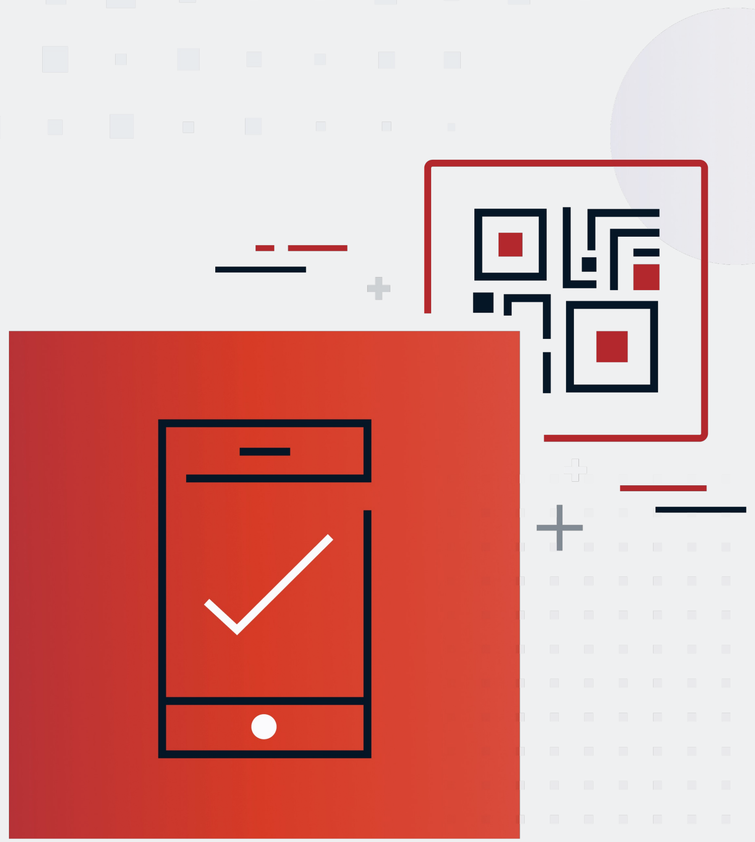
Journey to Passwordless



What Is Passwordless?

Objective

- **Features that reduce or eliminate the need for passwords**
- **Balance security and experience through risk management**

Typical Steps

First reduce footprint

SSO & MFA
Authentication Authority
Standards
Risk Signals

Then eliminate altogether

1st factor FIDO
Continuous AuthN
Zero Login

Eliminate The Weakest Authentication Factor

Authentication Factors	Example
Something You **Know**	**Password, PINs, KBAs**
Something You **Have**	**Smartphone, Device Key**
Something You **Are**	**Biometrics**
Something You **Do – Where/How**	**Location/Time**
Something You **Do - How**	**Behavior**

Eliminate The Weakest Authentication Factor

Authentication Factors	Example
Something You **Know**	**Password, PINs, KBAs** — **Eliminate**
Something You **Have**	**Smartphone, Device Key** — **Increase adoption here**
Something You **Are**	**Biometrics** — **Increase adoption here**
Something You **Do – Where/How**	**Location/Time** — **Increase adoption here**
Something You **Do - How**	**Behavior** — **Increase adoption here**

Passwordless Value

Customers

Reduce Customer Churn

Utilize Biometric Methods Familiar To Customers

Eliminate Password Replay Risk

User Experience

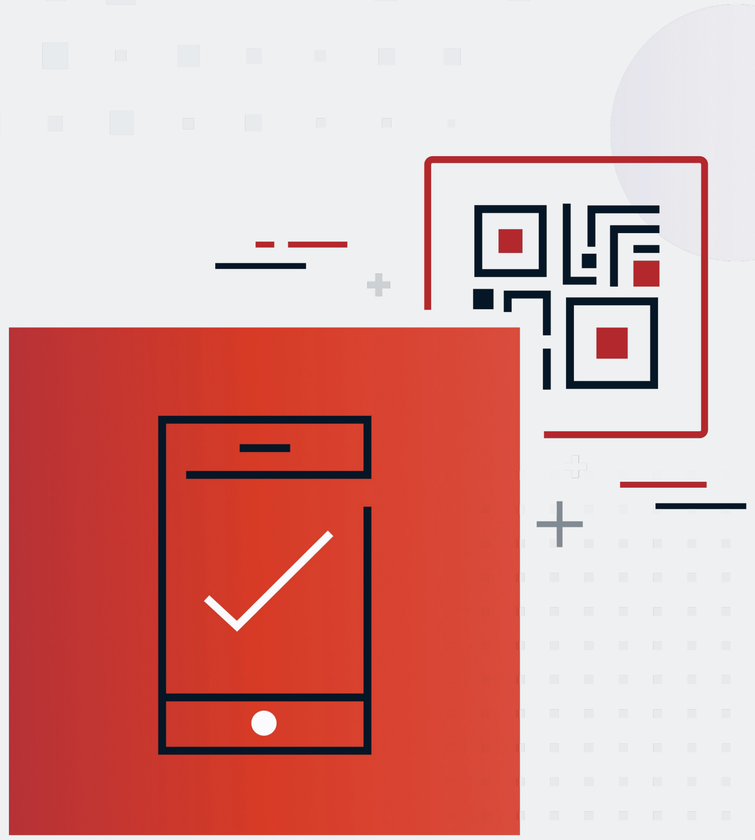
Employees

Increase Productivity & Cost Savings

Enhance Security & Phishing Protection (FIDO)

Reduce Data Breach Risk

Phased Approach to Passwordless



Passwordless Journey

Centralized Authentication

Phase Out Passwords

FIDO

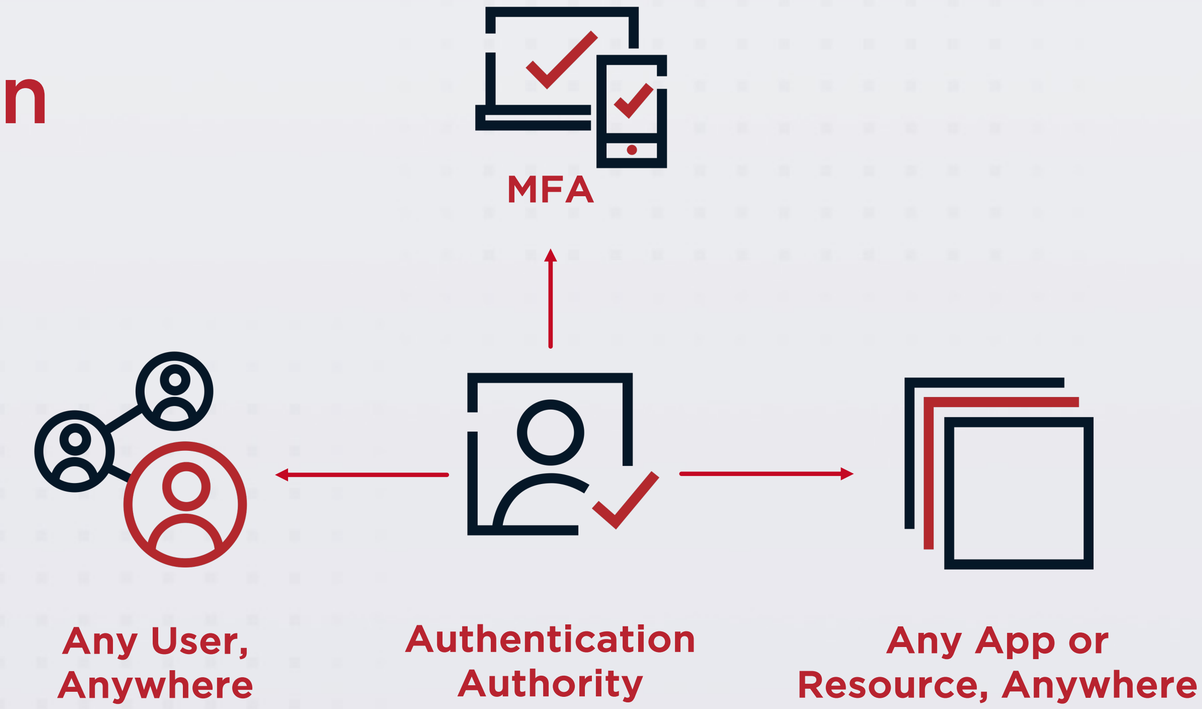
Zero Login
(True Passwordless)

Better Security & User Experience

Step #1
Centralized Authentication

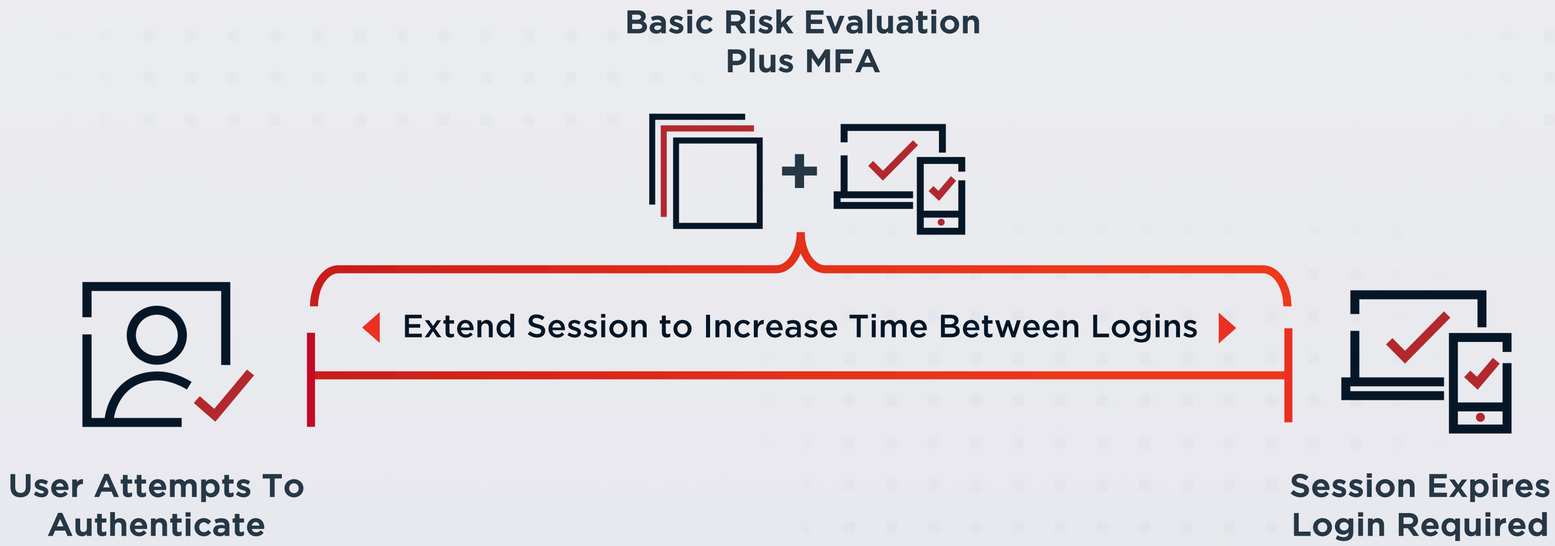
Goals

- Centralize SSO & MFA on an Authentication Authority Foundation
- Add Risk-Based MFA



Extended Session

This scenario centralizes and extends user sessions across all applications, reduces friction for users in between MFA prompts, while also significantly limiting risk.



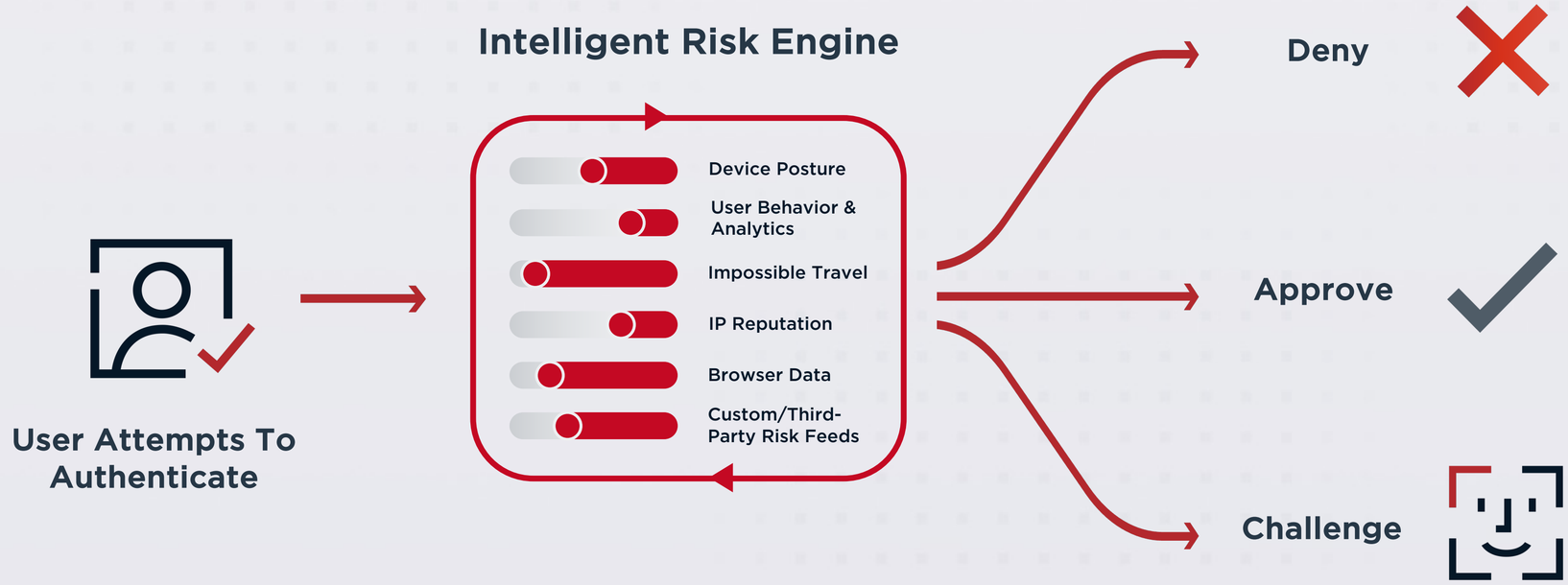
Results

- Require only MFA (no passwords) during extended sections
- Provide users with less friction-filled experiences
- Limit risk

Required Capabilities: SSO + MFA

Policy-Based Authentication with Risk Signals:

This scenario layers on risk signals to establish baselines of normal user behavior so that users are only prompted for MFA when there is elevated risk offer an even more frictionless experience without compromising security.



Results

- Risk signals run invisibly in the background to continuously authenticate users' sessions
- Baselines of normal user behavior are established
- Users experience even less friction via fewer MFA prompts

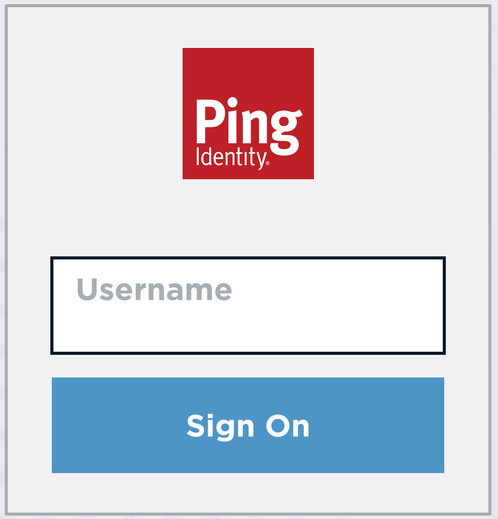
Required Capabilities: SSO + MFA + Risk + Orchestration

Step #2
Phase out Passwords

Goals

- Replace Passwords with More Robust and Convenient Methods
- All Logins Are Passwordless After Initial Registration

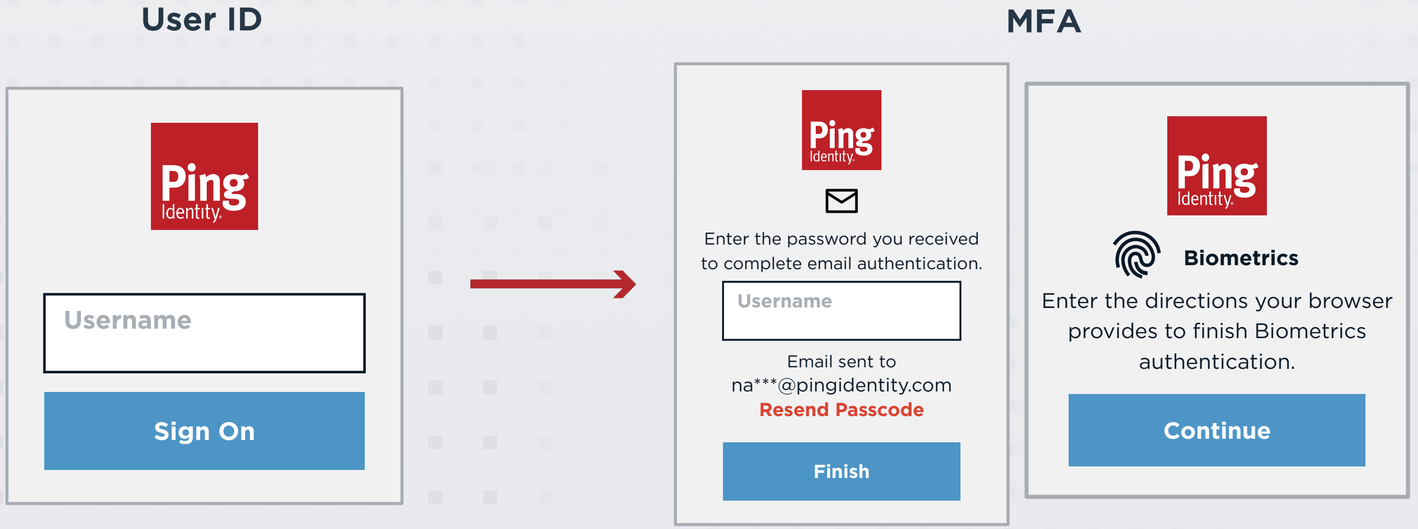
Login With User ID



Password Replaced With...

User ID + MFA

Users fill out a user ID form without entering a password and are then prompted with an additional authentication factor such as an OTP, biometric scan, or push notification.



Eliminate the weakest factor (passwords)

Boost security by replacing something you know with something you have

Results

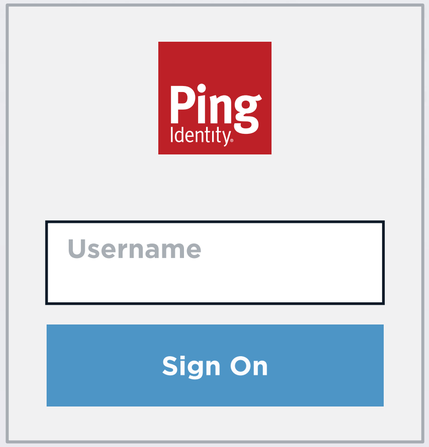
- All logins are passwordless after initial registration
- Passwords with more convenient and robust authentication factors to improve security
- Even less-friction-filled experience (compared to prior scenarios)

Required Capabilities: SSO + MFA

Email Magic Link

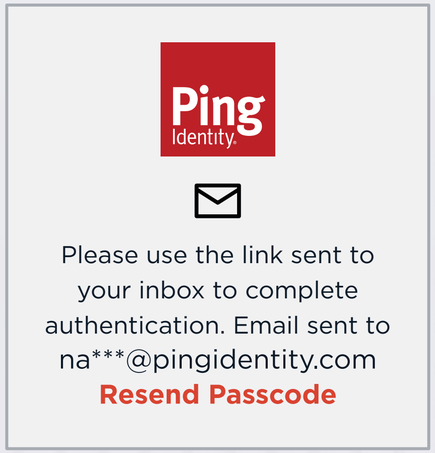
Users fill out a user ID form and then receive an email with a link to the resource they want to access.

User ID



Eliminate the weakest factor (passwords)

Unique link sent to email



Clicking the email link completes the authentication flow

Results

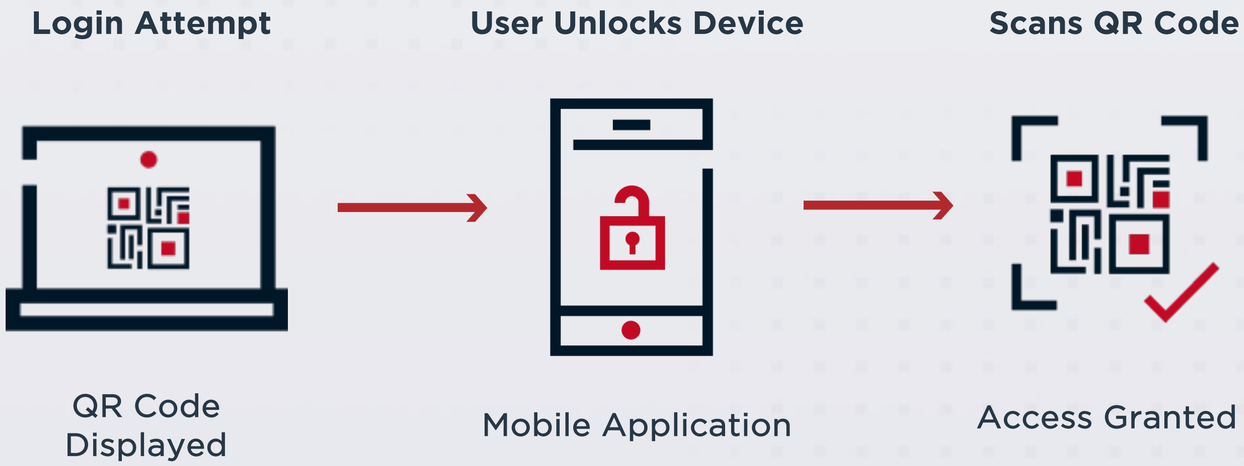
- All logins are Passwordless after initial registration
- Passwords with more convenient and robust authentication factors to improve security
- Authentication via email provides a great CIAM user experience

Required Capabilities: SSO + Orchestration

Customer use cases only

QR Code (Application-Based)

Application-based QR codes enable users to leverage their mobile devices as authenticators with minimal friction. Users can access customer applications on new devices by scanning QR codes directly from within the same providers' applications that they are already logged into on their smartphones.



Results

- Fast, frictionless, usernameless, and passwordless authentication across devices
- Users can leverage their mobile devices as authenticators with minimal friction
- Great CIAM user experience

Required Capabilities: SSO + MFA + Mobile SDK

Customer use cases only

QR Code (App-Less)

Similar experience to application-based QR codes, but without requiring users to have a specific application installed on their phone. Users scan a QR code from an application on a smart device directly from their phone's camera and are instantly logged in on their phone's browser.

Results

- Fast, frictionless, usernameless and passwordless authentication across devices (after initial registration)
- Users can leverage devices such as smart TVs, tablets, and phones as authenticators
- Great CIAM user experience

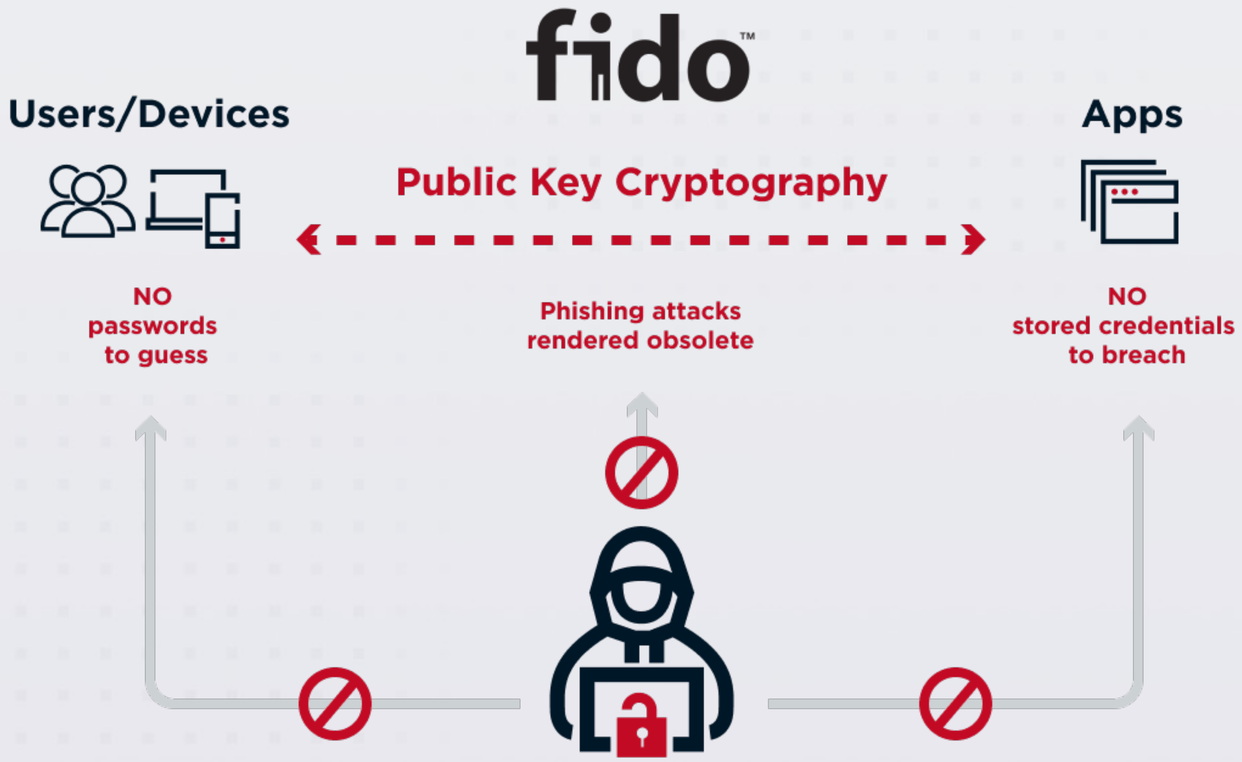
Required Capabilities: SSO + MFA + Orchestration

Customer use cases only

Step #3
Embrace FIDO

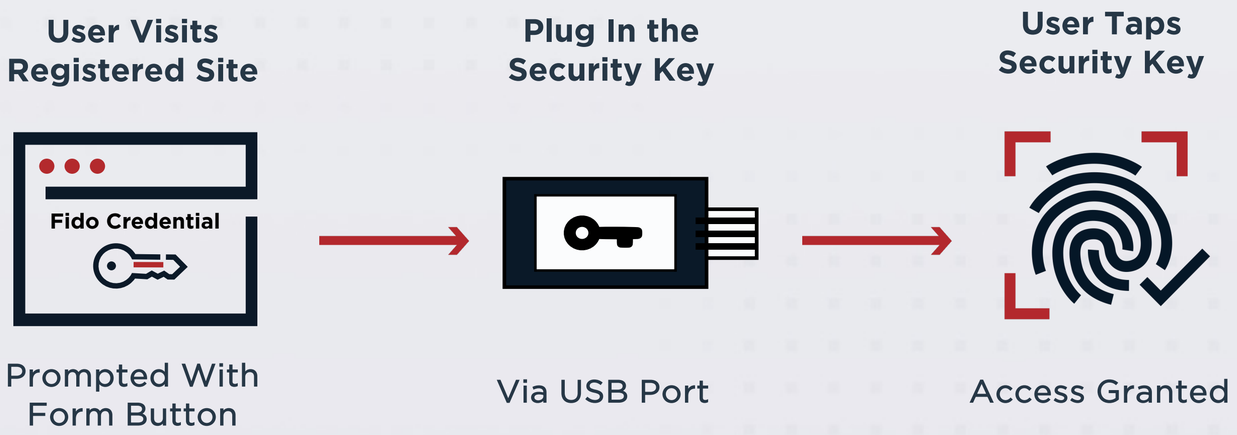
Goals

- **Even Better Security Through Fido And Public Key Cryptography**
- **Biometric Data Resides On Device**
- **Phishing Attacks Attacks Are Rendered Obsolete**



FIDO Security Key

Also referred to as cross-platform authenticators, FIDO security keys are external hardware devices that plug into users' devices via USB. Upon visiting a registered site users can plug their security key into their device and tap it to complete authentication.



Results

- Quick, frictionless authentication; users connect a physical key to a device and login with a tap
- Even better security through public key cryptography
- Private keys and biometric data are stored locally and never leave the device
- Completely removes any risk of phishing attacks

Required Capabilities: SSO + MFA + FIDO Security Key

FIDO Device (Platform)

Platform authenticators contain an embedded cryptographic key tied to a single user device. Users attempting to gain access to the device, registered applications, or sites on that device are prompted with a biometric factor (fingerprint or facial scan) to complete authentication.

User Attempts To Access Device, Registered Applications, or Sites

Biometric Factor

Common Compatible Platform Authenticators

Embedded Cryptographic Key

Completes Authentication

Windows Hello, Apple FaceID, and Android

Results

- Quick, frictionless authentication; users can login to a device or registered applications via biometrics
- Even better security through public key cryptography
- Users' private keys and biometric data are stored locally and never leaves their device
- Completely removes any risk of phishing and replay attacks

Required Capabilities: SSO + MFA + FIDO Device

Step #4
Zero Login

Goals

- **Eliminate Passwords With ID Verification At Account Creation**
- **No Longer Need Usernames Or Passwords**

Initial Verification

Live Selfie

Gov’t ID

Future Authentication with Risk Scoring

Device

Biometrics

Risk Scoring

Zero Login

Users no longer ever need to use passwords or usernames to complete the initial registration process or for future logins through a combination of the above passwordless options and continuous authentication via risk signals.

Initial Verification

Live Selfie

Gov't ID

Eliminate Passwords with ID Verification at Account Creation

Future Authentication with Risk Scoring

Device

Biometrics

Risk Scoring

No Longer Need Usernames or Passwords

Required Capabilities: **SSO + MFA + Risk + ID Verification + Orchestration**

Results

- No usernames or passwords ever exist
- Registration is usernameless and passwordless; Account creation via biometrics and ID verification
- Users can login via a their trusted device and a passwordless medium (like a QR code or a biometric)
- Risk signals further optimize both security and user experience

Summary

Reduce > Eliminate

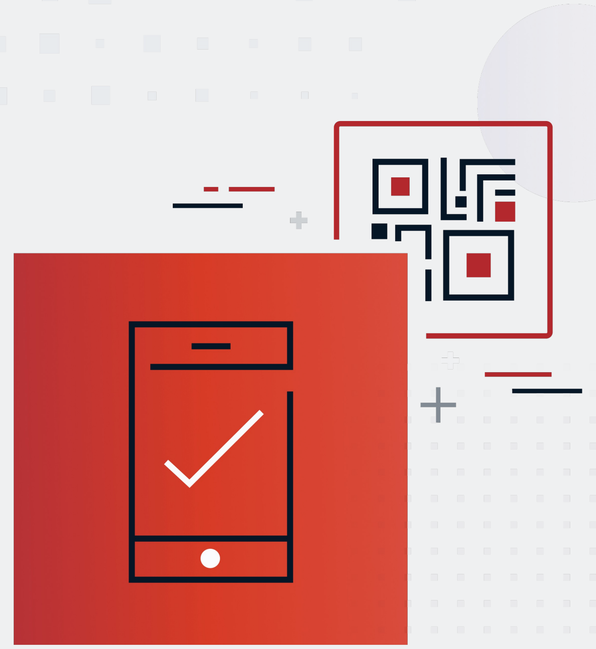
First, limit your passwordless footprint, then work towards eliminating them altogether.

No “One-Size-Fits-All” Approach

Each organization has unique technology investments and user scenarios.

True Partnership is Scalable

Identify a partner that can help you get to a passwordless future for all apps and authentication use cases.



Questions?

Thank You

PingIdentity®