BCNET

Shared IT Services for Higher Education & Research

Conference 2018

Contextual Access and Multi-Factor Authentication

Lessons learned on getting past single-factor authentication!

Panelists

Corey Scholefield - Team Lead, Identity Services

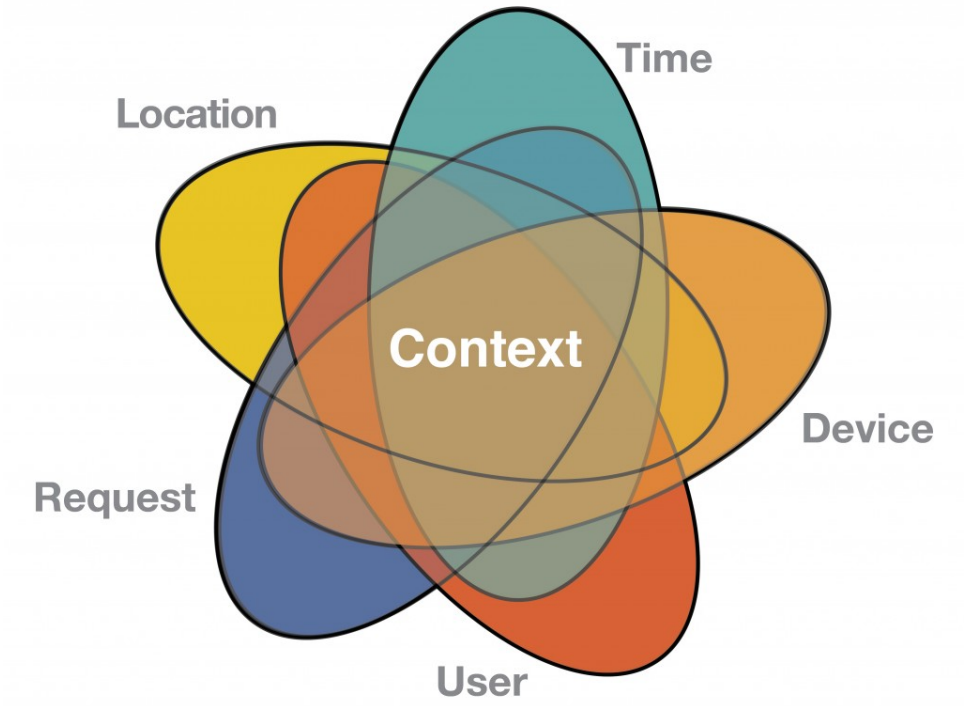
Wendy Blake – Director, Network and Technical Services

Sean Feil – Specialist, Identity, Information Technologies

Sebastian Gonzales, Sr. Mgr – Identity & Access Mgmt.

What are we talking about?

- Contextual Access Control



- Multi-factor Authentication

Meet your neighbour!

- **Meet your neighbour and discuss multi-factor authentication capability at your organization…!**
  - **Deployed or not ?**
  - **Support for or not ?**

Use Case - TRU

- **Business Drivers**
  - Restricting privileged access
  - Reduce risk of ransomware/phishing
  - PCI Compliance

Use Case - TRU

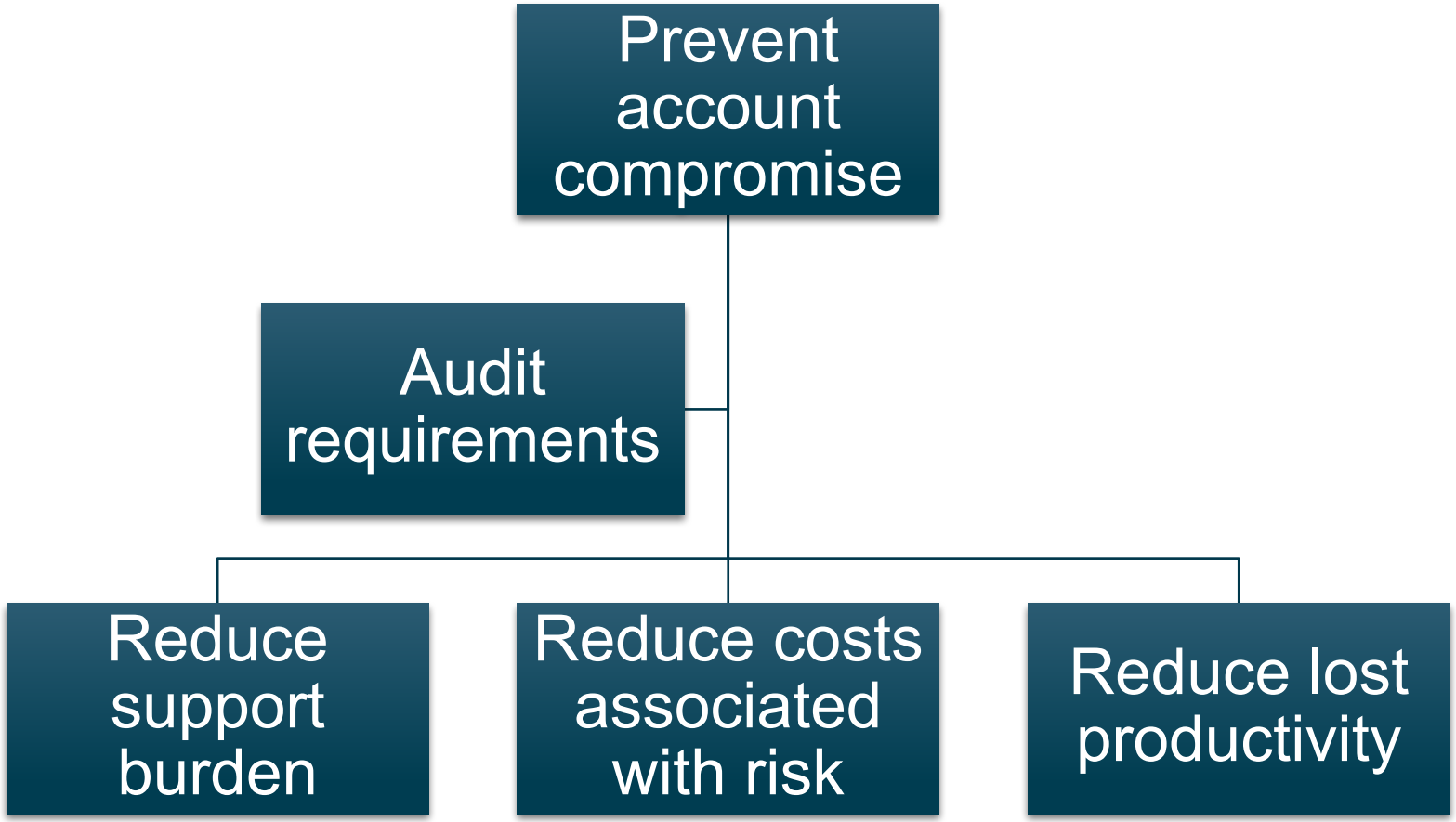
- Systems in scope for deployment
  - Primary
    - Password vault (thycotic)
    - Firewall UI (Panorama)
    - RDP to desktops (users who use VPN to access network)
  - Secondary
    - VPN
    - Servers (Linux and Windows)
    - Banner privileged accounts
      - Root/administrator accounts
      - BANSECURE named accounts
      - INB accounts

Use Case - TRU

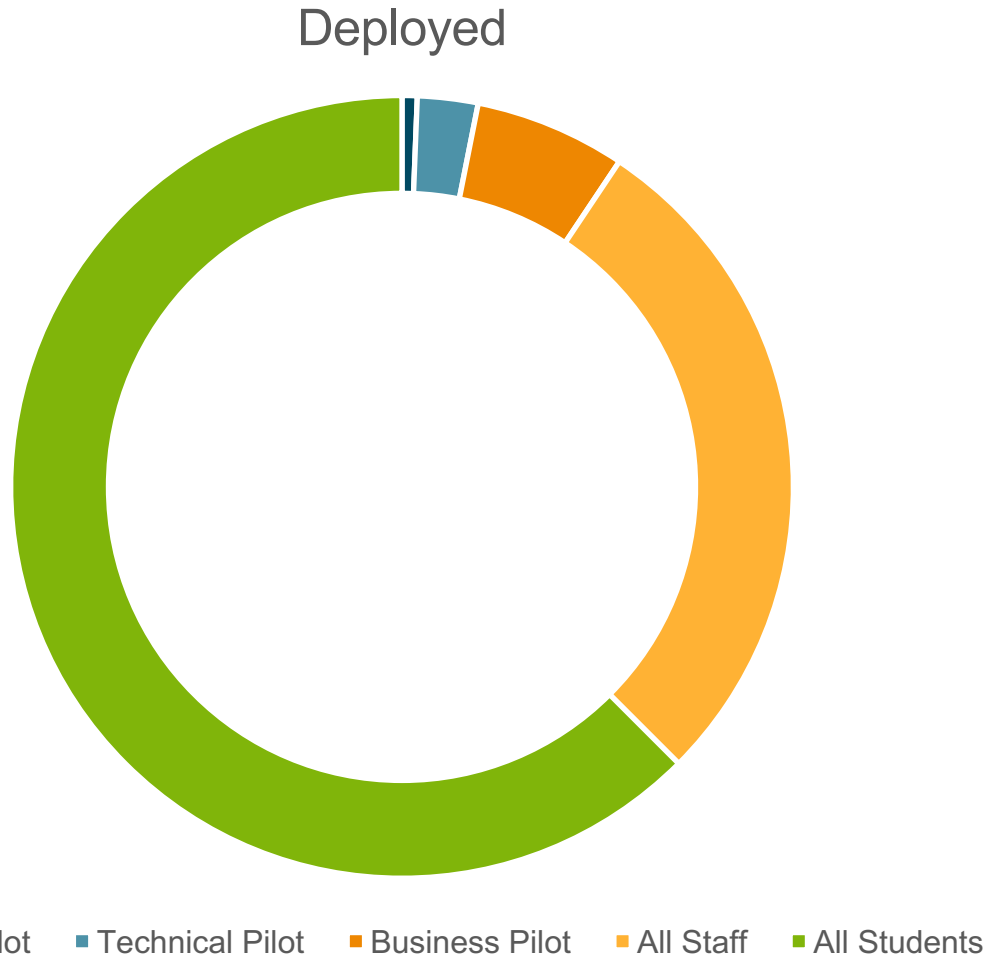
- Lessons Learned
  - Have a well defined plan
- If we knew now…..?
  - Overall we have had a good experience

Use Case - UCalgary

UCalgary – Business Drivers



UCalgary – Deployment



UCalgary – Deployment

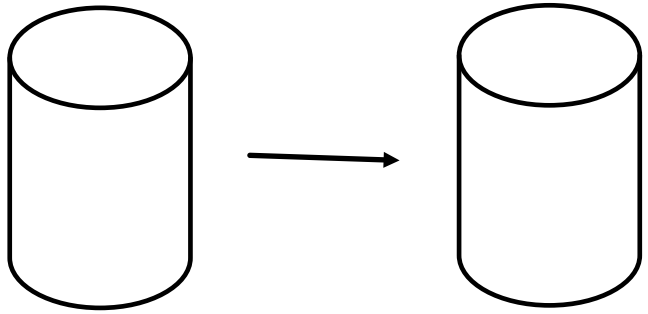
Legacy Interfaces (technical)

LDAP

SecurID native

RADIUS

CAS (custom)



New Interfaces (technical)

SAML 2

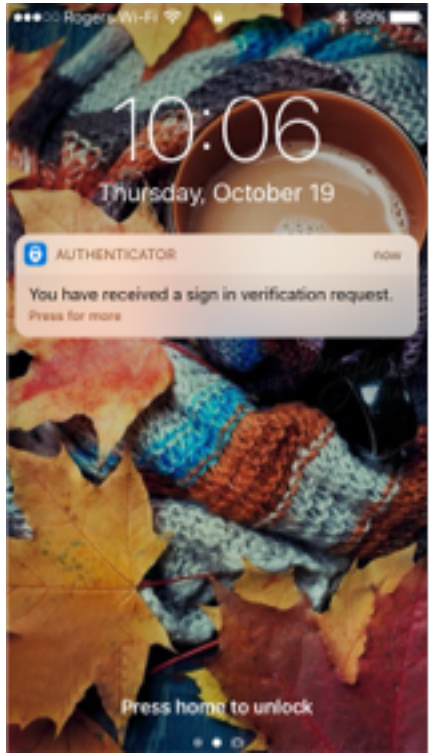
WS-FED

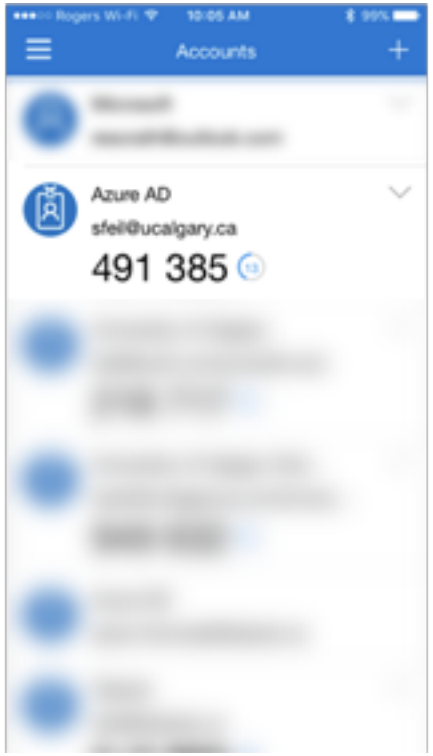
OpenID Connect

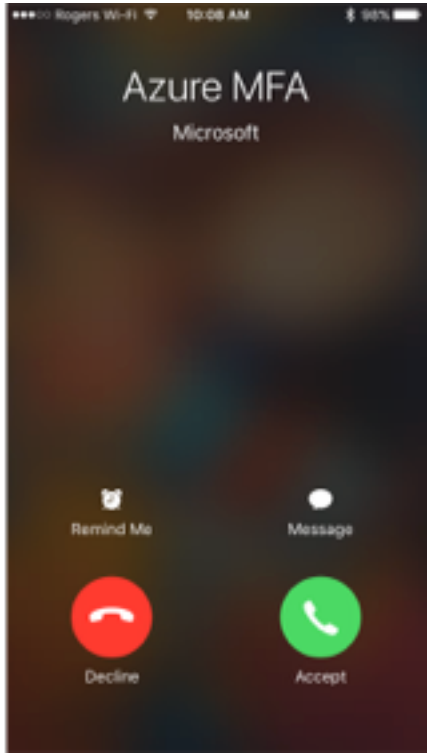
OAuth

RADIUS

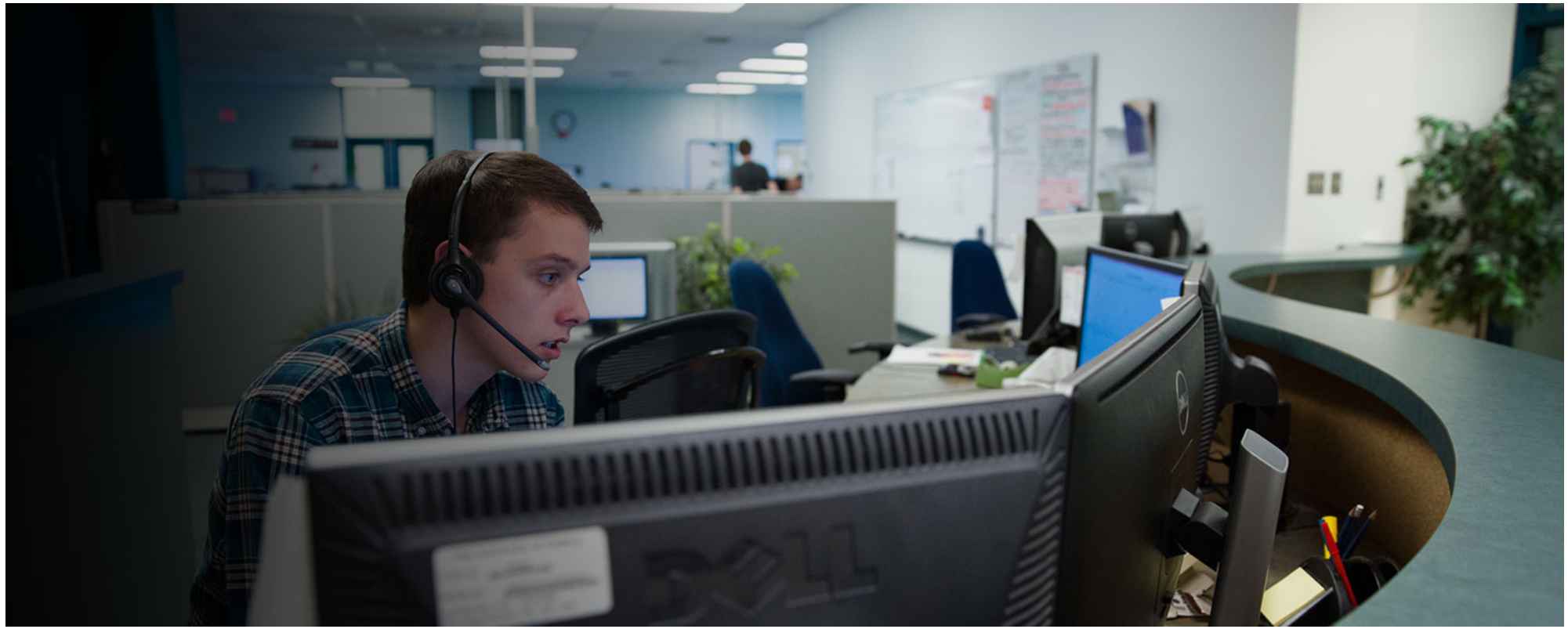
UCalgary – Deployment



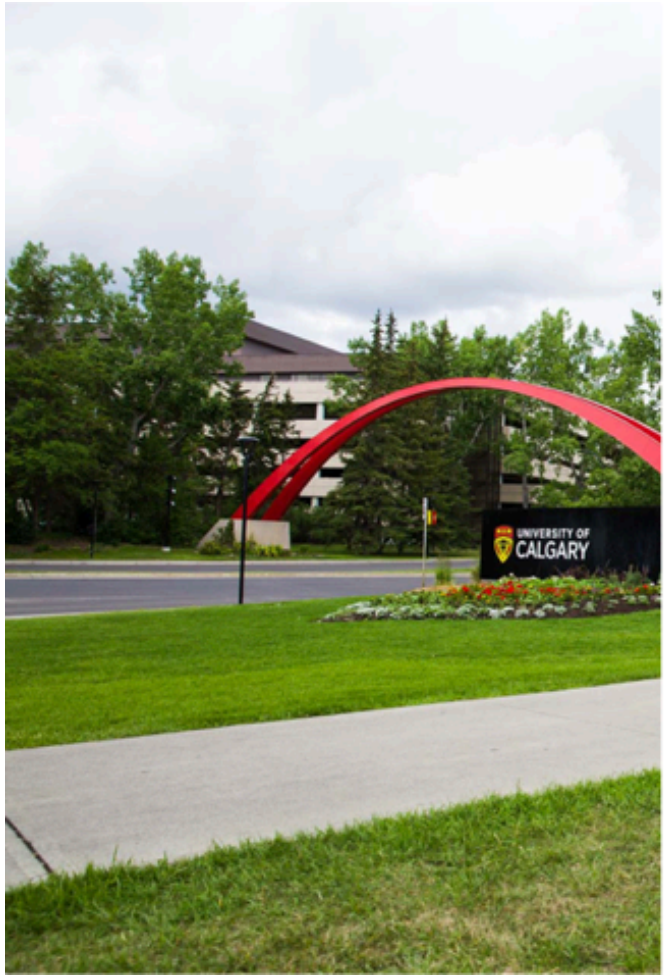




UCalgary – Lessons Learned



UCalgary – Lessons Learned



UNIVERSITY OF CALGARY

For added security, we need to further verify your account

sfeil@ucalgary.ca

Your admin has required that you set up this account for additional security verification.

Set it up now

Sign out and sign in with a different account

More information

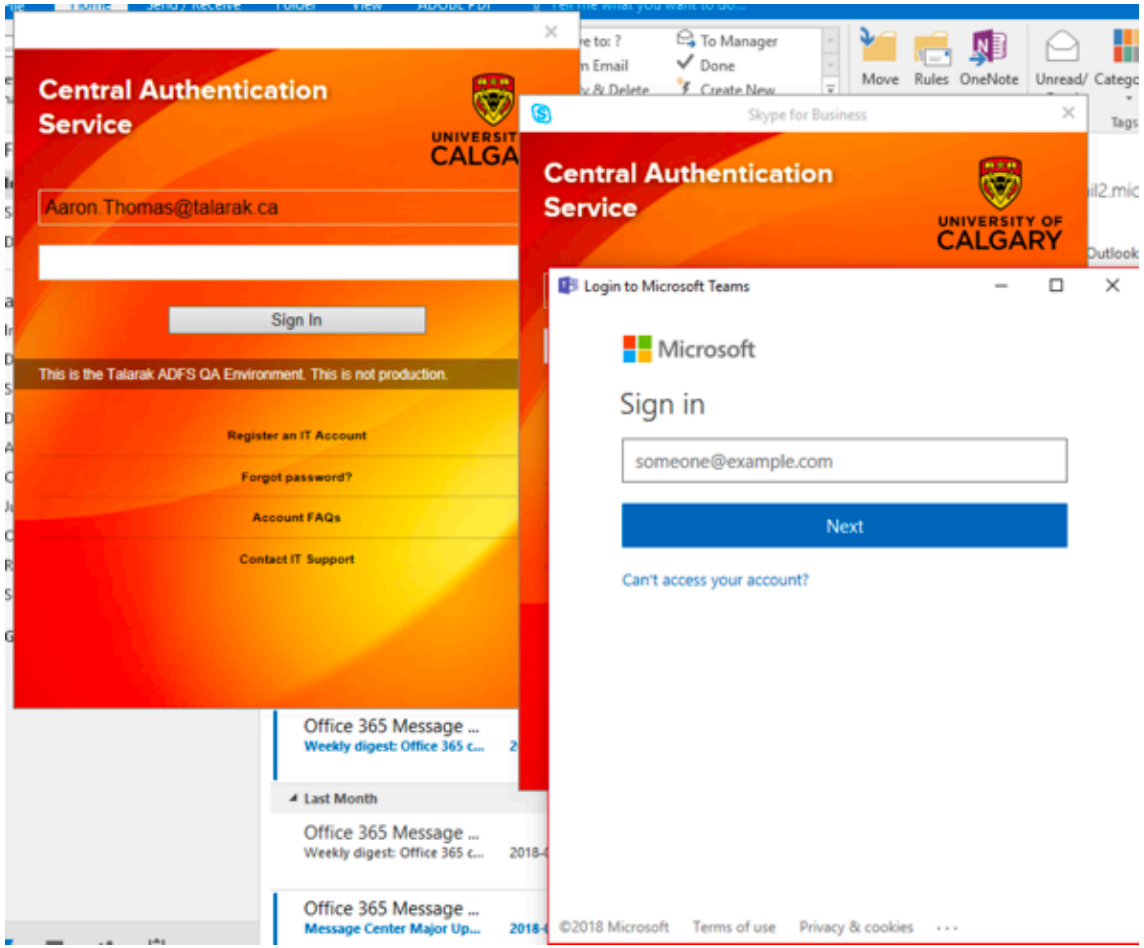
©2018 Microsoft

Terms of use Privacy & cookies

Microsoft

UCalgary – Lessons Learned

UCalgary – Lessons Learned

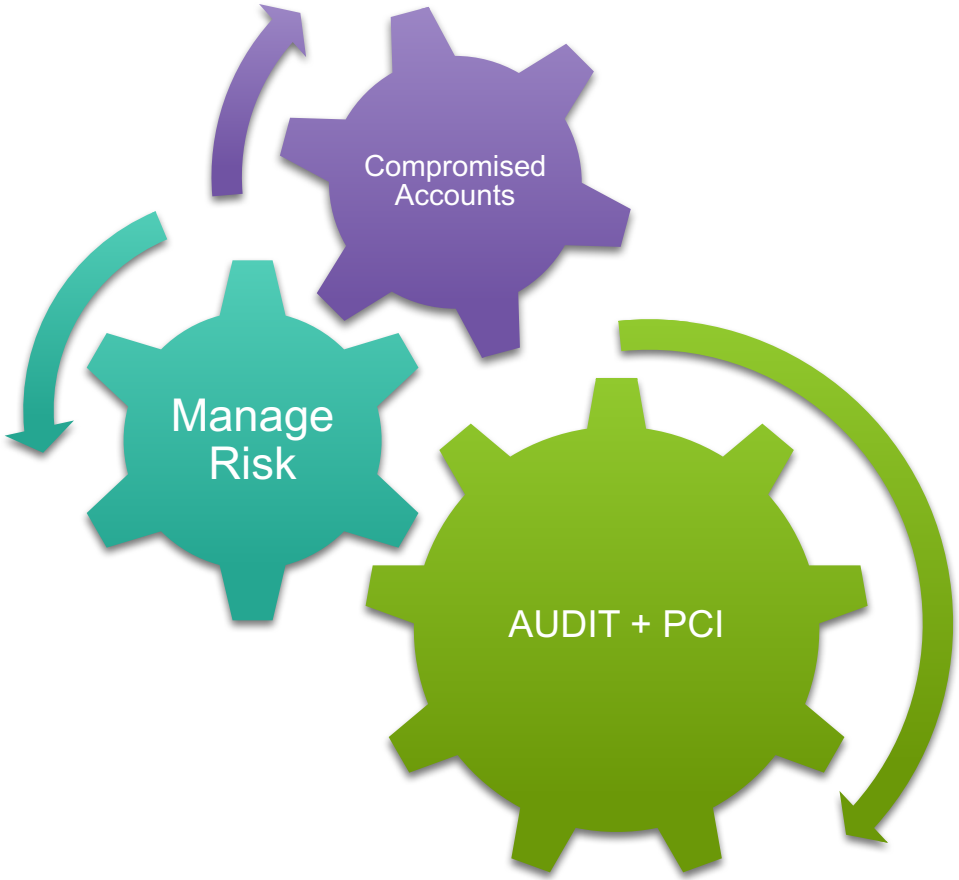


UCalgary – Lessons Learned

UCalgary – Next Steps

- Hardware token support and deployment strategy
- Deploy to remaining staff and students
- Expand systems protected by MFA
- Strengthen contextual access to reduce need for token authentication

UVic – Business Drivers



UVic – YubiKey MFA applications

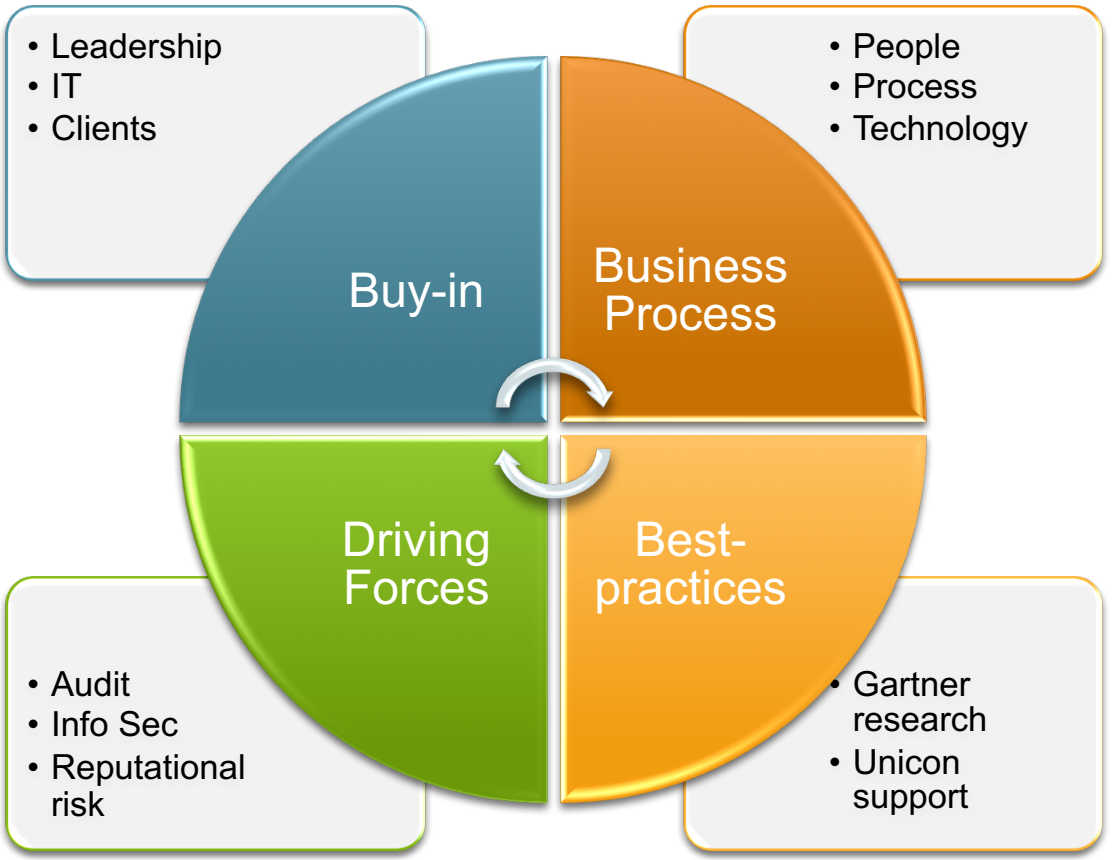
2012
- Cisco VPN – for NETS Staff

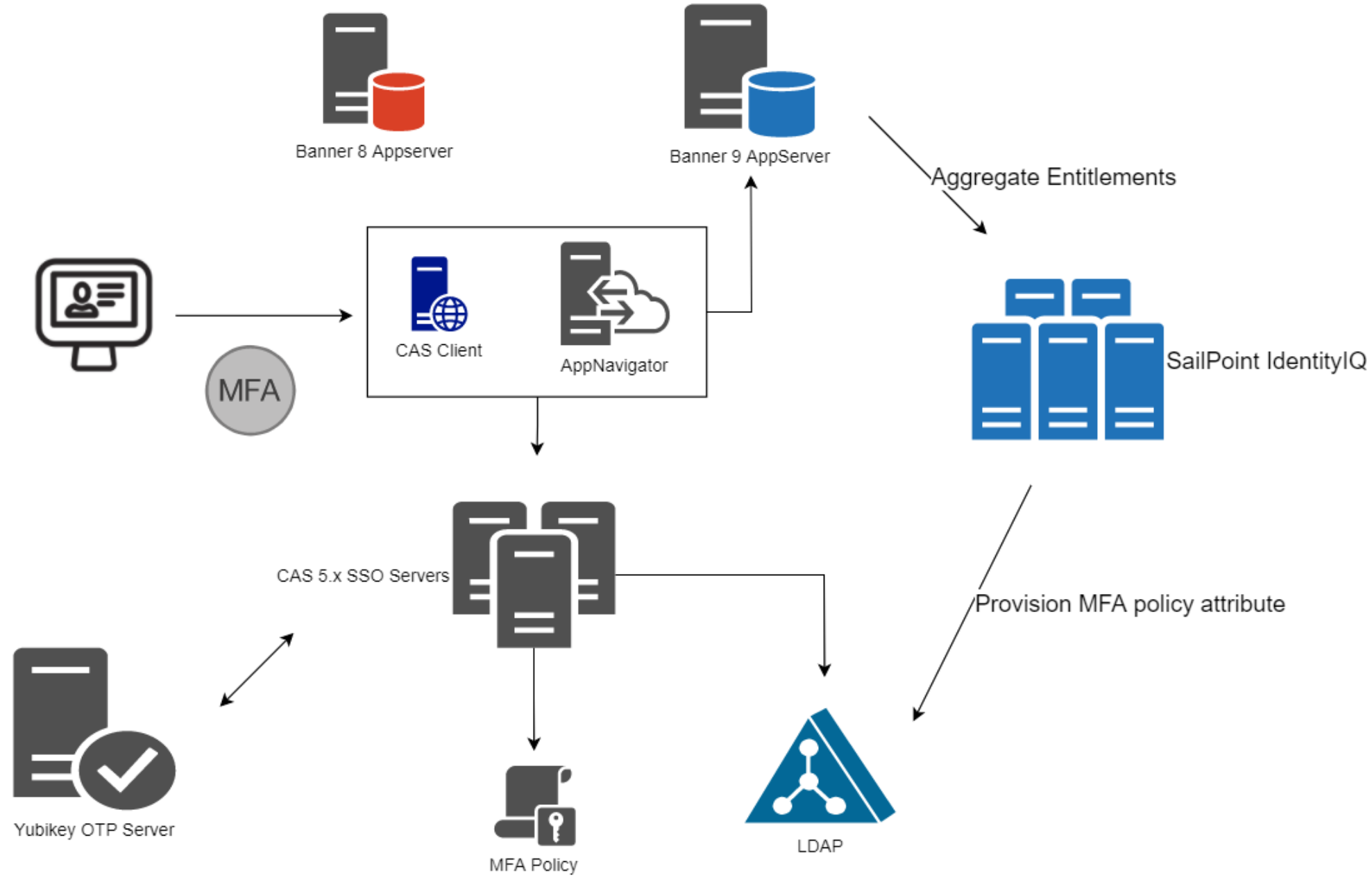
2014
- Unix Shell - for Privileged Admins

2017
- Banner 8 Forms – Finance
- On-premise Yubikey OTP Server + Key Management in IdentityIQ

2018
- VPN MFA access expanded to IT staff
- CAS 5.2 SSO + Banner 9 / AppNavigator

UVic – Lessons Learned




Banner 8 Appserver
Banner 9 AppServer
Aggregate Entitlements
CAS Client
AppNavigator
MFA
SailPoint IdentityIQ
CAS 5.x SSO Servers
Provision MFA policy attribute
Yubikey OTP Server
MFA Policy
LDAP

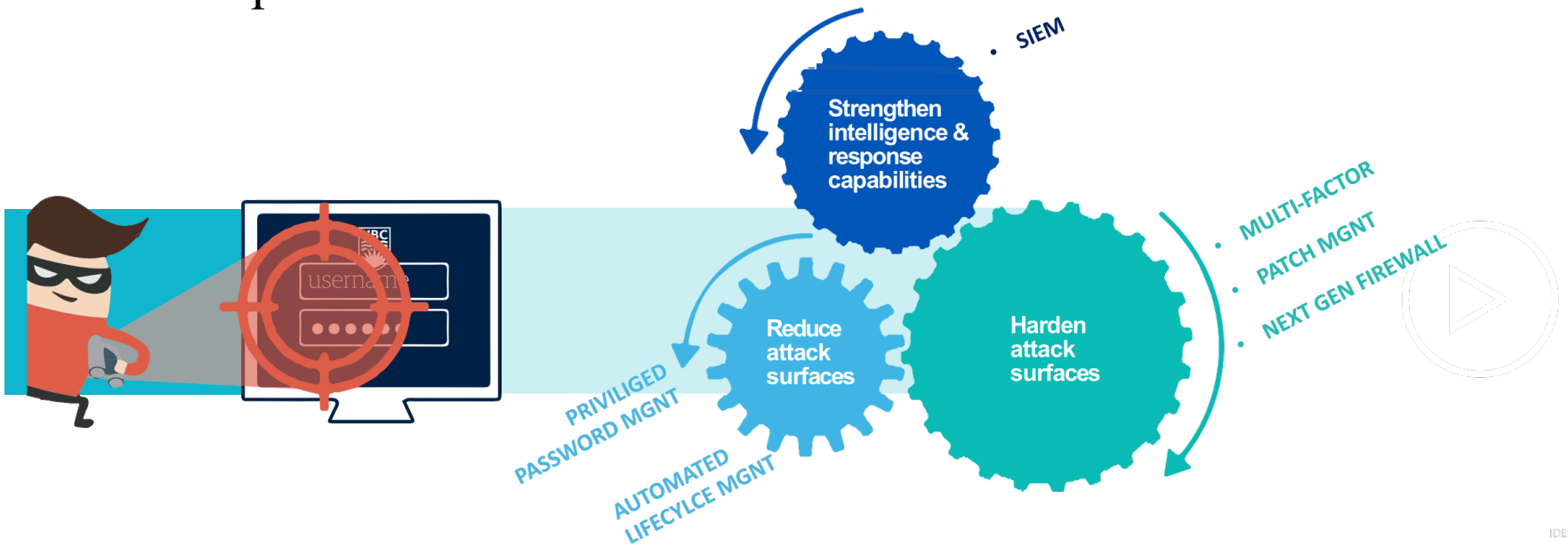
UVic – Next Steps

Use Case

- Business Drivers
- Deployment
- Lessons Learned
- If we knew now…..
- Next Steps

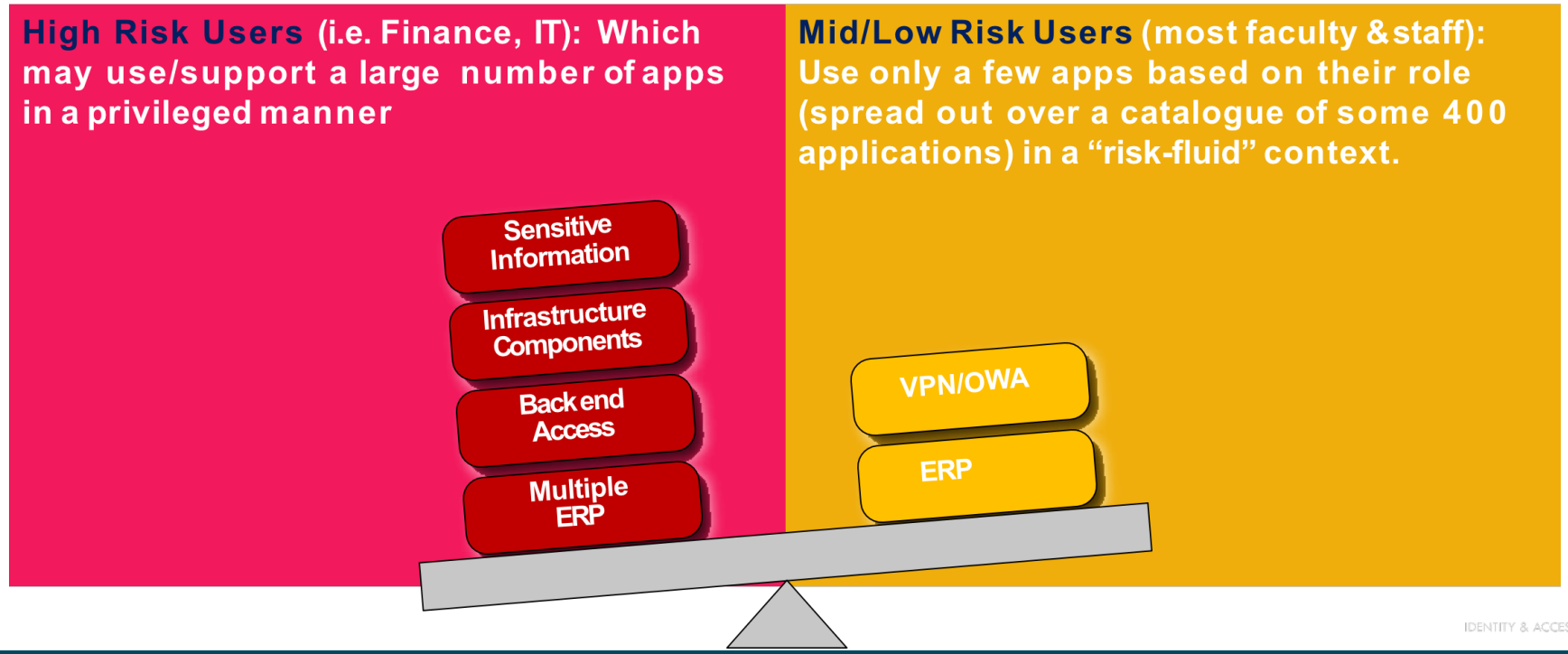
Business Drivers –
Why do we need MFA?

Part of a broader Security Strategy. Multi-factor Authentication is one of the most effective ways of protecting against the exploitation of compromised accounts.

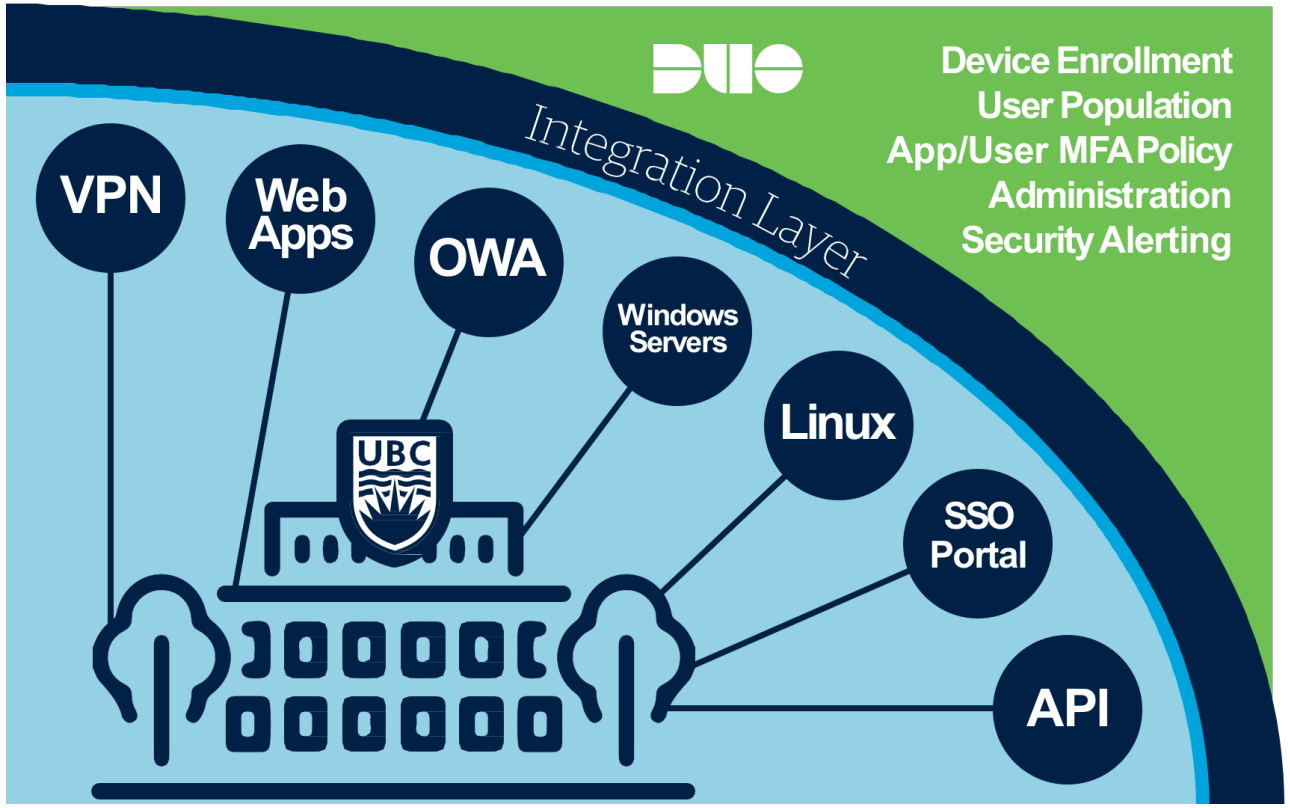


UBC Context

We are trying to solve the same problem in 2 very different arenas.



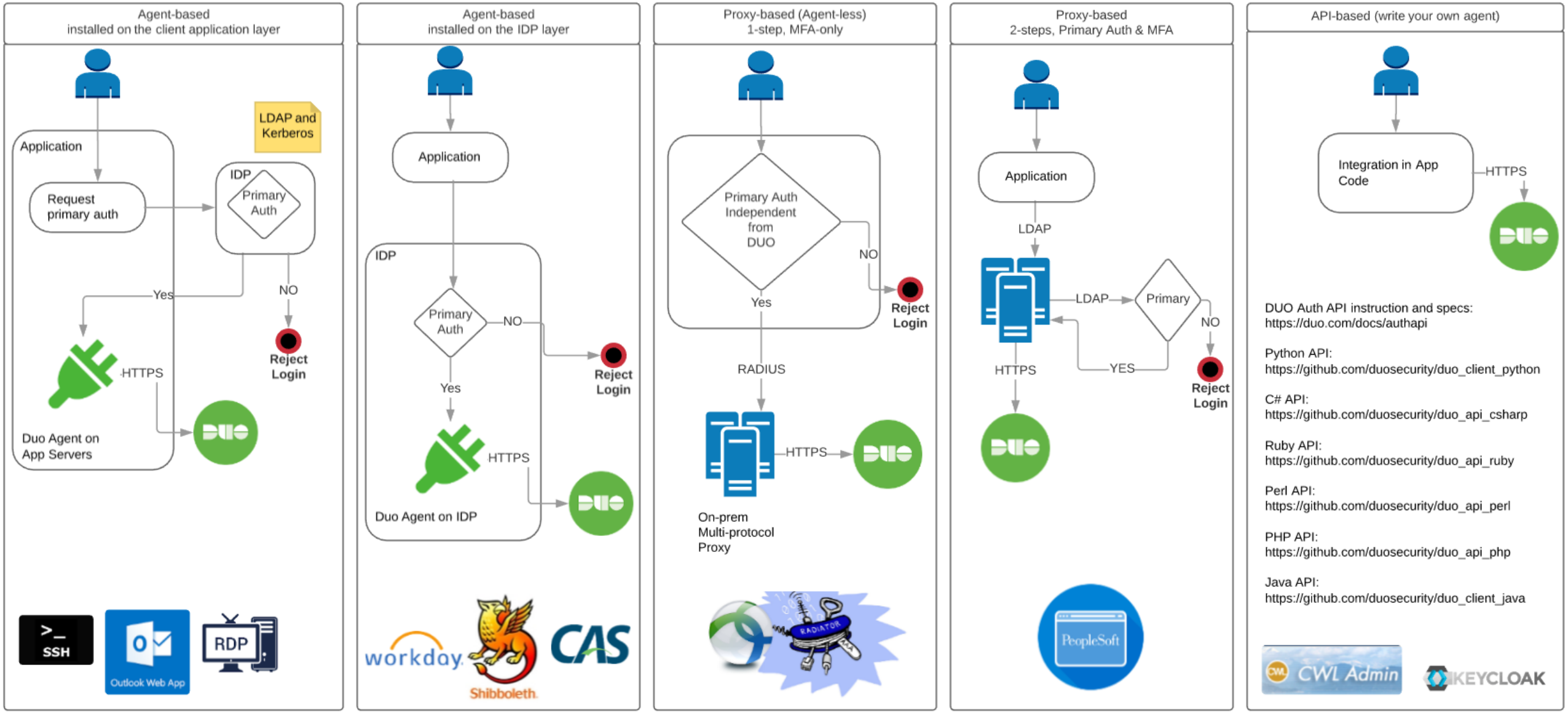
The User Experience



The ultimate goal is to protect every application that UBC supports - on-premises, in the cloud, or hybrid environment, without changing the way most users go about their day.

IDENTITY & ACCESS MANAGEMENT

MFA INTEGRATION TYPES

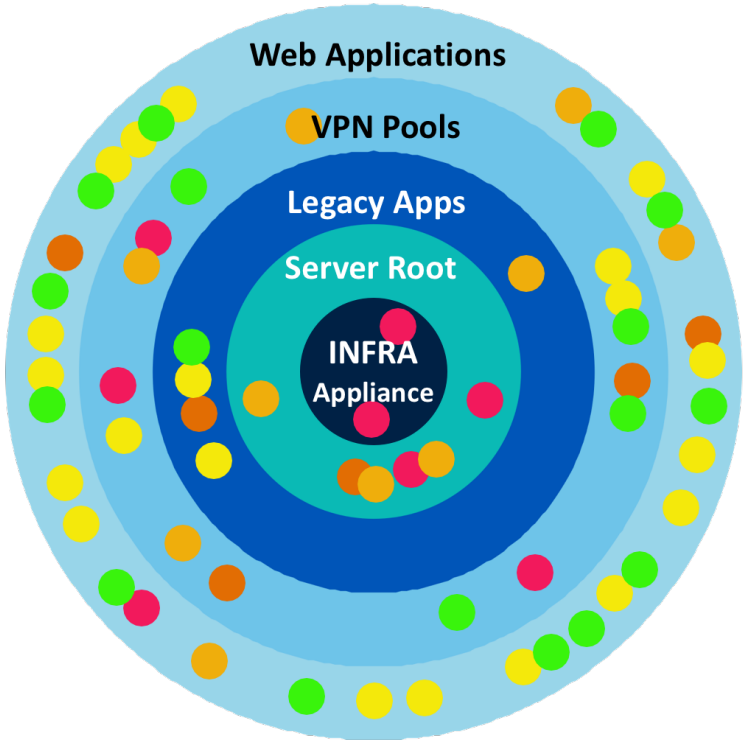


Setting Policies

To address the complexity of the UBC environment (over 400 applications across *SaaS, Shib, CAS, SAML2, Linux, Oracle, Windows, OIDC, Radius etc.*), a Risk-Based access framework needs to be used to prevent a bloated policy repository that becomes unmanageable.

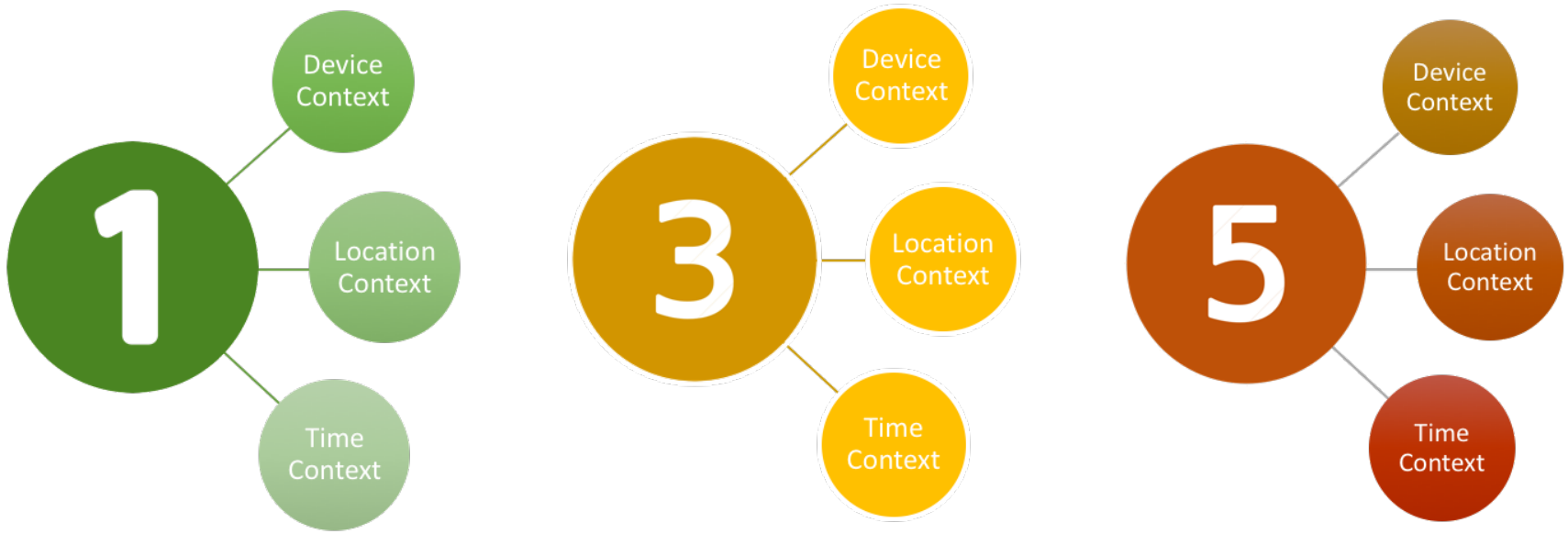
UBC'S Policy Engine allows for policies at various levels that interact with each other.

Global • Application • Groups • Users

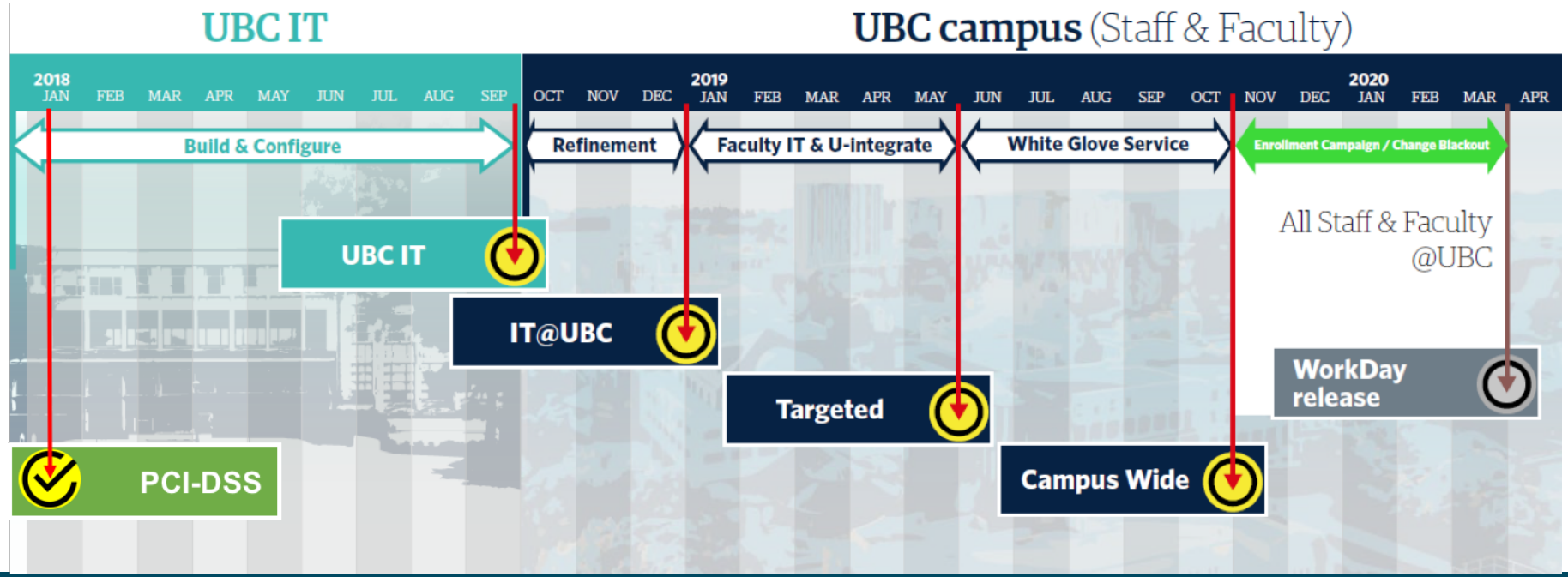


IDENTITY & ACCESS MANAGEMENT

POLICY BASED RISK RATINGS –ALLOWS FOR GREATER TRANSPARENCY AND GOVERNANCE



MFA TIMELINE



Use Case

- Lessons Learned.
  - Don’t be afraid to ask for ….
  - Some of the best support is in the communities…
  - Set a 25 min floor to present…
  - Test your communications not just your tech…
- If we knew now…..
  - Portion Control….


Q
A