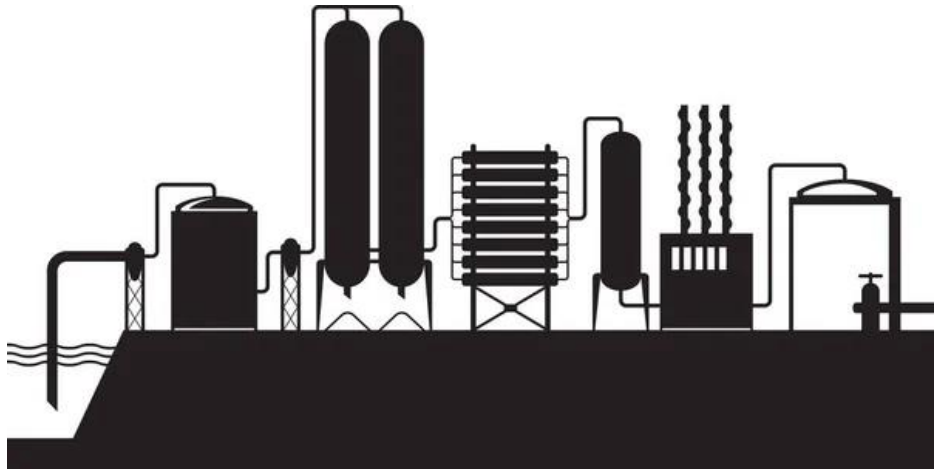
Critical Infrastructure: Can Legacy Apps and Modern MFA Coexist?

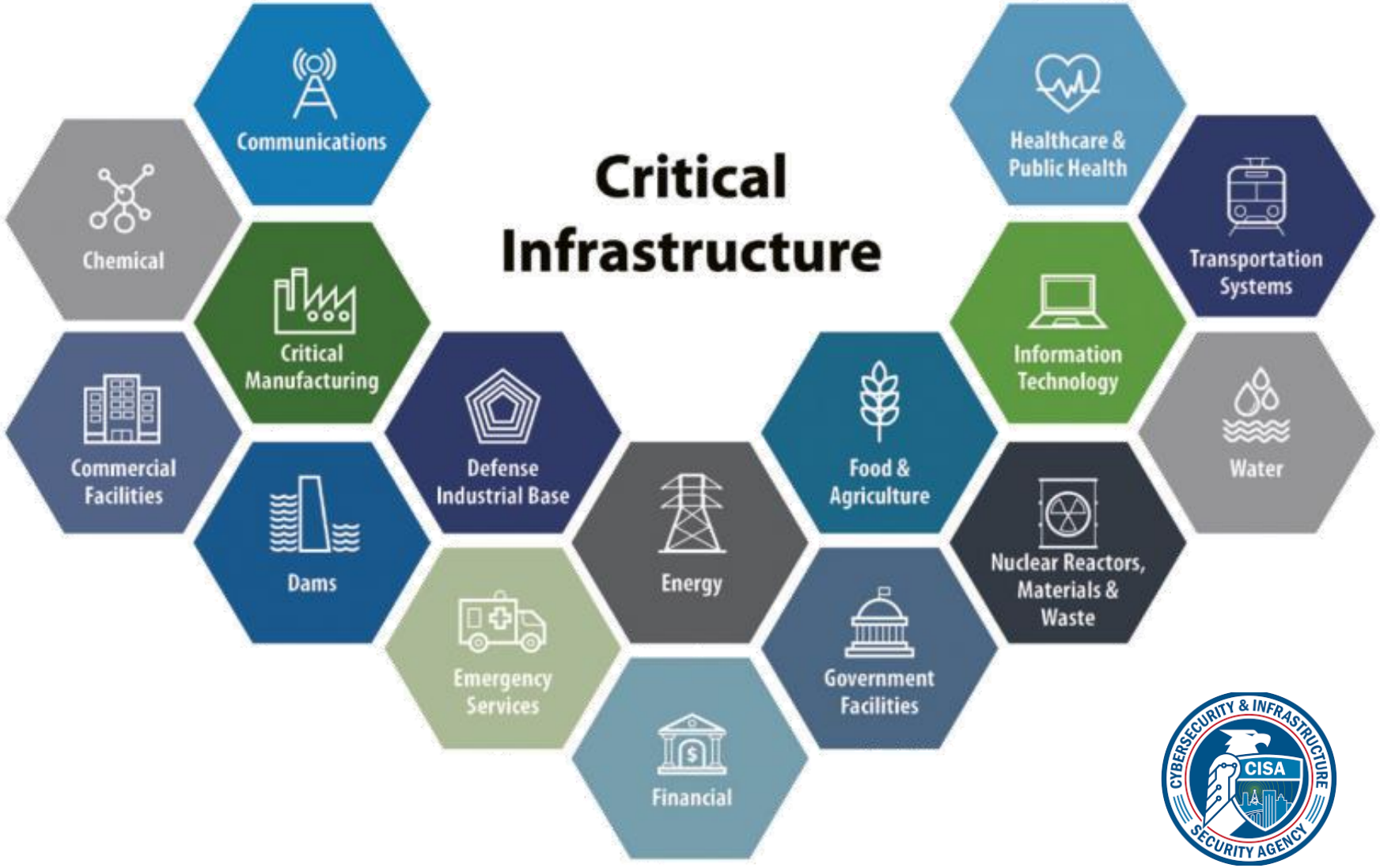


Michael Rothschild

Vice President, Product

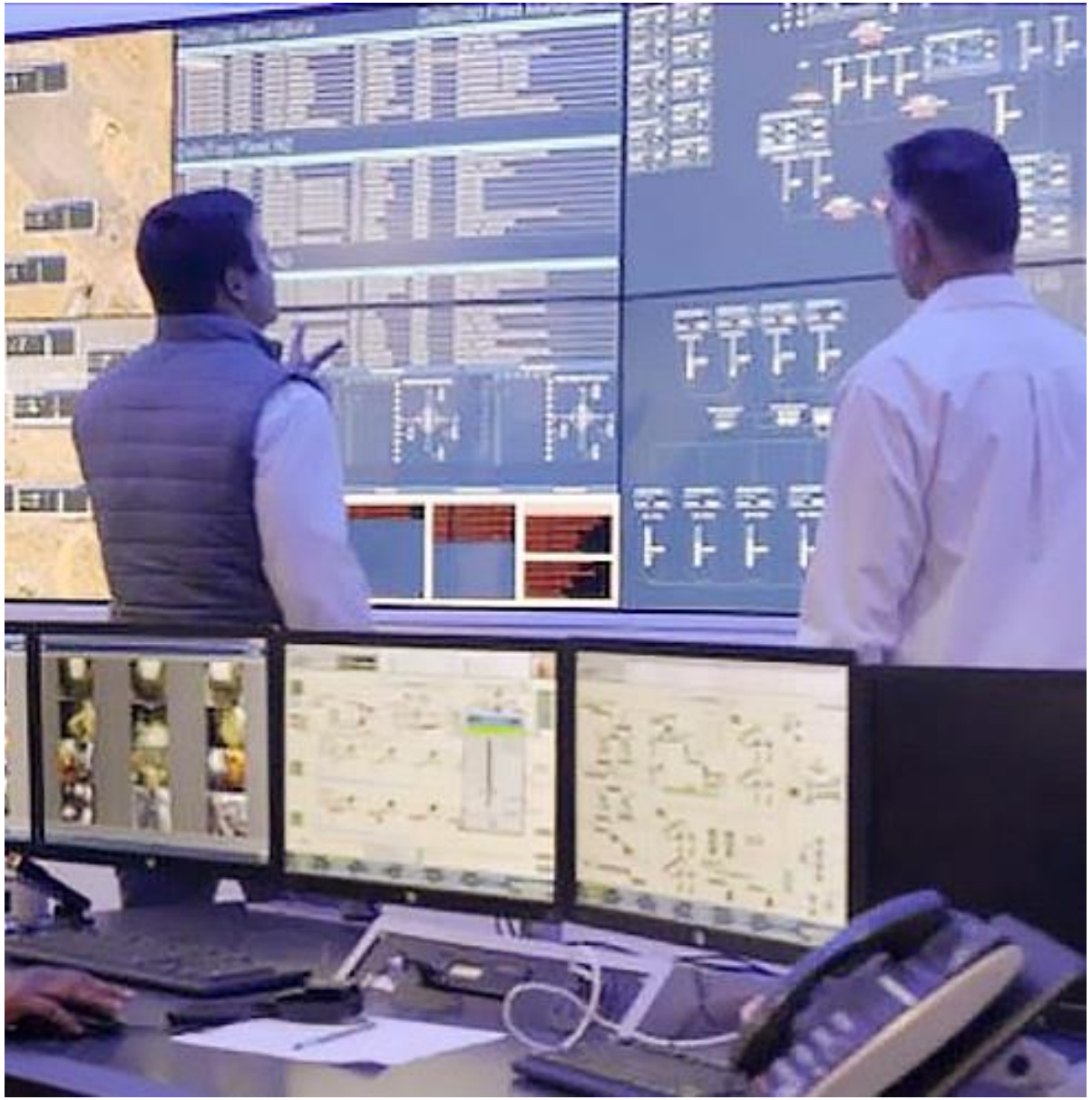
HYPR


606AG
606 AJ




KV-8000
1.Device Mode
2.Error Clear
3.Unit Test
4.Storage
KEYENCE
KV-XLE02
KV-CA02
PORT1
PORT2
CAMERA1
CAMERA2
ECAT IN
ECAT OUT


LINK
EtherNet/IP



The Commonality Of Recent Attacks

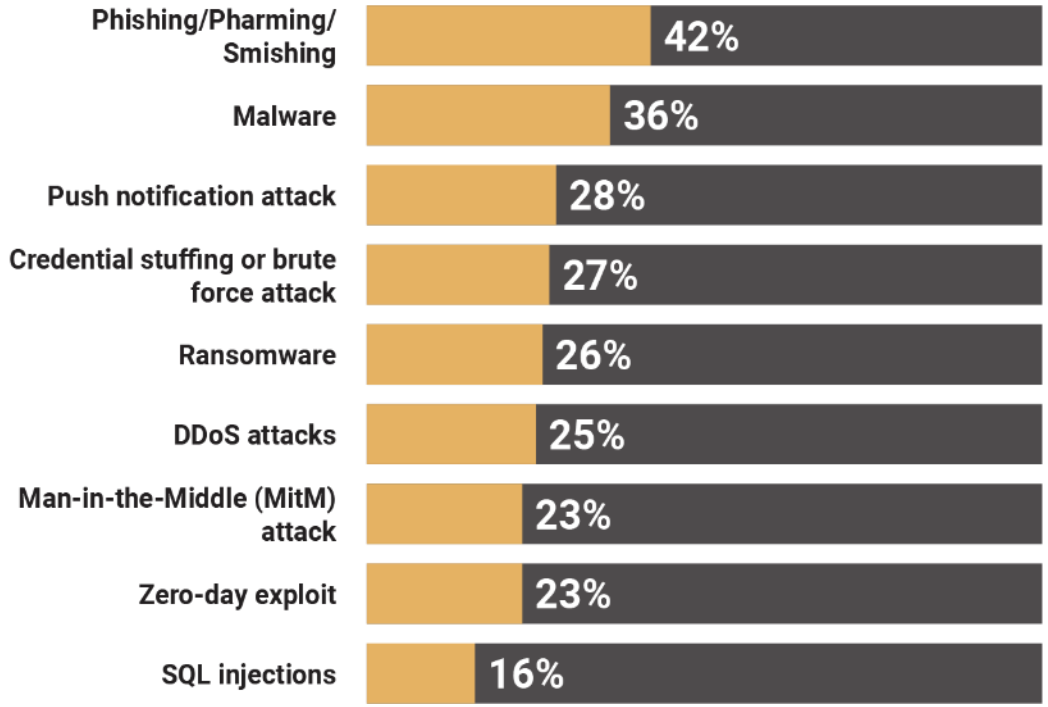
Kudankulam Nuclear

Oldsmar Florida Water Breach

Colonial Pipeline

Attacks Are Targeting Authentication

Types of Cyberattacks Faced in the Last 12 Months



74%

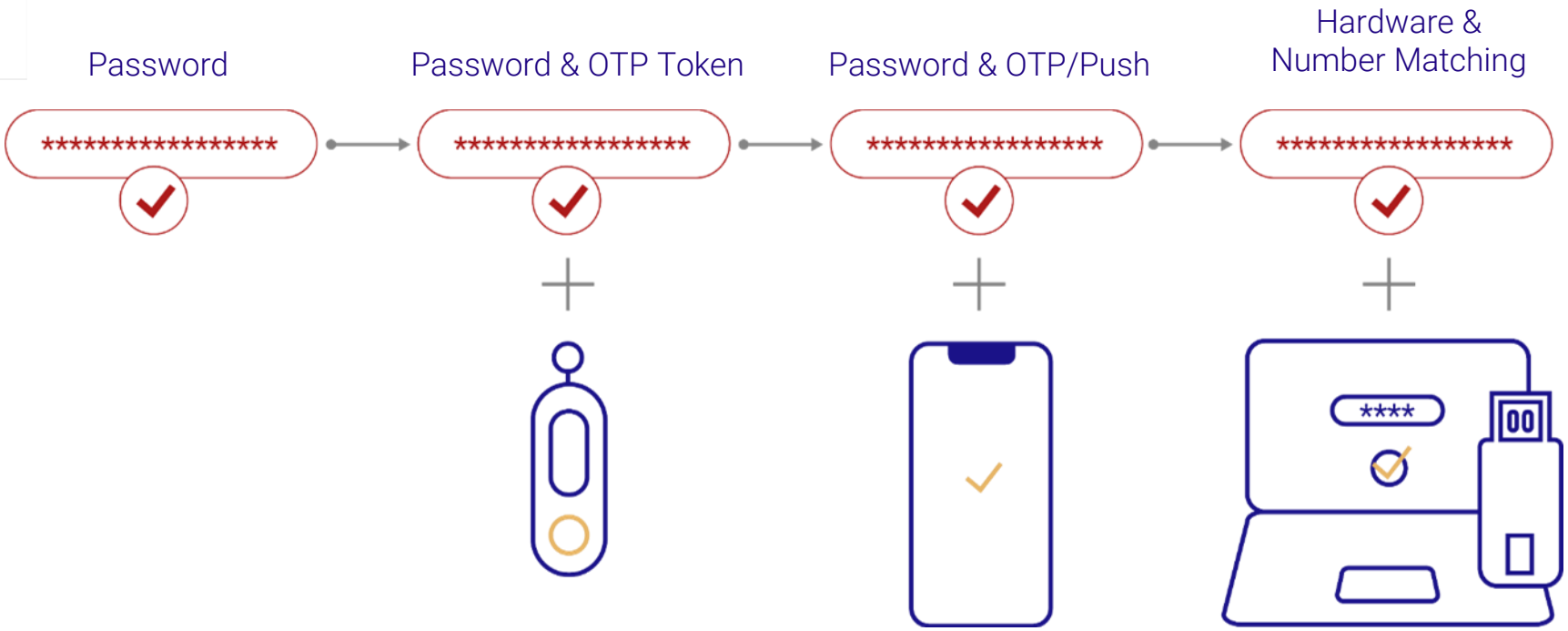
of all organizations report that they experienced a cyber breach in the last 12 months

82%

of those breached organizations attribute credential misuse or authentication weaknesses as a root cause

identiverse

Adding Complexity To The Password



$2.95M

average cost of authentication-related cyber breaches in the last 12 months

3 in 5

organizations were breached due to credential misuse or authentication weaknesses

HYPR 2023 State of Passwordless Security Report

identiverse

#identiverse

Regulation Is Evolving

National

"Multi-factor authentication methods…shall not include telephone or SMS-based authentication methods and must be resistant to phishing attacks"

Federal

"For agency staff, contractors, and partners, phishing-resistant MFA is required"

"FIDO as the gold standard for MFA and the only widely available phishing resistant authentication"

International

"Avoid using SMS and voice calls to provide one-time codes and consider deploying phishing-resistant tokens such as smart cards and FIDO2"

Misperceptions & Complacence

87%
consider their solution to be completely or mostly secure

YET 3% are truly using phishing-resistant MFA

58% did nothing after a breach

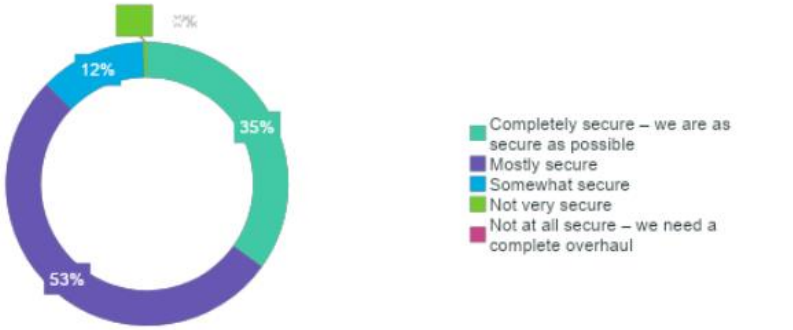


Figure 5: How secure do you consider your organization's approach to authentication to be? [1,000], omitting some answer options

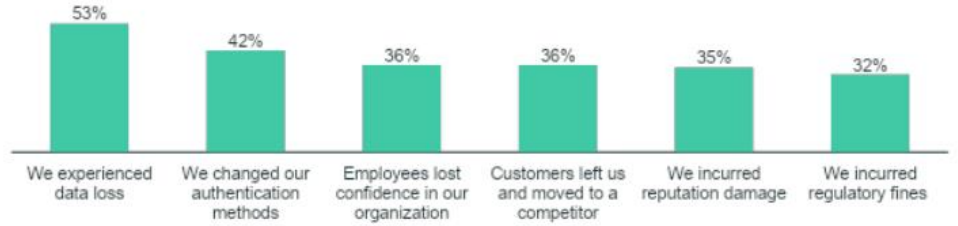
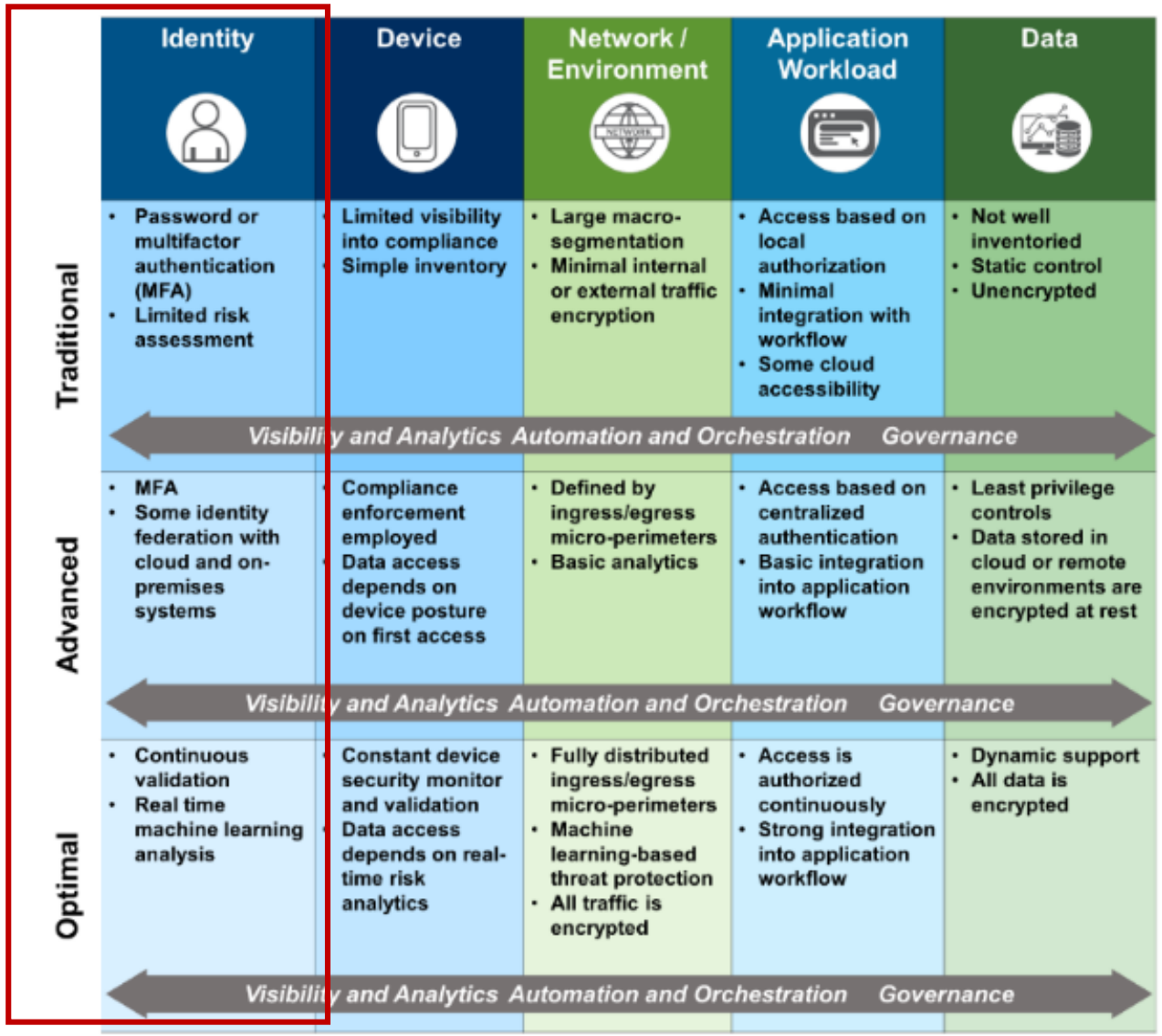


Figure 3: What was the impact of the cyber breach(es) that your organization experienced in the last 12 months? [737] omitting some answer options, only asked to those from organizations that have been a victim of a cyber breach in the last 12 months, omitting some answer options

identiverse

#identiverse

Zero Trust Approach & CISA Guidance



identiverse

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

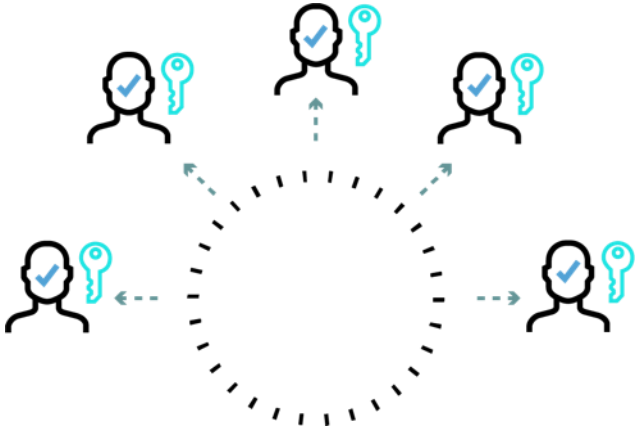
Change The Economics Of An Attack

The Vulnerability of Legacy Authentication

Centralized Password DB

- Security must always be right
- The hacker only needs to be right once

Phishing-Resistant Passwordless MFA



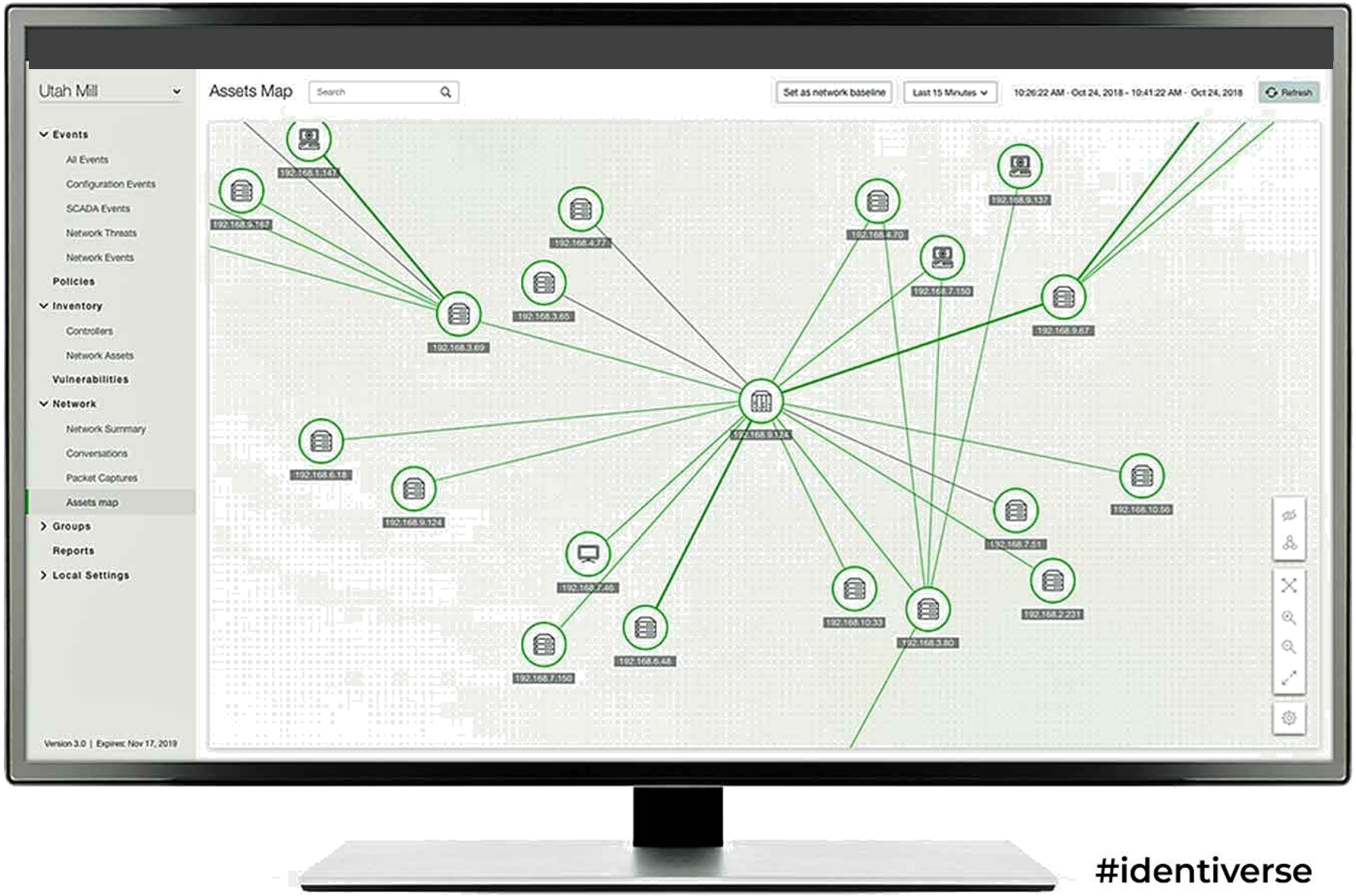
No Password DB

- The hacker must locate and defeat **every** individual's FIDO device
- Not economically feasible for the hacker

“Hands Off My OT!”

Up to 50% of what is in an OT environment is IT

An accurate and up to date asset inventory is crucial



1 - Phishing-Resistant MFA, Everywhere

On all devices, on all applications, on all platforms

Private key stored on device

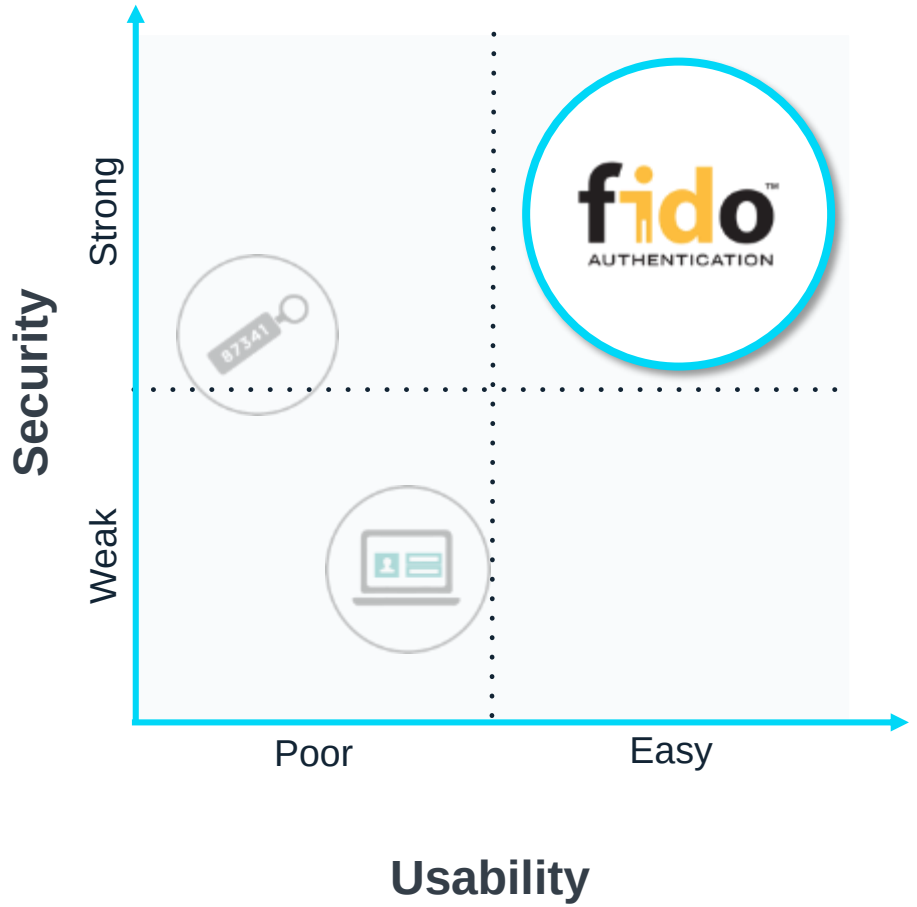
User-initiated authentication via challenge and signature

Public key stored in HYPR cloud

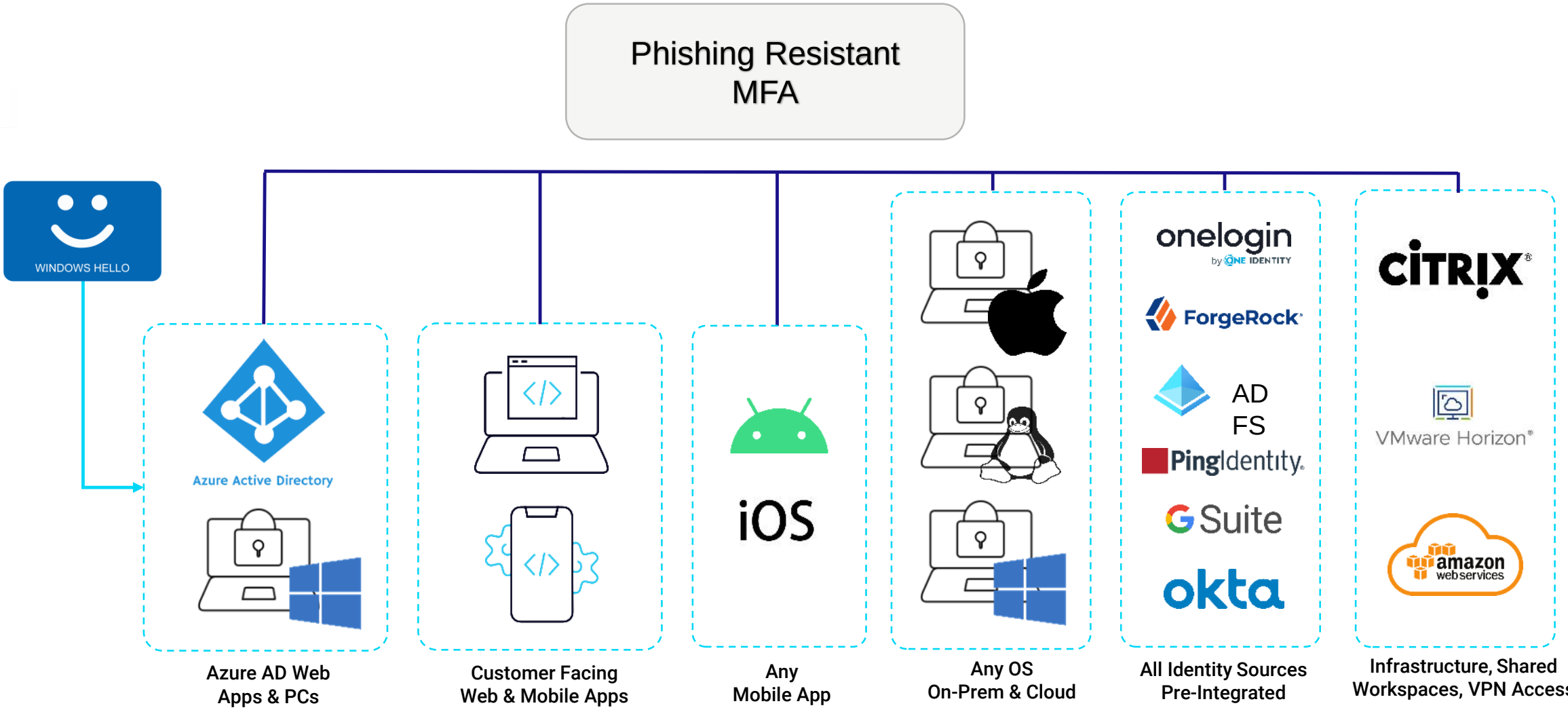
Ping Identity okta

Passwordless MFA into desktops and SSO

2 – Follow “The Standards

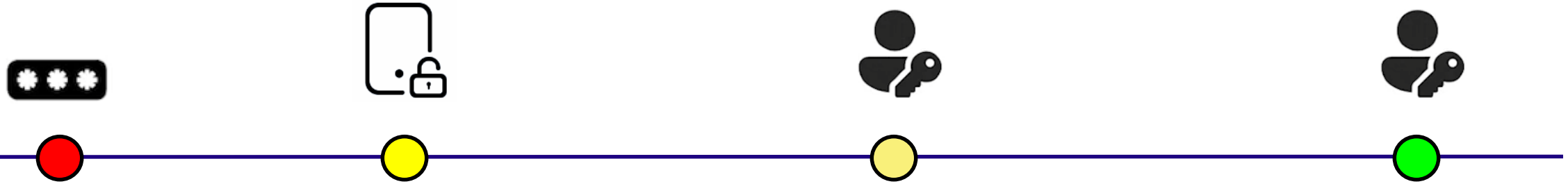


3 – Silos Are For Grain– Partial Security Is No Security



What About Passkeys?

Least Secure



Most Secure

Password

- Convenient

Password + MFA

- More secure than password alone
- Convenient-ish

Multi-Device Passkey

- More secure than password + MFA
- Phishing resistant
- Convenient

Single Device Passkey

- More secure than password + MFA
- Phishing resistant
- Convenient
- Non Synched
- Meets the burden of possession for MFA* (something you have)

Phishing-Resistant MFA

Intuitive, Simple Experience

Proven Passwordless Deployments

THANK YOU!

identiverse

#identiverse