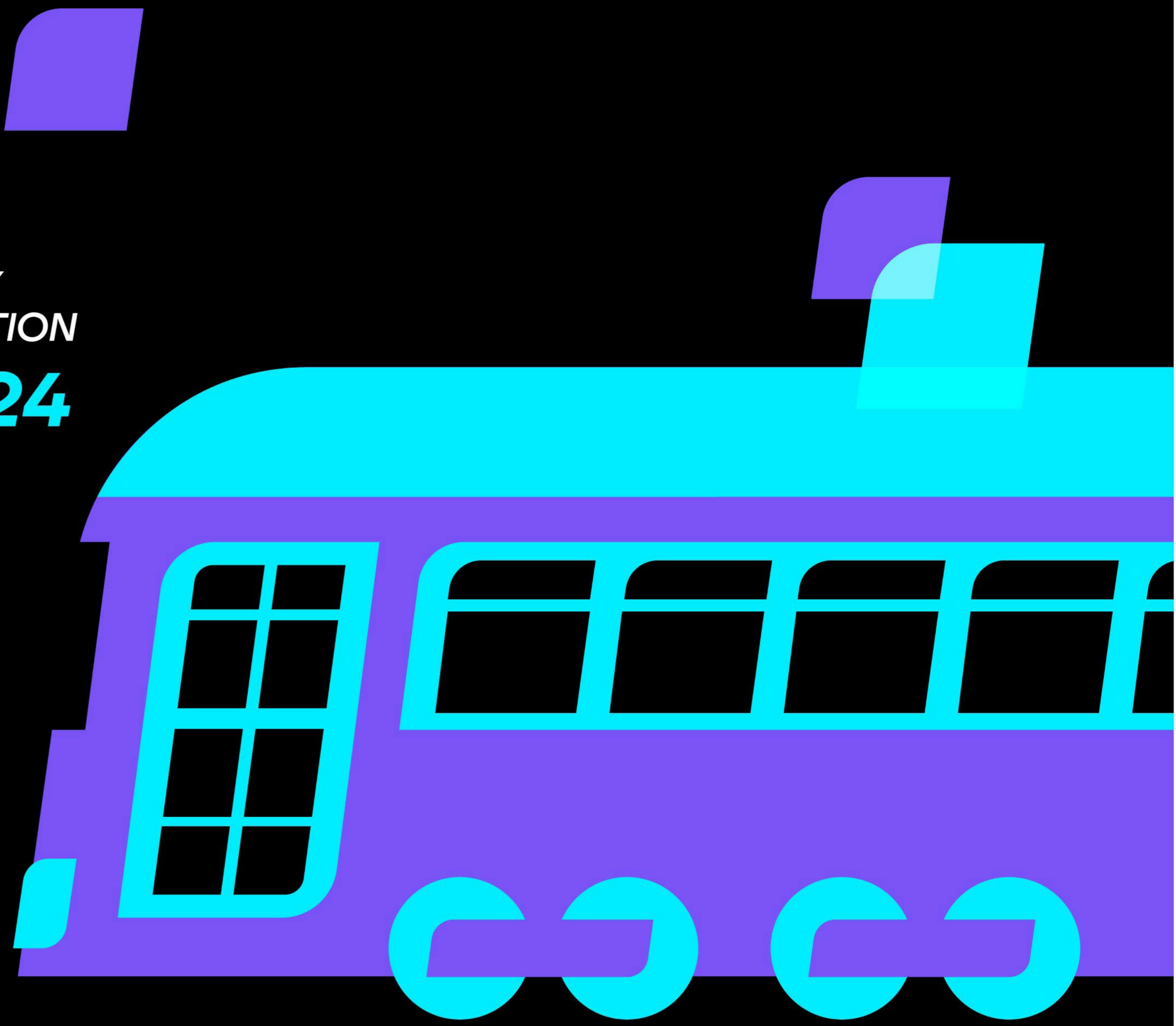




HYBRID  
IDENTITY  
PROTECTION  
**conf24**





# Making Your Passwordless Environment Fully Phishing- Resistant

**Joe Kaplan**

Identity Lead, Accenture  
Global IT

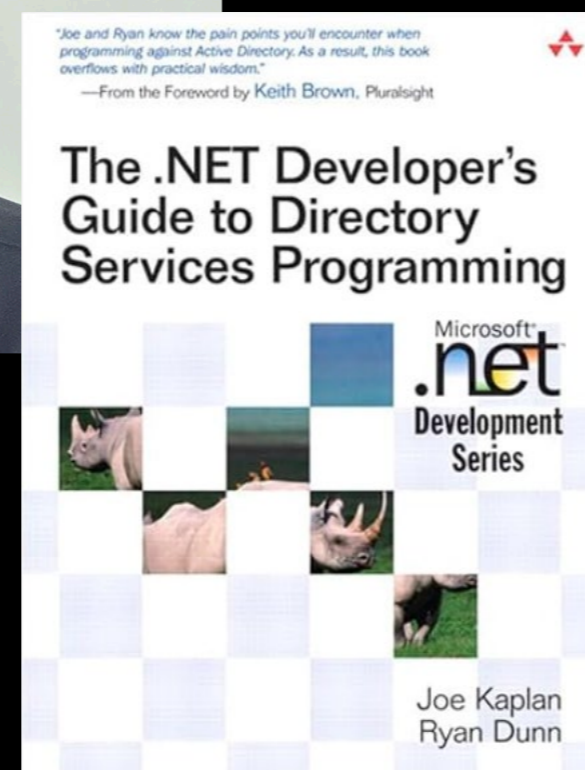




# Joe Kaplan

## Global IT Identity Lead, Accenture

Joe Kaplan is the Identity Lead in Accenture's Global IT organization. He focuses on solving real world problems for a large, complex business of over 750K employees globally. He has over 30 years of professional experience in IT, with 20+ focused on directories, identity, and cybersecurity.





# How Accenture Got to Passwordless

# Modern authentication at Accenture

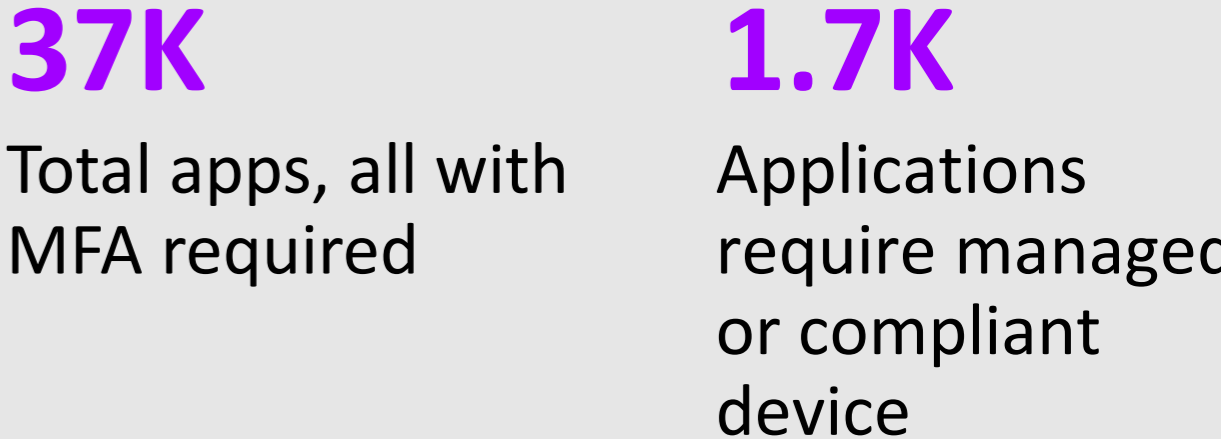
## Accenture by the numbers



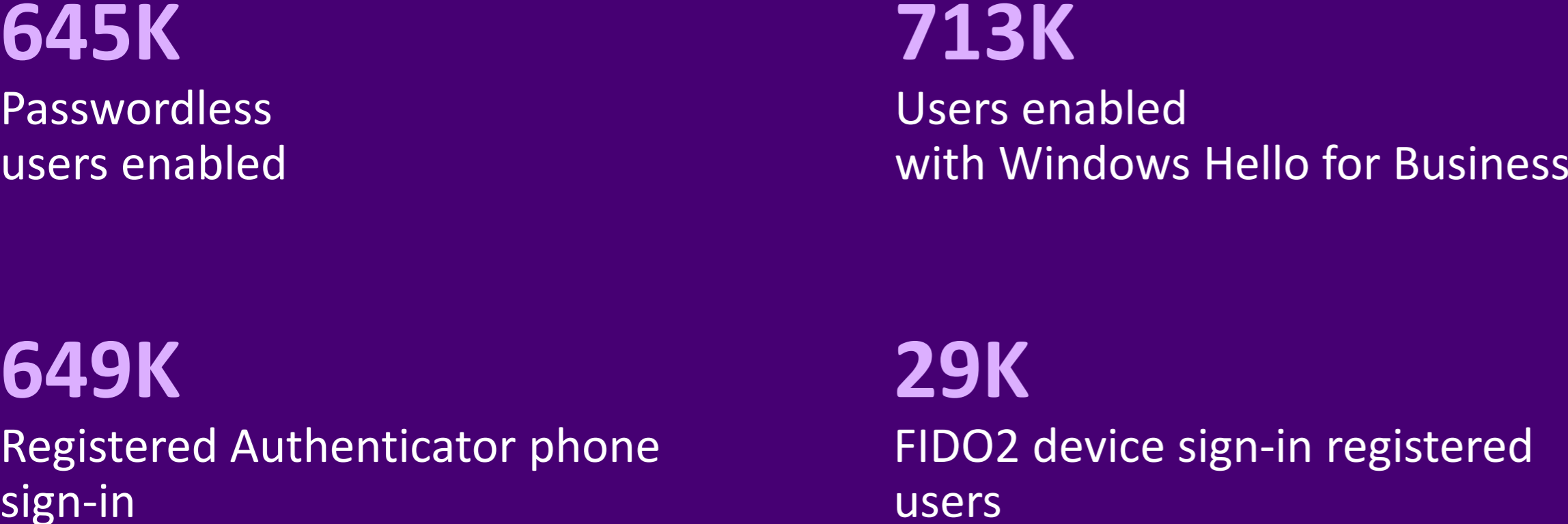
## User sign-on



## SSO Applications



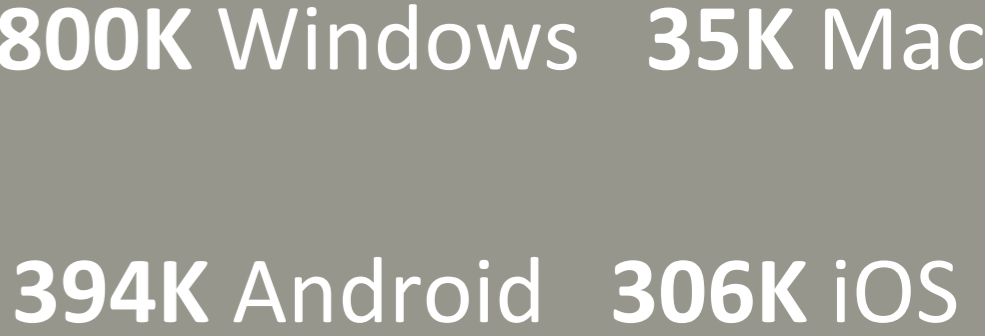
## Passwordless journey



## Entra Users



## Devices



# Our security principles

Run in  
the cloud



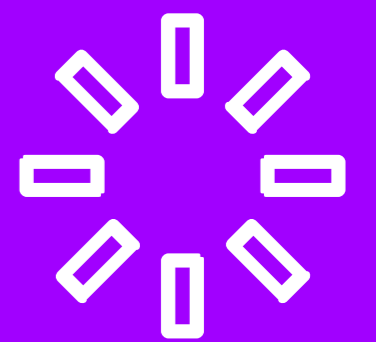
Strong  
authentication



Hardened  
attack surface



Little  
technology  
behind a VPN





# Why go Passwordless?

## Increased security



### Phishing resistance

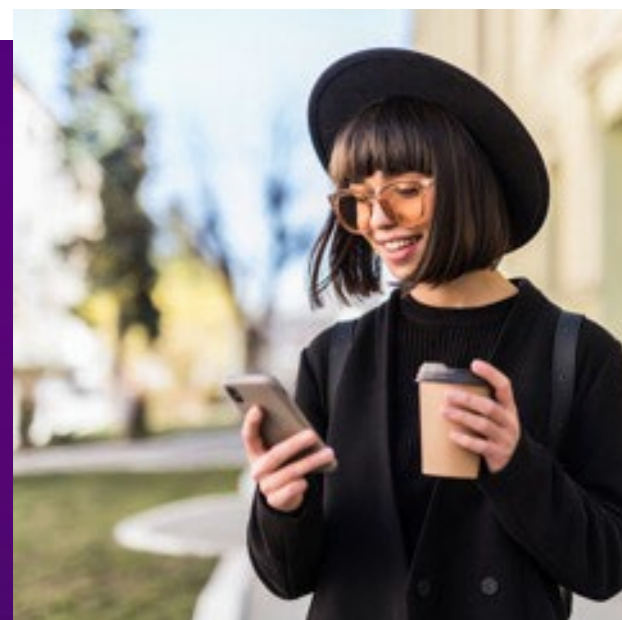
Passwordless solutions are at the device level and cannot be attacked remotely

### Dual layer of security

Hackers need the physical device **and** passwordless unlock method to gain network access

### Reduced risk

Passwords are easily comprised and at high risk of unauthorized access



## Business and user benefits

### Enhanced experience

Passwordless methods are convenient, and easy to remember

### Less maintenance

Tasks such as password resets and user lockouts are no longer needed

### Cost savings

Less IT support means reduced costs



# Our strategy

Move applications to Microsoft Entra ID as part of our cloud-first cloud-only vision

## Questions

### Device mix

- | What is our employees' device mix?
- | What devices do we need to support?

## Actions

- | Conduct compatibility checks for device hardware and software

### Applications

- | How do we migrate our applications to Entra ID and a passwordless solution?

- | Catalog all legacy apps and confirm compatibility to passwordless solutions and Entra ID

### Entra ID

- | How do we migrate our identity infrastructure?
- | How do we support our users' move to passwordless?

- | Redefine app onboarding processes
- | Outline updated reporting needs
- | Define analytics capabilities

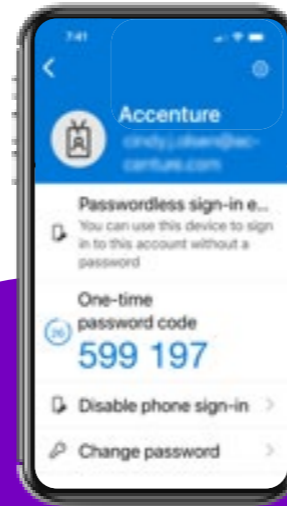




# Device mix: Authentication for all

## Microsoft Windows Hello for Business

Replaces passwords with strong two-factor authentication on all Windows workstations deployed by Accenture. Users of these devices can enroll in passwordless and start authenticating to their device and applications with a PIN or biometrics.



## Microsoft Authenticator w/ Phone Sign In

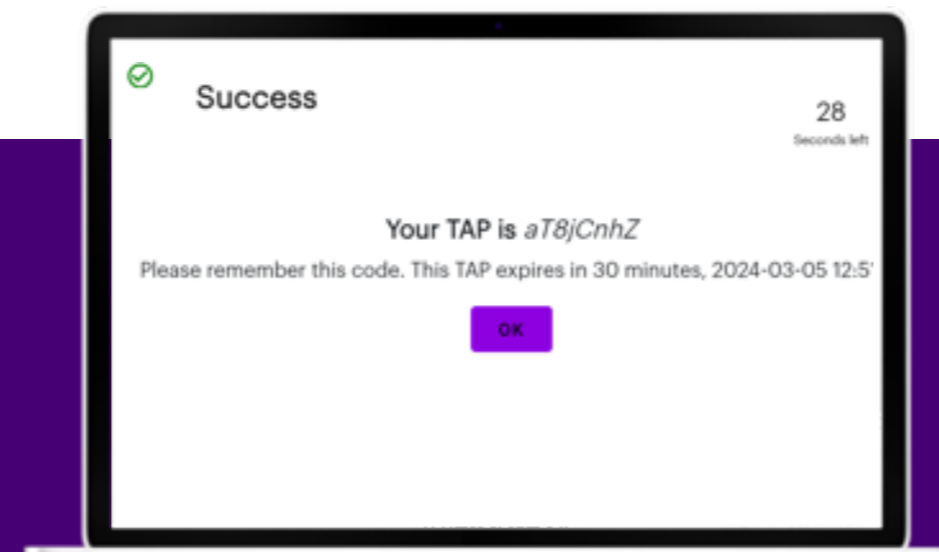
Enables our people to use their phones to complete two-factor authentication. By completing a number match, users can authenticate to any application on multiple devices.

## FIDO2 token

Limited set of users on as-needed basis  
A separate physical device that typically resembles a familiar USB thumb drive. The tokens can be used to complete device and application sign-in on any Accenture workstation.



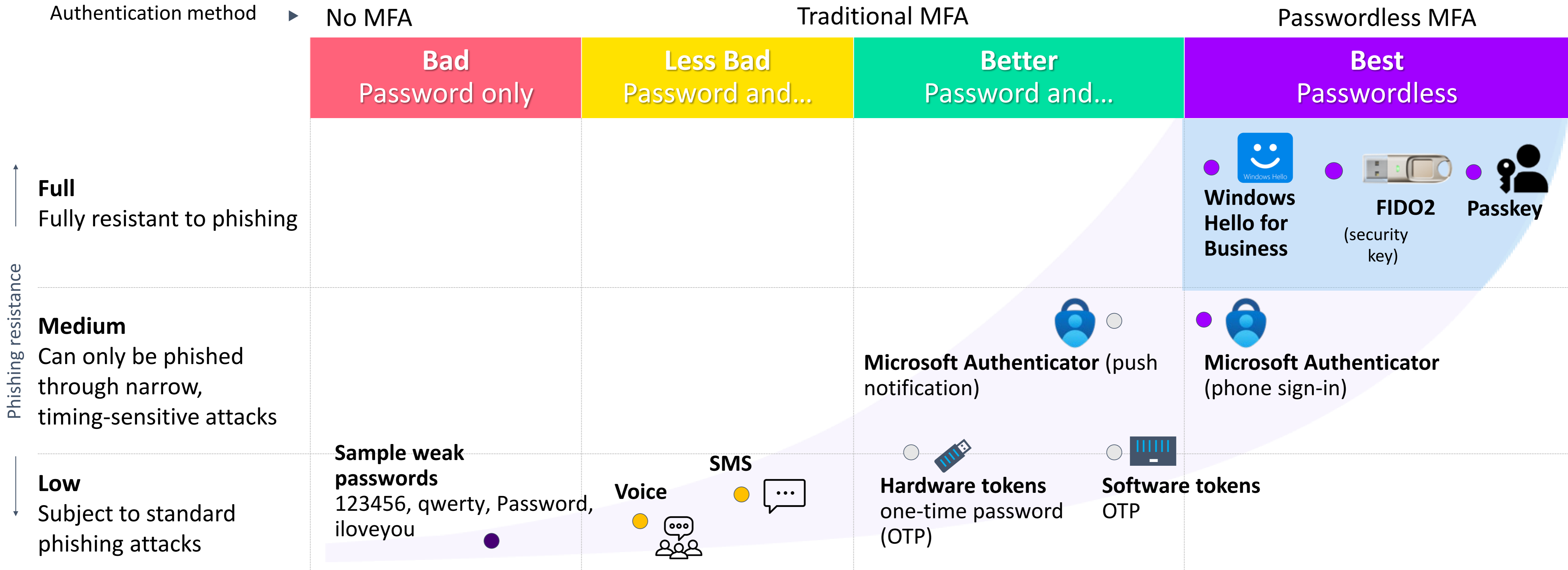
## All users for bootstrapping Temporary Access Pass (TAP)



A time-limited passcode given to verified users so they can register passwordless methods and recover access to their account without the need for a password.



# Authentication vision: Passwordless, fully phishing-resistant credentials






# From Passwordless to Full Phishing- Resistance

# Three Big Goals

Deploy passkeys  
and use them to  
replace Authenticator  
Phone Sign-In



Deploy Mac Platform  
SSO and bring Mac  
up to par with  
Windows



Close gap of  
remaining 20% of  
users who are not  
fully Passwordless to  
< 5% of total





# Replacing Phone Sign-in with Passkeys

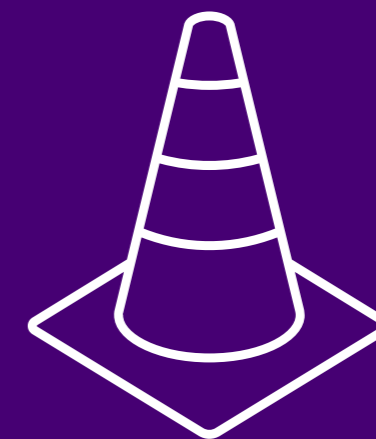
## The plan

- Roll out device-bound passkeys with Microsoft Authenticator to all users currently enrolled with phone sign-in
- Eventually remove the ability to use phone sign in and disable ability to enroll



## Key challenges

- 150K Android users below version 14
- Lots of change management to drive adoption
- New technology
- Not totally clear how we'll roll back our deployment of phone sign in



# Deploying Mac Platform SSO

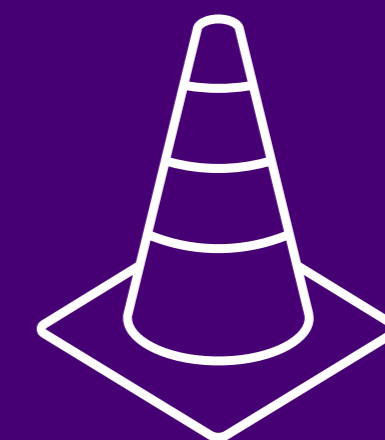
## The plan

- Enable Mac Platform SSO for Entra using the Secure Enclave model
- Deploy to all current MacOS users



## Key challenges

- Mostly change management: not clear if there is a way to do this without substantial end user action that requires significant hand-holding
- Need analytics to measure progress

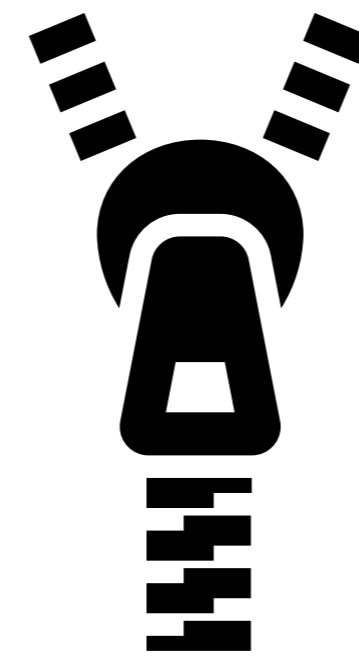




# Closing the Passwordless Gap

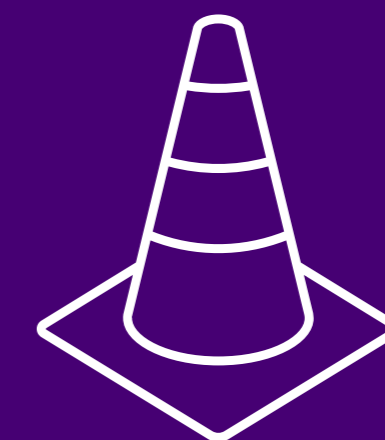
## The plan

- Tighten our eligibility criteria for password removal
- Tackle a few remaining legacy authentications
- Incremental progress for privileged admin accounts



## Key challenges

- May need to provide more hardware-based passkeys (FIDO2 tokens)
- May need to enable more users with certificates for RDP
- Difficult to eliminate passwords in all IT admin use cases

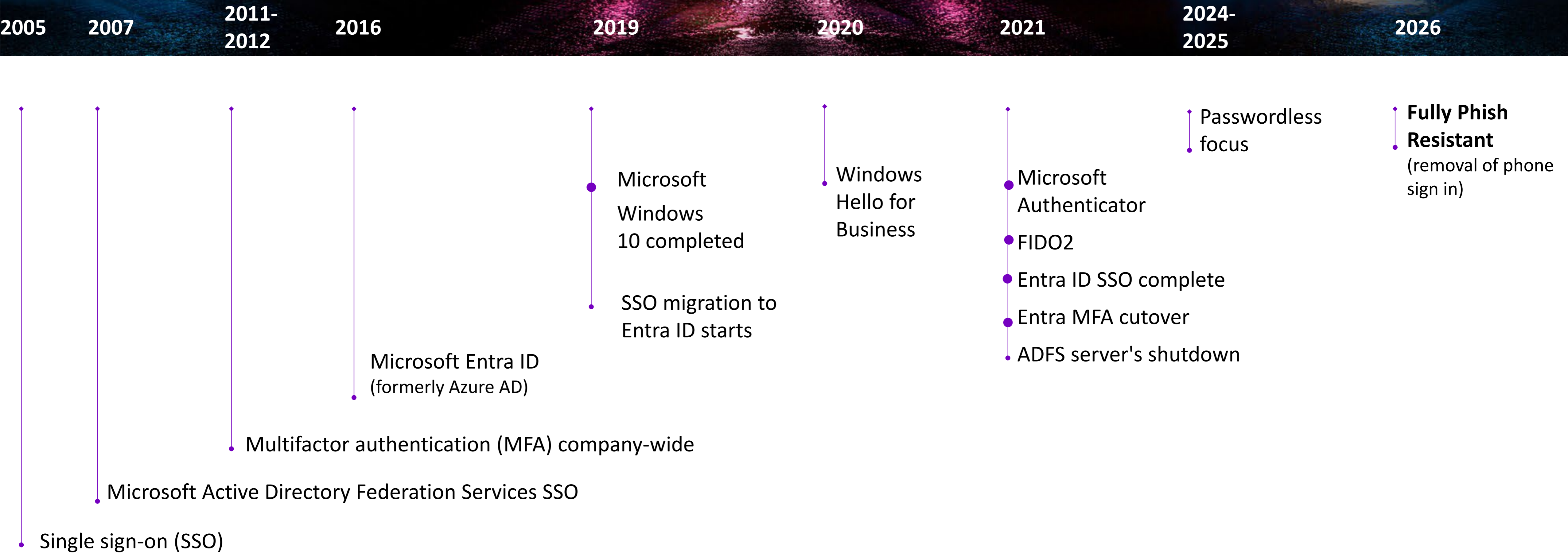


*Questions?*

# Appendix



# Accenture's multi-year authentication journey





# Learnings from the transition go beyond the technology

## Device considerations

Passwordless methods differ for Mac v. Windows and iOS v. Android devices.

Verification of compatibility for each solution takes time but is essential for a good user experience.

## Application readiness

Will require rigorous effort without a single source of truth and legacy apps may not be compatible, requiring a focused remediation strategy.

## Ecosystem efforts

Identify the ecosystem and any other large changes, technical or organizational. Where possible, combine messaging and end-user actions to reduce confusion.

## Local engagement

Involve local geography leadership teams to understand local needs and partner on a successful implementation.

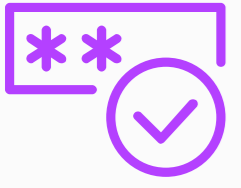
Consider local laws and customs.

## Change management

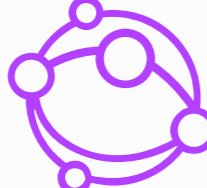
A core component of a large-scale Passwordless deployment and should not be underestimated. The focus will shift from technical enablement to a human-focused behavioral change, encompassing communications, end-user support, and having an impact on every team across the organization.



# How Accenture makes a user passwordless



Users with two or more passwordless authentication methods are targeted for password removal.



The user's password is replaced by a long, randomized string. This often includes non-typeable characters.



The account option "Smart card is required for interactive logon" is enabled on the user's on-premise Active Directory account.



This data is synchronized to Entra ID. Users no longer know their password and will not be asked to enter it anywhere.



User no longer needs, has or can use a password!



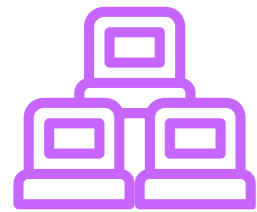


# Application transition example challenges

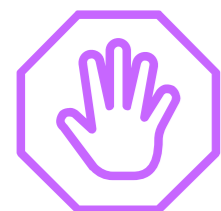


## Applications that couldn't move

Some legacy business applications  
Certain infrastructure apps



## First-time hybrid workstation log-ins



## Use cases that will never be passwordless

- Legacy non-interactive log-ins
- Secondary directories
- Some IT admin

## Example: An application that didn't work and what we did

- SQL Server Reporting Services (SSRS), an important reporting platform for Accenture, with 30K users
  - Reconfigured at the application side
  - Used a different SSO integration method using Azure App Proxy and Kerberos Constrained Delegation





# Tooling takeaways

## Custom tooling

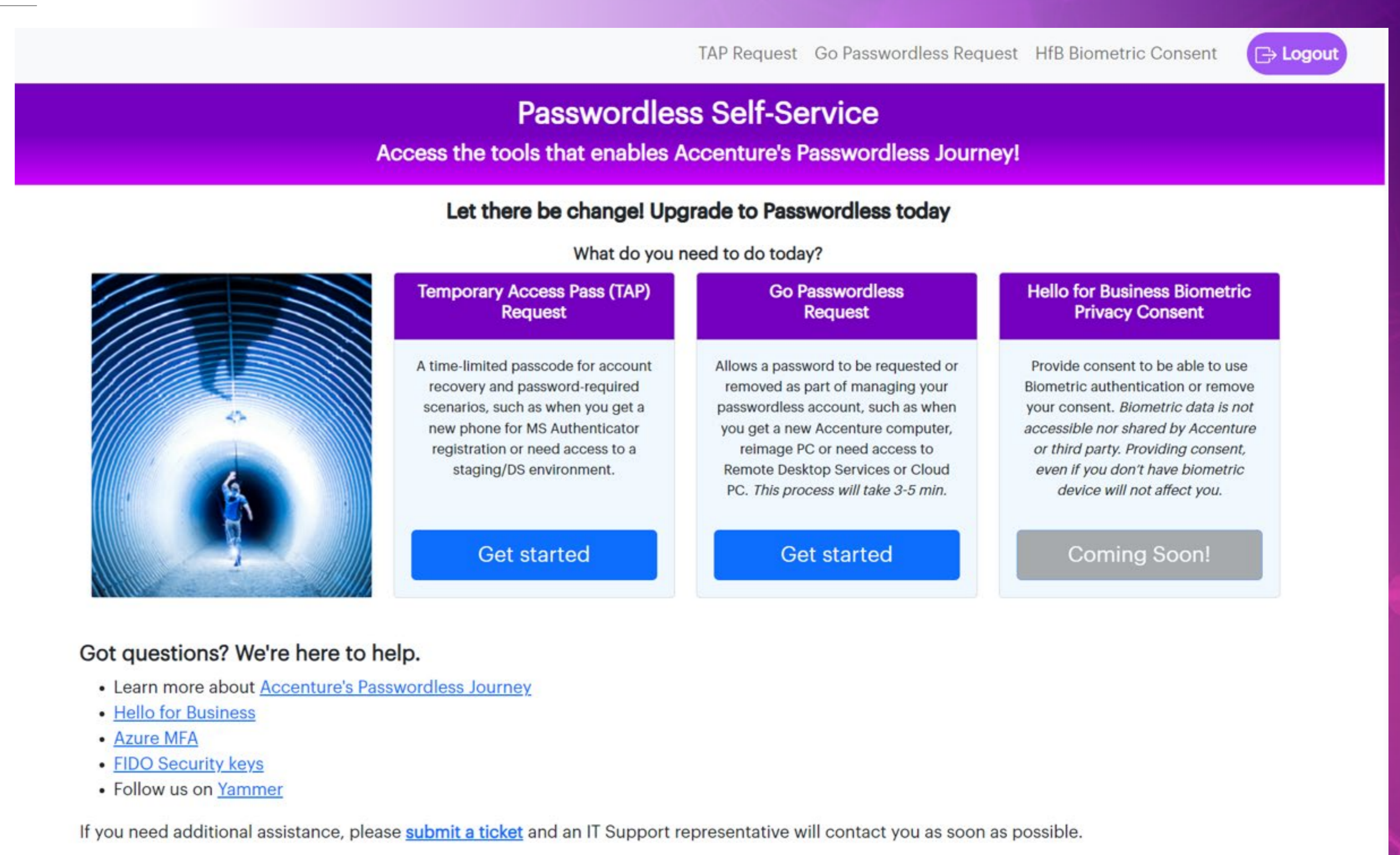
Enabled a self-service passwordless journey for Accenture people

## Our analytics dashboard

Steered the ship, and was the centerpiece of our change effort

## It takes substantial effort

To develop tools and processes to drive and maintain enrollment



The screenshot shows a web portal for 'Passwordless Self-Service'. At the top, there are navigation links for 'TAP Request', 'Go Passwordless Request', and 'HfB Biometric Consent', along with a 'Logout' button. The main heading is 'Passwordless Self-Service' with the sub-heading 'Access the tools that enables Accenture's Passwordless Journey!'. Below this, a call to action reads 'Let there be change! Upgrade to Passwordless today'. A question 'What do you need to do today?' is followed by three service cards: 'Temporary Access Pass (TAP) Request', 'Go Passwordless Request', and 'Hello for Business Biometric Privacy Consent'. Each card has a 'Get started' button, except for the last one which says 'Coming Soon!'. To the left of the cards is an image of a person in a blue shirt standing in a futuristic, glowing tunnel. Below the cards, there is a 'Got questions? We're here to help.' section with a list of links: 'Accenture's Passwordless Journey', 'Hello for Business', 'Azure MFA', 'FIDO Security keys', and 'Yammer'. At the bottom, a note says 'If you need additional assistance, please submit a ticket and an IT Support representative will contact you as soon as possible.'





# Tooling takeaways

## Custom tooling

Enabled a self-service passwordless journey for Accenture people

## Our analytics dashboard

Steered the ship, and was the centerpiece of our change effort

## It takes substantial effort

To develop tools and processes to drive and maintain enrollment

