mobile mentor

# PASSWORDLESS AUTHENTICATION

A non-technical overview for executives and board members

mobile-mentor.com

## What’s holding you back from going passwordless?

Passwords were a great invention in 1961, but in 2021, we discovered passwords were the main cause of cyber-attacks.

Why are we so reliant on a 60-year-old solution when we have the technology to be passwordless?

A passwordless environment is more secure, saves money, and improves the end user experience.

If you are using Microsoft 365, you can go passwordless at **no additional cost**.

Let's get you started on the journey to a passwordless workplace.

## What's wrong with passwords?

We all have **too many passwords,** resulting in password fatigue and poor ***password hygiene***.

We are fallible human beings, not walking databases. We cannot possibly manage unique and complex passwords for each application and digital service.

We cheat and we hack.  We chose the simplest possible passwords by using predictable patterns. We re-use the same passwords for our work and personal lives.
And we are careless in managing all our passwords.

The 2022 endpoint ecosystem research study in the USA and Australia found that 31% of people write their work passwords in personal notebooks, 24% on their personal phones and 21% in documents and spreadsheets.

National Cyber Security Centre in the UK found that 15% of the British population used pets' names, 14% use a family member's name, and 13% use a notable date.

Six percent of people use "password" as their password. The most popular password in the UK in 2019 was "123456" used by a stunning 23 million people!

**97**

Passwords that the Average Knowledge Worker keeps

**80%**

of security breaches involve compromised passwords

**35%**

of helpdesk tickets are for password resets

**69%**

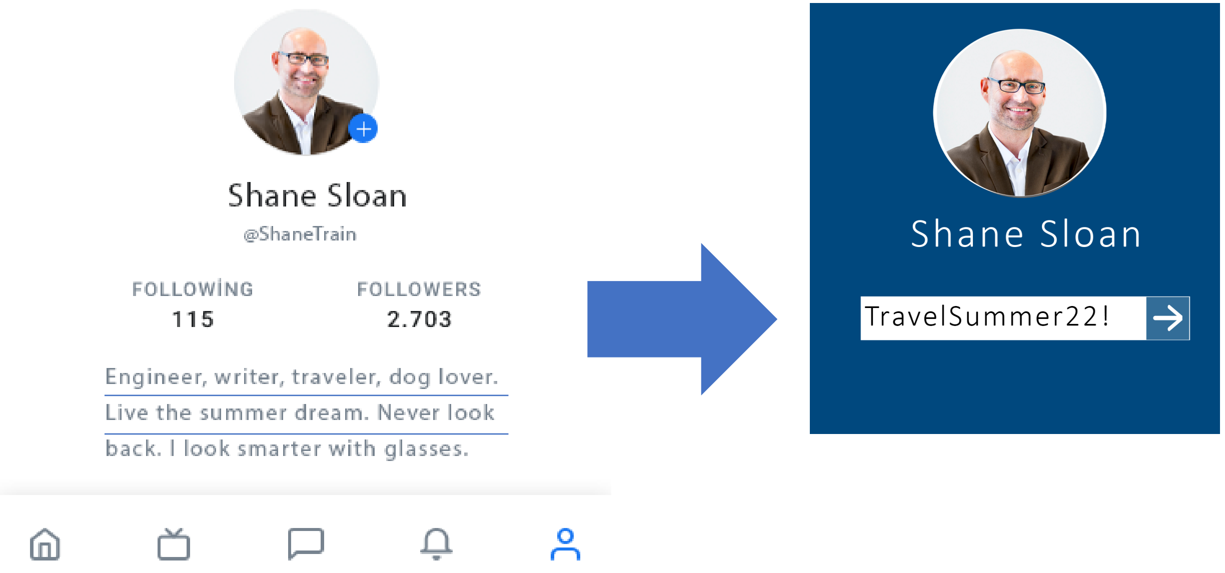
of workers choose passwords that are easy to remember

## So what?

These days, hackers no longer need to “break in” to your account or corporate network. **They simply login with your weakest password.**

A quick glance at anyone’s social media profile will probably yield their pet’s name, family member names, and birth dates.  Combine a couple of these……and you probably have a password.

Compromised credentials lead to devastating data breaches, adverse publicity, regulatory fines, stress, embarrassment and costs in the millions.


Shane Sloan
@ShaneTrain
FOLLOWING 115
FOLLOWERS 2.703
Engineer, writer, traveler, dog lover. Live the summer dream. Never look back. I look smarter with glasses.

Shane Sloan
TravelSummer22!

**80%**

of security breaches involve compromised passwords

**$4.37 Million**

Average cost of a breach caused by compromised credentials in 2021

## Here’s the Good News

The era of **passwordless authentication** is already here, and you may be using it already if you have an iPhone.

When you pick up your phone it scans your face and detects about 300,000 data points to verify your face. That signs you into the iOS operating system.

Then, you are automatically signed in to trusted apps through a process called Single Sign-On (SSO).

For other apps and websites, you may be prompted to enter a verification code – which is two factor authentication.

Bingo, that was a passwordless experience.  Now, lets map that process to all your other devices and you will be living the dream.

### Biometrics at Work

Windows Hello uses **facial recognition** and **fingerprints** to validate your identity and login to a Windows PC.

**Did you know that 92 percent of businesses believe passwordless authentication is the future? Source**

## How does it work?

### There are 5 building blocks in a passwordless architecture:

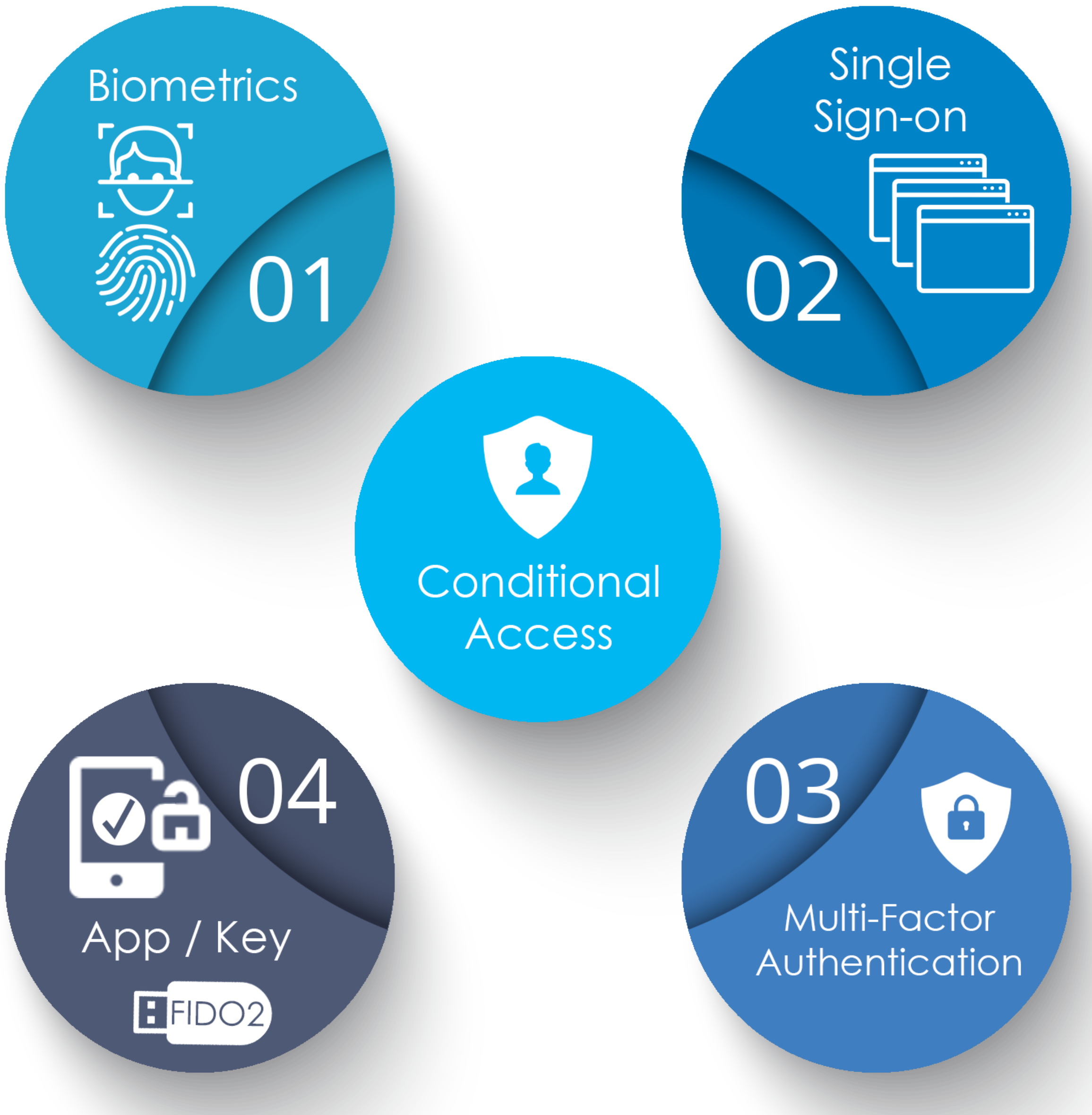
Biometric Sign-In

Single Sign-On

Multi-factor authentication

App or FIDO Key

Conditional Access Policies



## 1. Biometric Sign-in

**Windows Hello for Business** is the biometric component of a passwordless solution on a Windows device (laptop or desktop).

Depending on the device specification, Windows Hello uses fingerprints or facial recognition to log in. When purchasing new devices, choose devices with the **TPM 2.0** encryption chip and an **infrared camera**.

**Windows Hello for Business** addresses the "Something You Are" component of the passwordless strategy.

Windows Hello for Business leverages biometrics and uses a facial recognition, a fingerprint or a pin number to allow end-users to log in.

Like Single Sign-On, the intention behind Windows Hello for Business is to eliminate risk by reducing the number of times an end-user needs to enter credentials. The basic principle being the less credentials are typed, the less end-users and companies are being exposed.

## 2. Single Sign-On (SSO)

Once your employees have authenticated to the Windows OS, the next step is to authenticate to the required applications, services and storage locations.  Rather being prompted for unique passwords for each application, Single Sign-On automatically authenticates the user to trusted applications and resources.

When vetting new software applications, choose products that are **SAML compliant** so you can leverage Single Sign-On.

## Frictionless User Experience

Each time your employee types their credentials, they create a possible point of failure and risks being compromised. The philosophy behind SSO is to eliminate as many login events as possible.

Once authenticated, the user will be able to access all their cloud services (that are configured with Single Sign-On) without having to type their credentials again.

When a browser is opened, the cloud service will simply open and sign in. To a user, everything will just appear to work – most will never realize that an intelligent authentication process has even occurred.

## 3. Multi-Factor Authentication

Multi-factor authentication (MFA) is the verification step to ensure the person logging in is the person who they claim to be. MFA is proven to prevent 99% of all malicious attacks.

**MFA should be used everywhere, all the time.**

If multi-factor authentication is not active, research shows that 0.5% percent of user accounts will be compromised every month through brute force attacks. Source

Also, consider that the incubation time for an average hack is 197 days. That means from the time the breach occurs to the time it is detected is over 6 months! That's a long time for a cybercriminal to watch, wait and gather data before making their move.

### THREE COMPONENTS OF MFA

01 **SOMETHING YOU KNOW**
Your password, username, or a pin code.

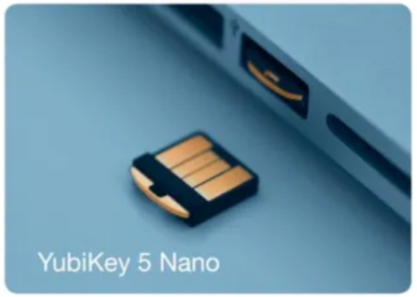
02 **SOMETHING YOU ARE**
Biometrics like facial recognition or a fingerprint.

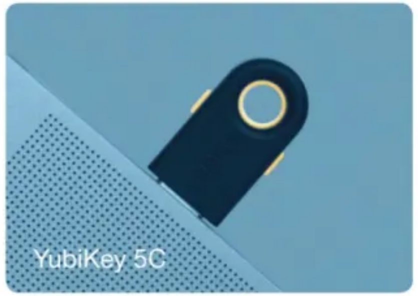
03 **SOMETHING YOU HAVE**
Device with an authenticator app, a certificate or a token.

## 4. Authenticator App or FIDO2 Key

Your employees will quickly get tired of receiving text messages with 6-digit codes. A more elegant solution is the Authenticator app that simply presents an option to Accept or Decline an access request.

Some employees may not have a smartphone or may not be able or willing to use a smartphone as a second factor. In these cases, a FIDO2 key enables the employee to log-in securely and quickly.





## 5. Conditional Access Policies

Conditional Access Policies are the brain and decision engine for a passwordless authentication solution.

You define a set of rules that enforce Multi-Factor Authentication for your business, with the assumption that anyone attempting to access your environment must have multifactor authentication (MFA) enabled.

Be deliberate in designing how you want to implement these Conditional Access policies to achieve the right **balance between security and employee experience** for your business.

## How will going passwordless benefit my business?

1. Improve security by removing the reliance on passwords

2. Lower IT support costs by eliminating password resets

3. Delight employees with a frictionless sign-in experience

"I haven't typed a password for about 18 months, and I don't miss it."

-Denis O'Shea
Founder
Mobile Mentor

## Get it right the first time

Avoid costly errors and unintended consequences by engaging an experienced partner like Mobile Mentor to deploy your passwordless authentication solution.

There are no short-cuts, and getting it right the first time will require a **5-step process:**

1. **Analysis**
2. **Design**
3. **Implement**
4. **Validate**
5. **Transfer Knowledge**

The result is an **elegant passwordless experience** that can confidently be deployed to your employees.

mobile mentor

## ABOUT MOBILE MENTOR

Mobile Mentor is a global leader in the endpoint ecosystem and Microsoft's 2021 Partner of the Year in Modern Endpoint Management.

Certified by Microsoft, Apple and Google, our engineers work tirelessly to balance endpoint security with employee experience for our clients. Check out our other whitepapers.

# ARE YOU READY TO GET STARTED?

mobile-mentor.com

| | |
|---|---|
| **United States** | +1 877 707 3848 |
| **New Zealand** | +64 9 888 0512 |
| **Australia** | +61 2 9575 4827 |