BEYOND IDENTITY

PASSWORDLESS AUTHENTICATION: WHAT IT IS AND HOW IT WORKS

Table of Contents

Highlights

- Passwordless authentication is significantly more secure, reduces user friction, and saves organizations time, effort, and money.
- Instead of a password, passwordless authentication uses something they have or something they are, none of which is stored by the provider
- Beyond Identity leverages the technology built into modern devices to provide secure authentication, through biometrics and the Trusted Platform Module
- Read more about the pros and cons of going passwordless below

Introduction

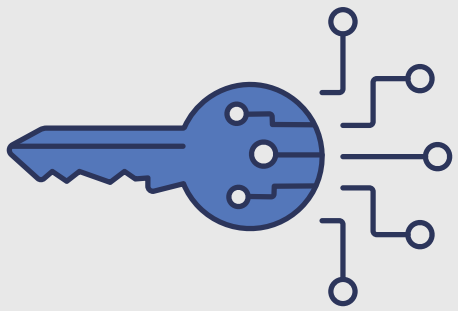
Passwordless authentication promises to eliminate the number one weakness in security: passwords. For that reason, passwordless authentication is generating a lot of discussion, including differing opinions that can, unfortunately, be misleading and confusing. This guide provides some clarity on what password authentication is and how it works.

Passwords have long been known for being the weakest link in security. Users reuse passwords across multiple systems, they forget their passwords or write them down, and passwords are easily compromised. According to the 2020 Verizon Data Breach Investigations Report, over 80% of breaches resulting from hacking involve brute force or the use of lost or stolen credentials.

Over the years, a number of password alternatives have been developed. We've seen Common Access Cards (CAC), smartcards, and biometrics—just to name a few. However, passwords continue to be used as a backup for these methods. As long as a password is used, you remain vulnerable to password-based threats like phishing attacks, SIM swaps, and more.

Traditional multi-factor authentication (MFA) isn't much better. Traditional MFA is thought to improve security by layering additional authentication methods on top of a password. After the user enters their initial password, MFA asks for more proof by using other factors to validate identity. Unfortunately, with MFA, the second factor may not be much stronger than a password. Out-of-band (OOB), SMS, and mobile push authentication methods are also vulnerable. But at the end of the day, traditional MFA doesn't eliminate the most insecure factor in the login process: the password. Finally, MFA adds friction to the authentication process, impacting the user experience for minimal benefit. For the user, MFA is time consuming and frustrating to the point of affecting company productivity.

Passwordless authentication replaces traditional MFA's weak factors with significantly stronger ones. As a result, a passwordless authentication solution improves security and the user experience by removing friction from the login process.



Passwordless authentication: What it is and what it isn't

Passwordless authentication is just that: a form of authentication that does not use a password—ever. Passwords aren't used as an alternative authentication method or even as a backup. Even if antiquated systems like Microsoft Active Directory require passwords, passwords aren't used to authenticate. Nor are passwords stored in a password vault or manager.

This is an important point to understand, because some technology providers say their authentication solutions are passwordless when they're not. They continue to use passwords as a backup, so anyone can use that password to get in, and you're still vulnerable to password-based attacks.

The point of passwordless is to use an authentication method that's more secure. A password is a knowledge factor. It's not much of an improvement if you replace a password with another, just as insecure, knowledge factor.

The benefits of our passwordless authentication

Passwordless authentication offers a number of benefits:

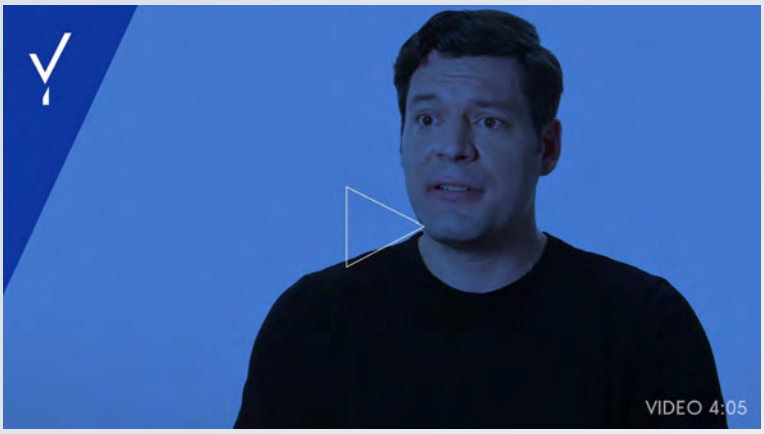
Stops account takeovers from credential attacks: Removing passwords as an authentication method eliminates all password-based attacks. Attackers simply can't use passwords to login because they don't exist. Passwordless authentication can protect against login credentials being stolen or leaked in credential stuffing, credential cracking, ransomware via RDP, social engineering, and phishing attacks.

Improves the user experience: With its zero-click logins, passwordless authentication eliminates the friction of authenticating. Users do not need to refer to a second device, check their email, remember passwords, or go through the hassle of resetting them.

Saves time and money on password resets and help desk calls: Users no longer need to remember unique passwords or regularly reset them as part of a strong password policy, which means less work for IT.

Strengthens your security posture with continuous risk-based authentication: Users are re-authorized with each access request to ensure that the user's risk posture hasn't changed.

How does passwordless authentication work?



Passwordless authentication refers to a method of verifying a user's identity without the use of a password. Instead of a password, the user authenticates using something they have (such as a mobile device) or something they are (such as a biometric). Every time a user requests access, a new authenticating message is generated. Hence, no credentials are fixed within the passwordless platform so there is nothing for an attacker to steal.

Passwordless authentication from Beyond Identity leverages the technology built into modern devices to provide secure authentication. These technologies are biometrics and the Trusted Platform Module (TPM). The TPM is a secure enclave where sensitive data can be stored. In the case of passwordless authentication, that sensitive data is a private cryptographic key. The TPM signs a certificate with the private key that can be validated using the corresponding public key.

This model is inherently trusted. In fact, it is used countless times a day by people everywhere submitting private information over the Internet. The model is used by Transport Layer Security (TLS) to ensure that the private data exchanged with servers remains private and secure. TLS employs X.509 certificates that are based on asymmetric cryptography and public-private key pairs.

Beyond Identity's passwordless authentication solution leverages X.509 certificates without the need for a certificate authority or any certificate management. It simply extends the Chain of Trust™ established by TLS to users and their devices.

Using X.509 certificates and public-private key pairs is more secure than other authentication methods. A password, passphrase, and PIN use a shared secret—a piece of data that's stored in a database that may be vulnerable to compromise. Hardware keys have known security issues with Bluetooth and Near-Field Communication (NFC). They also lack a comprehensive, granular device security posture.

In addition to the vulnerabilities mentioned, MFA increases exposure through SIM hacking, malware, and notification flooding. However, with X.509 and TLS technologies, the private key is securely stored in the TPM of a personal device. The private key cannot be removed or viewed by anyone—not even the user.

Some organizations have legacy systems that still require users to have a password in the directory. You can use passwordless authentication for these systems, too. In the Beyond Identity console, you can set up an access policy so that no one can use a password to login. If an attacker attempts to access systems with a stolen password, an alarm is set off and the attacker is denied access.

Downsides of some passwordless approaches

Not all passwordless solutions are created equal. Some solutions, like Windows Hello for Business and FIDO/WebAuthN, only support some device types or use cases. Or they leverage passwordless authentication as part of an MFA solution that requires shared secrets.

Other passwordless solutions authenticate users from a second device, which is not only inconvenient but also insecure, because the second device must communicate with another device. Most of these solutions use insecure methods like OOB, SMS, and mobile push notifications for these communications. There's also no guarantee that the person initiating the login is in possession of both devices or that the devices themselves are clean and healthy to ensure a secure transaction.

Getting started with passwordless authentication

A strategic approach to passwordless authentication can help you avoid adopting the wrong solution. Start by mapping out all the places your workforce uses passwords, including device types and log in locations. Then roll out passwordless in phases, beginning with areas where you can easily integrate and enhance existing security infrastructure to decrease time to value.

Your single sign-on (SSO) solution is a great place to start. It's easy to connect a passwordless solution to SSO. As the number one entry point for thousands of apps that have historically been protected by a single password, SSO's highly trafficked resources impact the majority of the **workforce**, and there's a high risk of credential-based attacks.

Choosing a passwordless authentication solution

Look for a passwordless solution that:

- Replaces insecure factors ("something you know") with more secure factors ("something you are," as in biometrics, or "something you have," as in a device).
- Eliminates passwords entirely as an authentication method—not even as a backup.
- Uses industry standard protocols to make it easy to set up without fewer help desk calls for a quick time to value.
- Provides a frictionless user experience and makes it easy for users to manage and recover credentials to help reduce IT help desk costs.
- Provides a consistent login experience across all devices and operating systems so users know what to expect.
- Utilizes risk-based policies to enforce a risk threshold when granting access to systems and data.
- Continuously analyzes user and device risk at every transaction.
- Assesses risk before users are granted access.

Beyond Identity provides passwordless identity management, enabling organizations to truly eliminate passwords. Our **passwordless identity platform** is a cloud-native solution that's simple to set up and lowers operational costs.

The Beyond Identity Passwordless Identity Platform enables organizations to leverage robust MFA, deliver continuous, risk-based authentication, and improve the user experience. The platform **plugs in easily with your existing identity infrastructure** and integrates with SSO solutions such as **Okta**, **Ping**, **Forgerock**, and Microsoft ADFS.

Ready to ditch passwords once and for all?

About Beyond Identity

Beyond Identity's mission is to eliminate passwords and radically change the way the world logs in.

Our authenticator runs on Windows, MacOS, iOS, iPadOS, and Android.

Authenticates users on mobile and desktop devices, to web-based and native applications.

Supported industry standards: OIDC, OAuth, SAML, and SCIM.

Visit beyondidentity.com for more information.