TAGCYBER

# A JOURNEY TO PASSWORDLESS AUTHENTICATION AND DIGITAL IDENTITY PROOFING

KATIE TEITLER

The persistence of password-based cyber attacks and the damage they cause are the driving forces behind enterprise adoption of passwordless authentication. Security operations teams, along with digital experience and human resources teams, are demanding hardened ways to verify the identity information of customers and employees interacting with their systems; current password-based approaches are simply too vulnerable. In this report, we examine the factors facilitating the journey to passwordless login and the role of digital identity proofing in authentication.

## INTRODUCTION

In an age when many sensitive transactions are conducted online and even more data and information about individuals is collected, stored, and processed in digital formats, the risk of cyber compromise is greater than ever before. Today, highly connected workforces demand access to business productivity tools and applications without friction, while security teams must enforce strong authentication and access protocols. Businesses must deliver seamless experiences to customers and partners while ensuring secure and private transactions, yet traditional approaches to authentication and access, namely, password-based and "what you know" mechanisms, have repeatedly fallen short.

With cyber security now a business priority, companies see a pressing need to evolve to protect against data breach, digital impersonation and fraud, account takeover, and more. But protecting data and systems has become a complicated and cumbersome task, especially when companies are relying on legacy tools and techniques.

Despite the inherent risks of password-based authentication, companies continue to use it.

Why?

Because password-based authentication is ingrained in our society, and despite the well-known security enhancements of passwordless authentication, barriers exist. First, true passwordless adoption requires behavior change by employees and customers who might be reluctant to accept passwordless options. Buy-in from these audiences is harder to obtain than from security and IT professionals.

Second, passwordless adoption requires the acquisition of new technological capabilities, which means that security and IT teams must be ready to support interoperability between new and legacy systems. This means that they must also have the bandwidth and skill set to do so.

Third, teams must ensure that any new technology or process implementation does not result in new vulnerabilities (as the technologies are deployed and integrated) that raise organizational risk. Though the end result of hardened authentication will be achieved by passwordless adoption, the process of migrating from old to new can be daunting.

Thus, enterprise security teams must carefully consider where they are in their authentication journey and develop a risk-focused plan to support passwordless. One must keep in mind, though, that the journey is not necessarily a wholesale shift; varying use cases for authentication and identity assurance exist. Certain systems and data access do not require more stringent authentication processes and can therefore remain as is, providing a balance between security and convenience for users.

## IDENTITY AS THE BASIS FOR STRONG AUTHENTICATION

As security has evolved, practitioners have realized that authentication must be predicated on more than "what you know," i.e., a username and password. Identity, therefore, has become a central component of next-gen authentication.

Today, strong authentication must include aspects of "what you have" and "what you are," including:

- validation of any supporting digital identity documentation or assertion;
- verification of the systems and devices that users are using to authenticate; and
- an assessment of behavior and context around the use of an identity.

As such, security technologies have incorporated identity collection and correlation that support next-gen authentication use cases. Multi-factor authentication (MFA) was one such enhancement, but the means by which MFA was implemented in some cases (email and text-based codes) was not sufficient to prevent cyber compromise. Companies have therefore started adding biometric information or data about the health and hygiene of users' login devices to the authentication equation, thereby amping up security. Even more stringent approaches, such as adding a "live selfie" for identity proofing, are now becoming accepted where the business case dictates.

However, barriers to acceptance and adoption have included not only the friction and interoperability mentioned previously, but also the heavy governance of multiple, disparate tools to accomplish varying levels of authentication and identity proofing for assorted systems, access, and business requirements. In other words, there were too many tools to manage, too many rules for different authentication requirements, and too many use cases to support. Fortunately, passwordless options are coming to market, and they provide a holistic, streamlined approach to tiered authentication and identity proofing. In addition, they help organizations balance security versus convenience without compromising on risk.

## INCORPORATING BIOMETRICS INTO IDENTITY AND AUTHENTICATION

The first laptop to ship with a fingerprint scanner became available in 2004.[1] The IBM ThinkPad T42 required the owner/user/admin (or one and the same) to authenticate via a fingerprint swipe. The first smartphone to use fingerprint scanning for authentication and authorization (in addition to unlocking the device) was the iPhone 5s with Touch ID, launched nearly a decade later. [2]

In the intervening years, all forms of passwordless biometric authentication and access have been included in consumer-focused devices. Like many other technology advancements, widespread acceptance and comfort with biometric authentication and authorization was ushered in by consumerism. Yet passwordless and biometric authentication have been slower to catch on in the corporate realm.

Why? Because passwords are familiar and don't require overarching process, behavior, or technology changes (or buy-in from executive teams who don't want to risk any business disruption from altering accepted practices, regardless of the security threat).

Today, though, because of the persistence of password-based authentication, security practitioners and business executives understand this risk of weak authentication. With reliable passwordless biometric technologies commercially available, it is becoming harder to argue against passwordless authentication, which is likely to become the default authentication mechanism for corporate systems in the next five years.

## IMPROVING ON DIGITAL IDENTITY

Applying a static control (passwords) to an entity that is ever-changing has proven ineffective; that is why password-based breaches and identity fraud persist. The bigger problem that requires a solution is the dynamism and ephemerality of digital identity, which has led to the emergence of passwordless authentication and digital identity proofing.

Indeed, the NIST SP 800-63-3[3] notes the precarious nature of applying a single definition to digital identity, given that "a subject can represent themselves online in many ways." Further, the publication notes, "Digital identity is hard. Proving someone is who they say they are — especially remotely, via a digital service — is fraught with opportunities for an attacker to successfully impersonate someone." These are the very factors that threat actors exploit. When organizations fail to properly protect digital identities because they're employing known-weak controls like passwords, they cannot be certain that their employees and customers are who they say they are, and they cannot reasonably expect to prevent a security compromise.

As such, in the past few years, digital identity has become "the new perimeter" of sorts, and new approaches to identity protection have emerged. Remote work, mobile devices, and the predominance of cloud-based systems have all changed the requirements around identity and access control. Just as organizations can no longer rely on one north-south perimeter to govern "good" from "bad" traffic, organizations can no longer rely on one user/device/service/system to have one static digital identity that can be protected with a password. To be an effective security control, identity must account for modifications:

- Where a user is physically located
- What type of device they are using
- The security hygiene of that device
- The type of browser in use
- When/at what times a user requests access

The above conditions are just the tip of the iceberg. Yet, all the conditions contribute to a digital identity and digital footprint. These conditions must be incorporated into next-gen authentication systems to ensure hardening of the process.

Newer technologies that support blockchain/distributed ledger, IPFS (a peer-to-peer hypermedia protocol that surpasses HTTP/HTTPS in its security capability), sharding (an encryption mechanism to decentralize risk), and the FIDO2 certified public-private key pairing are helping enterprises move toward tamper-proof digital identity.

Further, industry standards such as NIST 800-63-3 certification and W3C Verifiable Credentials for credential verification are becoming critically important, and both vendors building next-gen authentication technologies and users of these technologies must ensure that products and processes meet these standards. Lack of compliance to any of these standards exposes organizations to potential vulnerabilities, and buyers can use these guidelines to help them select the best tools for digital identity proofing and passwordless authentication.

## IDENTITY PROOFING

Identity proofing — processes and technologies that can definitively match a stated user to their true identity — is a topic that has become so important that it is mentioned in NIST SP 800-63-3 and given its own special publication, NIST SP 800-63A,[4] which addresses digital identity guidelines for enrollment and identity proofing. The process of verifying identity according to collected attributes is covered in great detail, and is especially important when users (employees, customers, partners, etc.) must be authenticated for transactional purposes.

In a world where it is easy to steal or spoof identity information, verification systems must validate against an authoritative source that is immutable. Biometrics provide one source of proof via a reliable and unmodifiable authentication mechanism that would be extremely difficult for any attacker to steal or spoof.

Identity proofing has become such an important topic in security and compliance because it touches so many aspects of business.

*Onboarding*
When vetting new employees, HR teams must validate individuals' identities through the presentation of government-issued IDs and other official documents. From enrolling employees in HR, payroll, and benefits systems to providing keycard access to physical locations, it is imperative to have a method of verification and authentication that is reliable and not prone to vulnerability. For online access to network resources, though documentation is typically not required, employees must be able to prove that their identity is valid and their access request is appropriate. Though usernames and passwords are easily stolen or guessed, biometric authentication allows businesses to confirm employees' identities against an authoritative database and ensure that requests are legitimate.

*Customer service*
When banking online, purchasing goods or services online, using streaming services, or conducting numerous other transactions via their personal and mobile devices, consumers are asked to present various forms of identification — documented proof. In the case of financial transactions like applying for a loan, identity documents must be validated. In other cases, like online retail purchases or hailing a rideshare, businesses must check that the consumer is authorized to request the transaction. Biometric-based identity proofing verifies consumers against these requirements.

*Authentication and authorization*
Organizations' workforces require access to corporate resources and, as explained above, password-based authorization and authentication methods are highly exploitable. Identity proofing with biometric capabilities removes the need for usernames and passwords and enhances security by providing an immutable second factor of authentication.

Removing passwords for identity proofing (as well as other authentication mechanisms) and replacing them with advanced biometrics also allows companies to comply with NIST 800-63-3 and FIDO2,[5] a new set of specifications that allows users/consumers to leverage the biometric features of their personal devices (e.g., fingerprint readers, camera phones) to authenticate to online systems. Both of these industry-leading standards ascribe high levels of identity assurance (IAL3) and identity authentication (AAL3) that are not possible without the inclusion of passwordless authentication.

## WHERE IDENTITY AND ACCESS MERGE

In today's digital, perimeterless world, it is nearly impossible to separate identity from access. Identity — be it human identity, device identity, software and services identity, or the identity of any other entity communicating on a network — must be verifiable through a combination of collected attributes that, in their aggregation, cannot be decoupled from the entity itself. Only then can identity be used as the basis for access.

Therefore, to ensure the highest levels of security and privacy, not only must identity be immutable and tamper-proof (i.e., based on factors/attributes other than passwords), access permissions must also be hardened against exploit. This means that organizations should set access policies to be contextual, conditional, and based on least privilege.

That said, modern workplaces must offer employees accessibility and flexibility in how and when they connect to corporate resources. Repeatedly timing out an employee's access to a sensitive database, for instance, won't be tolerated, regardless of any security argument. Ease of use is paramount in a corporate setting, but security and privacy cannot take a backseat. Access policies that can definitively prove identity (i.e., not passwords) and incorporate elements of zero trust are an organization's best bet to meet all requirements.

When interacting with consumers, the less friction, the better. Consumers expect to transact with businesses using their mobile devices, even when submitting private information like government-issued IDs and other identity information online. Consumers today don't want to go to a Staples/FedEx/UPS store to print out documents to then send to businesses. And fax and email can be insecure. At the same time, consumers expect businesses to protect their identities while using the products/services offered. For these reasons, identity and access control are inextricably linked, but they must be tamperproof.

In short, on the journey to passwordless, strong authentication, organizations will need to decide on business policies that guide the implementation. Where access to financial information is involved, for instance, hardened authentication may be desired. Whereas for less sensitive information, lower levels of authentication may be acceptable. Every decision should be based on the business's risk tolerance and operating model.

## REMOVING PASSWORDS TO INCREASE SECURITY

The primary use case for taking your business on a journey to passwordless authentication — and adding biometrics and blockchain — is hardened multi-factor authentication.

In line with best practices and industry regulations, MFA should be the default for every login attempt. However, traditional approaches to MFA either introduce friction and frustration or are insecure.[6] Biometric-based authentication eliminates the need for usernames and passwords; reduces reliance on SMS, OTPs, and other forms of MFA; reduces the burden on technical staff (no more password resets, decreased infrastructure to support secure storage of usernames and passwords); and provides a way for organizations to move toward a zero trust framework by supplying the necessary context around identity and access.

Other top use cases include:

- Improved privileged access management
- Secure remote access (for both employees and partners/contractors)
- Compliance with industry standards (such as IAL2/IAL3)
- Digital resiliency
- Consumer/customer protection against financial fraud

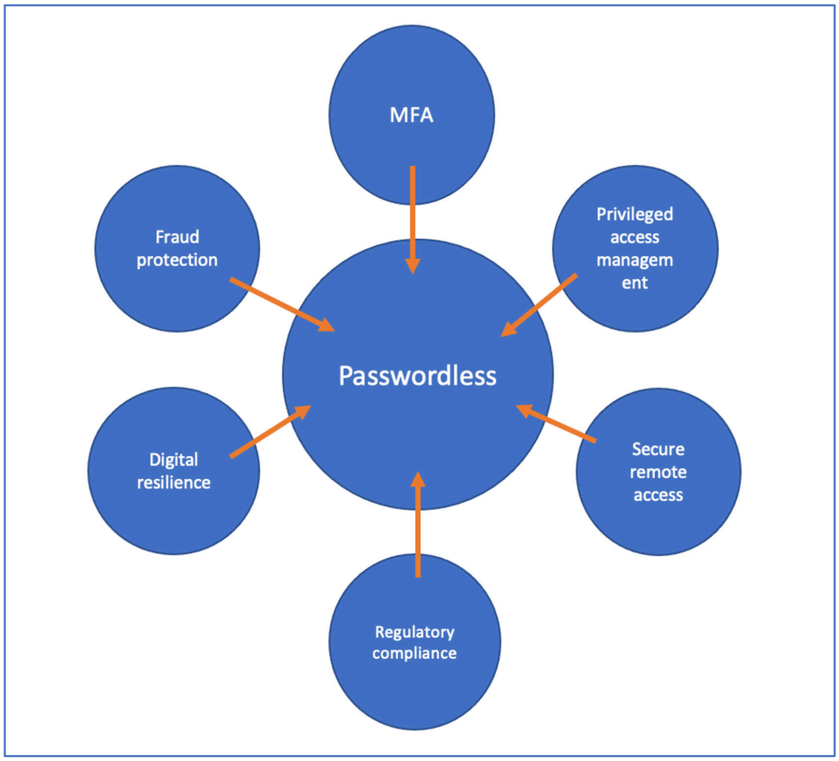

**FIGURE 1.** Passwordless authentication use cases

At an industry level, there are many use cases for which identity proofing should be incorporated into user authentication. A sampling of industry examples include:

*Government*

Government employees, contractors, and suppliers have access to highly sensitive, sometimes classified information. As such, it is necessary not only to deploy the strongest authentication and access controls to systems and data, but also to ensure that insider risk is at its lowest. Identity proofing and biometric-based authentication allow government agencies to meet these requirements, as well as the numerous data protection and privacy regulations imposed upon them.

*Financial services*
As with government agencies, financial services employees have access to highly sensitive information. They must also comply with know your customer mandates (KYC), for which identity proofing is essential, along with the added pressure of privacy protection, as the information belongs to consumers. Thus, financial services companies need to secure both internal and external access with strong controls, and apply strong customer authentication to guard against fraudulent logins and financial transactions.

*Health care*
Health records are some of the most valuable records sold on the dark market. They must be protected with strong controls to ensure that health care providers (physicians, staff, pharmacists, etc.) are not intentionally or accidentally leaking information, that fraudsters are not posing as patients for access to drugs or other malfeasance, and that their systems, both IT and OT, are adequately secured from illicit access.

*Higher education*
One tenet of higher education is openness and collaboration, which seemingly stands in contrast to traditional security. However, passwordless, biometric-based identity proofing in education helps academic environments to securely enroll students in programs, prevent fraudulent enrollment, ensure the confidentiality and integrity of online testing, and mitigate the potential for individuals to claim that they've earned a degree when they have not.

## BENEFITS

Benefits of adopting passwordless, biometric authentication and digital identity proofing include:

- A simplified way to satisfy compliance requirements, including federated identity
- Reduced friction with employees and customers
  - ◇ No more usernames and passwords to remember
  - ◇ Elimination of paper documents, scanning, and insecure transmission of PII
  - ◇ Simple and quick login processes without outdated and unreliable forms of MFA
- Lower operating costs
  - ◇ Automated verification removes administration overhead from the business
  - ◇ Eliminates employee help desk costs related to password reset requests
  - ◇ Accelerated transactions
- Adapts to modern infrastructure requirements without increasing security teams' workloads
  - ◇ No infrastructure changes
  - ◇ No firewall rule changes
  - ◇ No DMZ components
- Improved security
  - ◇ Immutable proof of identity and identity documentation
  - ◇ Mitigates the need for disparate MFA
  - ◇ Reduces reliance on vulnerable passwords

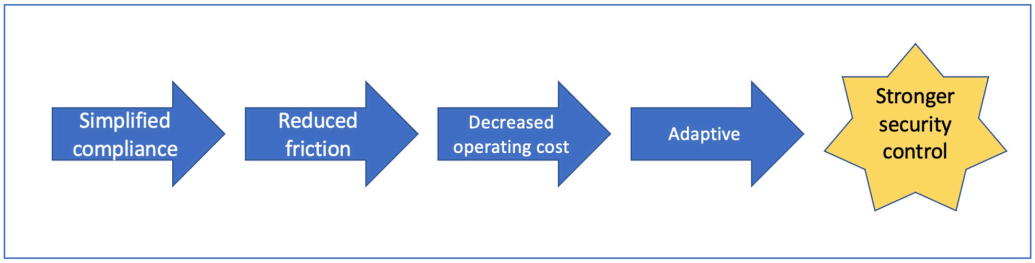

**FIGURE 1.** Benefits of adopting passwordless, biometric authentication

## EVALUATING IDENTITY PROOFING WITH PASSWORDLESS TECHNOLOGY

Without question, inertia has historically stood in the way of business adoption of passwordless authentication. Plus, in a world where a majority of transactions are conducted online, it is no longer acceptable to make employees, customers, partners, and other users jump through hoops to supply identity proof. Nonetheless, the highest standards of security and privacy of users, their identities, and their actions online must be incorporated into security programs.

Today's passwordless technologies, especially those that include elements of biometrics — like a LiveID or a live selfie, coupled with FIDO2- and NIST 800-63-3-certified authentication backed by a proven, immutable identity — provide a newly paved pathway for the journey.

When evaluating identity proofing and passwordless authentication platforms, the following questions will help determine which type of platform your organization needs:

1. *Risks* – How is your company currently verifying and authenticating employees, partners, and customers?
    a. Tech-related questions
        - *What technologies do you use?*
        - *How will you manage 2FA and MFA for systems that can't go passwordless?*
        - *Do you have disparate technologies and processes for different onboarding?*
        - *What data do you capture and store about identities and access permissions?*
        - *What are your data retention and destruction policies?*

    b. People- and process-related questions
        - *How are you managing the different processes of employee and customer enrollment?*
        - *What are the different levels of identity proofing required for customers, partners, employees?*
        - *How much time is spent managing employee and customer authentication (e.g., password resets)?*
        - *What is the impact of login/authentication friction on customer satisfaction? Churn?*
        - *How do you ensure compliance with regulatory requirements?*
        - *How easy or hard is it to audit security and privacy of employee/customer/partner identity information?*
2. *Assets* – What systems for identity verification do you maintain?
    *a. How many identity-based tools do you use?*
    *b. What types of authentication technologies and processes are in use?*
    *c. Where is identity and authentication information stored?*
        - *How is it protected?*

    *d. How are you currently managing access controls?*
    *e. How do you handle multiple identities?*
    *f. How do you protect PII, including biometric information?*
    *g. What systems do you have for backup and recovery, when need be?*
    *h. Can your deployed technology scale alongside your business?*
3. *Compliance* – Which regulatory requirements is your organization subject to?
    *a. How are you meeting compliance requirements?*
    *b. How are you auditing compliance requirements?*
    *c. Are there additional industry standards (e.g., NIST 800-63-3 and FIDO2) that are required or desired?*

## CONCLUSION

Employees, partners, and consumers expect frictionless experiences when transacting with businesses. And businesses need hardened methods of verifying the true identities of individuals. Passwords are slowly becoming obsolete, since they have been the basis for many damaging cyber attacks. Passwordless capabilities today are stable, reliable, and readily accepted by users. Coupling passwordless authentication with biometric data and immutable technologies like blockchain helps companies achieve low-risk, highly compliant security and privacy postures.

Further, the journey toward passwordless allows companies to comply with leading industry standards while affording a tiered system of authentication (e.g., stronger authentication requirements for more sensitive data and systems). This last point is important, because very few companies will be able to achieve an "all-or-nothing" shift to passwordless. Not all authentication requires the most "locked-down" methods.

Using next-gen technologies that move companies toward passwordless piece by piece — without infrastructure changes or the incorporation of multiple new technologies — decreases risk, removes vendor lock-in scenarios, and increases flexibility and security control.

## ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.

[i] https://www.technewsworld.com/story/37017.html#:~:text=The%20ThinkPad%20T42%20notebook%20will,to%20offer%20the%20fingerprint%20reader.

[2] https://www.apple.com/newsroom/2013/09/10Apple-Announces-iPhone-5s-The-Most-Forward-Thinking-Smartphone-in-the-World/

[3] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

[4] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf

[5] https://fidoalliance.org/fido2/

[6] https://securityboulevard.com/2020/12/how-the-solarwinds-hackers-bypassed-duos-multi-factor-authentication/