

Frictionless Security:

Protect Critical Resources with Seamless Authentication

BEYOND
IDENTITY

You aren't the only one who groans when encountering annoying [one-time passwords](#) or push notifications with password-based multi-factor authentication (MFA), especially if you're trying to get something done quickly. And you can bet other employees and contractors aren't happy with it either.

Simply put, friction-filled MFA makes you stop your task, and breaks your concentration—which means less productivity. You may have to go find a second device to get the one-time code to enter, find an email with a [magic link](#) in your already overflowing inbox, or look for a notification from a separate app.

No matter the specifics, friction-filled MFA disrupts workflows. While a few minutes may seem negligible, those productivity losses multiply very quickly. These seemingly insignificant productivity breaks can easily mean hundreds of lost hours a week for your company. One survey found that complex IT security procedures, like friction-filled MFA, contribute to [US employees losing 22 minutes of work a week](#). Extrapolate that out over a whole year and you can see the real damage to productivity it is causing.

Password-based MFA used to be the security standard. But time (and breaches) have shown us that [it's not enough](#), and users will avoid adoption because they dislike the cumbersome factors involved. There are better, more user friendly MFA solutions that will leave users happy and your resources more secure.

Friction-filled authentication hurts adoption

MFA adoption rates remain low in many organizations even though it does help provide a base level of security. [Microsoft](#) said only 22% of Azure Active Directory (AD) customers used MFA to secure their accounts in 2021. It doesn't matter how effective MFA is; if no one adopts the solution then it's not going to work. The problem is friction, and frustrating your employees and contractors keeps them from adopting the very security solution you need to protect your data.

Additionally, friction-filled authentication can add vulnerabilities. The more employees and contractors find ways to circumvent the security solution, or refuse to use it at all, the more holes there are of which an attacker can take advantage.

Improve productivity with frictionless authentication

There is a better option. With Beyond Identity's frictionless multi-factor authentication, your users don't have to remember a password because our solution is truly passwordless. They don't have to accept a push notification or enter a code.

- Users no longer need to have a second device, download an MDM, or deal with the hassle of monthly password resets.
- Beyond Identity is a frictionless, invisible MFA. The authentication factors are invisible to both the user and any potential attacker.
- The user can easily self enroll, with no need to schedule time with an IT person to come do anything with their laptop.
- It's easy to add the Beyond Identity Authenticator to whatever devices the user wants to access work resources.
- Users will readily adopt it, and this gives the organization a lot more security.

Beyond Identity uses three phishing-resistant factors that create no friction for the user while providing the most secure authentication on the market:



Biometrics to prove the owner of the device is using it



Cryptographic security keys that bind the user's identity with the hardware of their authorized device(s)



Device-level security checks to protect against data loss by checking the device security posture

All the user needs to do is scan a fingerprint and the security checks run seamlessly in the background with no disruption to workflows or access to resources.

As administrator, you have the transparency you need to do your best work—a signed, immutable record of who is accessing your resources, which device they are using, and the current security posture of the device each time the user authenticates. And each time your employees or contractors need help with migrating a device or recovering an authentication, they can use the self-service tools.

Best of all, your organization increases both productivity with a single new tool. Instead of frustration caused by forgotten or lost passwords, your employees and contractors are thrilled with the easy experience, logging in becomes an easy process, and productivity will increase. The best part is, you are not sacrificing security. Your data is even more secure than it would be with friction-filled authentication.

[Set up a time today for a demo](#) and see how Beyond Identity can make a difference in your organization's productivity.

Beyond Identity

Beyond Identity is fundamentally changing the way the world logs in—eliminating passwords and all phishable factors to provide users with the most secure and frictionless authentication on the planet. Our invisible, passwordless MFA platform enables companies to secure access to applications and critical data, stop ransomware and account takeover attacks, meet compliance requirements, and dramatically improve the user experience and conversion rates. Our revolutionary zero-trust approach to authentication cryptographically binds the user's identity to their device, and continuously analyzes hundreds of risk signals for risk-based authentication. For more information on why Snowflake, Unqork, Roblox, and IAG use Beyond Identity, check out www.beyondidentity.com.

GET A DEMO

beyondidentity.com

info@beyondidentity.com

BEYOND
IDENTITY