

Everything You Need to Know About Phishing-Resistant MFA

Jim Dickens, Senior PM,
Thales TCT



Thales Trusted Cyber Technologies: Who We Are

Trusted, U.S. Provider of Cybersecurity Solutions Dedicated to the U.S. Federal Government



Corporate Snapshot

- Business Area of Thales Defense & Security Inc.
- President: Lloyd Mitchell
- Headquarters: Abingdon, MD
- Maintain required U.S. Federal Government approvals and certifications to develop, support and sell products to government clients
 - Proxy Agreement with DCSA for Foreign Ownership, Control and Influence (FOCI)
 - National Security Agreement with the Committee on Foreign Investment in the United States (CFIUS).
- Trusted U.S. Source of Supply of Key Technologies for the Federal Government
- Provide U.S. based support for all products developed and sold through Thales Trusted Cyber Technologies

Today's Discussion

01

What is Phishing?

02

Why Phishing?

03

Compliance & the
Move to Phishing-
Resistant MFA

04

Phishing Resistant
Devices

05

Devices in today's
Ecosystems.

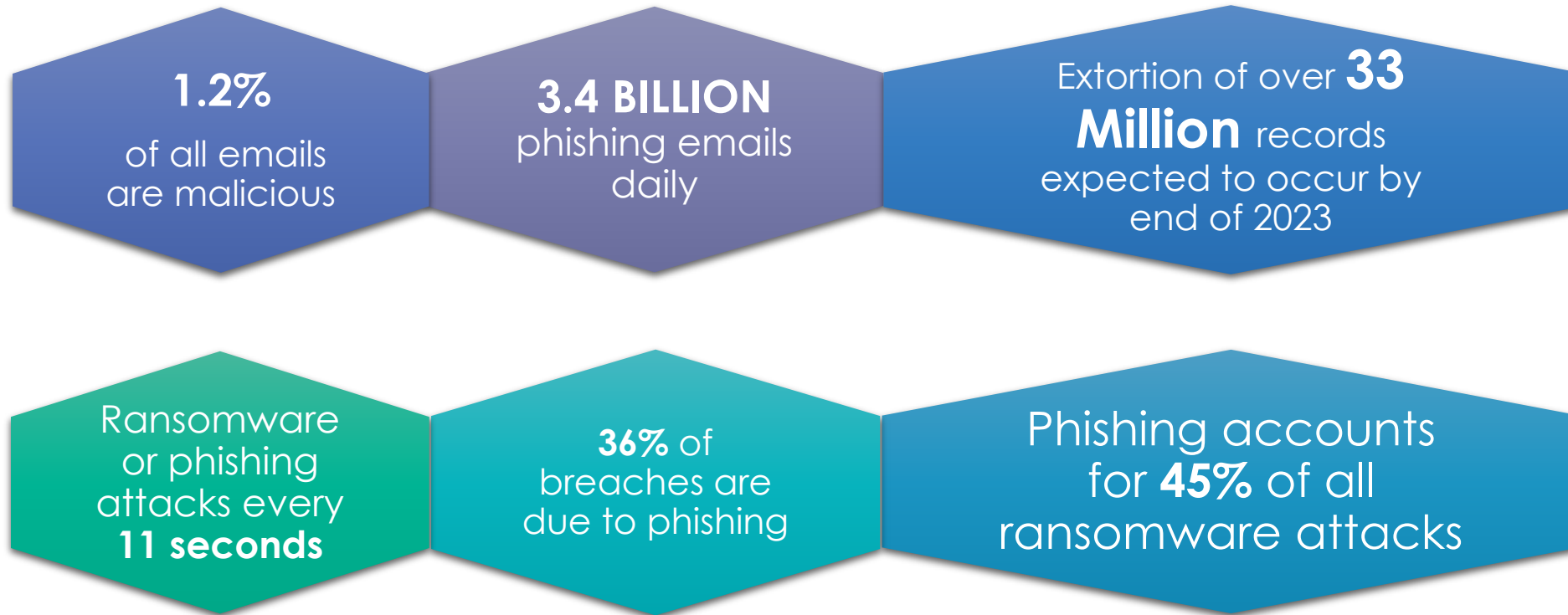
Discussion Point

01

What is Phishing?



Why is Phishing-Resistant MFA Necessary?



But just wait... **Worse in 2024 & 2025**

Why is Phishing-Resistant MFA Necessary?

135% increase in malicious campaigns

1 in 5 organizations provide phishing awareness training

95% cyber security breaches due to human error

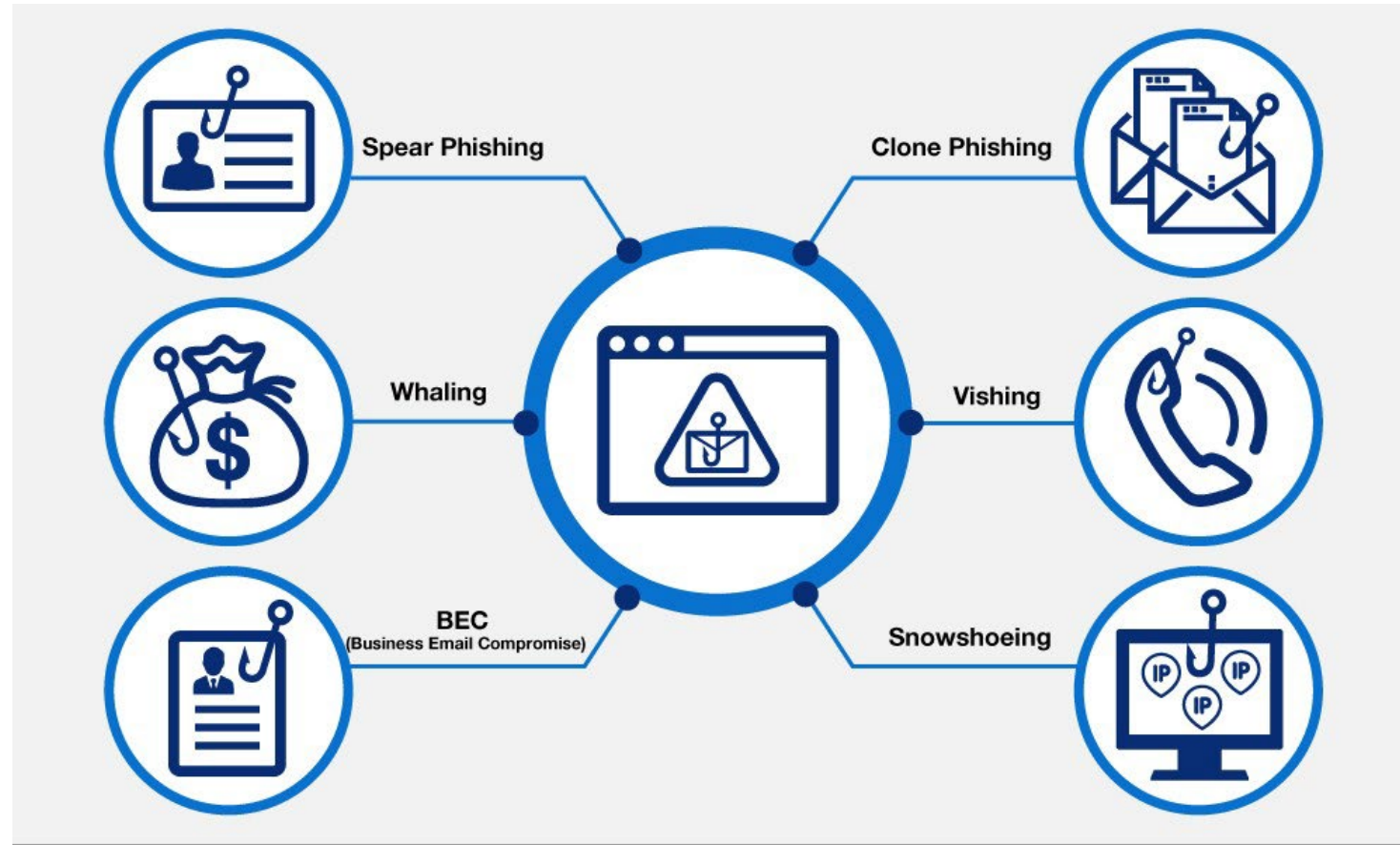
~58% of employees ignore cyber security guidelines

90% of confirmed phishing email attacks in orgs. w/Secure Email Gateways

Discussion Point

02

Why Phishing?



We're Only Human



55%

of respondents who experienced a recent cloud data breach said the #1 root cause of cloud data breaches is **human error.**

Identity and Access Management (IAM) has been identified as a **top mitigating control** for data breaches



28%



of respondents identified IAM as the top security technology most effective in protecting sensitive data from cyberattacks.

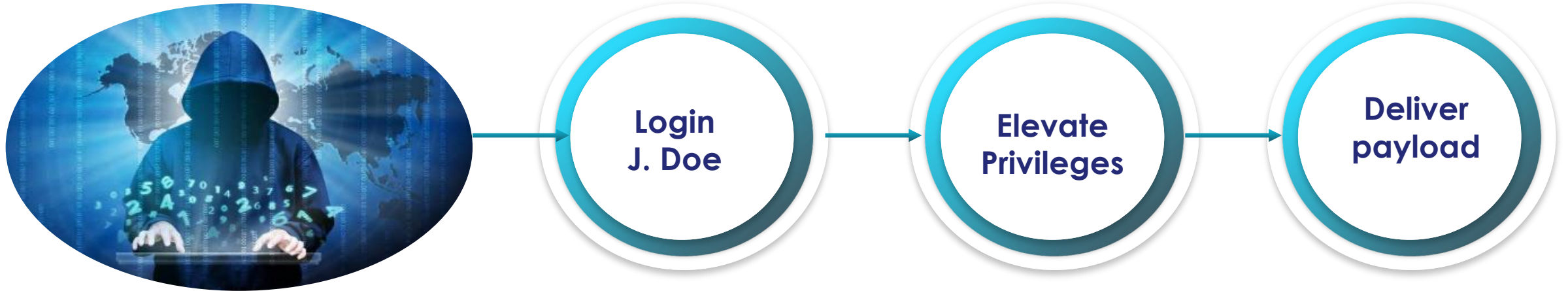


Strong MFA adoption increased to

65%

2023 Thales Data Threat Report

What is Phishing?



Bad Guys Don't Break In, They Log In!

Discussion Point

03

Compliance & the Move to Phishing-Resistant MFA



Compliance Driving the Move to Phishing- Resistant MFA





Federal Policy Driving Compliance

- > **Executive Order 14028, 12 May 2021 (Section 3 (d) (iii))**
 - ▶ Within 180 days of the date of this order, agencies shall adopt multi-factor authentication and encryption for data-at-rest and data-in-transit, to the maximum extent...
- > **National Security Memo 8, 4 May 2022 Section 1 (b) (iii)**
 - ▶ Within 180 days of the date of this memorandum, agencies shall implement multifactor authentication and encryption for NSS data-at-rest and data-in-transit.



Global Policy Driving Compliance

> Cybersecurity Act in EU

- ▶ Companies doing business in the EU will benefit from having to certify their ICT products, processes and services...

> Private Sector

- ▶ Cloud Service Providers
- ▶ Banking
- ▶ Health Care

Discussion Point

04

Phishing Resistant Devices



What is Phishing- Resistant Multi-factor Authentication (MFA)?



What is Phishing-Resistant MFA?

Phishing-resistant MFA is immune from attempts to compromise or subvert the authentication process, commonly achieved through phishing attacks.



A light red rounded rectangular box containing five circular icons representing non-phishing-resistant MFA methods:

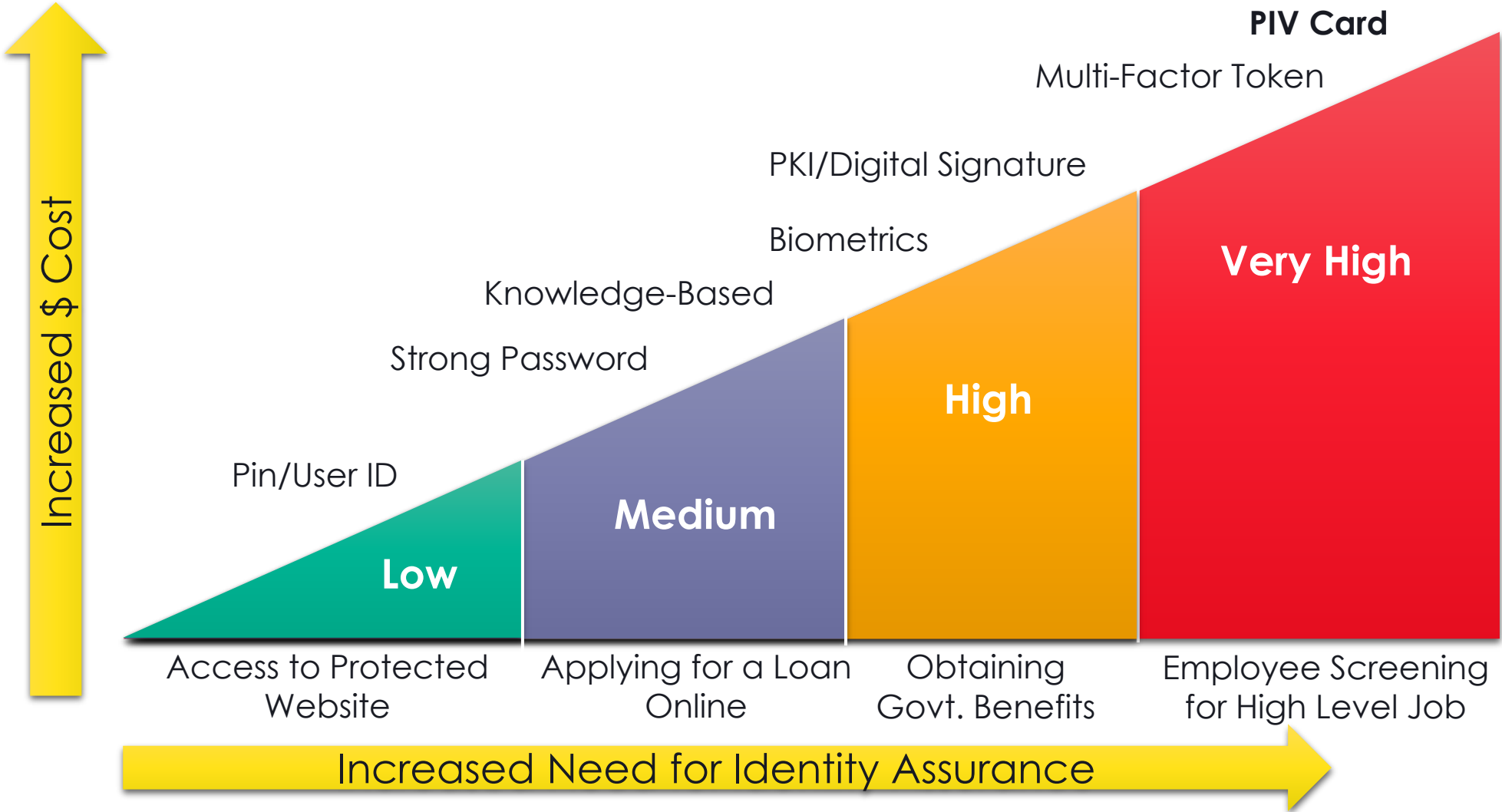
- OTP Push**: An icon of a hand pointing at a screen.
- OTP Hardware**: An icon of a blue Thales hardware token.
- Pattern-based**: An icon of a 4x4 grid of numbers (3 0 9 7 4, 0 4 6 9 6, 7 2 0 8 2, 1 5 5 5 8, 3 2 8 1 1).
- SMS**: An icon of a mobile phone.
- User Name Password**: An icon of three asterisks.



A light green rounded rectangular box containing two circular icons representing phishing-resistant MFA methods:

- FIDO**: An icon with the text "fido ALLIANCE" and "FIDO".
- PKI CBA**: An icon of a blue card.

Four Authentication Assurance Levels to Meet Multiple Risk Levels



Phishing Resistant MFA Devices



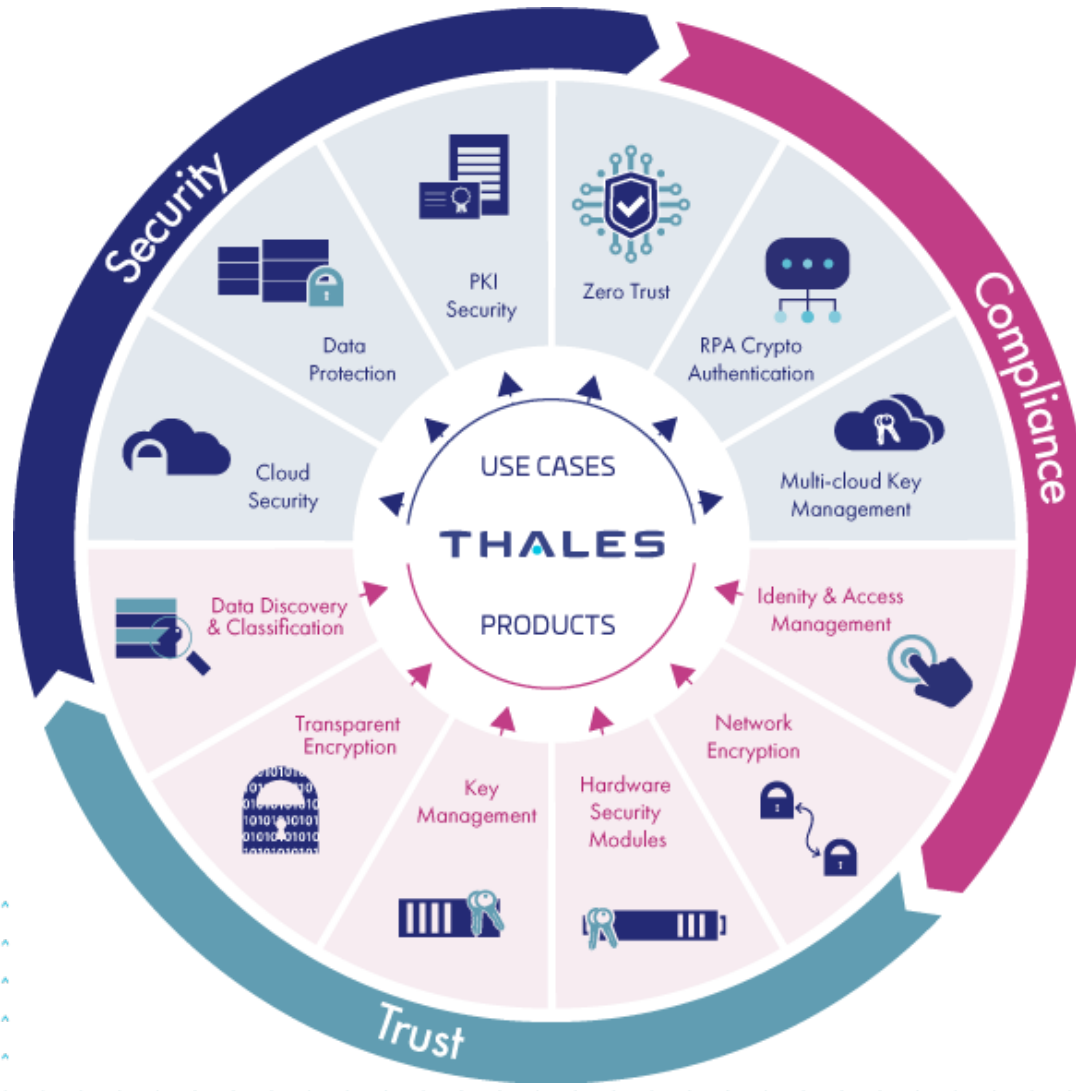
PKI
FIDO
Fusion



Discussion Point

05

Fitting MFA Into Today's Strategies & Ecosystems





How it Fits into Zero Trust & ICAM Solutions

Zero Trust: Identity Pillar



Traditional

- Password or MFA
- On-prem identity stores
- Limited risk assessment
- Permanent access with periodic review

Initial

- MFA with passwords
- Self-managed and hosted identity stores
- Manual risk assessments
- Access expires with automated review

Advanced

- Phishing-resistant MFA
- Consolidated and integrated stores
- Automated identity risk assessments
- Need/session-based access

Optimal

- Continuous validation and risk assessment
- Enterprise-wide integration
- Tailored, as-needed automated access

Authentication & Access Management



SafeNet
Trusted Access



SafeNet
Authentication Service

Non-Person Entities



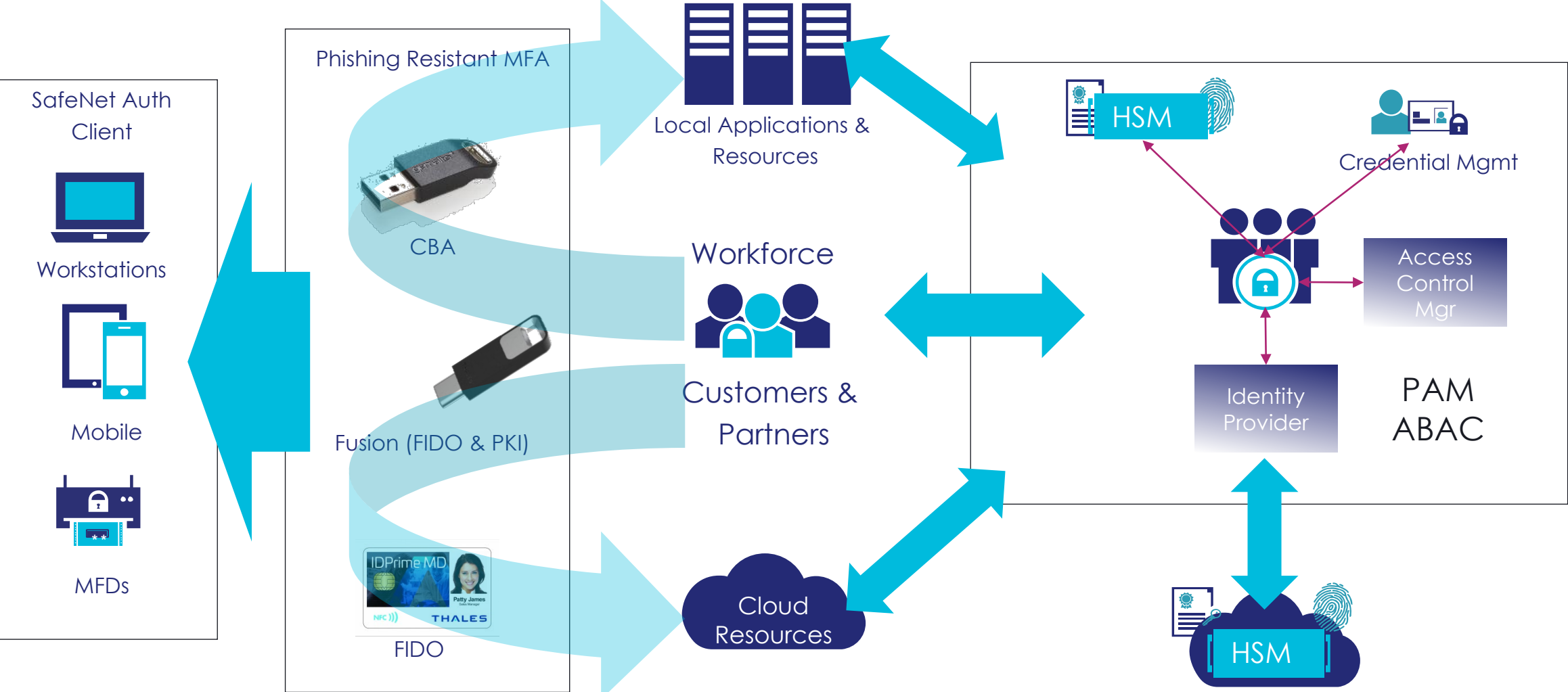
Luna
Credential System

PKI Root of Trust



Luna T-Series HSM

Identity Credential Access Management (ICAM)



Q & A?

