You can stop using passwords for your work accounts with this tool

Okta's FastPass feature works with biometric logins to unlock all your work stuff.

When you start your workday on a computer, it can be time consuming to log into what feels like a million accounts before you can get anything else done. Single sign-on services from companies like Okta, OneLogin and others try to take the bother out of the chore. You sign into their service, and you're logged into all your work-related accounts at the same time.

Okta wants to take things a step further. With its new FastPass feature, unveiled Wednesday, you don't sign into anything. Instead, you use the biometric login feature TouchID and FaceID on Apple devices, fingerprint login on Android, or Windows Hello to access your device. That logs you into your phone or laptop, as well as your Okta account and all your connected work accounts in one go.

The idea is that if you authenticate yourself on your device with a biometric like your fingerprint, you should be able to access everything. "It's binding the device with the user's identity," said Joe Diamond, vice president of product marketing at Okta.

FastPass can also work from a personal computer, meaning you could still have passwordless access from a home system. As millions of people in the US are under orders to stay home during the global coronavirus pandemic, many workers are logging into corporate accounts from personal devices. That's been the case for years, Diamond said, but it's especially true now.

The feature helps move users further from relying on passwords, a path that security experts say we need to keep going down. While we likely won't stop needing to log into our accounts until the end of civilization, it's better if we can do it without passwords. Passwords are very difficult to use correctly, and most people have some combination of bad habits, like reusing passwords and using weak, easy-to-guess passwords. Services like password managers can make us better at using passwords. In the future, technology like security tokens and biometrics will keep making it easier to skip passwords while still keeping accounts safe.

Okta's FastPass feature, which the company said would be available to its customers in the coming months, works at the level of the operating system, or the software that runs your entire device. There, it can tell you've authenticated using a biometric login.

It can also coordinate with the security software running on your computer or phone, receiving alerts if you've downloaded malicious software or are showing signs of compromise. Your IT department can use that data to determine if you should be locked out of other accounts, like your business email or finance software, so that hackers can't use your device to access sensitive information or do other mischief while posing as you.

Lumping together more and more accounts under just one form of authentication means it's especially important that the one place you do login be secure. If hackers steal the master password to your password manager, for example, then they have the keys to your kingdom (or if you forget that password, you're locked out of your entire kingdom). That principle applies to single sign on services, too. A compromise would let hackers into several accounts, not just one.

But since Okta is relying on biometric systems from Google, Apple and Windows, it doesn't have to invent its own secure biometric technology. Instead, the security features that make it safe to log into your device with your fingerprint or face are extended to your work accounts with FastPass. That includes segmented portions of the microprocessor where your biometric data is stored, keeping it on your device and separate from other processes running on your computer.