RONNY DE JONG

PRINCIPAL CONSULTANT & MICROSOFT MVP

INSPARK

@RONNYDEJONG

Going Password-less in 60 minutes!

Sensitivity: Regular

Out with the old…

Passwords or watchwords have been used since ancient times by Roman military

…in with the new.

Passwords are considered as a relic of the past.

“they just don't meet the challenge for anything you really want to secure.“

Bill Gates, 2004

Why eliminate passwords

Helpdesk costs
Operational costs

Increasing costs
of a breach

Omnipresence
Social media makes passwords easier to guess

Password reuse
Multitude of passwords
Error prone on mobile
Hard to remember

Source: https://www.telesign.com/resource/infographics/future-account-security-report-infographic/

Sensitivity: Regular

Strong authentication comes with…

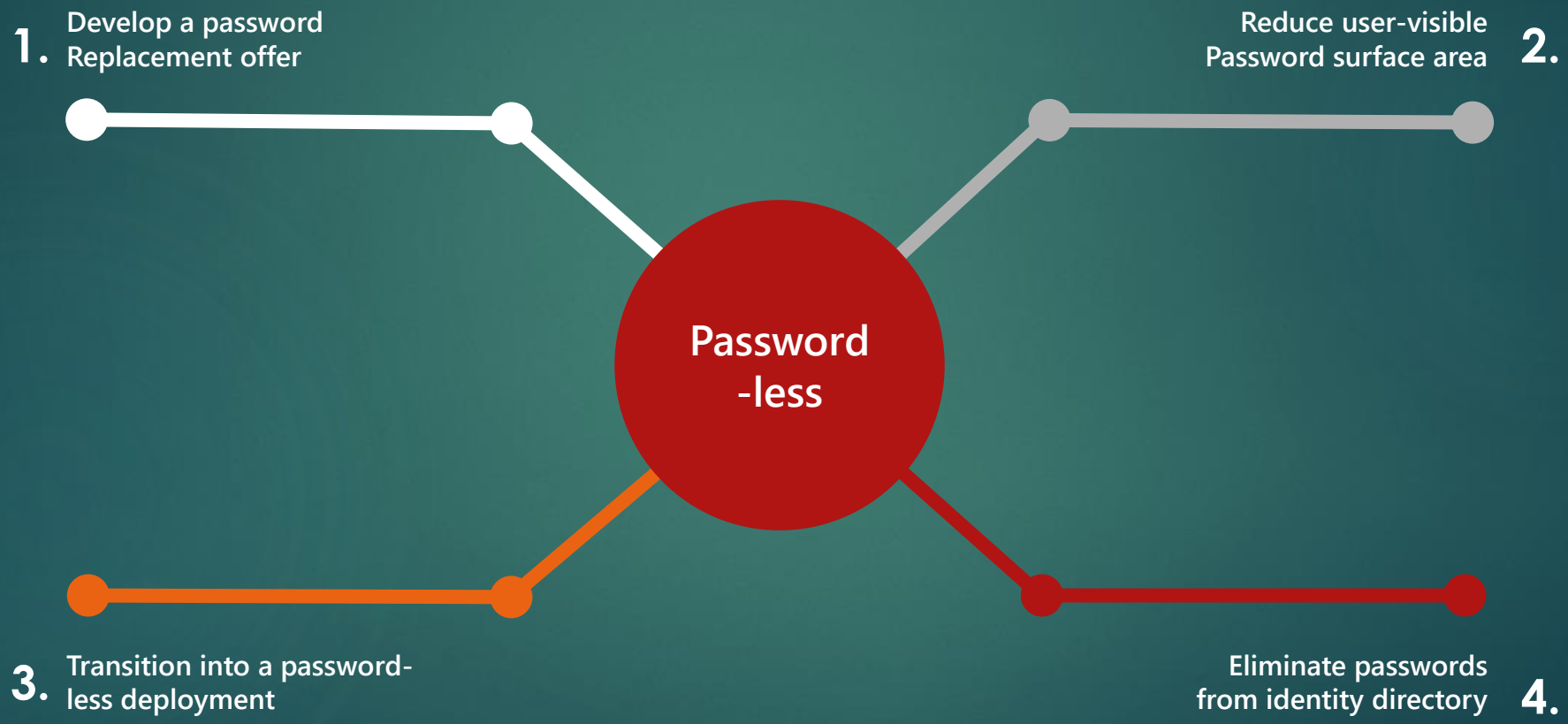
Scytale

https://en.wikipedia.org/wiki/Scytale

Clicker

https://en.wikipedia.org/wiki/Clicker

Four steps to Password-less



Sensitivity: Regular

There must be a better way

Passwords + standard 2FA

High Security

Inconvenient

Convenient

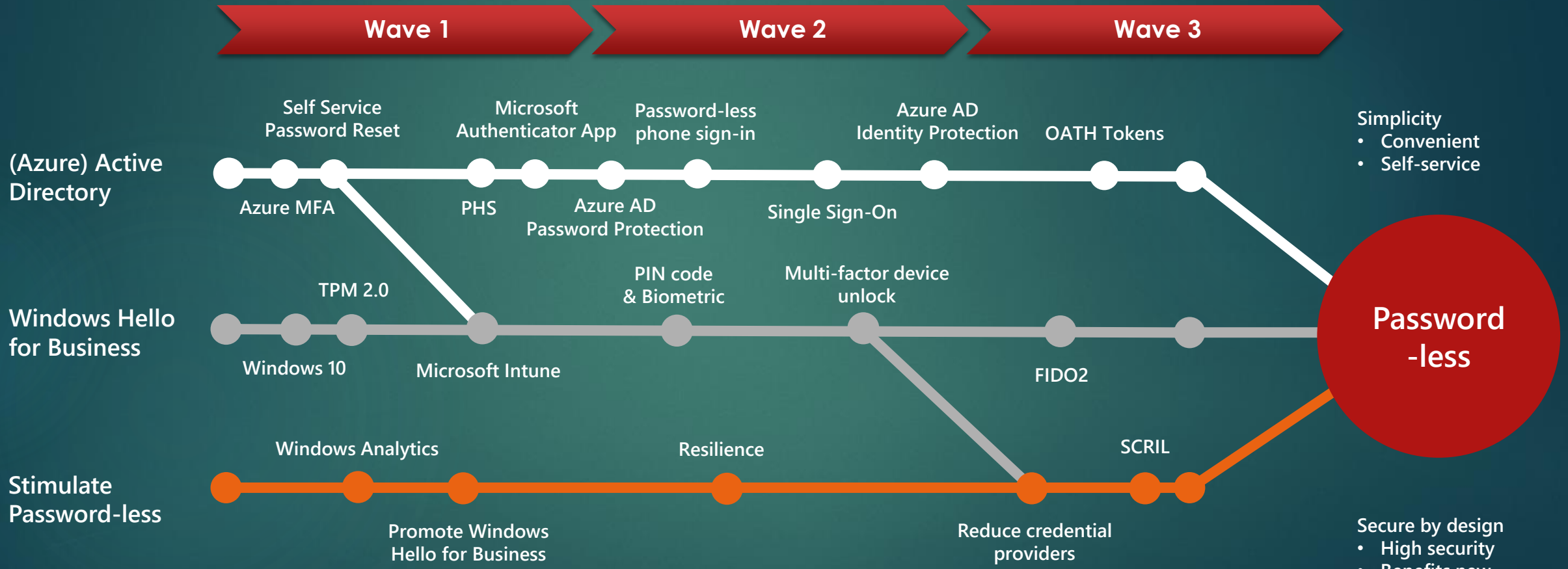
Low Security

?

Passwords

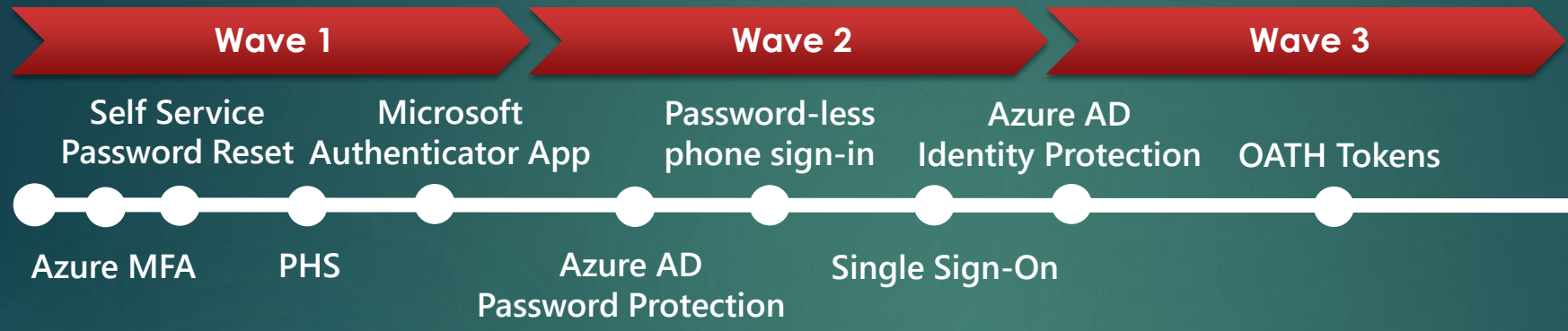
Sensitivity: Regular

Password-less strategy



Sensitivity: Regular

(Azure) Active Directory



- **Scenarios enabled in (Azure) Active Directory:**
  - Make sure you've enabled MFA!
  - Enable Self-Service capabilities
  - Start hardening your current password surface area

- **Impact and timing of transition:**
  - Wave 1: Building up
  - Wave 2: Expand capabilities
  - Wave 3: Unlock new scenarios

Sensitivity: Regular

Secure Authentication Flow

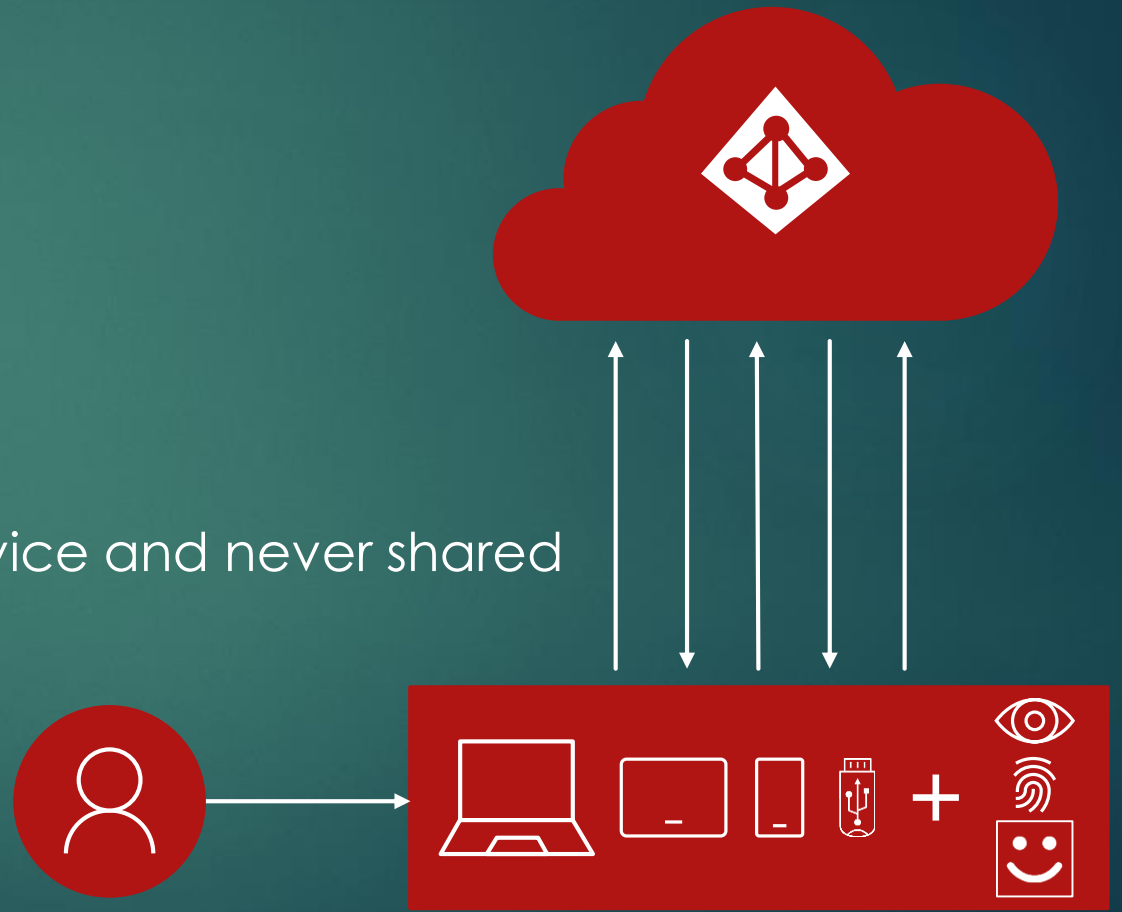
A simple, common architecture

Based on public-key technology

Private-keys are securely stored on the device

Requires a local gesture (e.g., biometric, PIN)

Private-keys are bound to a single device and never shared



Sensitivity: Regular

Password-less phone sign-in with Microsoft Authenticator app

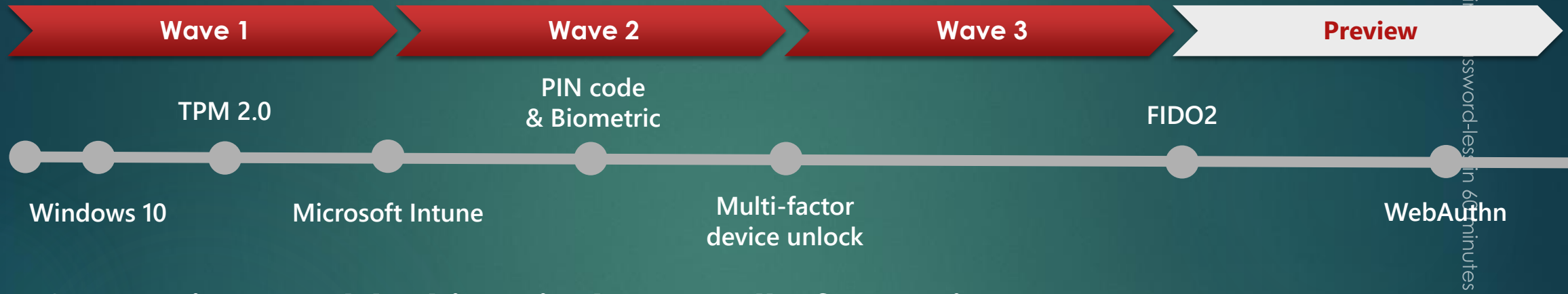
```
New-AzureADPolicy -Type AuthenticatorAppSignInPolicy -
Definition
'{"AuthenticatorAppSignInPolicy":{"Enabled":true}}
' -isOrganizationDefault $true -DisplayName
AuthenticatorAppSignIn
```


Sensitivity: Regular

Demo #1

PHONE SIGN-IN WITH MICROSOFT AUTHENTICATOR & WINDOWS HELLO FOR BUSINESS WEBAUTHN

Windows Hello for Business



- **Scenarios enabled in Windows Hello for Business:**
  - Windows 10 built-in security, not bolt-on
  - Set & deploy your security controls
  - Cloud scale protection

- **Impact and timing of transition:**
  - Wave 1: Building up
  - Wave 2: Expand capabilities, extensive testing, target to personas
  - Wave 3: Unlock new scenarios, raising the bar of convenient & security

Sensitivity: Regular

Demo #2

FIDO2 WITH AZURE AD ACCOUNT & WEBAUTHN

Adopt Password-less

- **Scenarios enabled for Adoption:**
  - Get insights with Windows Analytics
  - Stimulate Windows Hello for Business
  - Reduce Password surface area

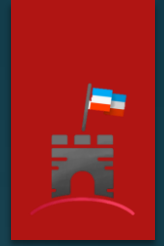
- **Impact & timing of transition:**
  - Wave 1: Building up
  - Wave 2: Expand capabilities (Adoption of password-less)
  - Wave 3: Eliminate the use of passwords (Reduce password surface area)

Sensitivity: Regular

Demo #3

THE ULTIMATE PASSWORD-LESS EXPERIENCE

Reality check…



01

Cloud only provides best experience

02

Windows Hello for Business coexistence scenarios requires:

- Additional planning
- Additional infrastructure footprint

03

Hybrid is more complex, remains sub-optimal

Summary

Going password-less is a long-term approach for secure authentication, and it's still evolving. It can take time to transition.

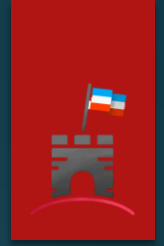
Start with a pilot of one or more options. For users that can't go password-less, turn on MFA to validate users and minimize prompts based on the risk of the sign-in with conditional access capabilities.

Use password filter to block leaked credentials and common passwords from being used with password protection policies.

Microsoft whitepaper Password-less Protection

https://www.microsoft.com/en-us/cloud-platform/passwordless

Sensitivity: Regular



Thank you

RONNY DE JONG
PRINCIPAL CONSULTANT
INSPARK

@RONNYDEJONG

Sensitivity: Regular