VERIDIUM
TRUSTED DIGITAL IDENTITY

WHAT ORGANIZATIONS NEED TO KNOW ABOUT PASSWORDLESS AUTHENTICATION

NO ONE LIKES USING PASSWORDS

Security and IT professionals loathe them because of their security risks. Chief digital experience officers or anyone who handles user experience dislike passwords because they're not very user friendly. Lastly, there are the users, a category that encompasses everyone. While they don't like using passwords for many reasons, having to remember them likely tops the list.

Although we complain about passwords, they've been the main way we authenticate since their invention in the 1960s. But that's changing. Passwordless authentication is now an option. By eliminating passwords, companies can improve their security posture while providing people with a better user experience.

This guide provides an in-depth perspective on passwordless authentication. You'll learn what user experience and security benefits passwordless authentication provides, how it saves businesses money and why organizations, including Microsoft, are adopting this technology.

With passwordless authentication, no passwords are used. Nothing is hashed or transmitted and there's nothing for employees to remember, forget, type in or reset.

WHAT IS PASSWORDLESS AUTHENTICATION

The definition of passwordless authentication is straightforward: passwords aren't used in the authentication process. Nothing is hashed, transmitted between a laptop and a server or used for single sign-on. There are no passwords to remember, forget, type in or reset. And there aren't any credentials for threat actors to steal. How passwordless authentication is carried out is a bit more complicated. Some methods that can be used for passwordless authentication include using biometrics, a soft token that's delivered by either text or email, a hard token or a magic link.

Each of these passwordless authentication methods comes with benefits and drawbacks. People have grown accustomed to using biometrics to unlock their smartphones and mobile apps. The experience is faster and easier than using a password. But security concerns over what happens if biometric data is exposed in a breach could hinder wider adoption of this technology.

Magic links and tokens also offer a better authentication experience compared to passwords. But neither one validates a person's identity. The assumption is that the person opening the email or text with the passcode is the intended recipient. But after an account is compromised, especially if it's an email account, attackers have a direct path to taking over other accounts linked to that email address. Even novice attackers can search an inbox, learn what other services a person uses and initiate a password reset, giving them control of the account. Cell networks can be hacked, allowing attackers to intercept text messages sent over the network, and tokens are cumbersome for people to carry around and costly for organizations to maintain.

WHAT ARE THE BENEFITS OF PASSWORDLESS AUTHENTICATION

Better user experience

Passwordless authentication provides an overall better user experience. Eliminating passwords means people don't have to remember them and provides faster access to applications and services. You break the cycle of remembering your password, typing it in, trying another password because the first one didn't work and repeating this process until one works or you give up and reset it (only to be told you can't use that password since you've used it before). Instead, you use your biometrics and smartphone, for example, to efficiently and quickly authenticate. Here's how eliminating passwords benefits employee, consumer and transaction authentication.

Eliminating passwords benefits employee, consumer and transaction authentication

Employee authentication

At work, keeping track of passwords becomes more challenging as we use more cloud services and applications. There's a password to log in to your laptop, another for Salesforce, another for Gmail, another for Dropbox, among the many applications employees use. While browsers can store passwords, many enterprises have password management policies that require users to change their passwords at frequent intervals (there's also the challenge of remembering your password when you access a cloud-based application from another browser, like the one on your home computer). In theory, people should use unique passwords for each account. In reality, most people reuse passwords or modify them slightly. Password reuse is a major security violation that can have major repercussions but more on that in the section that talks about passwordless authentication's security benefits.

Removing passwords from the enterprise increases worker productivity by changing the dynamic around password resets. Typically, resetting a password means contacting the IT department and waiting for someone from the department to field your request. The wait time is impacted by other projects the IT administrator is working on, meaning you could be waiting awhile to reset your password and get back to work. Or, in larger enterprises, a password reset can trigger a multi-step, time-consuming process that includes contacting a worker's manager. Password resets can mean people spend their day resetting a password instead of working.

Then there are the operational costs to password resets. Password resets cost companies $70 per employee, according to Okta. Veridium estimates that password resets annually cost organizations $1.9 million based on an enterprise with 10,000 employees. Out of all the tasks IT administrators handle, passwords resets probably rank low. Their time could be better spent on projects that add value to the business.

Consumer authentication

People expect consumer technology, especially any activity involving a smartphone, to provide fast and seamless user experiences. Passwords, however, deliver the opposite experience. Take mobile banking apps. Customers could type in either a password or PIN to authenticate, approve high-risk transactions or transfer money.

But manually entering this information isn't efficient and doesn't offer the experience people expect from mobile apps. Given the ubiquity of smartphones equipped with biometric sensors, people have grown accustomed to using "what they are" instead of passwords to complete tasks like unlocking a phone or mobile app. They want to press a fingerprint sensor, take a selfie or snap a picture of their fingerprints to prove who they are.

Consumer technology is now associated with passwordless authentication. Companies that realize people expect passwordless authentication in consumer use cases and adopt this technology stand to retain customers and attract new ones. With so many companies offering similar services and products, authenticating with as little friction as possible offers a competitive advantage. People want to use technology that simplifies their lives, especially one that does away with passwords.

Password resets annually cost organizations $1.9 million based on an enterprise with 10,000 employees, according to Veridium's estimates

Transaction authentication

Quickness and efficiency are associated with online shopping. People want to quickly buy items without entering credit card information, a billing address or a password. But the checkout process could slowdown as governments pass regulations similar to the strong customer authentication (SCA) component of PSD2 in Europe, which requires two-factor authentication for certain transactions. Passwordless authentication provides two-factor authentication while allowing shoppers to checkout seamlessly if the right authentication elements are used. For instance, authentication using biometrics and a smartphone provides a faster, better experience than making customers switch between their email app and browser in order to enter a password that's been emailed to them.

Selecting the right authentication method is also key in transactions that involve step-up authentication, like transferring money to another account. While customers could enter a one-time password that's texted to them, toggling between screens doesn't provide an ideal or seamless experience.

Improved security

Passwords have a security problem. Turns out, they're not an ideal way for protecting data. Passwords are frequently stolen in data breaches or phishing attacks and end up with threat actors who use them in other attacks. Just look at the Verizon Data Investigations Breach Report. Each year it seems to list phishing and stolen credentials as two of the top tactics used by attackers. The 2019 report was no exception: 32 percent of the 41,686 security incidents covered in the report involved phishing and 29 percent involved stolen credentials.

Leveraging usernames and passwords remains a key tactic for threat actors. In an attack that targeted 10 mobile carriers, collecting usernames and passwords from compromised machines was integral to the campaign. Having credentials allowed the attackers to move laterally and eventually compromise the Domain Controller, giving them full control of the victims' network.

Adding to the security issues around passwords is that people violate a cardinal security rule and reuse them (that's in addition to other poor security practices like slightly modifying passwords or using common phrases). With credentials commonly exposed in data breaches (Veridium calculated that 390 million passwords were exposed in some of 2018's largest data breaches), there's an increased chance that, eventually, a person's username and password will end up in the public domain. Attackers know people reuse passwords and there's a possibility that a stolen password could get them into users' high-value accounts.

By eliminating passwords, the security risks associated with them are mitigated. Phishing attacks lose their potency if there aren't any credentials to con out of employees. And if there aren't passwords to steal, threat actors can't use them to infiltrate companies.

Passwords are frequently stolen in data breaches or phishing attacks and end up with threat actors who use them in other attacks

WHY THIS IS THE TIME FOR PASSWORDLESS AUTHENTICATION

Call it the perfect storm for passwordless authentication. There's the perennial business and security need to reduce the risks with using passwords. Meanwhile, government regulation and user experience concerns mean companies are considering authentication methods that don't involve passwords.

From a business perspective, resetting passwords is expensive. Organizations have better ways to spend $1.9 million, which is how much business spend yearly on resetting passwords. Factor in the steady stream of stories about credentials being used in attacks and companies are even more keen to ditch passwords. Security incidents, regardless of the initial penetration vector, are costly. Repercussions can include data breaches (see Home Depot, Equifax and countless other companies), fines (see British Airways for violating GDPR), brand damage (see Sony) or lost revenue (see shipping company Maersk due to NotPetya). Rather than building walls to keep out attackers, enterprise information security focuses on mitigating security risks, including relying less on passwords by rolling out passwordless authentication.

Reflecting enterprise interest in passwordless authentication, Gartner noted an uptick in passwordless inquiries from companies in 2018. The research firm predicted that by 2022, 60 percent of global companies and 90 percent of midsize companies will implement passwordless methods in more than half of use cases, up from 5 percent in 2018.

Microsoft is heavily vested in enterprise adoption of passwordless authentication. The technology giant is replacing passwords with biometrics for employee access this year and expects other companies to follow suit within six years. To encourage enterprise use of biometrics, the next major Windows 10 release will give people the option of using Windows Hello instead of a password to access Microsoft accounts.

Meanwhile, regulation calling for two-factor authentication, such as SCA, is forcing companies to reconsider how their customers authenticate. Instead of looking at compliance as a burden, some companies are using regulations as an opportunity to help their business. With regulation around two-factor authentication, companies want to provide people with the best user experience possible. Make it difficult for them to access accounts or services will upset customers and drive them to competitors. Aware that passwords provide a less-than-enjoyable user experience, companies are using compliance as a reason to eliminate them.

Gartner predicted that by 2022, 60 percent of global companies will implement passwordless authentication

THE CASE FOR PASSWORDLESS AUTHENTICATION WITH SMARTPHONES AND BIOMETRICS

While there are different ways to carry out passwordless authentication, using smartphones and biometrics is the ideal choice for users and enterprise security.

FAMILIAR TECHNOLOGY: People are accustomed to using smartphones and biometrics to authenticate. They know how to use a fingerprint sensor, take a selfie or take a picture of their fingerprints with a phone's camera.

PEOPLE THINK MOBILE FIRST: Given the ubiquity of smartphones, people expect anything that's related to technology, whether it's for their personal lives or at work, to have a strong mobile component.

CONVENIENT AUTHENTICATION: With one-time passwords and PINS, people have to toggle between either a text message or email and an authentication screen that's likely in another app. Biometric authentication eliminates the hassle of switching between screens to authenticate.

BIOMETRICS ARE SECURE: Biometric templates can be securely stored using encryption and a distributed data model, which breaks the template into two pieces and stores one on a person's smartphone and the other on a company's server. Attackers would need to access both the smartphone and the server to complete the biometric template. And even if attackers carried out the complicated process of spoofing biometrics, technologies like liveness detection and behavioral analysis mitigate the chances that the spoofed biometric will fool a biometric sensor.

EMPLOYEES ARE READY FOR PASSWORDLESS AUTHENTICATION AT WORK: A poll from research from identity and access management company Okta found that 70 percent of respondents want to use biometric authentication at work. A Veridium poll found similar enthusiasm for using biometrics at work, mainly so people don't have to remember passwords.

CURIOUS ABOUT GOING PASSWORDLESS?

HERE'S WHAT TO CONSIDER

For enterprises that are looking into passwordless authentication using biometrics, here's what to keep in mind:

- Find a passwordless authentication platform that works in complex IT environments. The product should work with many OSes, including Windows 10, Windows 7, older versions of Windows and macOS, and allow employees to authenticate with commonly used enterprise applications including Salesforce, G Suite and Citrix.
- Make sure the password is completely removed from the authentication process and not saved in the cloud, on a server, on a laptop or on another device.
- Focus on the user experience. People want to authenticate quickly and easily. The goal is to make authentication less cumbersome.
- Look for passwordless authentication platforms that leverage smartphones and biometrics. People have mobile-first and biometrics-preferred attitudes toward authentication. Extra hardware isn't appealing to users, who have to carry it, or organizations, which have to purchase and support it.

Using smartphones and biometrics for passwordless authentication is the ideal choice for users and enterprise security