Passwordless

The Future of Authentication

Duo Security is
now part of Cisco.

Passwordless

The Future of Authentication

Table of Contents

Security & Usability for the Digital Transformation

To achieve transformative business objectives, stay competitive and meet user expectations, enterprises are undergoing a digital transformation, also known as modernization.

Enterprises are migrating from legacy systems to the cloud, resulting in hybrid environments. Consumer markets are driving the push toward usable, mobile technology and always-on, always-available cloud, web-based applications. This move to the cloud includes both customers and all types of enterprise users – including employees, contractors, vendors, partners, etc.

This shift to a decentralized, identity-centric operational model has placed increased importance on ensuring secure access for users. The future of authentication demands both a **secure** and **usable** method of authorizing users to both cloud and on-premises systems.

The Shift in Authentication to Passwordless

The origin of the password arrived in the mid-1960s at the Massachusetts Institute of Technology (MIT) with the development of the Compatible Time-Sharing System (CTSS), according to **Computer History** and **Wired**. It allowed hundreds of users to share the computer with a common mainframe. The password was developed as an accounting tool to allow users access to their specific resources for a certain amount of time.

As time went on, some users shared passwords and others demanded better security, and the emphasis shifted to authentication. In the 1980s, Security Dynamics Technologies patented a "method and apparatus for positively identifying an individual" and paved the way for additional factors of authentication. In the last two decades, multi-factor authentication (MFA) has matured as a secondary authentication which provides an additional layer of security to the primary password authentication.

The password primary authentication and the MFA secondary authentication became imperative as password theft and data dumps became routine. The 60-year-old single-factor password simply hasn't stood the test of time. In 2019, an anonymous creator released 2.2 billion usernames and passwords freely across attacker forums, known at that time to be the largest collection of breaches (**Wired**).

Advances in secondary factors, from the proliferation of smartphones to the consumerization of biometrics, has led many to question the need for and the use of the password at all. If strong authentication is based on multiple factors, and passwords are the most vulnerable factor, why even require them? This realization has led the industry to move toward replacing passwords altogether with more secure, simplified methods of authentication.

Tech and security analysts predict enterprises will shift to implementing passwordless authentication for their users to enable this modern digital transformation.

> "Passwords have multiple weaknesses that attackers can exploit. Even the best password policy cannot mitigate spyware or phishing attacks."

– **Gartner IAM Leaders' Guide to User Authentication**

2.0

The Problem With Passwords

Passwords are plagued with problems, which make them an insecure factor for identity verification. Additionally, passwords cause a lot of user friction and frustration.

Passwords are costly and burdensome to manage.

Passwords take up a lot of IT and help desk support time each year – so much so, that many large U.S.-based organizations have allocated over $1 million annually for password-related support costs, according to **Forrester**.

“Passwords remain a significant source of risk for organizations – even when incorporated with another method for MFA – and of friction, frustration and fatigue for users and administrators,” notes the Gartner Group in their Market Guide for User Authentication.

Expired passwords cost a large, global enterprise tech and security company $30 per employee case, totaling over $500,000 in support and lost productivity every year.

Passwords cause poor user experiences.

A survey of 200 IT security leaders conducted by International Data Group (IDG), sponsored by MobileIron, found that 62 percent of respondents reported extreme user frustration at password lockouts. This isn’t a surprise – lockouts pause productivity and contribute to poor user login experiences.

In addition to password lockouts, the sheer number of cloud services and passwords that a user needs to log into to do their job has increased over the years. Now, the average enterprise uses 1,400 different cloud services, while the average business user must log in with as many as 190 passwords, according to **SkyHigh Networks** and **Security Magazine**.

Passwords are easily compromised.

There are also a number of other password-related threats and attacks that are commonly used by attackers, mainly because they are simple, and they work. A few examples include credential stuffing (large-scale, automated login attempts using stolen credentials); phishing (an attempt to deceive users and illegally acquire sensitive information, like passwords); brute-force attacks (password guessing); etc.

Passwords are inherently easy for adversaries to subvert. Due to password fatigue, users often choose weak passwords. They also often reuse or only slightly modify old passwords for different accounts. A **2018 Virginia Tech academic research paper** found password reuse was observed among 52% of all users.

As a result, Over 80% of breaches involving web applications is attributed to use of stolen credentials, while 50% of all breaches involved stolen credentials, according to **Verizon's 2022 Data Breach Investigations Report.**

What is Passwordless Authentication?

Passwordless authentication establishes a strong assurance of a user's identity without relying on passwords, allowing users to authenticate using biometrics, security keys or a mobile device. Duo is innovating toward a passwordless future that balances usability with stronger authentication. Passwordless gives users a frictionless login experience, while reducing administrative burden and overall security risks for the enterprise.

Business Benefits of Passwordless

Passwordless authentication provides a single, strong assurance of users' identities to achieve user trust. As a result, enterprises can realize the following benefits:

Better User Experience
By eliminating reliance on passwords, users benefit from a reduction in login fatigue and frustration, as well as an increase in user productivity.

Reduced IT Time and Costs
Similarly, administrators and enterprises can benefit from reduced burden due to password-related help desk tickets and password resets.

Stronger Security Posture
Eliminating system reliance on passwords can result in the elimination of related threats and vulnerabilities, including phishing, stolen or weak passwords, password reuse, brute-force attacks, etc.

> “Not only does this make UX a significant selection criterion for user authentication, but it also makes it a driver of new investments, when incumbent methods, however strong, fall short of UX goals. **Improved UX is a significant driver for client interest in passwordless authentication.**”

– **Gartner Buyer’s Guide for User Authentication**

THE CHALLENGE:

A Nascent Market

Today, many passwordless vendors only solve for one use case or enable a password-lite experience for users through single sign-on (SSO), changing the order of factors and session management. However, these piecemeal approaches can leave security gaps while not fully solving for the weakness of passwords. For example, will the passwordless solution cover every authentication flow, and even if it does, will it assess the posture of devices accessing without a password?

Modern enterprises cannot cover all of their access use cases today with a single passwordless solution.

There are additional business challenges to consider:

Complex and Hybrid IT Environments

Finding a solution that supports both legacy and cloud applications and provides a consistent, simplified user experience. Cloud federation provides passwordless only for cloud applications – users can log in and verify their identity using biometrics or a security key. But in reality, modern enterprises need to protect access to a hybrid mix of both cloud and on-premises applications.

Administrative and Management Costs

Supporting passwordless technology may involve cost-prohibitive security hardware and device management. The cost of security keys and biometric-based authentication can be a barrier to entry to supporting different types of users across an enterprise.

Compliance Regulations

Many companies or supply chain partner companies that need to meet compliance standards for data regulation have tied their policies to passwords, making it difficult to shift to stronger authentication methods. Federal standards like **NIST 800-63** outline more guidelines for passwords, MFA, and phishing resistant authentication methods, with more **recent guidance** on dropping password expiration and complexity requirements.

PROBLEM STATEMENT

Passwordless point solutions today do not solve for every common use case across modern enterprises, causing critical gaps in access security.

PASSWORDLESS CHALLENGE

Establish a basis for user identity trust that doesn't rely on passwords – no matter where the user goes or what they attempt to access.

THE SOLUTION:

Path to Passwordless

We recommend taking a phased approach to providing secure access for the workforce, with each step taking you closer to a fully passwordless future:

1.

Identify passwordless use cases and enable strong authentication.

Reduce your reliance on passwords and lower the risk of credential theft by identifying and selecting specific enterprise use cases. Rank the use cases by user experience, IT time and costs, and security and compliance risks. Group the use cases by applicable passwordless solutions, as to not end up with a series of point solutions. Create implementation plans for areas that have the biggest impact with the shortest time to value.

Strong Authentication for All Apps
Reduce your reliance on passwords as the only form of user authentication, and open up additional factors to later provide primary authentication. Protect cloud and on-premises applications with Duo's MFA. This enables you to lower the risk of credential theft by requiring a second method of identity verification that cannot be easily stolen remotely by an attacker.

2.

Streamline and consolidate authentication workflows.

Minimize Passwords for Cloud and Hosted Apps
Rationalize authentication for a set of use cases as part of the implementation plan. For cloud apps, achieve fewer passwords by using SSO for SAML-based applications. For on-premises services, integrate the workflows using access proxies and authentication proxies.

With MFA in place and a consolidated login experience, you can change password policies that require stringent and complex password characters, as well as policies around password reset frequency. This lowers the user frustration related to password security and reduces your reliance on password complexity as your primary authentication.

3.

Increase trust in authentication.

Increase Trust with Adaptive Policies
An often-raised concern about passwordless is the potential for increasing security risk when reducing the steps people take to authenticate. Address that head-on by increasing control based on the context of the user's authentication.

Is the authentication coming from a trusted device? Does the access device's security posture meet the organization's security hygiene standards? Finally, check for suspicious behavior like unusual authentication factors, unusual locations, strange times of day, or access attempts by high risk users or against high risk applications. Apply adaptive access policies based on the context of the user, device, location, behavior, and more, to ensure the authentication is trusted.

4.

Provide a passwordless experience.

If MFA is a password with one or more authentication factors, passwordless is best described as two or more authentication factors without passwords. People can log in using a biometric authenticator and possession of a trusted device to access applications. This would be **something they have** and **something they are**, instead of relying on something they know (a password).

In this step of the journey, implement standard technology to remove passwords as the primary authentication factor for the use cases and areas with the biggest impact on user experience, cost, and security.

For example, consider using passwordless authentication to securely log on to your SSO solution. In this way, all of the applications federated behind the solution receive the benefit of passwordless. Choosing the right passwordless authenticator will depend on your environment – leveraging hardware with built-in biometrics is one option, investing in security keys that support FIDO2 is another. There are also phone-as-a-token providers that can enable passwordless via a mobile application. To get concrete, many of these methods will leverage WebAuthn in the background. WebAuthn is an open standard that enables strong public key cryptography to ensure user presence at the point of authentication. It requires a supported web browser, operating system and built-in authenticator such as Touch ID, or USB-based security keys.

5.

Optimize the passwordless toolset.

Achieve passwordless authentication for all use cases, including passwordless for legacy tools using older protocols along with cloud-based applications. The path to passwordless is an iterative approach to selecting, streamlining, and securing authentication. The final step in the journey is integrating the technology and moving towards continuous improvement. Passwordless will eventually eliminate your need to rely on passwords for any login workflow, either behind the scenes or throughout your users' experiences.

This is the challenge in the market today that passwordless-pioneering technology platform providers need to solve. Duo is working on support for a comprehensive ecosystem that enables passwordless across every enterprise use case.

What You Can Do Today

Pairing passwordless technology with strong MFA to protect access across cloud and on-prem is a practical way to provide the broadest security coverage today. With MFA in place, you can reduce your reliance on passwords and modify password policies to require less frequent resets, alleviating help desk burden and reducing user frustration.

Duo recommends using the W3C open standard WebAuthn and cloud-based SSO to eliminate passwords for cloud applications. This doesn't completely eliminate passwords, but it does achieve the goal of reducing the reliance on passwords.

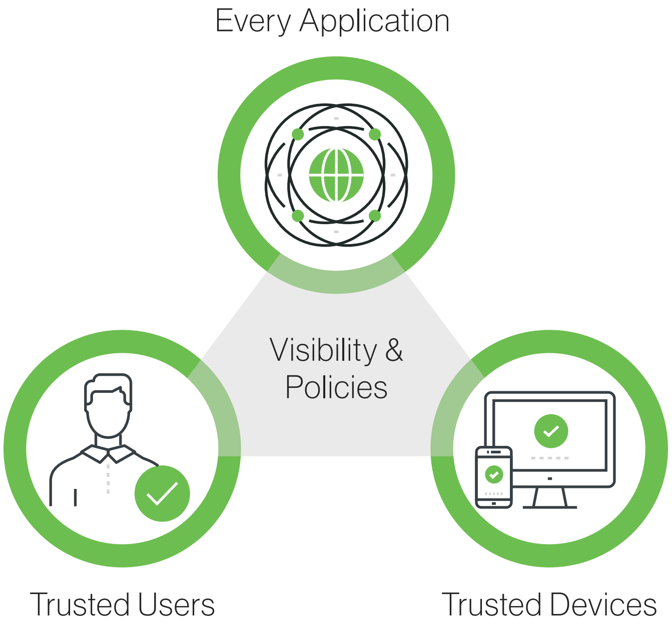
Passwordless Enables Zero Trust

Authentication – or secure access – enables the shift to a mobile and cloud-first enterprise, allowing users to work remotely, increasing productivity and driving business agility.

With identity as the new perimeter, enterprises need to secure the workforce: the users and the devices accessing applications. Passwordless authentication is a key building block to enabling zero-trust security for the workforce.

A combination of **user** and **device trust**, driven by **adaptive policies** ensures access to applications and data is secured.

Passwordless authentication improves the workforce's experience while strengthening our trust in authentication – a critical step in establishing a zero-trust architecture.

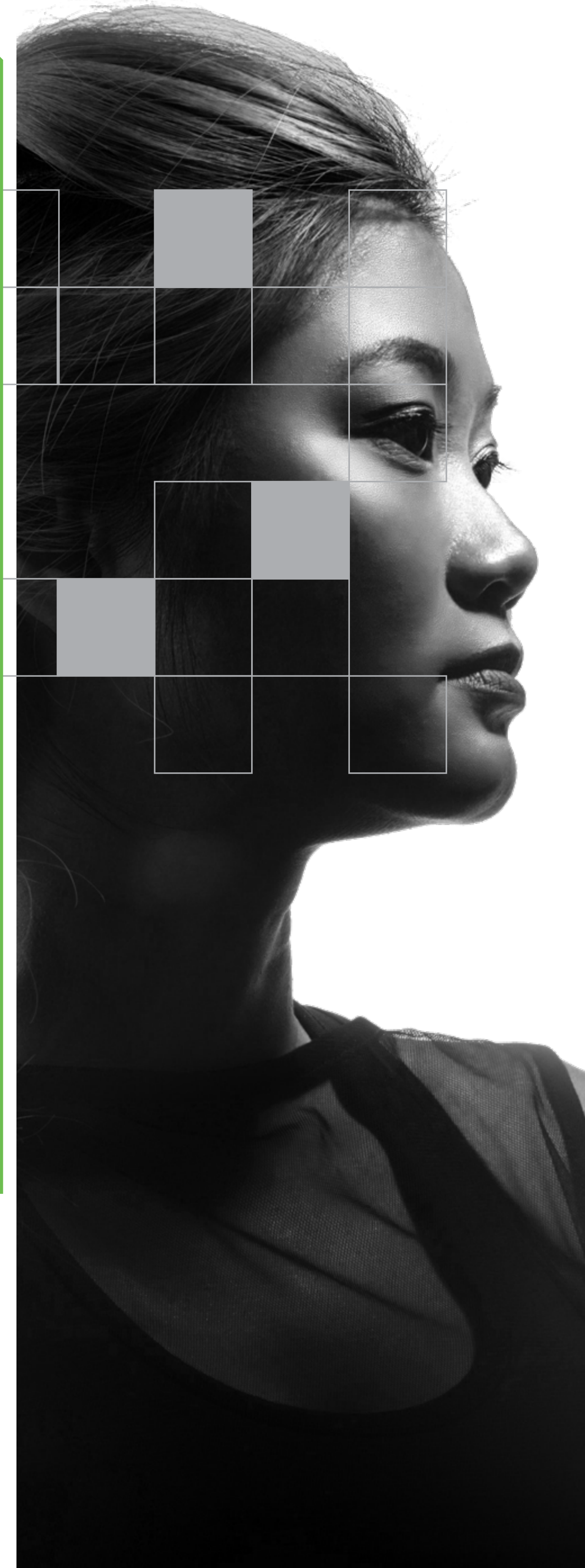


In its 10 principles of zero-trust architecture, the National Cyber Security Centre (NCSC) references passwordless as part of "**creating a single strong user identity**."

> “In order to remove trust from the network, you need to instead gain confidence in the authentication, verification and authorization of users and services. This is achieved by **building trust into the user's identity** (user authentication), their devices (device verification), and the services they access (service authorisation).
>
> For this model to be effective, each connection to a service should be authenticated and the device and connection authorised against a policy, regardless of where the connection request comes from.”

– **UK NCSC Zero Trust Architecture**

Passwordless is a building block for organizations on a zero-trust journey. It provides a key aspect of establishing a single, strong user identity and trust.



Building for a Passwordless Future

Duo is building out a secure access platform that will enable a fully passwordless future for the enterprise.

We can’t do it alone. Passwordless requires technology platforms like Windows Hello, Touch ID, Face ID and fingerprint APIs to work in tandem with hardware-based biometric authenticators, supported by open standards like WebAuthn and CTAP. But, we will do our best to partner across organizations and technology providers to provide seamless, secure passwordless experiences.

We are committed to paving a path to passwordless by:

- Building a passwordless authentication solution that is easy to implement and use
- Partnering with hardware and software providers to provide best-in-class experiences regardless of a company’s infrastructure or technology stacks
- Supporting FIDO2 security keys for major browsers
- Having Duo experts in the WebAuthn Working Group, W3C and FIDO Alliance to advocate for enterprise features

Additional Resources

Learn more about what Duo is doing to enable the passwordless future by working to make passwordless technology and standards open, accessible and easy for the broader community:

What is WebAuthn?

Web Authentication: What It Is and What It Means for Passwords

WebAuthn.guide

WebAuthn.io

VIDEO: **A Technical How-To Guide for WebAuthn 2019**

Introducing the WebAuthn Authenticator Open-Source Library

0
35
25