thalesgroup.com

THALES

Passwordless Authentication:

How Giving Up Your Password Might Make You More Secure

White Paper

Why Passwords Are Bad

Passwords are one of the oldest security tools in the world of software and the internet. But in today's environment, passwords cannot provide enough protection for businesses for several reasons.

Password Fatigue Leads to Bad Hygiene

Policy-driven password strengths and rotation leads to password fatigue, thereby contributing to poor password management. Verizon's Data Breach Investigation Report[1] indicates that **over 70 percent of employees reuse passwords** for work and personal accounts. A malicious actor could therefore abuse an employee's credentials to access other applications and sensitive customer information.

of breaches involve use of weak or stolen credentials

Average person has roughly 40 online accounts

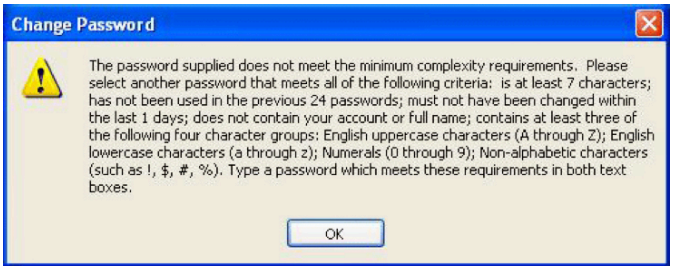
People reuse same passwords across different accounts

still among most popular password choices in 2018

People also tend to pick easy-to-hack passwords because of the trouble they have with remembering passwords. An analysis of over five million leaked passwords showed that 10 percent of people used one of the 25 worst passwords[2]. Seven percent of enterprise users had extremely weak passwords.

Passwords Hurt User Experience

Research by Carnegie Mellon University indicates that a properly written password policy can provide an organization with increased security. However, there is less accord over what should be in this policy to make it effective. To illustrate this fact, users commonly react to a policy rule that requires them to include numbers by picking the same number or by using the number in the same location in their passwords[3].



Some password policies may make passwords difficult to remember or type. In response, users can undermine the security of their passwords by writing them down, reusing them across different accounts or sharing them with friends. They also frequently forget them, creating more work for the helpdesk.

Passwords Can Hinder User Security

Ironically, passwords can be a detriment to security by serving as an attack vector. According to Verizon's Data Breach Investigations Report in 2018, **81% of hacking-related breaches** were a result of weak, stolen, or reused passwords[4]. Threats like man in the middle attacks and man-in-the-browser attacks take advantage of users by mimicking a login screen and encouraging the user to enter their passwords. It's even more unsafe in the cloud. Login pages hosted in the cloud are completely exposed, thus enabling a bad actor to carry out phishing or brute force attacks against publicly known login pages like outlook.com.

1 https://enterprise.verizon.com/resources/reports/dbir/
2 https://www.vice.com/en_us/article/paqd4m/too-many-people-are-still-using-password-as-a-password
3 https://cups.cs.cmu.edu/passwords.html
4 https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf

Focusing on password rules is just a distraction. To understand why, it is important to review the different attacks on passwords and how the password factors into the equation of an attacker. Here are the most common ways passwords are broken today[5]:

Attack	Also Known as	Frequency	Difficulty
Credential Stuffing	Breach replay, list cleaning	Very high – 20+ million accounts probed daily	Very easy: Purchase credentials gathered from breached sites with bad data at rest policies, test for matches on other systems. List cleaning tools are readily available.
Phishing	Credential interception	Very high. 0.5% of all inbound mails.	Easy: Send emails that promise entertainment or threaten, and link user to doppelganger site for sign-in. Capture credentials. Use Modlishka or similar tools to make this very easy.
Password spray	Guessing, hammering, low-and-slow	Very high – accounts for at least 16% of attacks. Sometimes 100s of thousands broken per day. Millions	Trivial: Use easily acquired user lists, attempt the same password over a very large number of usernames. Regulate speed and distributed across many IPs to avoid detection. Tools are readily and cheaply available.

When breaches occur, the consequences can be catastrophic. The average cost of a stolen record is $148, and the **total cost incurred from a data breach averages at $3.86m**[6].

Little Progress on the Password Problem

Thus far, organizations have attempted to address these issues by implementing a range of other authentication methods in addition to, or in place of, legacy passwords. The most prevalent method is two-factor authentication (2FA), known also as multi-factor authentication (MFA).

There are all kinds of authentication factors that can be used as part of a multi-factor system, but they all tend to fall into three broad groups:

- **Knowledge factor** ("something you know"): The system accepts you if you show that you know certain information. Examples include PINs, answers to security questions, tax return details, etc.
- **Possession factor** ("something you have"): The system accepts you if you can prove that you have a certain physical device with you. Examples include SMS codes, auth apps, USB keys, wireless tags, card readers, etc.
- **Inherence factor** ("something you are"): The system accepts you through the use of a biometric comparison. Examples include fingerprint scanners, retina scanners, voice recognition, etc.

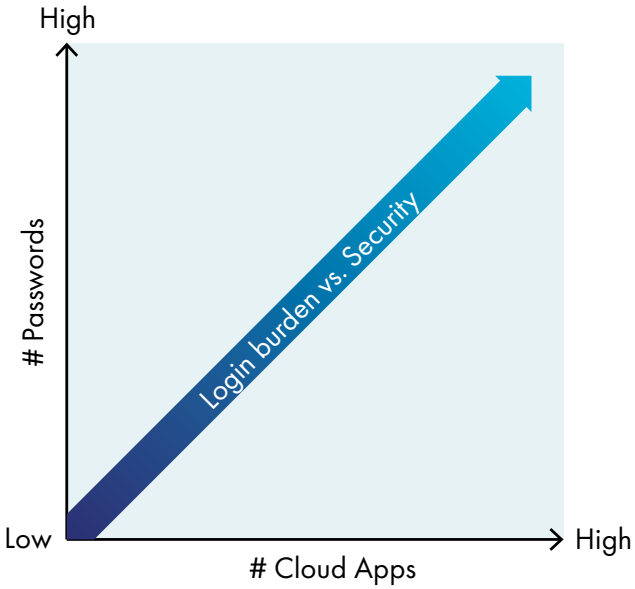
One method of MFA is through **SMS message**. This model of MFA can be extremely useful, but it comes with risks. First, you have to trust the service enough to share your phone number since some disreputable services may use your number for advertising or sell it off for monetary gain. As phone numbers aren't tied to devices, hackers can circumvent SMS-based authentication without ever touching your phone. All they need to do is conduct a SIM swap attack by calling the target's cell phone company and tricking the representative into transferring the target's phone number to a SIM card under their control.

One-time passwords (OTP) offer better security, as the codes are cryptographically generated based on a secret key created during account creation. This means you can get valid codes on your device even when you have no reception and/or no mobile service. OTP-based multi-factor authentication can be provisioned in the form of mobile token to a user's smart phone or as a stand-alone device such as a key fob.

With increasingly complex access environments and more access points than ever before, organizations have every reason to add multi-factor authentication. However, because of the sheer number of cloud services that need protecting, applying MFA to each and every login attempt is not practical from a user experience perspective.

5 https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Your-Pa-word-doesn-t-matter/ba-p/731984
6 https://www.ibm.com/security/data-breach

We find ourselves at a critical inflection point where the rise of cloud-based technology (and threats) is colliding with an increasingly mobile workforce that doesn't want to be hampered by inconvenient authentication deployments. What is needed, is a means of password-less authentication that offers high security and convenience. These types of solutions have been lacking due to a lack of appropriate technology up until now. But things are beginning to change.



What Has Changed and Why There Is Hope

In recent years, there's been an increase in awareness surrounding online security and privacy of users, especially among government agencies and regulators. While organizations used to suffer data breaches and security incidents, then expect few legal and financial consequences afterward, that's no longer the case.

Regulators have also started to act, resulting in more businesses adding strong authentication to their data protection practices. Among the most relevant regulatory actions is the General Data Protection Regulation (GDPR) which defines standards for access security. Companies that fail to comply with the rules and protect their customers' data will be severely fined. GDPR applies to the EU jurisdiction only, but since many companies that aren't based in the EU still do business in the region, it is now considered a golden standard for security.

At a time when more companies are adopting strong authentication and more data breaches are resulting from password compromise, it is going to be increasingly difficult for a business to make the case to a GDPR regulator that password-only authentication is appropriate security. This potentially exposes their company to fines that are far higher than the price of moving from passwords to strong authentication.

Other industry-specific regulations are more explicit about the use of authentication technology. An example is Payment Services Directive 2 (PSD2), which regulates e-commerce and online financial services in Europe and makes 2FA mandatory. PSD2 also encourages the use of security cards, mobile devices and biometric scanners to improve the user experience without compromising security.

Finally, NIST states in its digital identities guidelines that organizations should move away from passwords and one-time passcodes and adopt modern strong authentication. More specifically, NIST recommends that a device create and use cryptographic private keys as new account credentials and then securely store them in the same way most smartphones now securely store fingerprint data.

Technological innovations, such as the proliferation of mobile devices with integrated biometrics, geolocation and other sensors, have made possible the adoption of passwordless solutions that eliminate the use of traditional passwords by enabling adaptive and contextual authentication. Data on user behavior is gathered by these sensors in the background without requiring any dedicated activity by the user. Sensor metrics are then used to regularly and periodically check user behavior in order to transform user authentication into a seamless continuous process.

By assessing a range of attributes such as IP address, mobile parameters, known device, and operating system, contextual or risk-based authentication can verify a person's identity when they log into an application. In fact, it can do so without the user even knowing. Businesses are eager to adopt such passwordless authentication solutions that promote stronger security while improving user experience and applying IAM policies.

Passwordless Authentication – A Multi-Layered Approach

Passwordless authentication replaces passwords with other methods of identity validation, improving the levels of assurance and convenience. This type of authentication has gained traction because of its significant benefits in easing the login experience for users and overcoming the inherent vulnerabilities of text-based passwords. These advantages include less friction, a greater level of security that's offered for each application and—best of all—the elimination of the legacy password.

Gartner is predicting that 60 percent of large and global enterprises along with 90 percent of midsize employees will implement passwordless authentication methods in 50 percent of cases by 2022. This change will mark an increase from fewer than five percent today[7].

7 Embrace a Passwordless Approach to Improve Security, https://www.gartner.com/smarterwithgartner/embrace-a-passwordless-approach-to-improve-security/

There are various layers of passwordless authentication that offer varying levels of security. Implementation of a specific model depends on the authentication and federation approaches an enterprise wishes to apply based on the business and security risks and the sensitivity of the data to be protected.

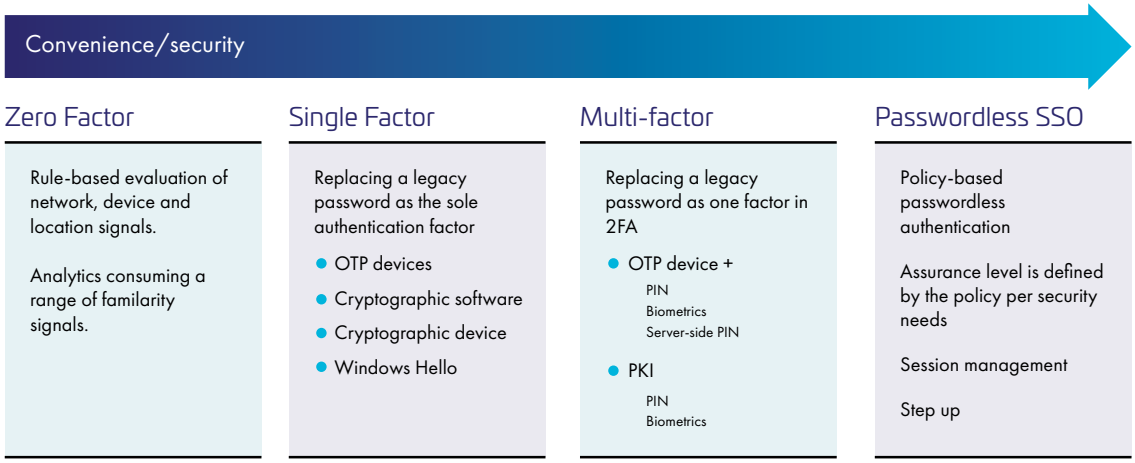
Zero-factor passwordless authentication may involve rules or knowledge-based authentication (security questions for example) or device and location indicators as familiarity signals. The drawback of zero-factor authentication is that it cannot completely ensure identity validation and should ideally be used as a backup method or in conjunction with other authentication methods.

Although passwords are considered a **single-factor authentication**, involving the "something you know" factor, the industry is deprecating their use, adopting single-factor authentication solutions that leverage the "something you have" factor. These solutions involve the use of either devices generating OTPs or cryptographic software and/or hardware. Single-factor schemes enable organizations to replace legacy passwords as the sole authentication factor with other means. While single-factor passwordless authentication is more secure than zero factor, it still doesn't offer the security of multi-factor authentication. Windows Hello, when relying only on the cryptographic secret stored in a device's TPM is an example of a single-factor authentication model, since the "something you have" secret is stored in the user's device and not separately.

Multi-factor passwordless authentication schemes allow organizations to replace passwords as a factor in a MFA deployment with a combination of an OTP device or a PKI based solution combined with a PIN or biometrics. Usually, the PIN or biometrics are native to a specific device, but increased security can be achieved when the PIN is defined and validated by the authentication server.

Today's next generation authentication and access management schemes offer extensive flexibility in the range of adaptive and multi-factor methods, which can be combined together within flexible access policies to offer the right level of passwordless security for varying access scenarios.

Models of Passwordless Authentication



Passwordless Authentication Does Not Necessarily Mean Less Security

The answer to whether something is actually secure is usually "it depends on your threat model." This time is no different. The security of passwordless authentication systems ultimately depends on the scheme's ability to validate a person's identity with a high level of certainty. Simply put, passwordless methods are as secure as the underlying authentication used.

For example, using secure push notifications to the account holder's mobile device is generally considered more secure than passwords. SMS codes to the account holder's mobile device can be considered less secure because SMS is an insecure communication channel, and there are multiple documented attacks against SMS authentication systems.

A password is not the route to take against determined, well-funded attackers. The best defense is to do away with the legacy password and instead practice passwordless security in depth, combining multi-factor authentication, adaptive security and anomaly detection. Such deployments of passwordless authentication can fit varying levels of security requirements depending on how they're implemented.

One Size Does Not Fit All

Given the diversity of identification and access management use cases within a single corporation, authentication solutions are not a one-size-fits-all. Security and business leaders should seek for authentication solutions that meet the needs of one or many use cases in their enterprises. Some methods suit a wide range of use cases, and many vendors offer tools that offer or support a variety of distinct methods. However, security leaders might not find a single solution that meets their needs across all use cases.

Before selecting an authentication method, security leaders need to evaluate the following criteria:

- **Trust versus risk**. Risk-appropriate authentication is a best-practice principle. It dictates that a leader must, for each use case, evaluate minimum levels of trust commensurate with the level of risk. Then select authentication methods that meet the level of trust required.
- **Total Cost of Ownership (TCO) versus justifiable and available budget** considering factors that can reduce operational costs such as the efficiency of cloud-based environments, and automated authentication provisioning workflows.
- **User experience (UX)/Customer experience (CX) versus users' needs**. CX is a heavily weighted selection criterion. Over 65% of IT professionals in Thales's annual Access Management and Authentication survey cited that they consider simplified access for end users, a key driver in deciding whether to implement an access management and authentication solution.
- **Other technical and operational needs and constraints** such as how an access management and authentication solution integrates with the established organizational IT framework and the applications that need protection.

Passwordless Single Sign-On

Single Sign-On (SSO) is the practice of using a session- and user-authentication service that permits an end user to enter one set of login credentials to access multiple applications. A user simply logs into their SSO portal or an application, and then they can seamlessly access all applications without having to authenticate again (during a single session, such as a normal work day). It's true that SSO helps organizations address important access challenges, while offering clear productivity and user experience benefits.

Implementing passwordless solutions along with SSO can greatly enhance the user experience because it takes passwordless authentication one step further: the user authenticates and then can have access to other apps and services without having to re-authenticate.

As always, user convenience and experience comes with an increased security risk. SSO adds security risk because users are re-using the same credentials for accessing several apps, either on-premise or in the cloud. It is therefore important to ensure that the SSO solution supports policy-based access, which enables step up authenticaiton and conditional access. This means that different policies can be enforced for different access use cases, depending on the profile of the user and the sensitivity of the data being accessed.

To maintain the required balance between convenience and security, organizations can implement two risk management best practices:

- Making sure that the initial passwordless authentication solution meets the right assurance level
- Making sure that conditional access policies are applied so that if the login scenario changes, the authentication level will be stepped up appropriately.

Looking into the future of access management and user authentication, passwordless authentication will evolve further into a continuous passwordless SSO, where the actions of a user within a continuous logon session will be monitored and will trigger additional identity verification in accordance with predefined scenario- and compliance-driven policies for re-authentication. User actions that could trigger re-authentication could include for example, massive file download, accessing sensitive information within a database, reconfiguring service settings or changing location.

Passwordless and Continuous Authentication are Intertwined

With a token, a password or a fingerprint – authentication is basically a yes / no decision: The system validates a user's identity and either allows or denies them access to an application. Traditional authentication methods validate the authenticity of a user once, at first logon. This one-time authentication might introduce vulnerabilities as the users change working environments. There is, hence, the need to assess in a continuous way the identity of the user.

A continuous authentication session ensures that a person is who they claim over a period of time, as they move from device to device and from app to app - at each access point. The access management service will revalidate the person's identity in a continous transparent manner, only requiring additonal authentication if a policy is triggered, or if an access anomaly is revealed.

With transparent authentication, the user is no longer required to explicitly authenticate in all situations because the adaptive and contextual attributes provide the basis for authentication decisions. Security and usability can be increased by transparent authentication due to the mobile device having a great source of user behavior[8] data.

The rich and potentially seamless nature of sensor-based data provides transparent authentication with the possibility of providing a more granular approach to application and data access by thresholding tasks. Thus, the user's actions within an application are assessed over time, with additional authentication required depending on the action taken. Thus, for example, if a user starts downloading huge amounts of data from an application, the access management service could trigger an authentication event which would provide a higher degree of identity validation.

The beauty of these schemes is that they offer the ability to maintain a very high level of access security while significantly reducing the login burden for users. They also offer flexibility in that different authentication methods can be applied for different access scenarios depending on the sensitivity of the app, profile of the user, and other conditions.

Beginning Your Engagement with Passwordless SSO

As Gartner predicted, a majority of organizations are going to begin migrating to passwordless authentication over the next few years. These organizations can get started with their own passwordless SSO implementations by discovering the applications and the data that a typical user access. With that knowledge, they can assess the sensitivity and the associated risks of the data that need to be accessed, and then map the right level of authentication assurance to each data set. It's then that they can set up access policies under their passwordless SSO program that maximize both security and convenience.

8 Alotaibi, Furnell and Clarke (2015), "Transparent authentication systems for mobile device security: A review", IEEE, available at https://ieeexplore.ieee.org/document/7412131

THALES

Americas
Arboretum Plaza II, 9442 Capital of Texas Highway North,
Suite 100, Austin, TX 78759 USA
Tel: +1 888 343 5773 or +1 512 257 3900
Fax: +1 954 888 6211 | E-mail: sales@thalesesec.com

Asia Pacific – Thales Transport & Security (HK) Ltd
Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel: +852 2815 8633
Fax: +852 2815 8141 | E-mail: asia.sales@thales-esecurity.com

Europe, Middle East, Africa
350 Longwater Ave, Green Park,
Reading, Berkshire, UK RG2 6GF
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-esecurity.com

> thalesgroup.com <