TechVision RESEARCH

Multi-Factor Authentication & Zero Trust

MACC 2019

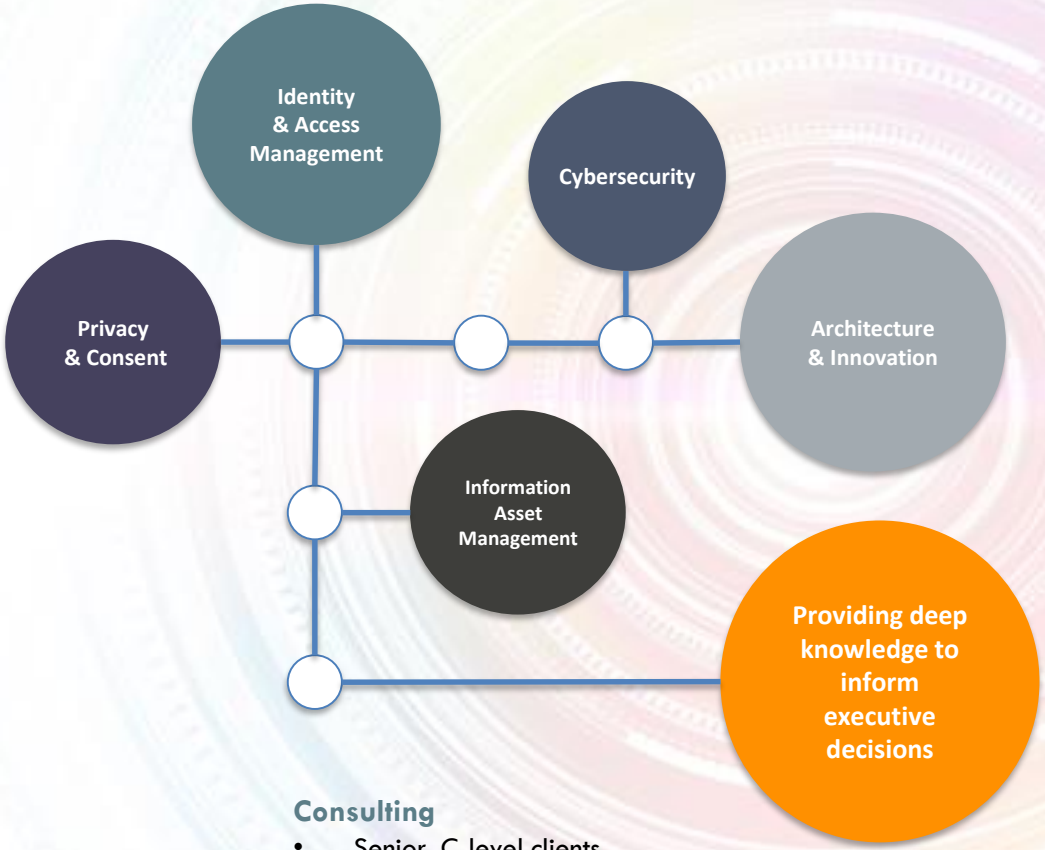
Sorell Slaymaker
Principal Consulting Analyst
TechVision Research

TechVision Research: What we do

Take a client theme

- Identity and Access Management
- Security and Risk Management
- Data Architecture & Strategies
- Digital Transformation
- Innovation and Disruption
- Privacy and Information Protection
- Blockchain Adoption
- Internet of Things
- Network Architecture & Security
- Public, Private and Hybrid Cloud

and Connect the Dots



Research

- Broad and deep experience
- Industry specialists
- Technology pioneers
- Global perspective

Consulting

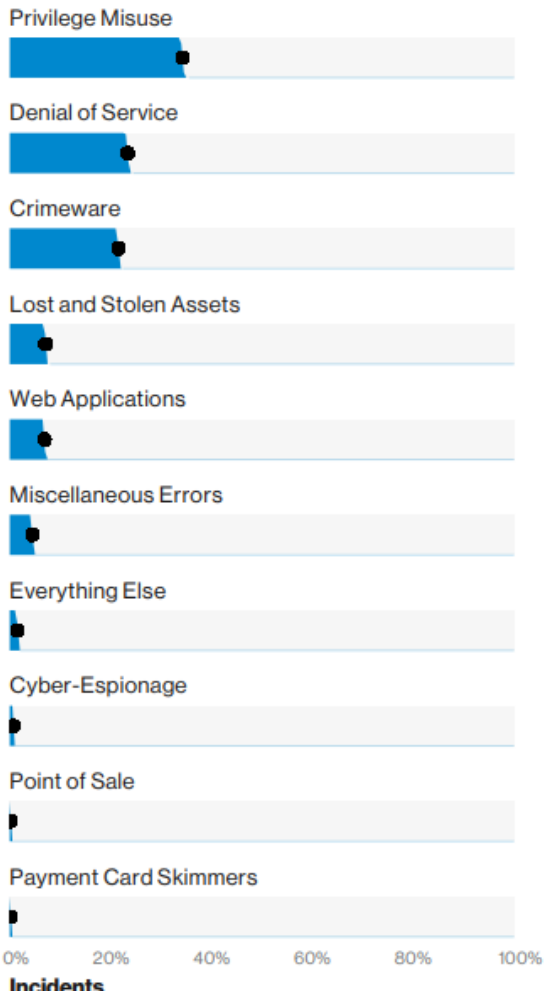
- Senior, C-level clients
- Bridge between board-level strategies and technical solutions

TechVision RESEARCH

Agenda

- MFA Foundations
- Moving To 6 Factor Authentication
- Conditional & Continuous Authentication
- Stop Using SMS for MFA
- MFA & Zero Trust
- MFA Futures
- Q&A

Why We Care About MFA



From Verizon 2019 Data Breach Report

1,000+ US data breaches yearly

190 days on average to detect a data breach

80% of breaches involve a privileged account being exploited

81% of breaches start with either stolen and / or weak passwords

Username & Passwords Are Not Good Enough

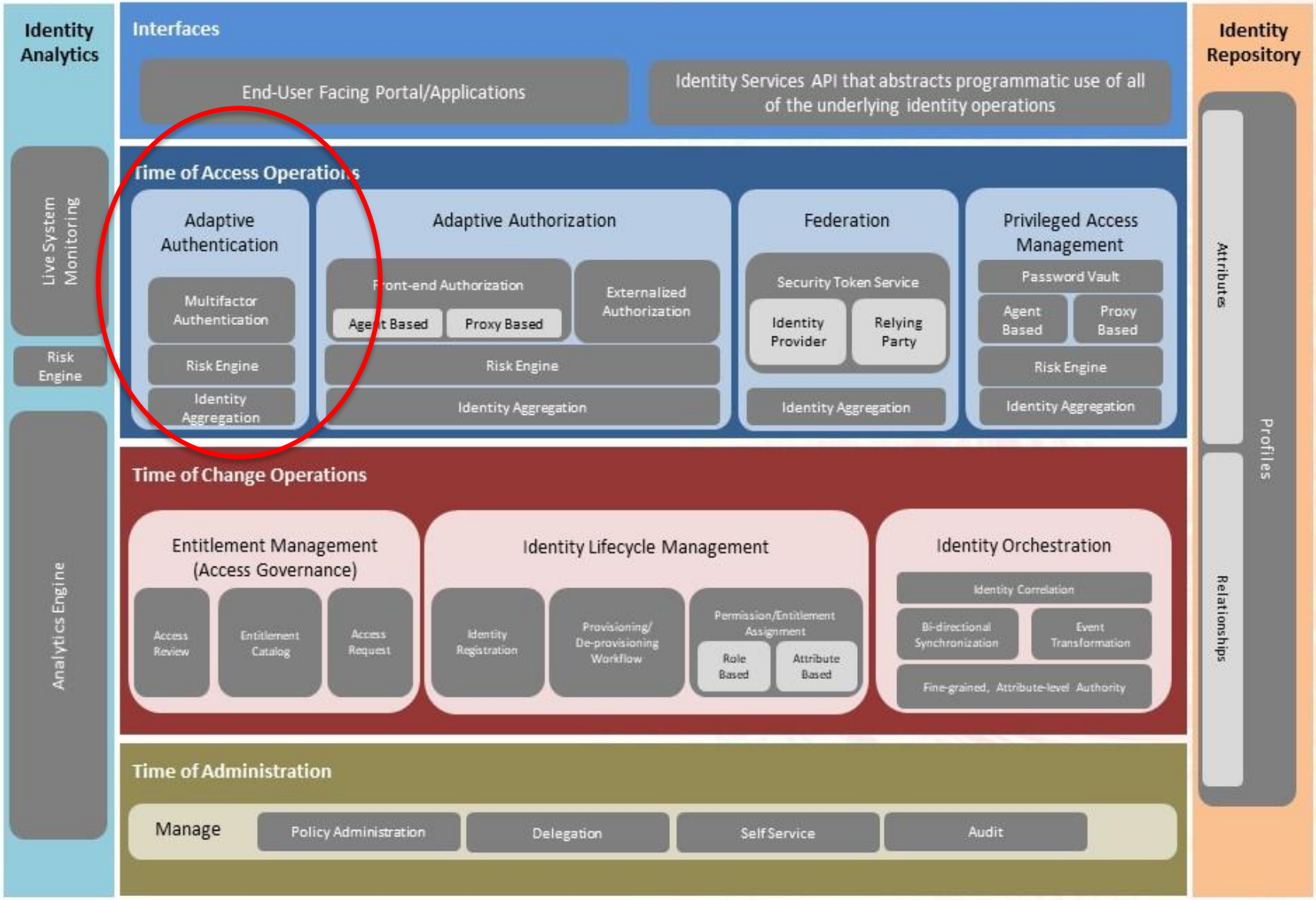
Thesis

- Multi-Factor Authentication is gaining traction as a best practice for enterprise security programs.
- It is based on the premise that traditional, single factor authentication schemes (like IDs and passwords) are relatively easy to break
- MFA is one of the cornerstones of IAM infrastructure.

Business Drivers for MFA

- ***Business Facilitation***
  - the need to improve interoperability and efficiency through interconnected systems to support employees, affiliates, business partners and customers
- ***Enhancing User Experience***
  - simplifying the process of authentication and letting the end user *not* have to remember another password
- ***Cost Containment***
  - planning to reduce the cost of management of multiple disparate authentication systems and processes
- ***Security Effectiveness and IT Risk Management***
  - improving the level of assurance that maps to an identity for appropriate authentication
- ***Support Administrative and End-user Efficiency and Effectiveness***
  - consolidating the authentication infrastructure and better defining and reducing the number of access points

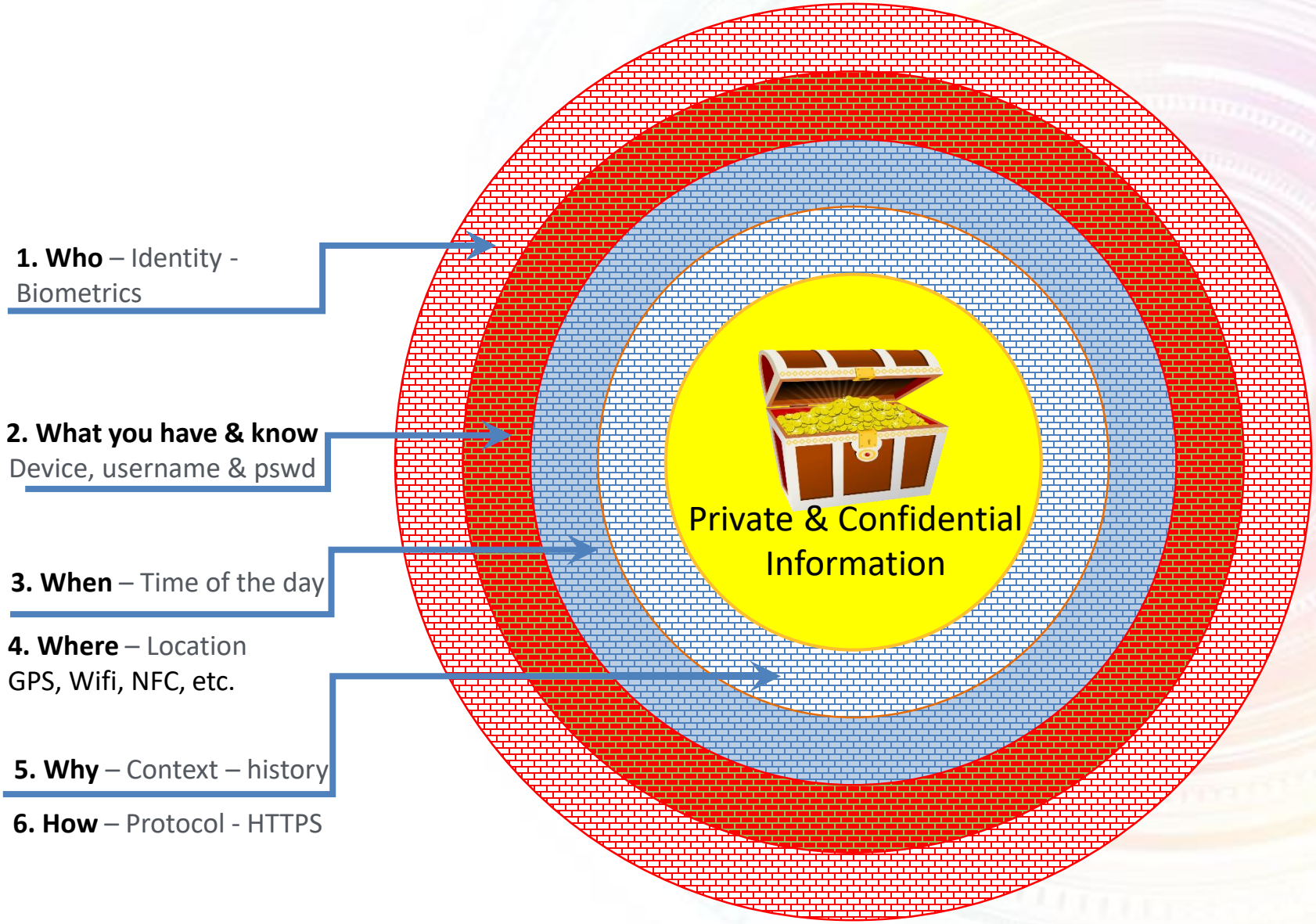
MFA In the IAM Reference Architecture



Agenda

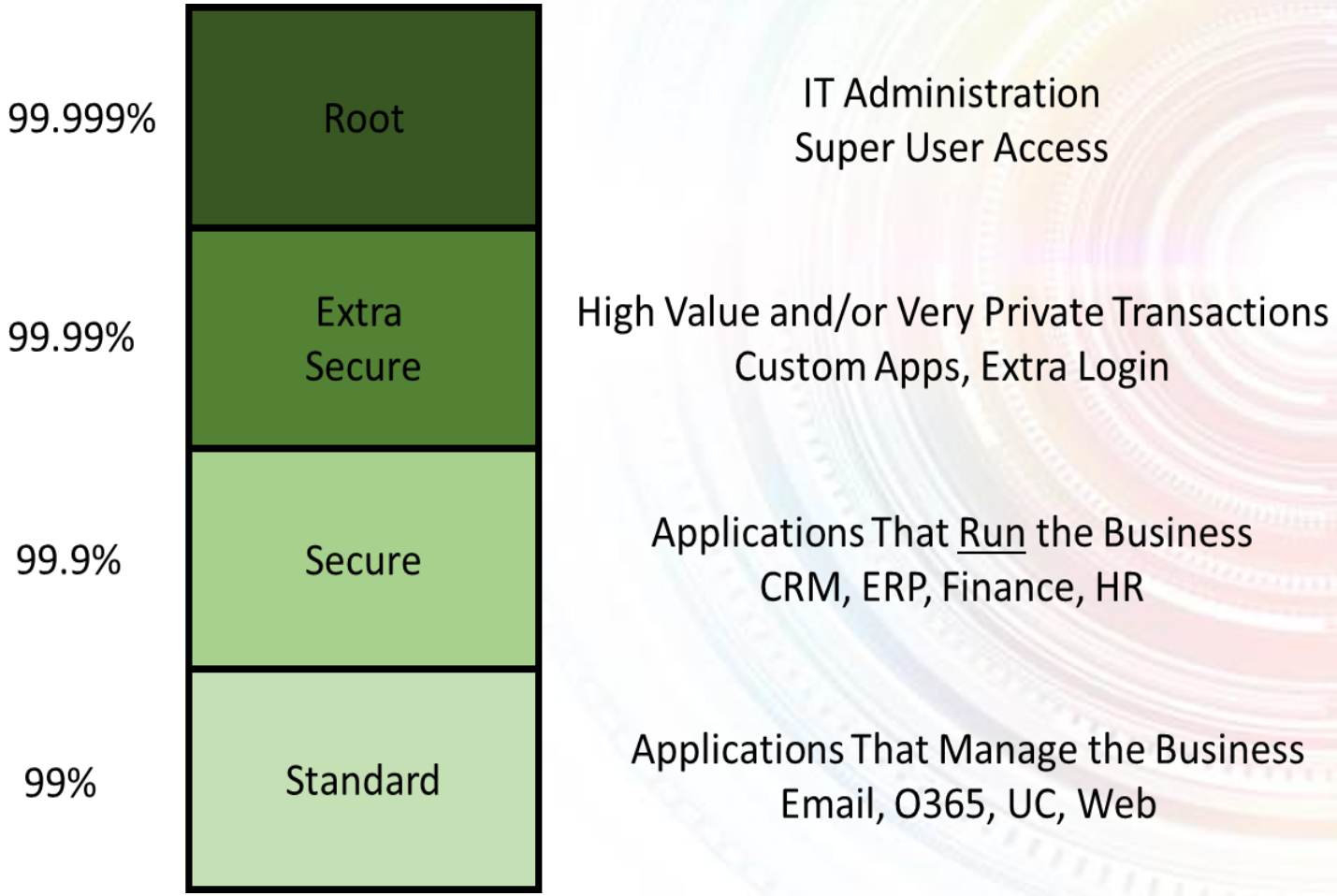
- MFA Foundations
- Moving To 6 Factor Authentication
- Conditional & Continuous Authentication
- Stop Using SMS for MFA
- MFA & Zero Trust
- MFA Futures
- Q&A

6 Factors For Authentication



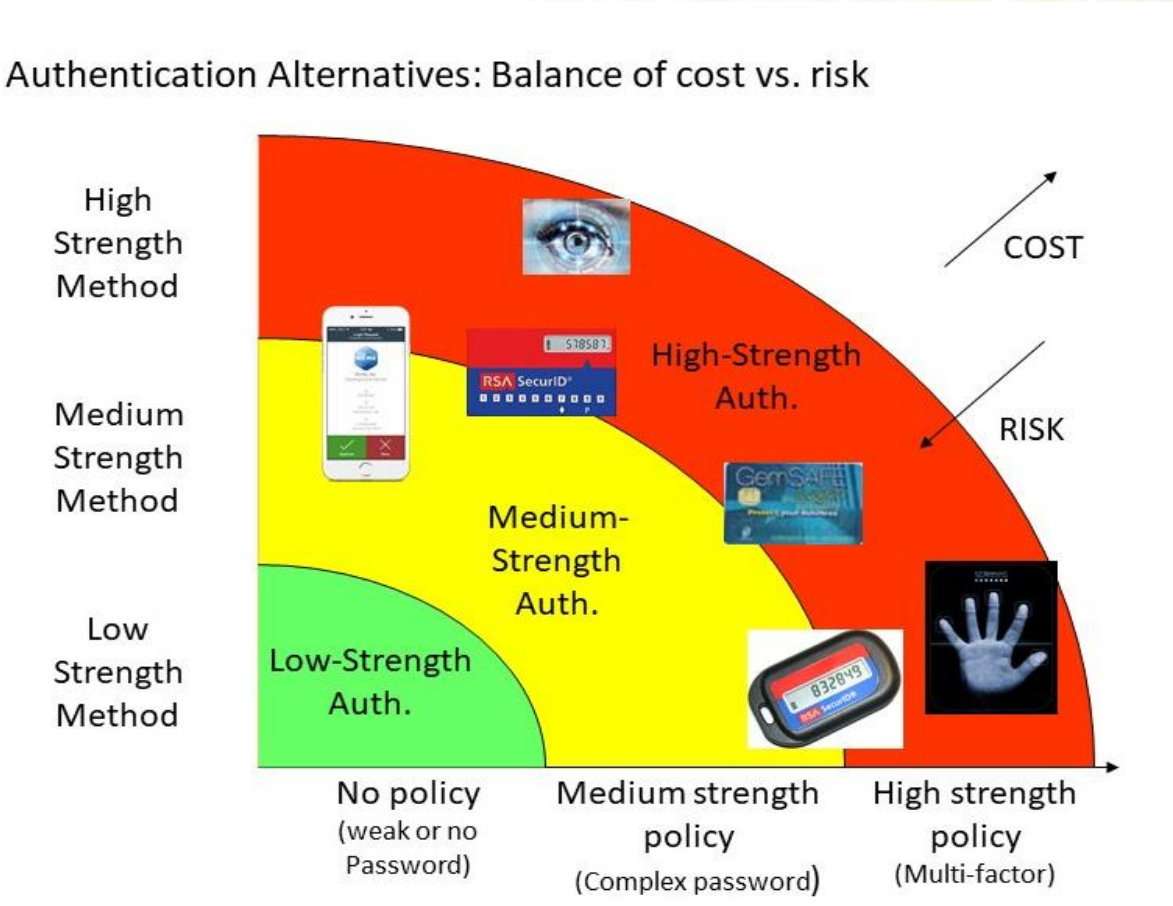
Level of Authentication is Based On Risk

Privileged Access Management (PAM) focuses on securing access to high value systems and data



Balancing MFA Requirements

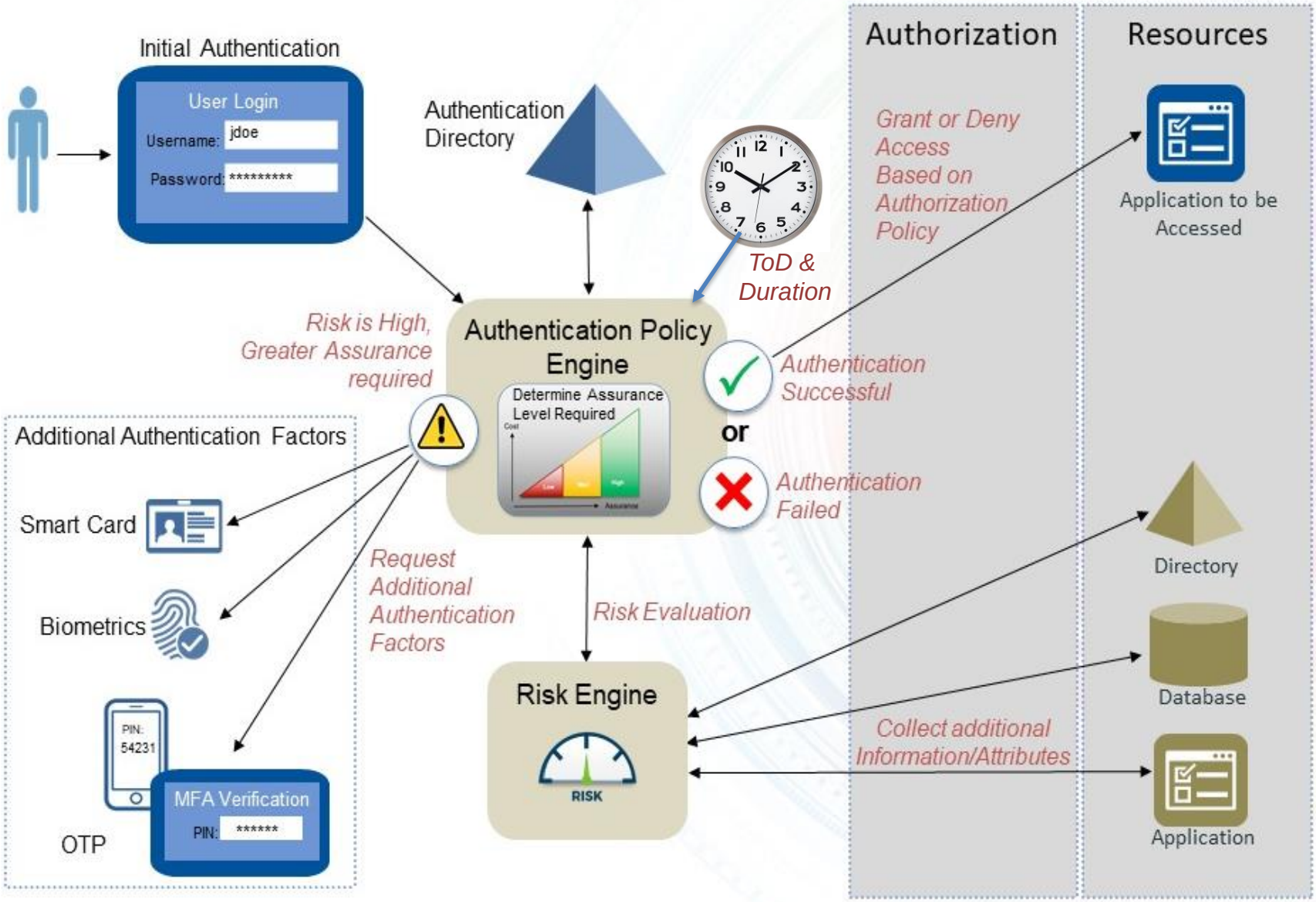
- MFA must be deployed with a well-thought-out strategy that weighs the risks, costs and usability



Agenda

- MFA Foundations
- Moving To 6 Factor Authentication
- Conditional & Continuous Authentication
- Stop Using SMS for MFA
- MFA & Zero Trust
- MFA Futures
- Q&A

MFA In Conditional Authentication Pattern



Agenda

- MFA Foundations
- Moving To 6 Factor Authentication
- Conditional & Continuous Authentication
- Stop Using SMS for MFA
- MFA & Zero Trust
- MFA Futures
- Q&A

SMS is not Secure

The US Department of Homeland Security recommends that government agencies and enterprises stop using SMS for sensitive communication.

SMS Vulnerabilities

No Encryption – SMS messages are sent as clear text that is readable by anyone on the sender's carrier network, anyone on the carrier-interchange network, and anyone on the recipient's carrier network.

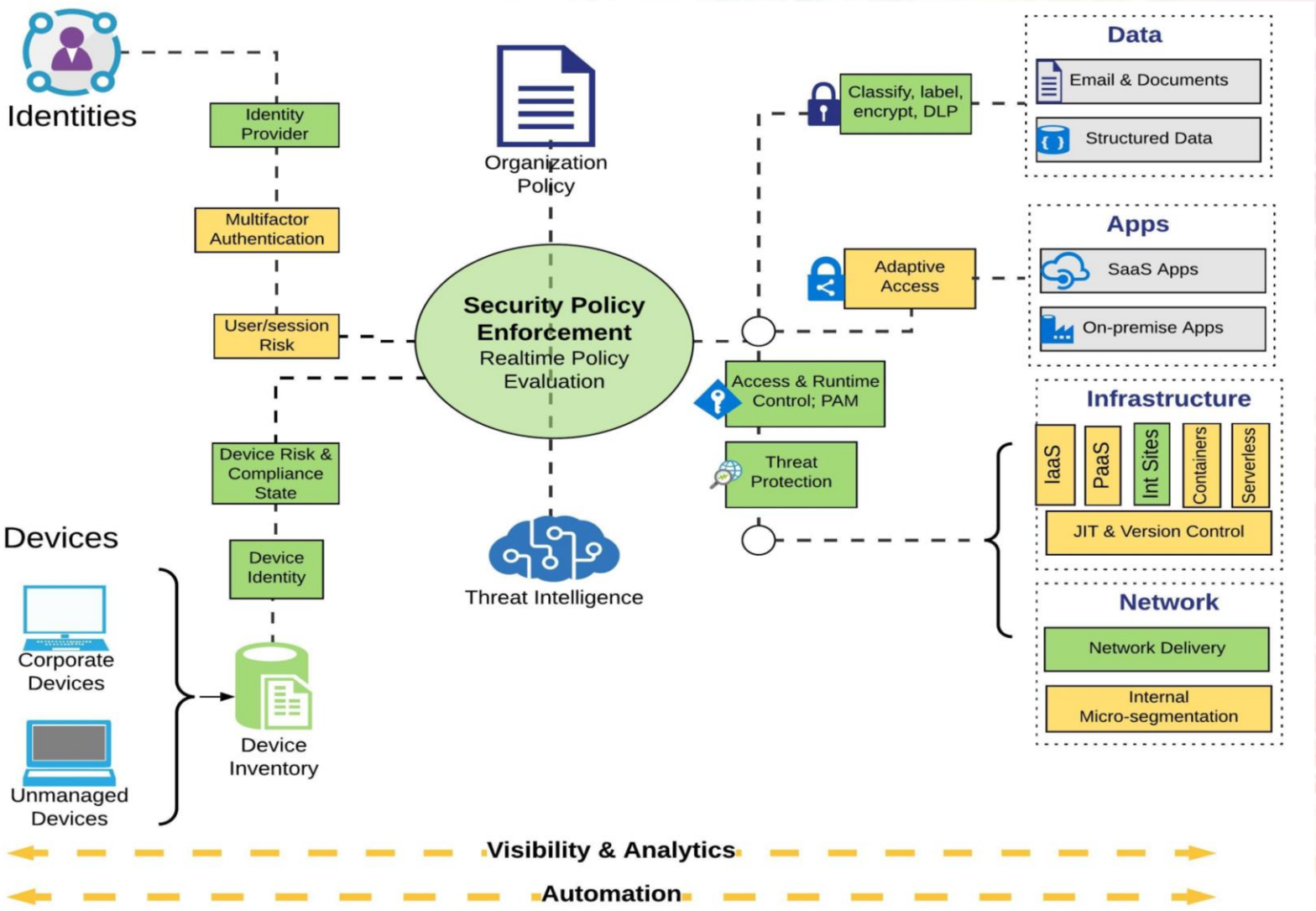
SMS Hijacking – Organized crime and hackers may motivate international mobile network operator employees to mis-direct SMS messages

SIM Swapping Exposure – The Subscriber Identity Module (SIM) inside a smartphone is used to uniquely identify its owner. Criminals who gather details about a victim such as their mobile phone number can get a wireless network company to transfer a phone number to a new phone for a short period of time.

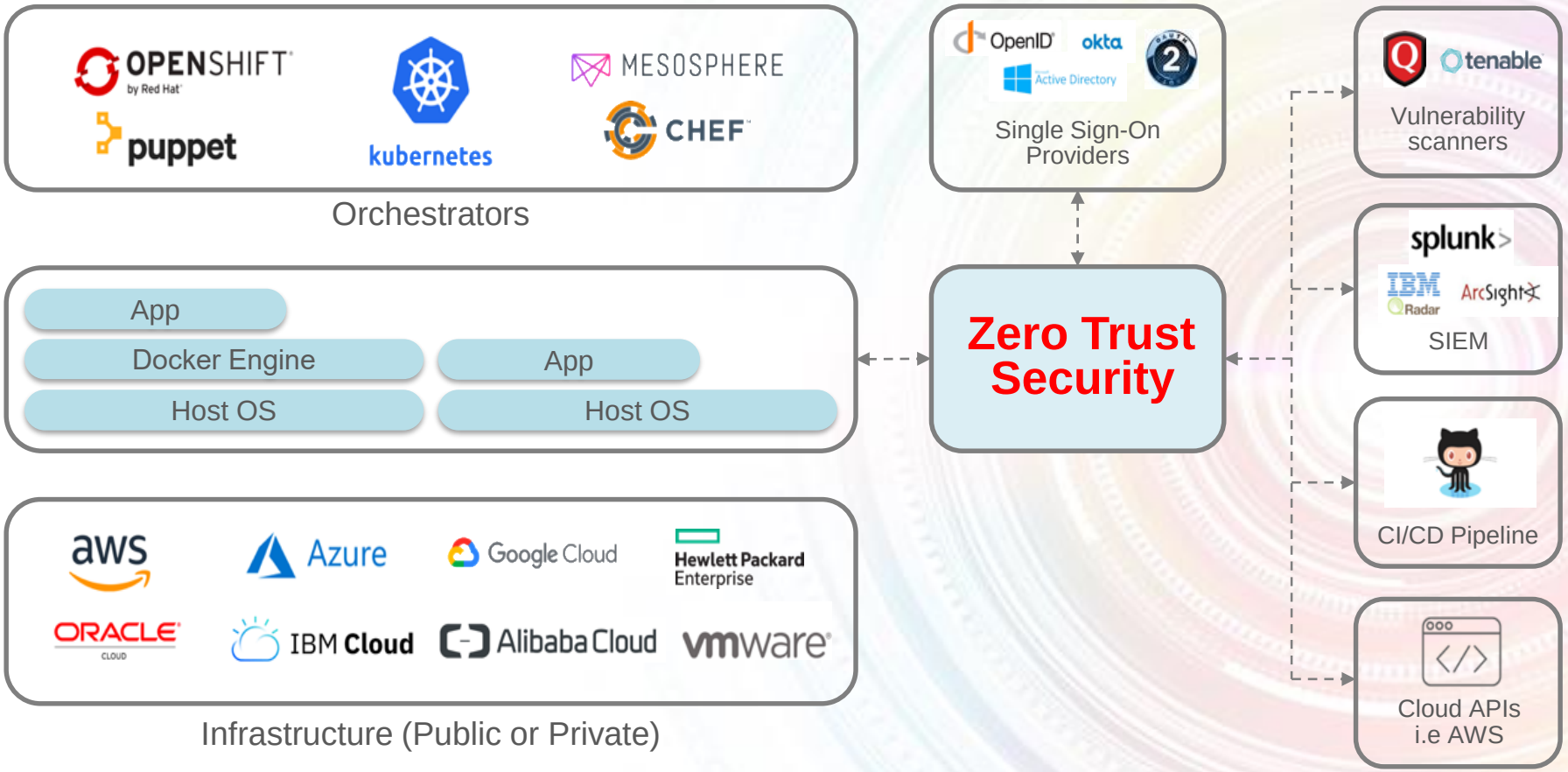
Agenda

- MFA Foundations
- Moving To 6 Factor Authentication
- Conditional & Continuous Authentication
- Stop Using SMS for MFA
- MFA & Zero Trust
- MFA Futures
- Q&A

Microsoft Zero Trust Architecture



Zero Trust Hybrid/Multi-Cloud

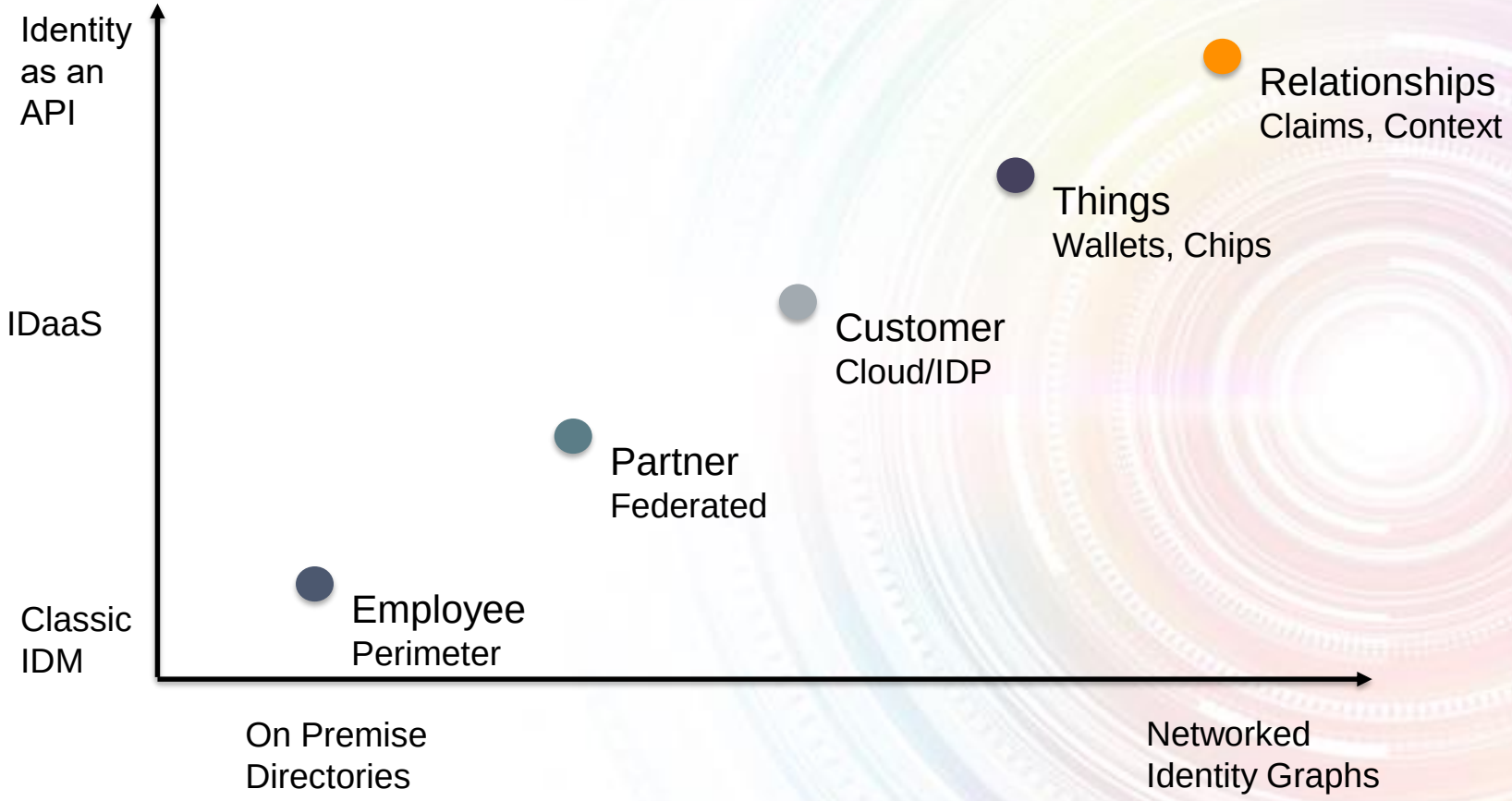


Zero Trust provides a 1:1 mapping of users, devices, services, applications, and data

Agenda

- MFA Foundations
- Moving To 6 Factor Authentication
- Conditional & Continuous Authentication
- Stop Using SMS for MFA
- MFA & Zero Trust
- MFA Futures
- Q&A

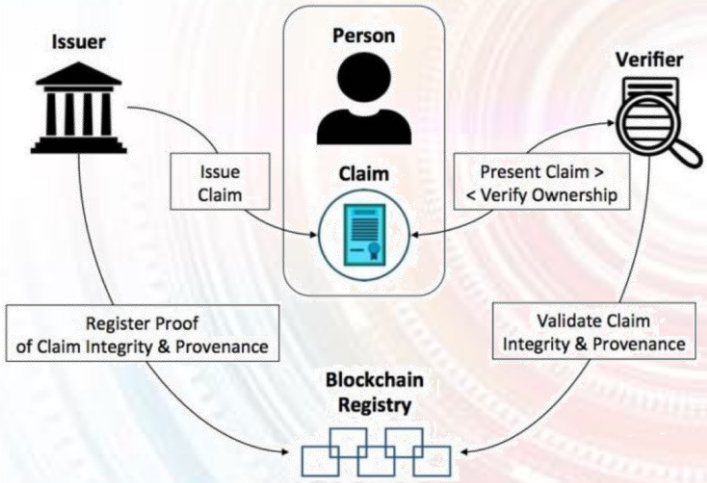
Evolution of Identity



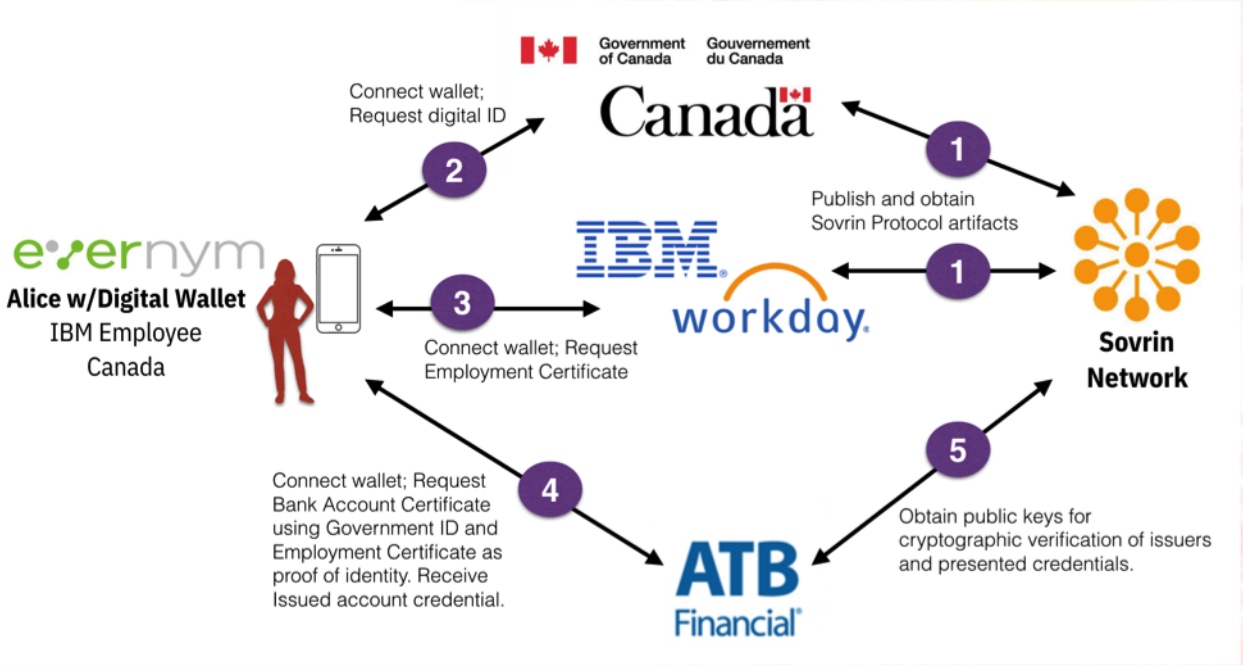
Great IAM is the foundation of great security

What is Decentralized Identity?

- Potentially reducing the hundreds of IDs/passwords often maintained today
- Move from BYOD to BYOI, to Decentralized (AKA Self-Sovereign) Identity
- Identity control by identity owner like in the physical world
- Peer-to-peer (no 3d party)
- Integrity of the identity record can be verified via blockchain
- Stronger authentication via digitally signed, verifiable credentials
- Better privacy by limiting non-essential verification data
- Requires the development of an underlying ecosystem
- Significant investment by Microsoft, IBM and several early stage companies



Decentralized Identity



Enterprises should be evaluating Decentralized Identity as part of their future-state IAM portfolio. There is a real opportunity to solve key security, privacy and usability challenge across the Internet in a "game changing" way.

Key Take-Aways

1) Identity using MFA will be the cornerstone of enterprise and government security
2) The industry is moving from a 3-tier authentication model (something you know, have, are) to a 6-tier (adds location, time, context/history)
3) Avoid using SMS for highly-secure MFA
4) Decentralized identity and authentication without passwords is worth looking into

Q&A

TechVision RESEARCH

Thank You