Statistics for Utmost Security (kommandotech.com)
6. "History of Online Security, from CAPTCHA to Multi-Factor Authentication", Caroline Delbert, May 31, 2022, accessed September 18, 2023, Message from Beyond Identity
7. "How Biometric Authentication Secures the Future of Digital Banking", The Lumin lab, accessed September 18, 2023, How Biometric Authentication Secures the Future of Digital Banking | Lumin Digital
8. "5 Popular Types of Biometric Authentication: Pros and Cons", Pavel Jiřík, September 9, 2021, accessed September 18, 2023, 5 Popular Types of Biometric Authentication: Pros and Cons | PHONEXIA
9. "FIDO becomes an international standard, accelerates its deployments in public and private sectors", Press release, Tuesday 25 December 2018, accessed September 18, 2023, FIDO becomes an international standard, accelerates its deployments in public and private sectors (digitimes.com)
10. "Our Passwordless Future: a new era of security" June, 2022, accessed September 18, 2023, PowerPoint Presentation (pingidentity.com)
11. "25 alarming data breach statistics [2023]: frequency of exposed records", Jack Flynn, Feb. 13, 2023, accessed September 18, 2023, 25 Alarming Data Breach Statistics [2023]: Frequency Of Exposed Records - Zippia
12. "The FIDO Impetus to Passwordless Authentications", Kurt Mackie, February 14, 2022, accessed September 18, 2023, The FIDO Impetus to Passwordless Authentications -- Redmondmag.com

Deloitte.