Identity-First Security
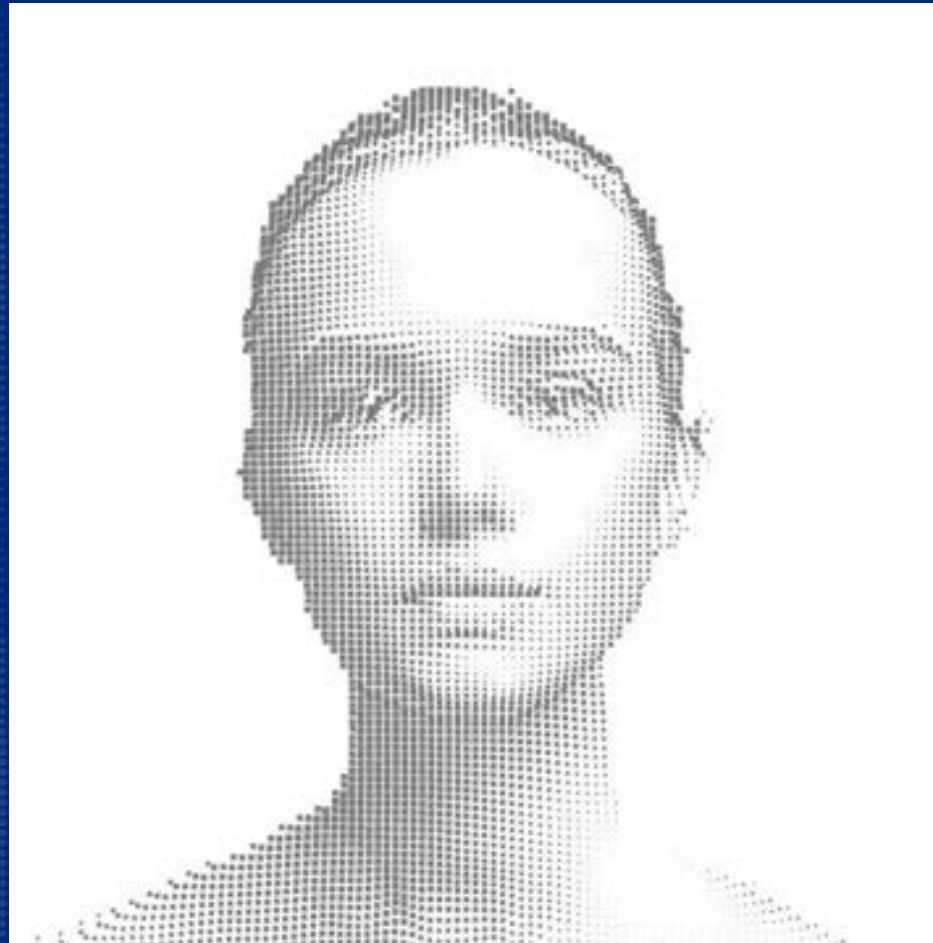## The state of Zero Trust in Asia Pacific

Kelvin Wong

Regional Head of Professional Services

Master Concept x okta
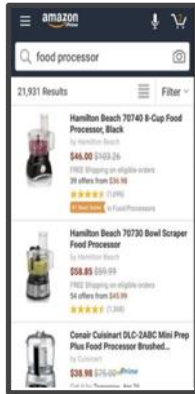
okta

The World is changing Rapidly

More and more of our lives being lived digitally....

....accessible anytime, anywhere, from any device...

... with a deeply personalized experience becoming the norm

Pandemic > Remote Work | New Website, Apps, SaaS | CyberAttack

Identity

okta

Getting Identity right is hard

83%

of consumers have abandoned a purchase or an account setup because the login process was too arduous[1]

65%

of the world's population will have its personal information covered under modern privacy regulations, up from 10% in 2020[2]

61%

of all breaches involve credentials, whether they be stolen via social engineering or hacked using brute force[3]

87%

of developers say that getting to use the SaaS components that they want and need in their apps improves their overall productivity[4]
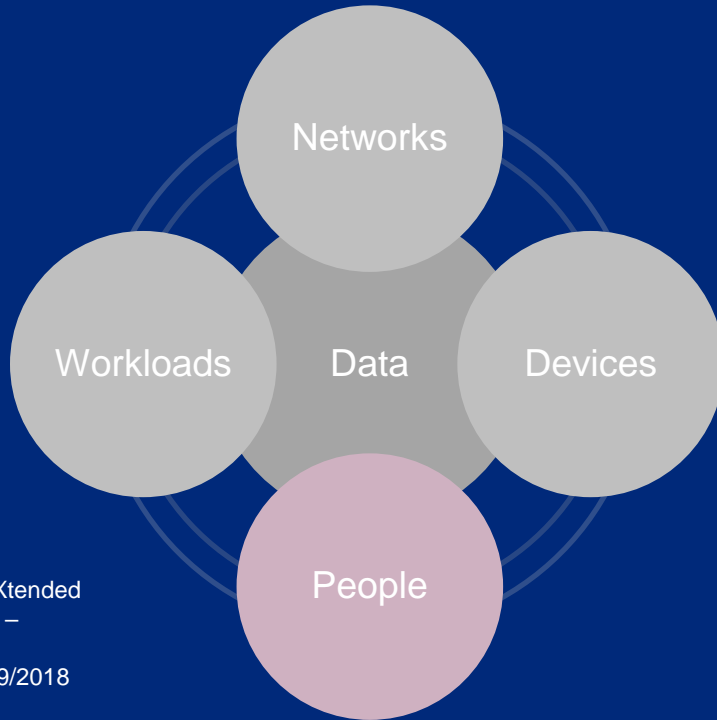
[1] Expectation vs. Reality at The Log Inn report, Auth0 in partnership with YouGov
[2] Predicts for the Future of Privacy, Gartner, 2020
[3] Data Breach Investigations Report (DBIR), Verizon, 2021
[4] How Development Teams Purchase SaaS, October 2020

okta

Forrester: Zero Trust eXtended Ecosystem

Networks

Workloads

Data

Devices
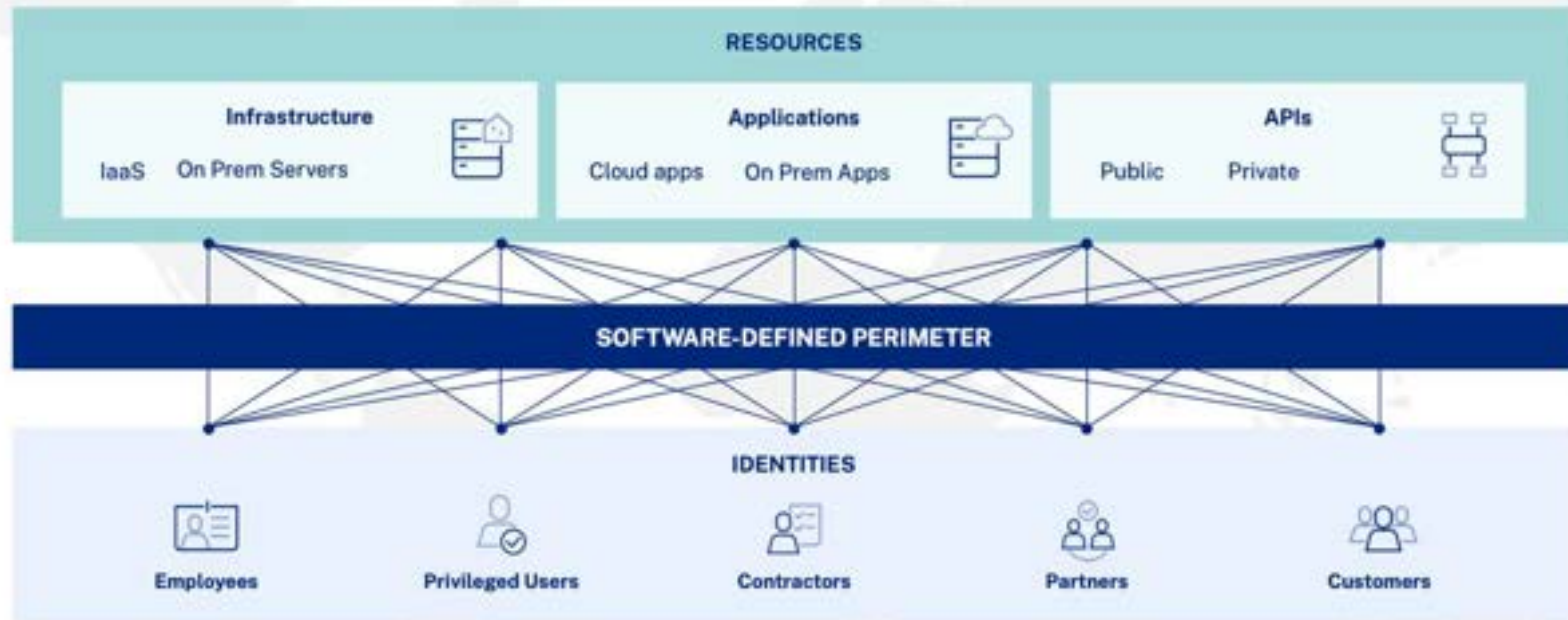
People

The Zero Trust eXtended (ZTX) Ecosystem – Forrester, Chase Cunningham, 1/19/2018

"...move away from a failed perimeter-centric approach... to a model that was much more data and identity-centric..."

okta

Cloud, Mobile Have Dissolved the Network Perimeter

RESOURCES

Infrastructure	Applications	APIs
IaaS On Prem Servers	Cloud apps On Prem Apps	Public Private

SOFTWARE-DEFINED PERIMETER

IDENTITIES

Employees Privileged Users Contractors Partners Customers

Zero Trust Reference Architecture

IDENTITY

User Identity + Device Identity

ACCESS

Risk Score

Policy

AuthZ Engine

CONTEXT

Third Party Context

User
Device
Location
Application
Network

User
Device
Location
Application
Network

RESOURCES

SAML, WS-FED. LDAP, RADIUS

Kerberos, Header-based

OAuth

SSH/RDP

Apps

APIs

Infrastructure

aws   Google Cloud Platform   Microsoft Azure

Cloud

On-Prem

ANALYTICS & ORCHESTRATION

splunk>   exabeam

DEMISTO   Phantom

QRadar

okta

Contextual Access Management

App Context

User Context

Network Context
- New IP
- Specified IP Zones
- Network anonymizers

Device Context
- Known device
- Managed device
- Registered device
- Secure device

Location Context
- New city/state/country
- New geo-location
- Impossible travel

Contextual Response
- Allow access
- Deny access
- Prompt for 2nd factor
- Passwordless Auth

← Risk level →

Secure & Frictionless Customer Experience

Okta make Identity Easier

Workforce and External Identity

Workforce and External Identity

Workforce and External Identity

Accelerate revenue and business outcomes

Tailored registration and sign-in user experiences

Reduced friction while maintaining user trust

Integration with marketing and sales platforms

Reduce security, compliance, and availability risks

Automatic protections against account takeovers

"Always on" and secured SaaS platform

Assistance with compliance and data residency requirements

Faster time to market

Less effort and time to add AuthN and AuthZ to apps and services

Simplified user lifecycle management

Reduced manual efforts with no/low code automation

okta

Less friction with social logins

What is it?

- **Out-of-the-box integrations for SSO with existing services**
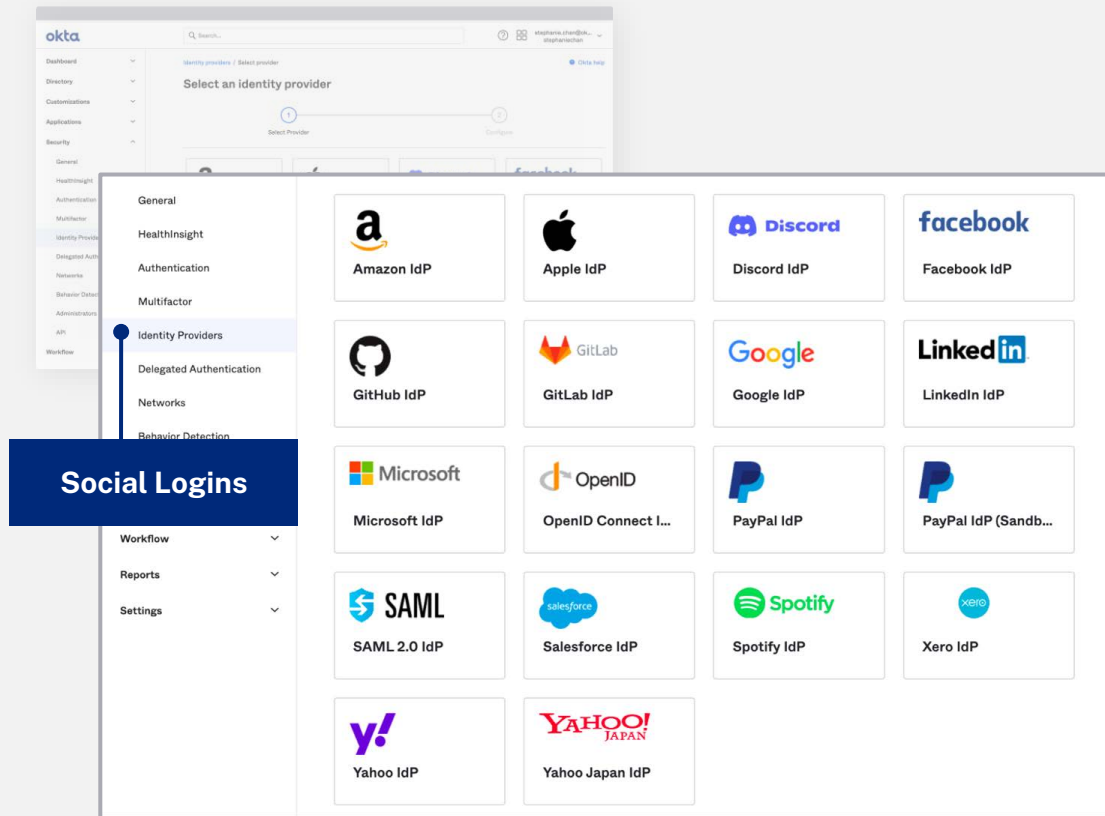
    Form of SSO that uses existing information from a service, available through Okta's social IdP catalog in the OIN

Why is it important?

- **Seamless sign-up & sign-in**

    Quickly sign up and/or sign in to apps without entering email addresses or creating a new password

    Less friction and less login details for end users to manage when using a new app or service

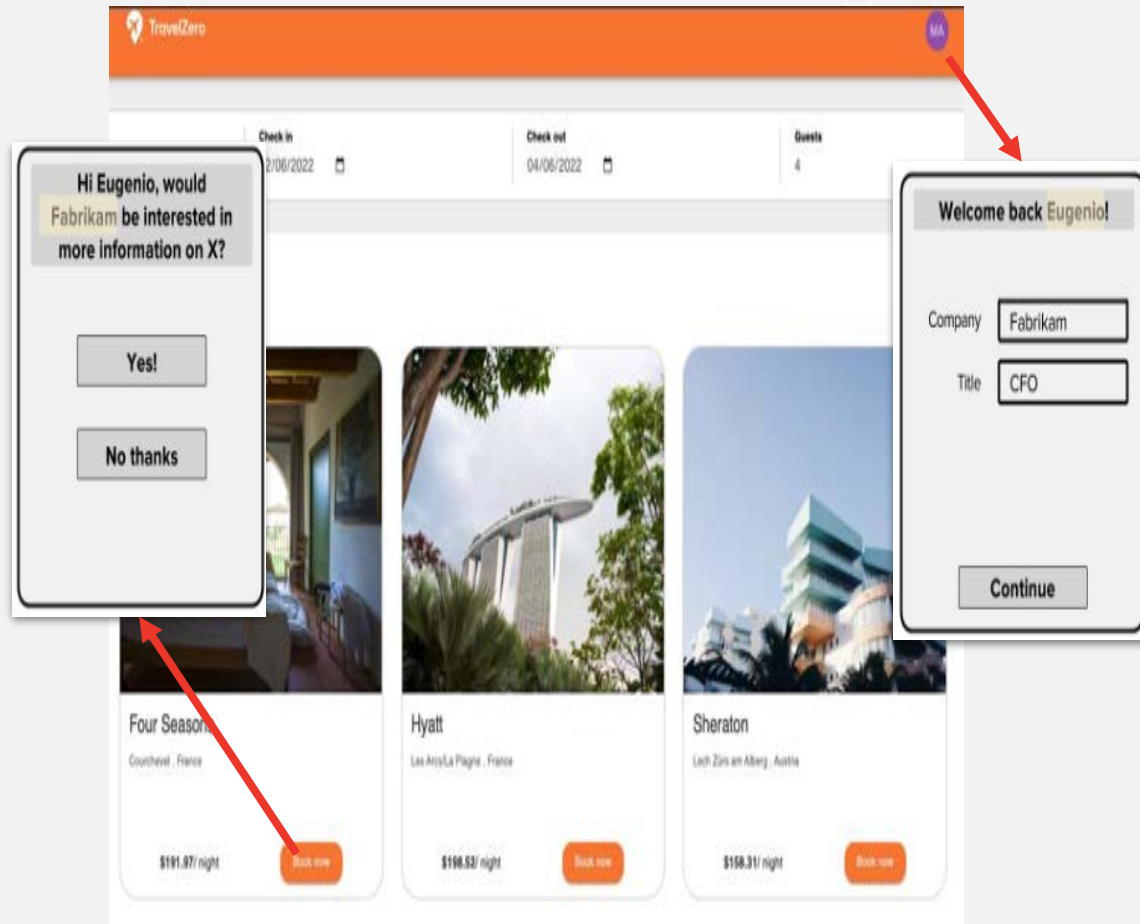okta

Progressive enrollment

What is it?

- **Phased onboarding and data collection for business verification**

  Capture additional information as external identities progress through the application and lifecycle

Why is it important?

- **Prioritize frictionless experiences and security**

  Reduce complexity and tediousness in user flows that hinder successful onboarding and completed tasks

okta
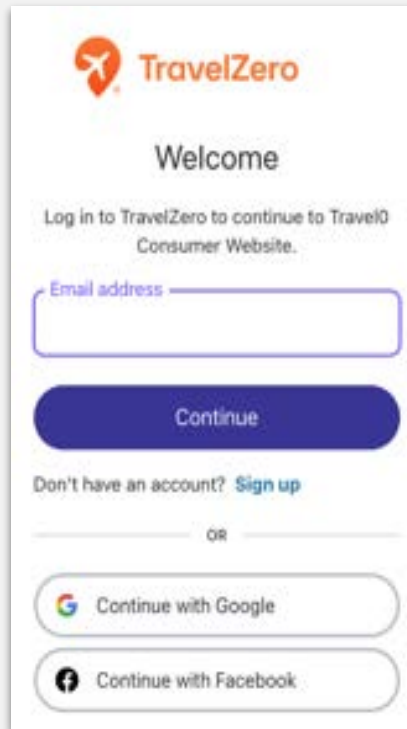
Extensibility Function

What is it?

- **Secure, tenant-specific, versioned functions written in Node.js**

  Execute at certain points during the authentication pipeline, used to customize and extend Okta capabilities with custom logic.
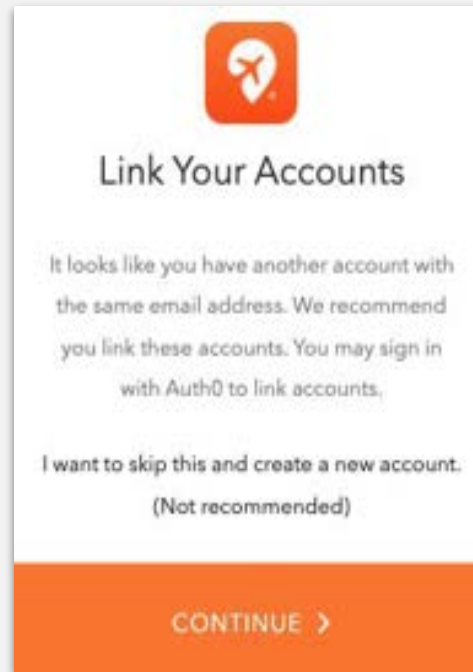
Why is it important?

- **Serverless extension to authentication pipeline**

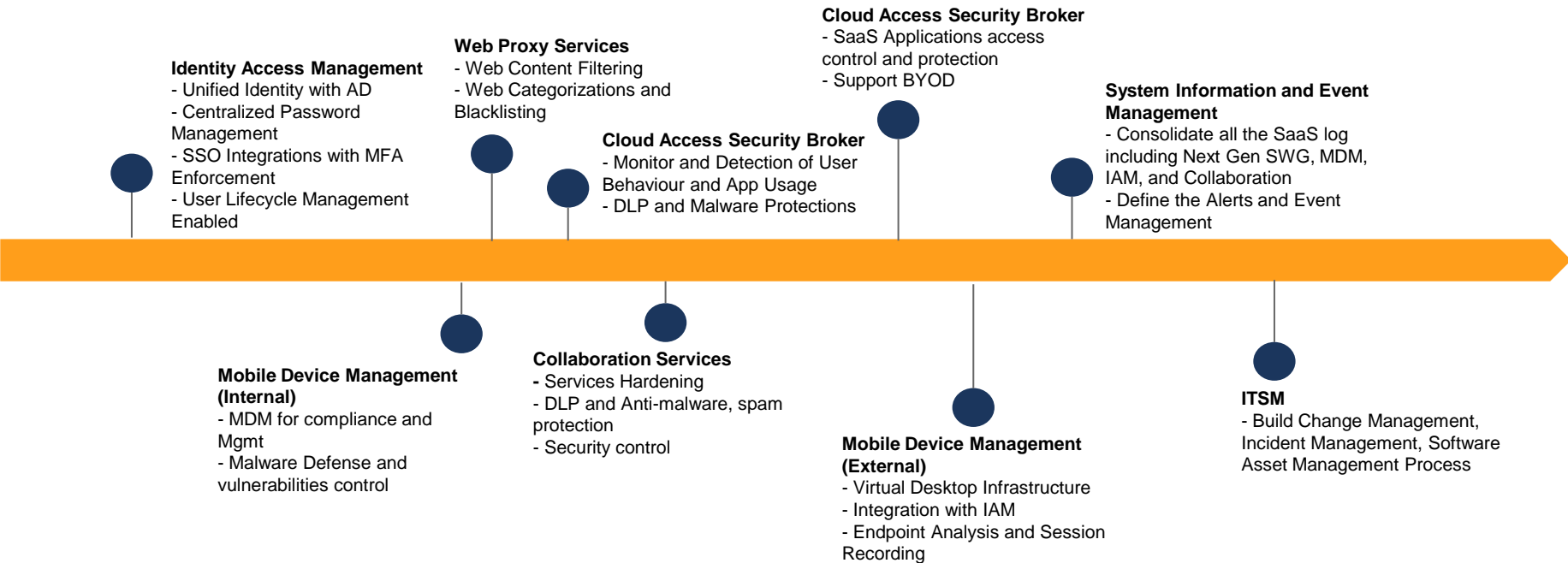 Serverless environment so developers just have to code and not worry about building and maintaining another stack

okta

Where to start?

Identity Access Management
- Unified Identity with AD
- Centralized Password Management
- SSO Integrations with MFA Enforcement
- User Lifecycle Management Enabled

Web Proxy Services
- Web Content Filtering
- Web Categorizations and Blacklisting

Cloud Access Security Broker
- Monitor and Detection of User Behaviour and App Usage
- DLP and Malware Protections

Cloud Access Security Broker
- SaaS Applications access control and protection
- Support BYOD

System Information and Event Management
- Consolidate all the SaaS log including Next Gen SWG, MDM, IAM, and Collaboration
- Define the Alerts and Event Management

Mobile Device Management (Internal)
- MDM for compliance and Mgmt
- Malware Defense and vulnerabilities control

Collaboration Services
- Services Hardening
- DLP and Anti-malware, spam protection
- Security control

Mobile Device Management (External)
- Virtual Desktop Infrastructure
- Integration with IAM
- Endpoint Analysis and Session Recording

ITSM
- Build Change Management, Incident Management, Software Asset Management Process

okta