UPGRADING AUTHENTICATION MODELS

CHRYSALIS PANEL DISCUSSION

TECHVISION
CHRYSALIS

Featured Speakers

Doug Simmons, TechVision Managing Director, Principal Consulting Analyst. Doug is a pioneer in the IAM space. Led consulting at Burton for 10 years and security & identity consulting at Gartner for 5 years. Has worked with hundreds of large enterprises. Doug helps companies get IT security, risk management, and IAM right in an accelerating and ever-changing digital landscape.

Alex Weinert, Microsoft Director of Identity Security. Alex and his team are the ones standing between you and the hackers when you sign into Xbox, Skype, Outlook, Office 365, Azure,and any number of our B2C sites or organizations using Azure AD. In addition to detection ISP delivers Azure AD Identity Protection, Conditional Access, MFA, and MS Authenticator app.

Archit Lohokare, Idaptive Chief Product Officer is responsible for product strategy, driving innovation, and bringing new products and services to market. He transitioned from Centrify as VP Product Management where he led the Identity-as-a-Service (IDaaS) and Unified Endpoint Management product portfolio.

Swaroop Sham, Okta Senior Product Marketing Manager for Security. He recently joined Okta, bringing with him over 10 years of experience in cybersecurity. Swaroop main focus areas include Multi-factor Authentication, Adaptive Authentication, and Security Integrations.

TECHVISION
CHRYSALIS

What is This Session About?

- We have anticipated the demise of password-centric authentication for decades
  - Our position is that this future is now or at least rapidly approaching
- For the reasons we have been discussing – device and network ubiquity, reliability, Bring Your Own Device (BYOD) initiatives coupled with the accelerating levels of fraud associated with password-based authentication, the time has arrived to deploy MFA or other means of dynamically authenticating given the risk profile within your enterprise
- MFA is becoming the standard, while password-less authentication, biometrics and other advances in authentication are being explored in support of the digital enterprise

TECHVISION
CHRYSALIS®

Background

- 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 and as threats escalate, simply not good enough.
- It is a good time to consider making MFA a cornerstone of your enterprise IAM infrastructure given improved MFA vendor offerings and the inherent weaknesses of phishing-vulnerable password-based authentication.

Requiring multiple authentication factors for high risk or high-value transactions is the emerging security best practice

TECHVISION
CHRYSALIS®

Background

- MFA is a subset of the authentication market and is often evoked based on adaptive authentication or step-up authentication based on security policy and/or contextual data regarding the person requesting access
- The challenge with MFA is to balance the need for security with ease of use
  - This balance is supported by the execution of policies that build on reliable contextual data to dynamically determine when MFA is needed and when single factor authentication is sufficient
- Measuring the degree of certainty that a user is who they say they are will increase as more data from more categories are collected

The more data that are collected in support of the user's request across the four ranges of what a person knows, who they are, what they have, and their history—the greater the degree of certainty

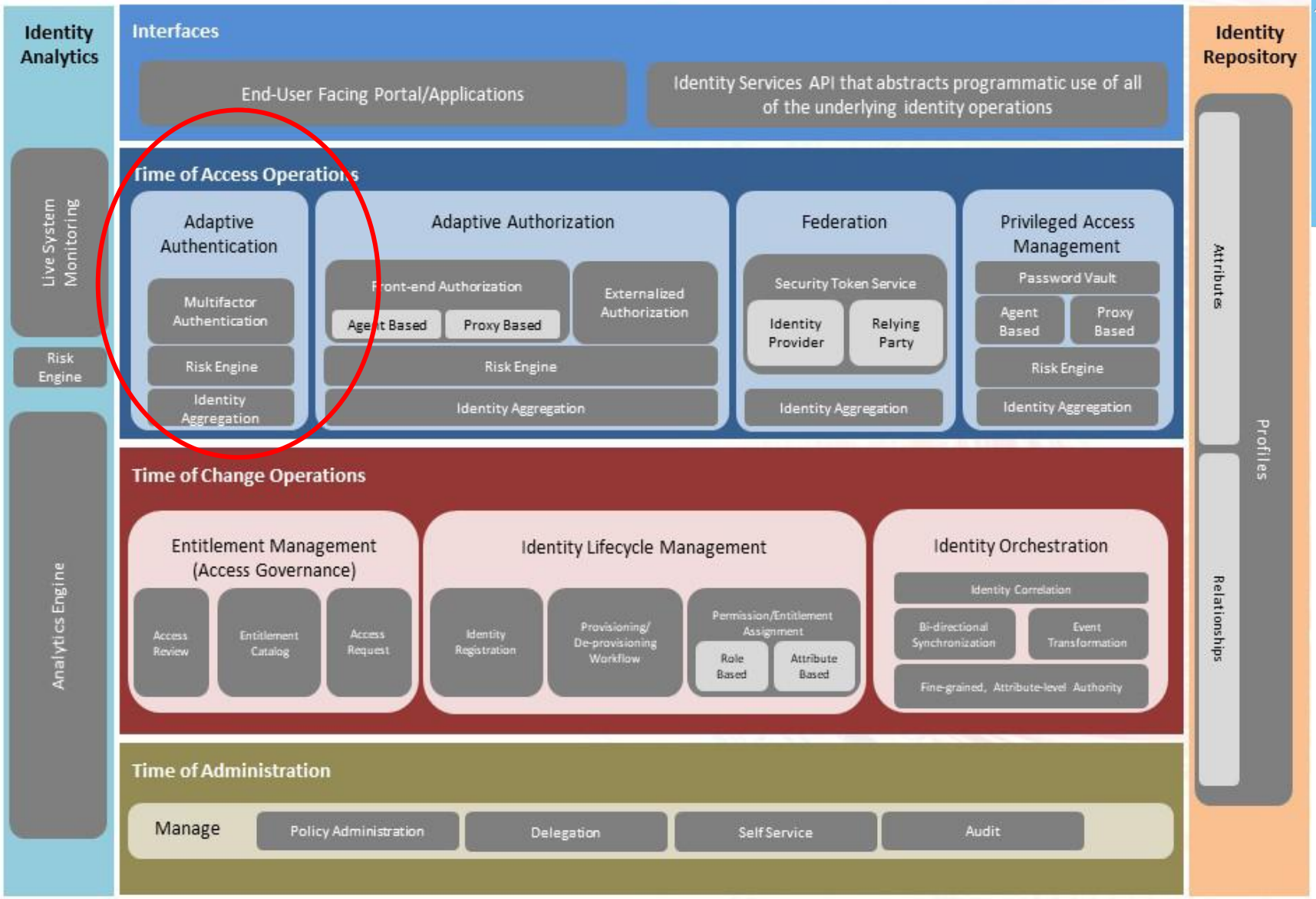
TECHVISION
CHRYSALIS®

What is MFA?

- The use of more than one set of credentials from multiple categories that are used in concert to better determine (hopefully unequivocally) that you are who you say you are
    1. Typically, one category of 'factors' is something that you know, such as a user ID and password
    2. A second factor that is added to this is often something that you have, such as a smart phone, smart card, token fob or other such unique device that when paired with the first factor (something that you know), increases the veracity of authentication
    3. A third factor can be something that you are
        - Biometrics typically fill this bill with digital representations of your face (facial recognition), fingerprint, retina scan or voice print
    4. Fourth is something that you have done
        - This can include where you have logged into from before (IP network address), recent transactions, time of day, last password reset, and flags for multiple failed login attempts

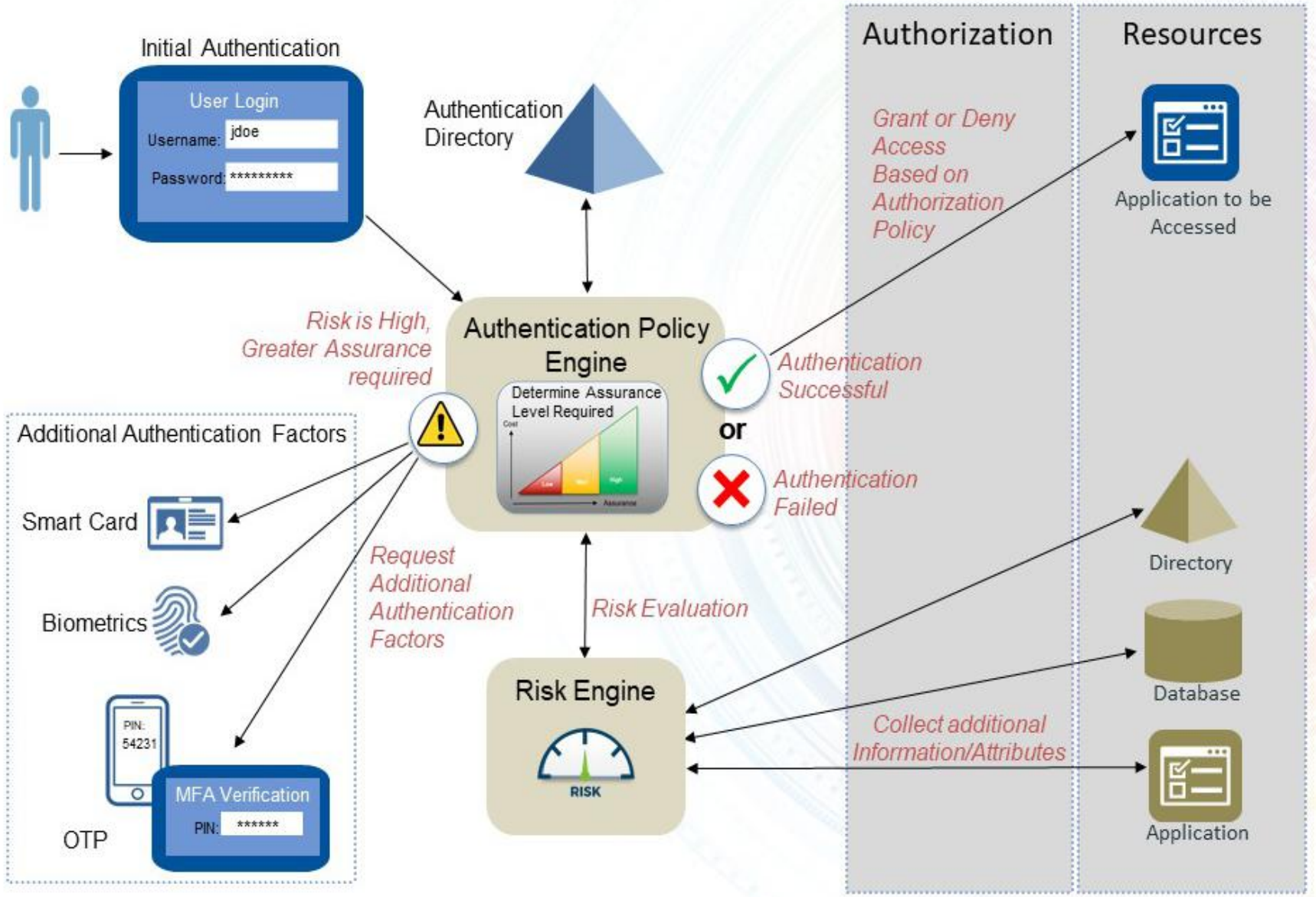
TECHVISION
CHRYSALIS®

MFA In the IAM Reference Architecture



TECHVISION CHRYSALIS®

MFA In Adaptive Authentication Pattern



TECHVISION CHRYSALIS®

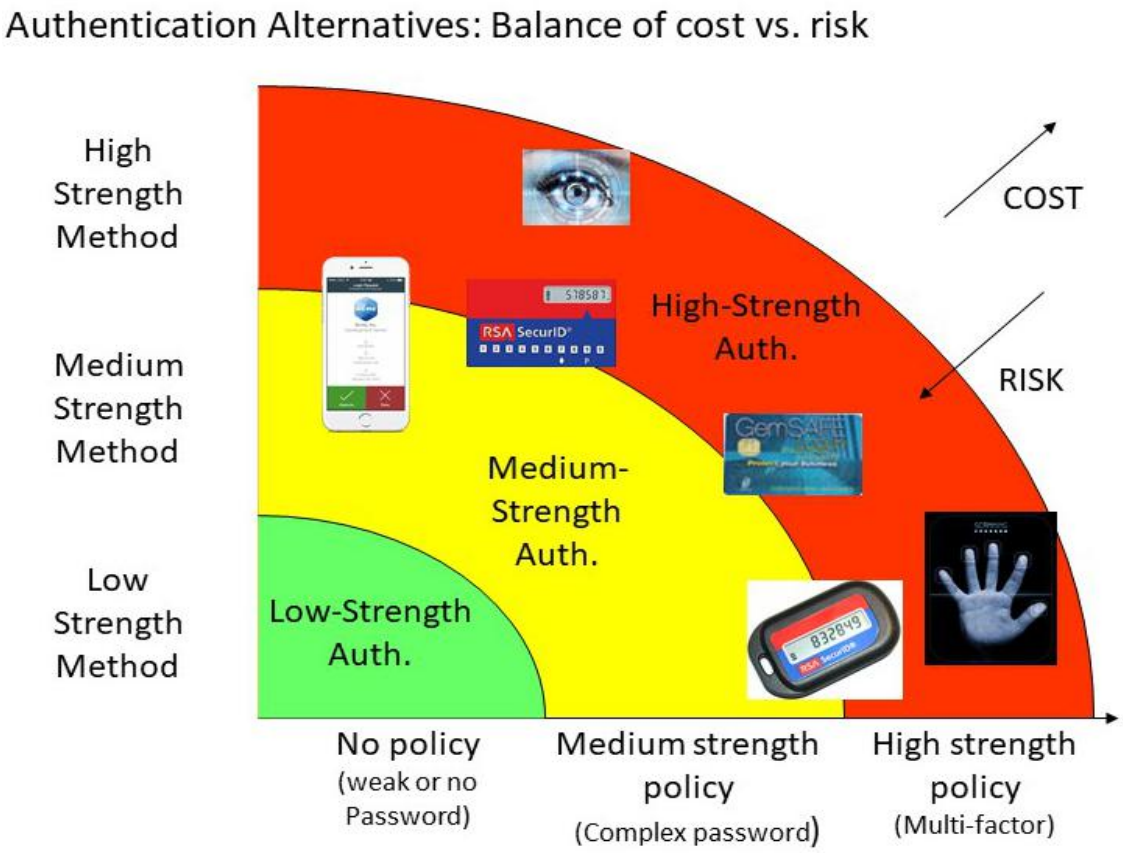
Authentication Architecture Principles

- Encompass risk-balanced user authentication to systems, networks, applications and services for the target users.
- Support a strong user experience
- Address the full range of assurance levels identified by the organization along with associated requirements
- Support MFA from a suitably wide range of devices
- Provide authentication for the organization's people, applications, devices and services regardless of platform and architecture
- Enable the organization's business processes and workflows
- Ensure compliance and mitigate IT risks
- Are easy to use, sustainable and cost-effective.
- Authenticate users for services and applications hosted both within organization's networks and external to them.

TECHVISION
CHRYSALIS®

Balancing Risk Reduction vs. Cost

- Authentication must be deployed without a well-thought-out strategy that weighs the risks, costs and usability
  - An enterprise MFA strategy must consider the association between authentication cost and risk reduction



TECHVISION CHRYSALIS®

Why MFA Now?

- With the advent of mobile device ubiquity and the willingness for end users to deploy apps on these devices, techniques such as 'mobile push' have gradually broken down the barriers of cost and complexity to deploy MFA
- As we begin re-architecting our enterprise environments to incorporate elements of Zero Trust, MFA becomes a critical piece of the ZT-puzzle
  - With the notion of 'identity as the new perimeter', it is actually "identity + device" that becomes the perimeter
  - In a ZT environment, the most critical facet of security is knowing who (or what) the end user is as well as the device being used to authenticate that user or thing

This is the new perimeter; this combination of coupling an identifier with something the user has with them (like a mobile phone)

TECHVISION
CHRYSALIS®

Don’t PUSH Me!

- Major phone vendors have helped support the MFA movement
  - For example, Apple released the Apple Push Notification service (APN) back in 2009 and less than a year later Google released its own Google Cloud to Device Messaging service (C2DM) for Android devices
- A ‘push notification’ is a message that pops up on a mobile device
  - Push notifications look like SMS text messages and mobile alerts, but they only reach users who have installed an app on the device to receive the messages
- Because the person with the phone (something they have) must be the same person logging into the online system with their UID/password (something they know), the end result is 2FA

TECHVISION
CHRYSALIS®

Don’t PUSH Me!

- Typically, the end user receiving the MFA push notification on his or her device must ‘push’ a soft button on the display that means they acknowledge the fact that they are logging into an online system
- Simply adding the requirement to provide their fingerprint (something they are) to this process-whether within the push app itself or by virtue of the smart device’s biometric capability, we can effectively deploy MFA

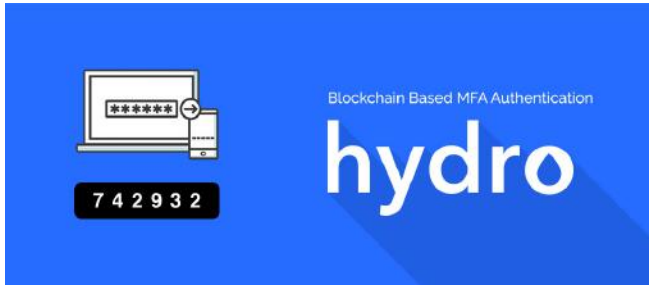
TECHVISION
CHRYSALIS®

The Future or Now? MFA and Blockchain

Furthering the development of identity solutions using blockchain and distributed ledger technology, emerging vendors are bringing MFA solutions that foster true BYOID

- ShoCard recently introduced ShoBadge, which allows identity management to be controlled by each user and shared within the workplace
  - With identification information stored on the mobile device, employees can securely share their personally identifiable information (PII) with their employer, while their information is independently verified with one way digital signatures of hashes of their data on the blockchain. The blockchain holds no PII - only verification signatures
- Drupal's now offers Hydro Raindrop MFA - its Blockchain based MFA plugin that uses a blockchain-based authentication layer

Watch This Space!



TECHVISION
CHRYSALIS®

Panel Questions

- Where is the evolution of authentication headed?
  - Do you see continuing widescale adoption of MFA?
  - What inhibits adoption and can this be overcome?
  - What do you see beyond the high-level picture I've presented here?

TECHVISION

CHRYSALIS