RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: PART3-W02

Zero Trust for the Real World

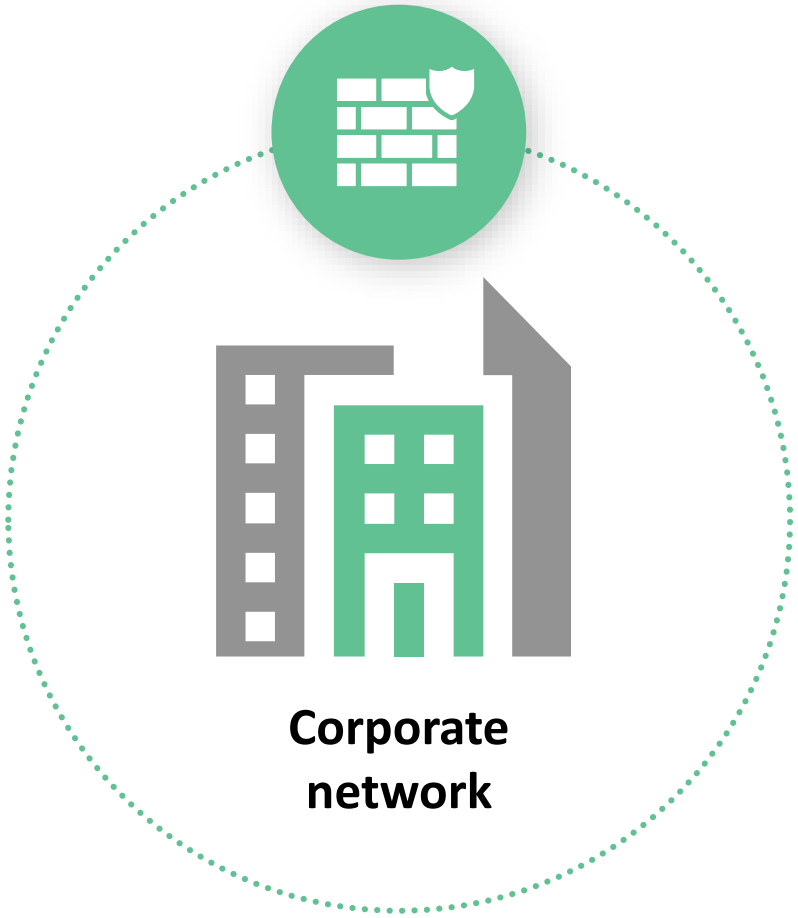
Nupur Goyal

Zero Trust Product Strategy
Microsoft
@nupur_11

Carmichael Patton

Zero Trust Security Architect
Microsoft / Digital Security, Risk, and Engineering
@Xanlythe

Traditional Model

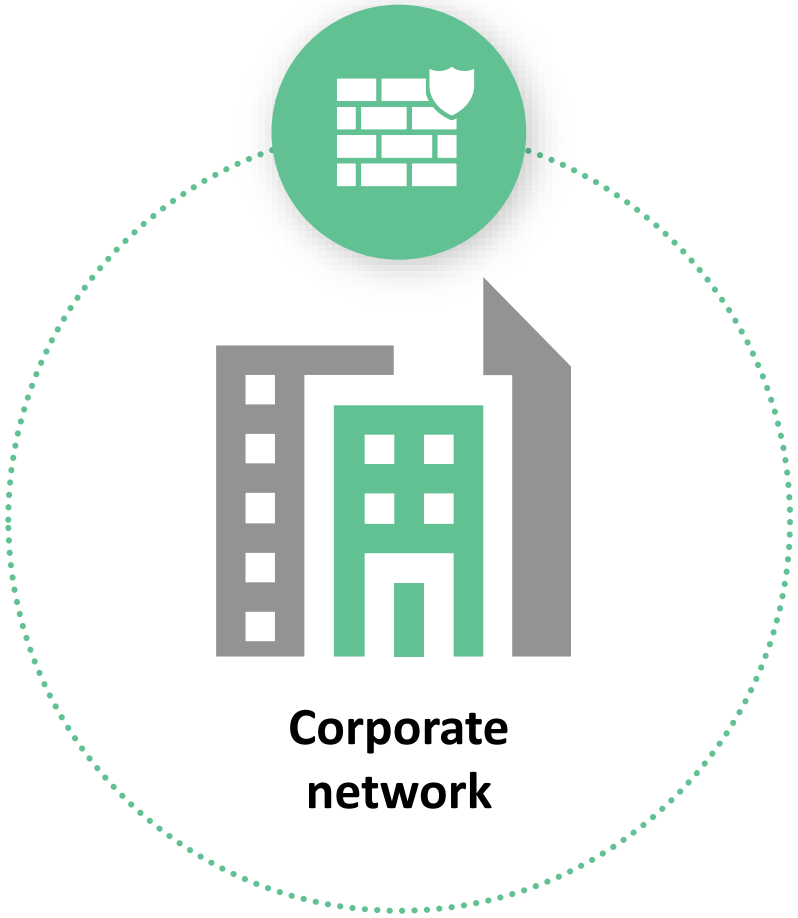


Users, devices, apps, and data protected behind a DMZ/firewall

Digital Transformation

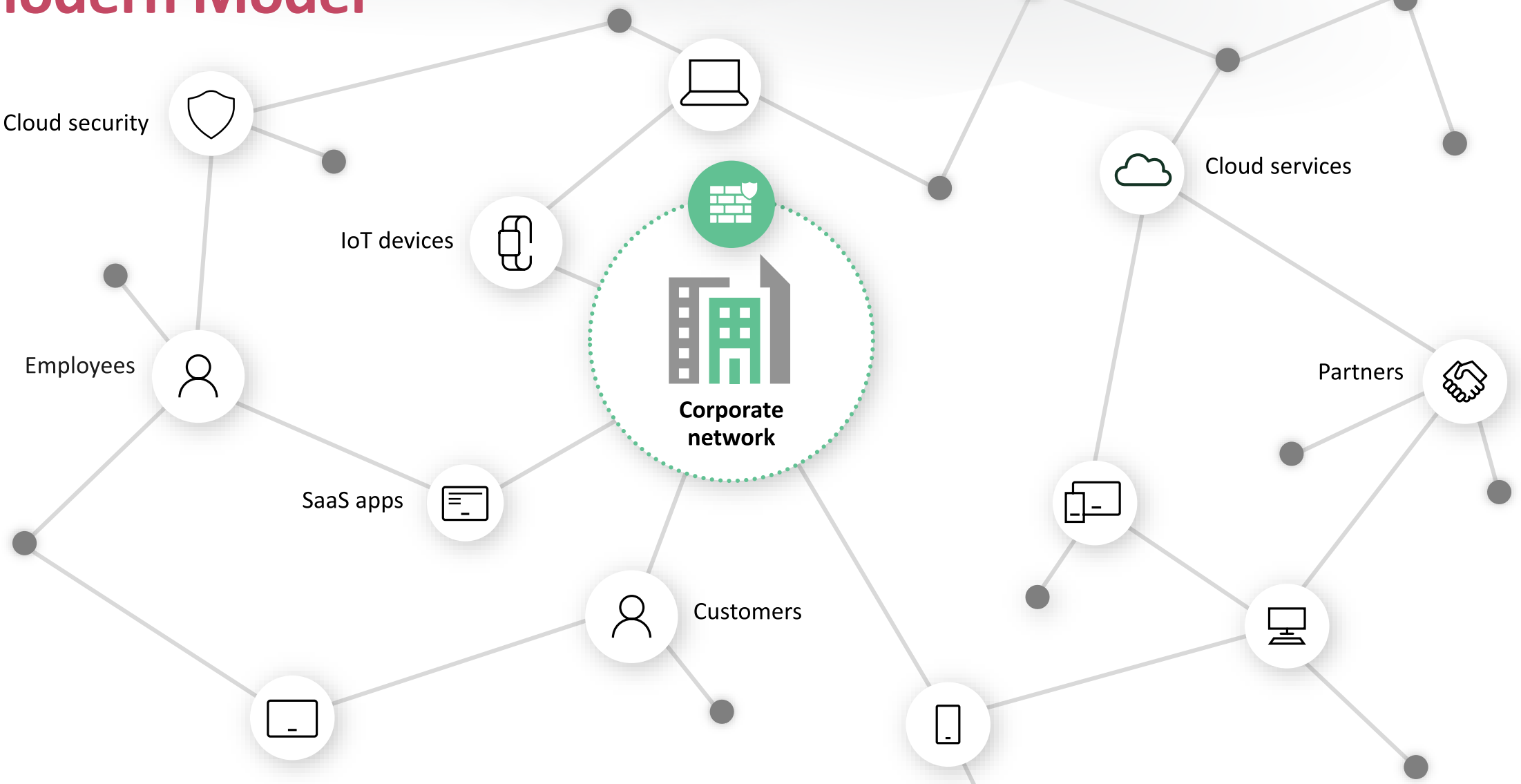
2000	2002	2007	2009	2011
Salesforce SaaS launched	Starbucks puts wifi in stores	iPhone	FITBIT Tracker	Office 365 launched

Traditional Model



Users, devices, apps, and data protected behind a DMZ/firewall

Modern Model



The world has changed

94% of organizations using cloud

5.2 mobile business apps accessed daily by employees

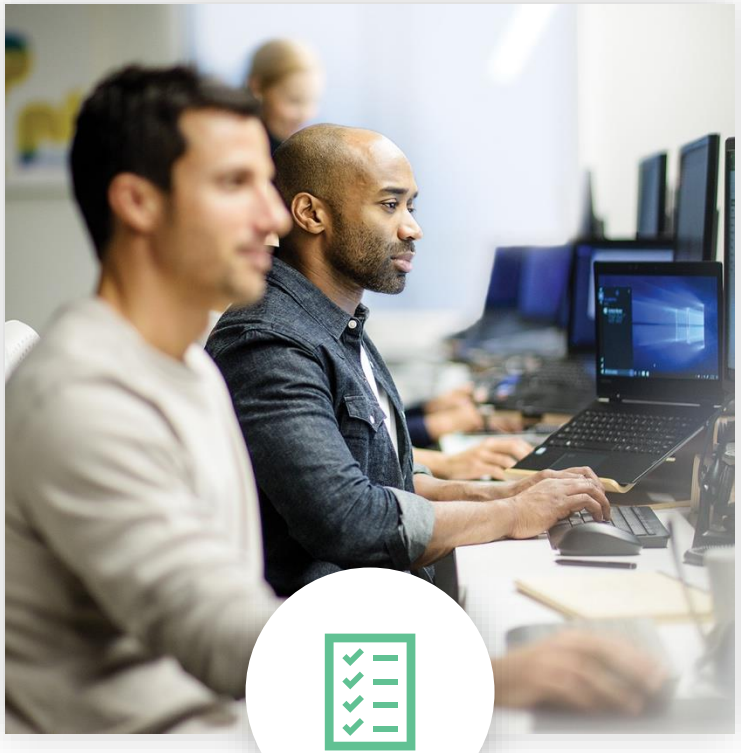
7B internet-connected devices in use worldwide

60% of organizations currently have a formal BYOD program in place

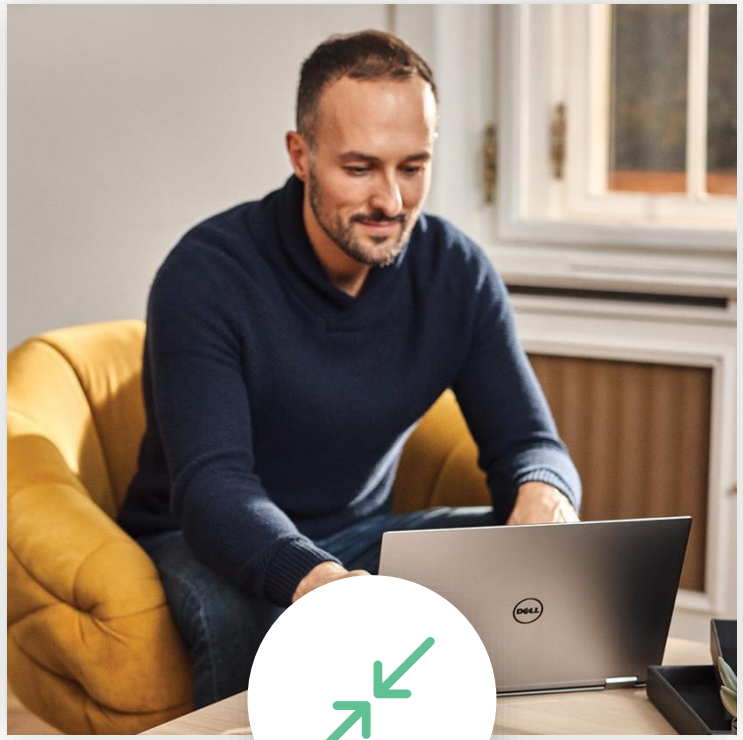
Old World vs. New World

~~Users are employees~~	>	Employees, partners, customers, bots
~~Corporate managed devices~~	>	Bring your own devices and IoT
~~On-premises apps~~	>	Explosion of cloud apps
~~Monolithic apps~~	>	Composite apps & public restful APIs
~~Corp network and firewall~~	>	Perimeter-less
~~Local packet tracking and logs~~	>	Explosion of signal

A new reality needs new principles



Verify explicitly



Use least privilege access

Assume breach

Zero Trust

A modern approach to security which treats every access attempt as if it's originating from an untrusted network.

Zero Trust – Where it all started?

2004
Jericho Forum concept of de-perimeterization

2009
Operation Aurora attack

2010
Forrester coins "Zero Trust" term

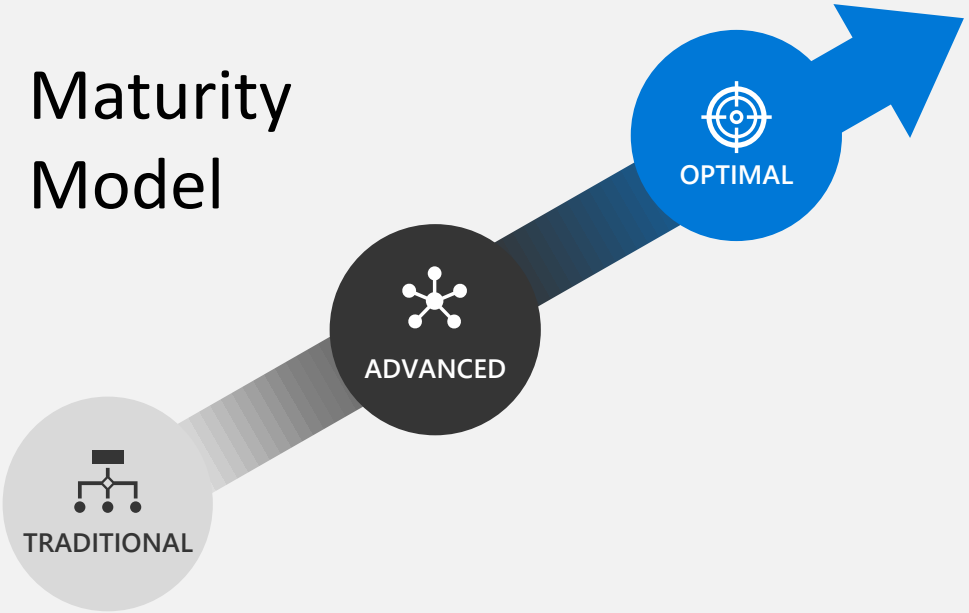
2014
Google BeyondCorp is published

Zero Trust hype takes off

Making Zero Trust a reality

- Do you know what is Zero Trust?
- Have you established a v-team with your stakeholders?
- Do you know where you are at today with your zero-trust journey?
- Do you have buy-in from C-level?

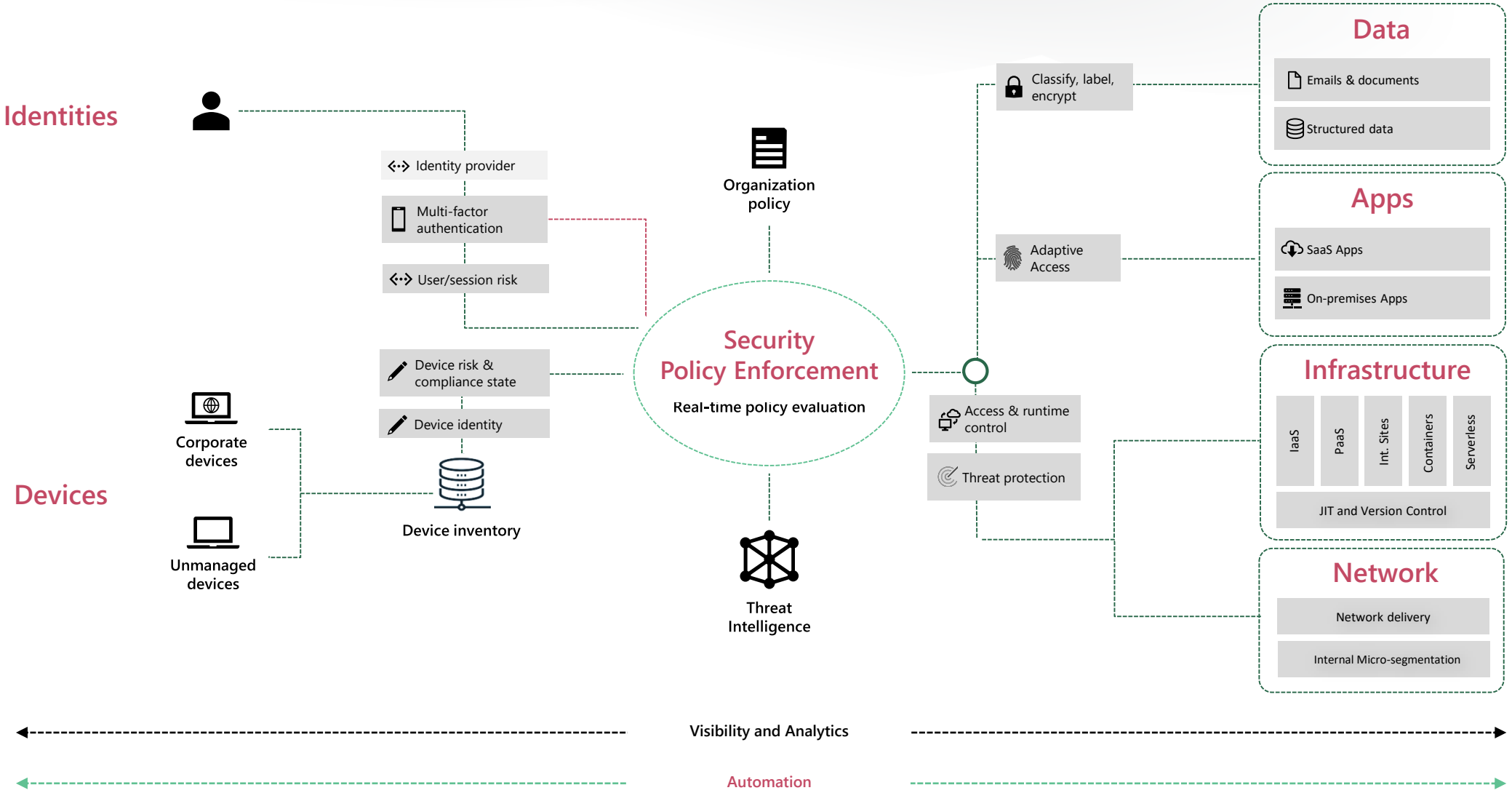
Maturity Model



Download today at
aka.ms/ztmodel

Microsoft

Zero Trust architecture



Identities

Verify identities and control access

Microsoft

Identity teams, here is your to-do:

01

Connect all apps for **Single Sign On**

02

Strong Authentication using Multi-Factor Auth and Risk Detection

03

Enforce **Policy Based Access** for breach containment

Devices

Protect devices and block access from non-compliant and risky devices

Microsoft

Device management teams, here is your to-do:

01

Register devices with your management solution

02

Implement security baselines & Compliance reporting

03

Use **endpoint threat detection** to monitor device risk

Network & Infrastructure

Remove trust from the network and secure the cloud perimeter

Microsoft

Network & Infra security teams, here is your to-do:

01

Enable a **Cloud Workload Protection** solution across your estate: Hybrid and multi-cloud

02

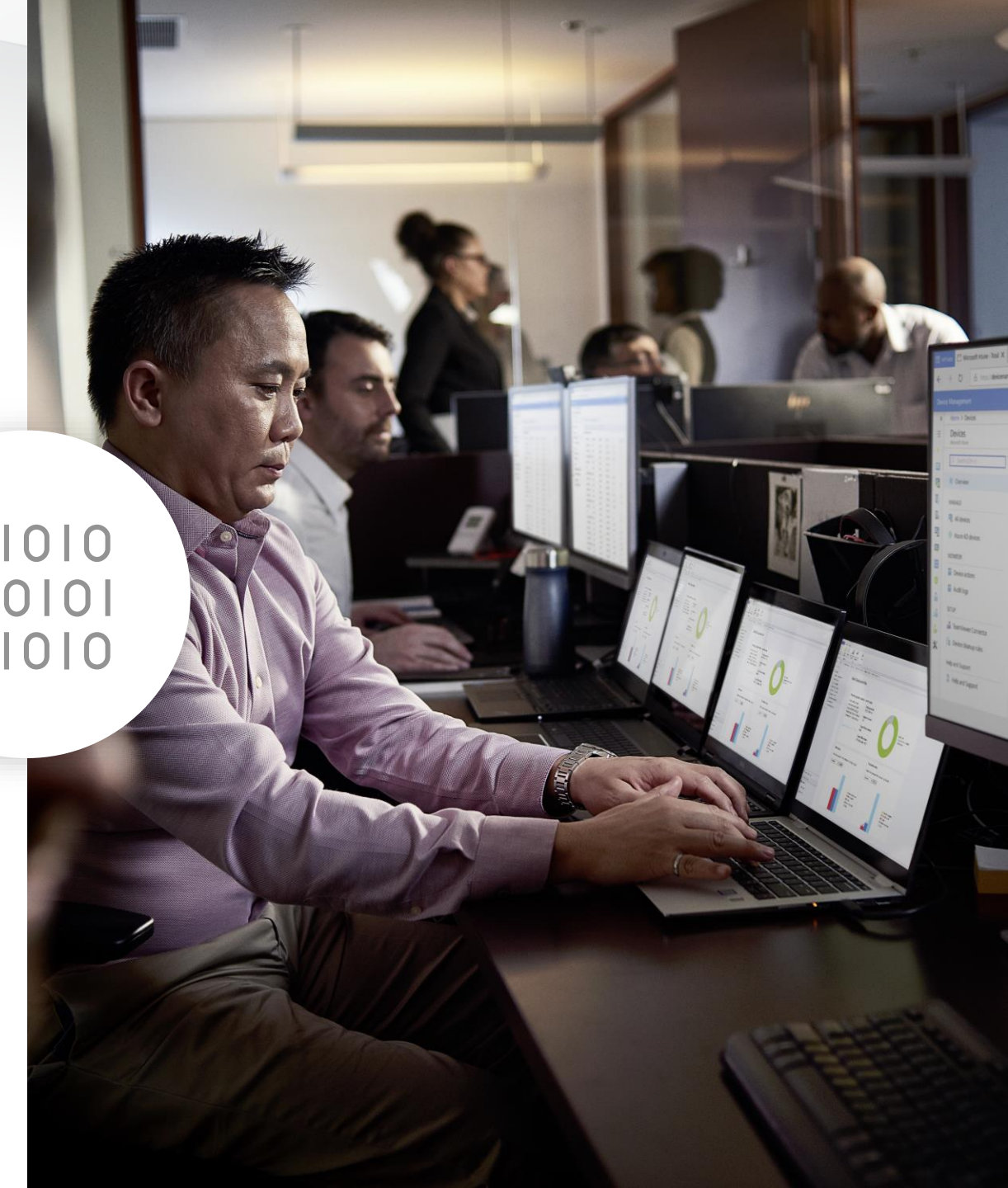
Use cloud-native controls to **create micro-perimeters** with real-time threat protection and enhanced visibility and control

03

Encrypt all traffic and **enable Just-in-time**, application, network and identity

Application and Data

Protect your sensitive data—
wherever it lives or travels



Microsoft

App and Data security teams, here is your to-do:

01

Perform Shadow IT discovery and a cloud control program

02

Agree on a **label taxonomy** and classify all documents & emails with the default label

03

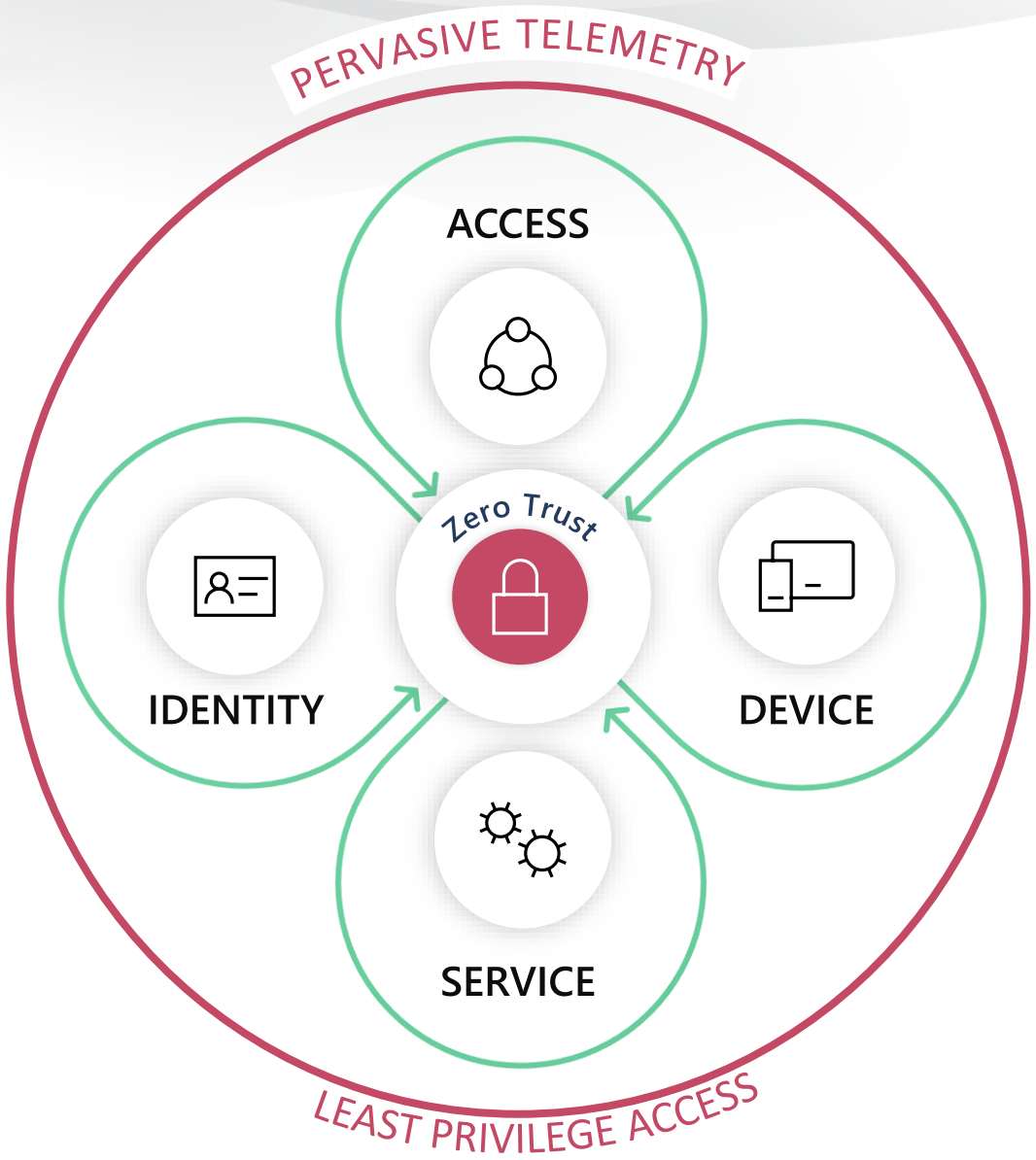
Apply real-time protection to high risk scenarios; sensitive data and unmanaged access in apps

RSAConference2020

Implementing Zero Trust at Microsoft

Zero Trust- Phase 1

- **Identity** – identities are validated and healthy
- **Device** - devices are validated to be managed and healthy
- **Service** - Health of applications, services, resources, and connections are verified
- **Access** – Network access is routed based on user role and device
- **Least privilege access** – limiting access to only the applications, services, and infrastructure required to perform job function
- **Pervasive telemetry** – understanding your environments, measuring risk reduction, and enabling artificial intelligence for anomaly detection



Core Scenarios

Scenario 1	As an employee, I can enroll my device into modern management system to get access to company resource.
Scenario 2	As an employee or a business guest I have a method to access corporate resources when not using a managed device.
Scenario 3	As a security stakeholder, I have systems in place to route network access based on user type and device role.
Scenario 4	As a security stakeholder, I have the systems in place to proof the device health and user before granting access to the application or service.
Scenario 5	As an employee I have user interface options (portal, desktop apps) that provides the ability to discover and launch applications and resources that I need.

Implementation goals of Zero Trust @Microsoft

IDENTITY	• Strong Identity is verified • Access to applications and data limited to minimum required to perform job function	Least privilege access	Pervasive telemetry
DEVICE	• All devices are enrolled and (modern) managed • Device health is verified • Unmanaged devices and non-FTE have alternative access methods to resources		
ACCESS	• Networks built using logical segmentation • Network access is routed based on user and device role		
SERVICE	• Applications and services enforcing conditional access • All applications are accessible via Internet by default • Applications and services health is verified		
EXPERIENCE	• Employees are only exposed to the applications and resources they can access • Tell the right story to the right audiences • Leverage telemetry to measure user experience • Provide visibility into the overall state of Zero Trust implementation		

Our implementation approach

IDENTITY	• Set up all user accounts to use modern identity service • Implement least privilege user rights • Create segmented identities based on role requirement (individual, admin, etc.)
DEVICE	• Implement policy enforcement platform to ensure device health • Implement policy deployment platform to manage devices • Provide indirect access solution to applications or resources from unmanaged devices
ACCESS	• Implement logical network segments • Deploy network access control system • Integrate with policy enforcement platform to validate the health of identity and devices
SERVICE	• Engineer applications to leverage modern auth platforms and libraries • Implement mechanism to evaluate application or service health and execute access decision based on health • Migrate application access routing from intranet to internet
EXPERIENCE	• Provide a single source of application discoverability tied to user entitlements • Develop comprehensive communications strategy • Develop metrics to measure impact of changes deployed in support of ZT • Develop dashboard which provides visibility into the Zero Trust coverage

Major phases of Zero Trust

Pre-Zero Trust

- ✓ Device management not required
- ✓ Single factor authenticatio n to resources
- ✓ Capability to enforce strong identity exists

Verify Identity

- ✓ All user accounts set up for strong identity enforcement
- ✓ Strong identity enforced for O365
- ✓ Least privilege user rights
- ✓ Eliminate passwords – biometric based model

Verify Device

- ✓ Device health required for SharePoint, Exchange, Teams on iOS, Android, Mac, and Windows
- ✓ Usage data for Application & Services
- ✓ Device Management required to tiered network access

Verify Access

- ✓ Internet Only for users
- ✓ Establish solutions for unmanaged devices
- ✓ Least privilege access model
- ✓ Device health required for corporate network

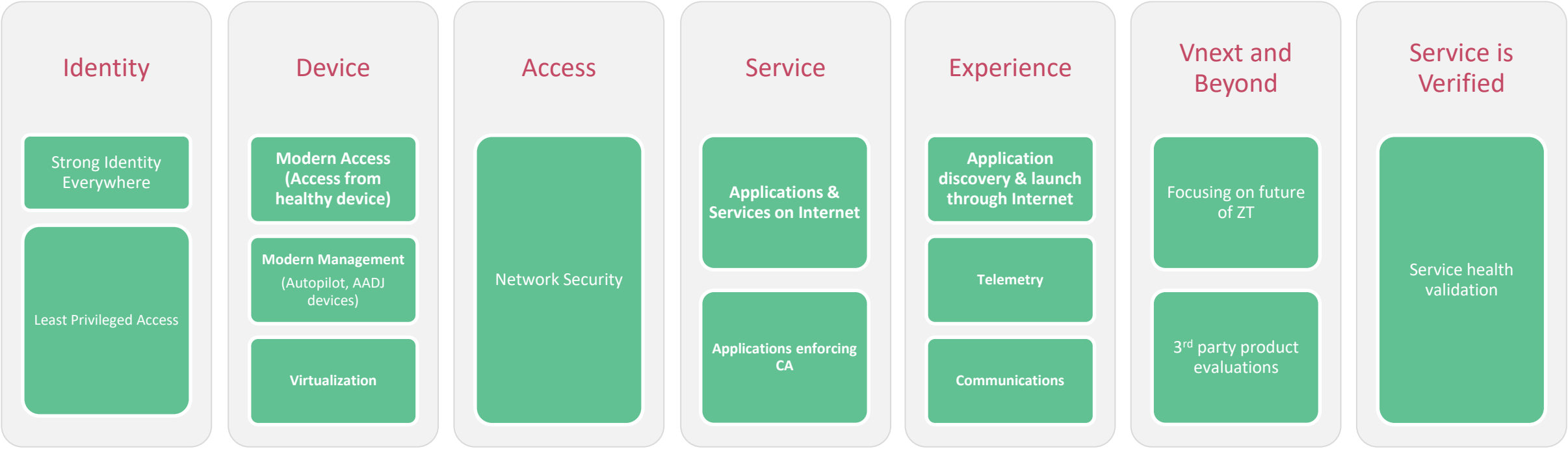
Verify Services

- ✓ Grow coverage in Device health requirement
- ✓ Service health concept and POC **(Distant Future)**

User and Access Telemetry

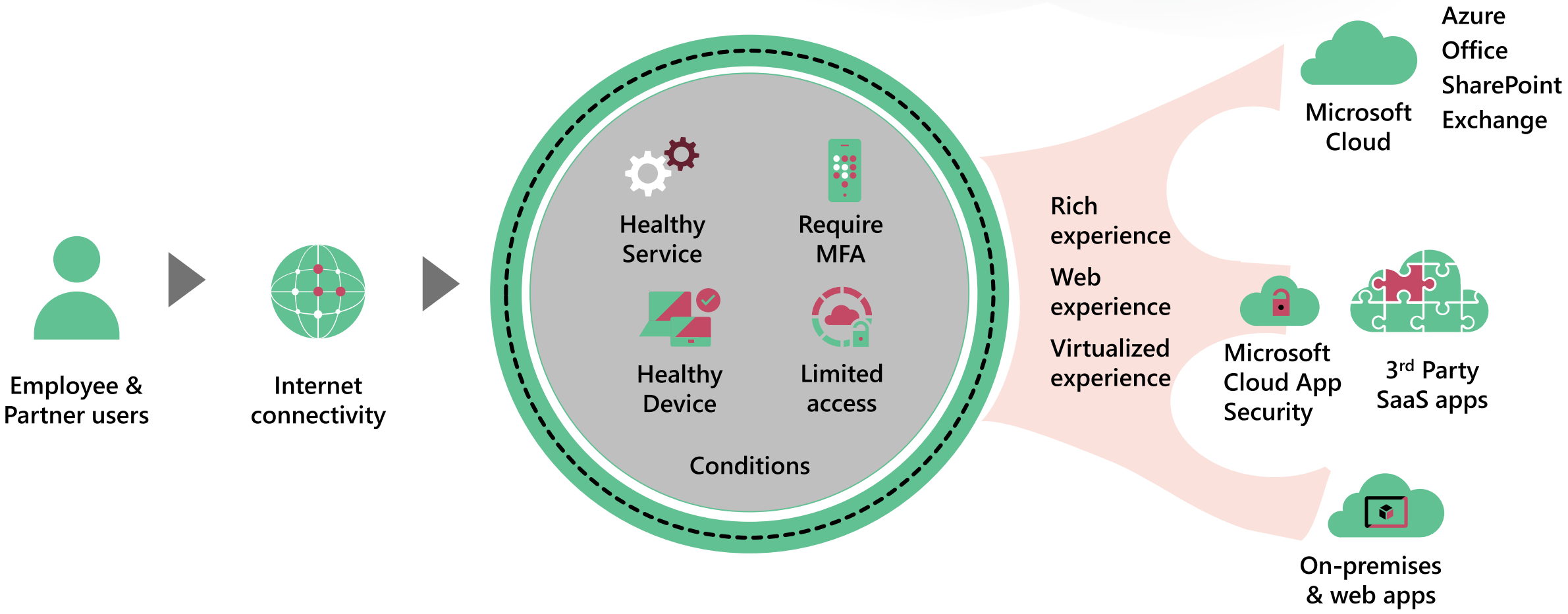
How are we managing Zero Trust implementation

- Scenarios-> Requirements->Workstreams owned by various sub-organizations
- Resulted in 15 sub programs reporting under ZT
- Yes, Zero Trust is a Super Epic ☺

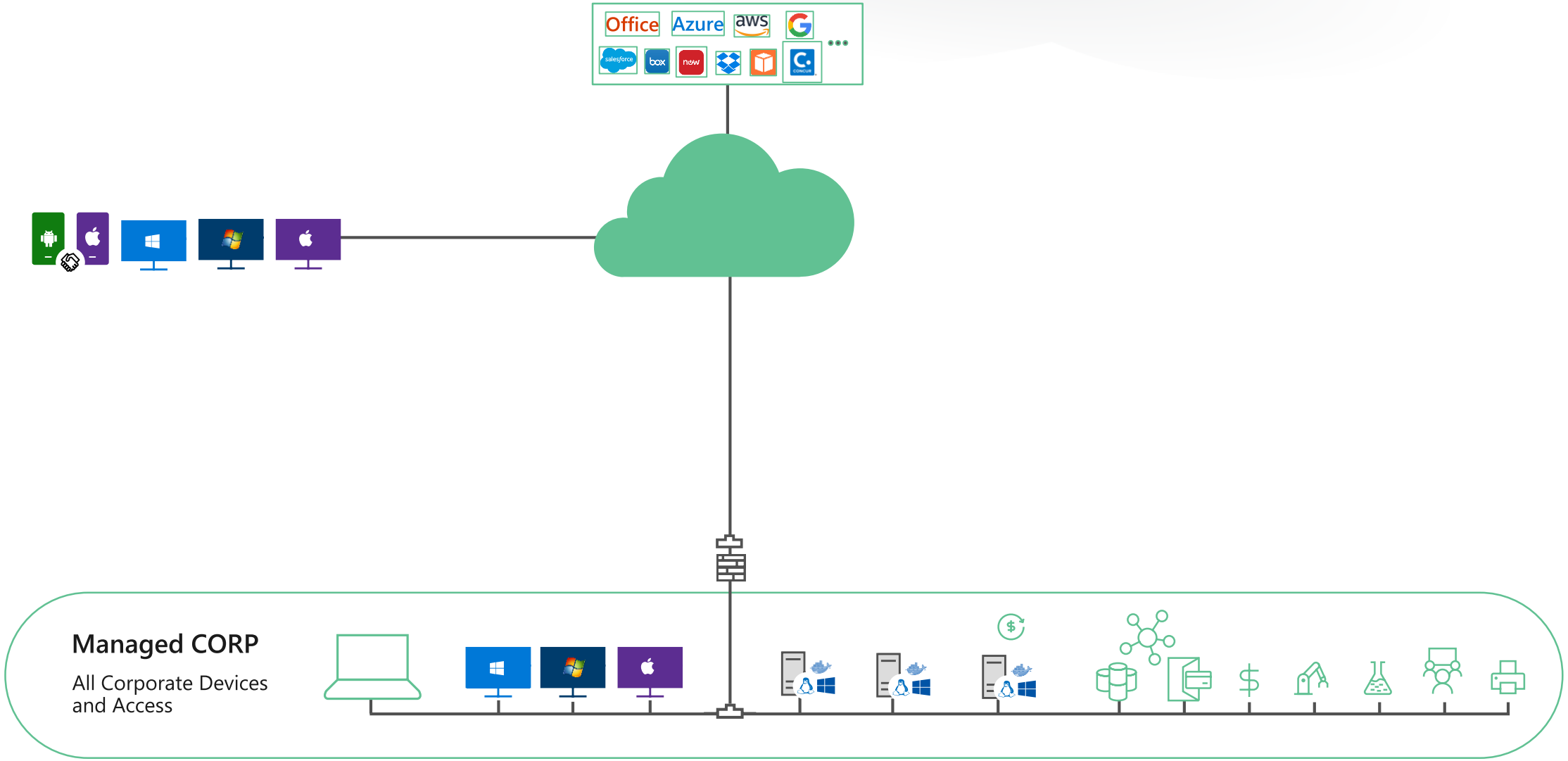


Future scoped

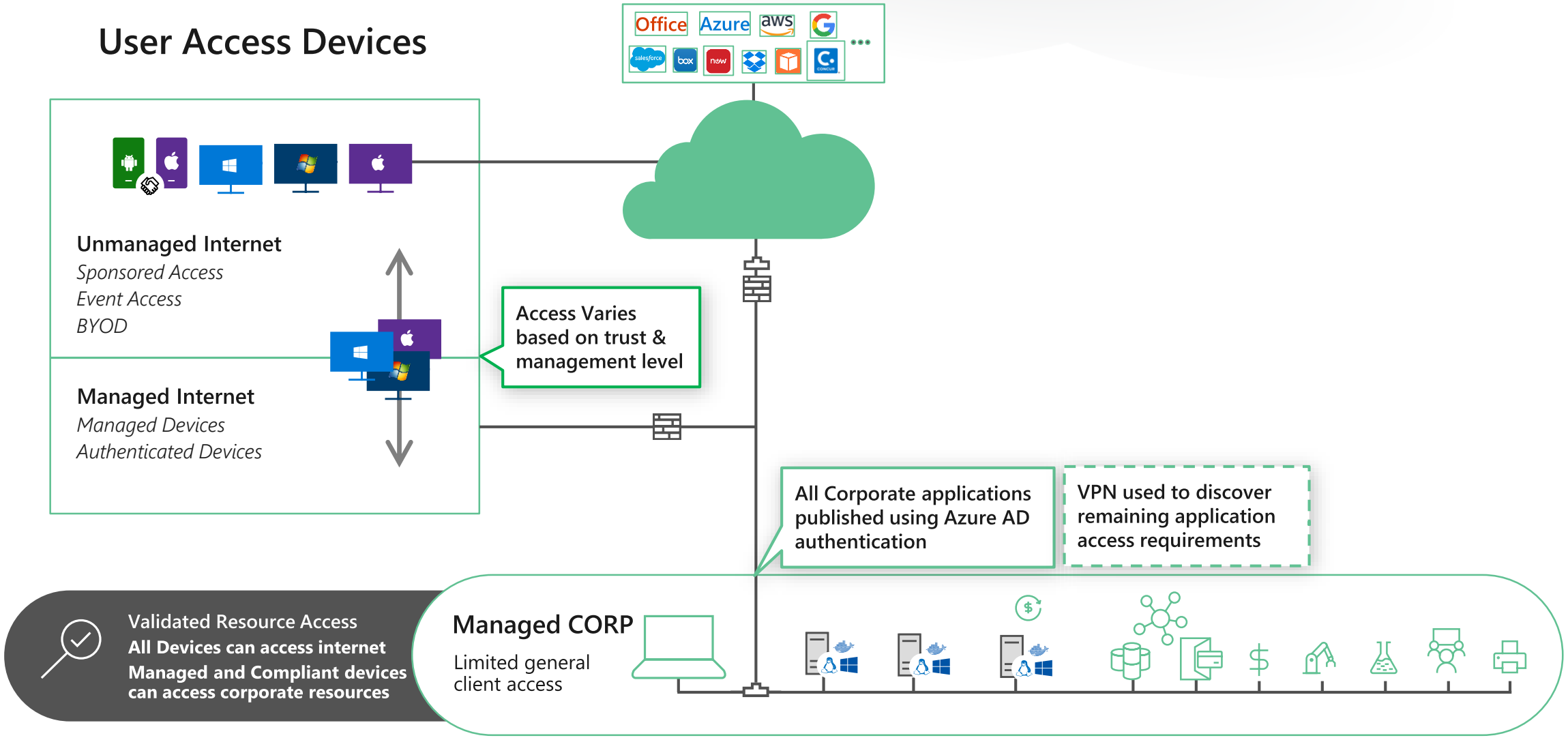
Zero Trust Access Model



Typical ‘Flat’ Network

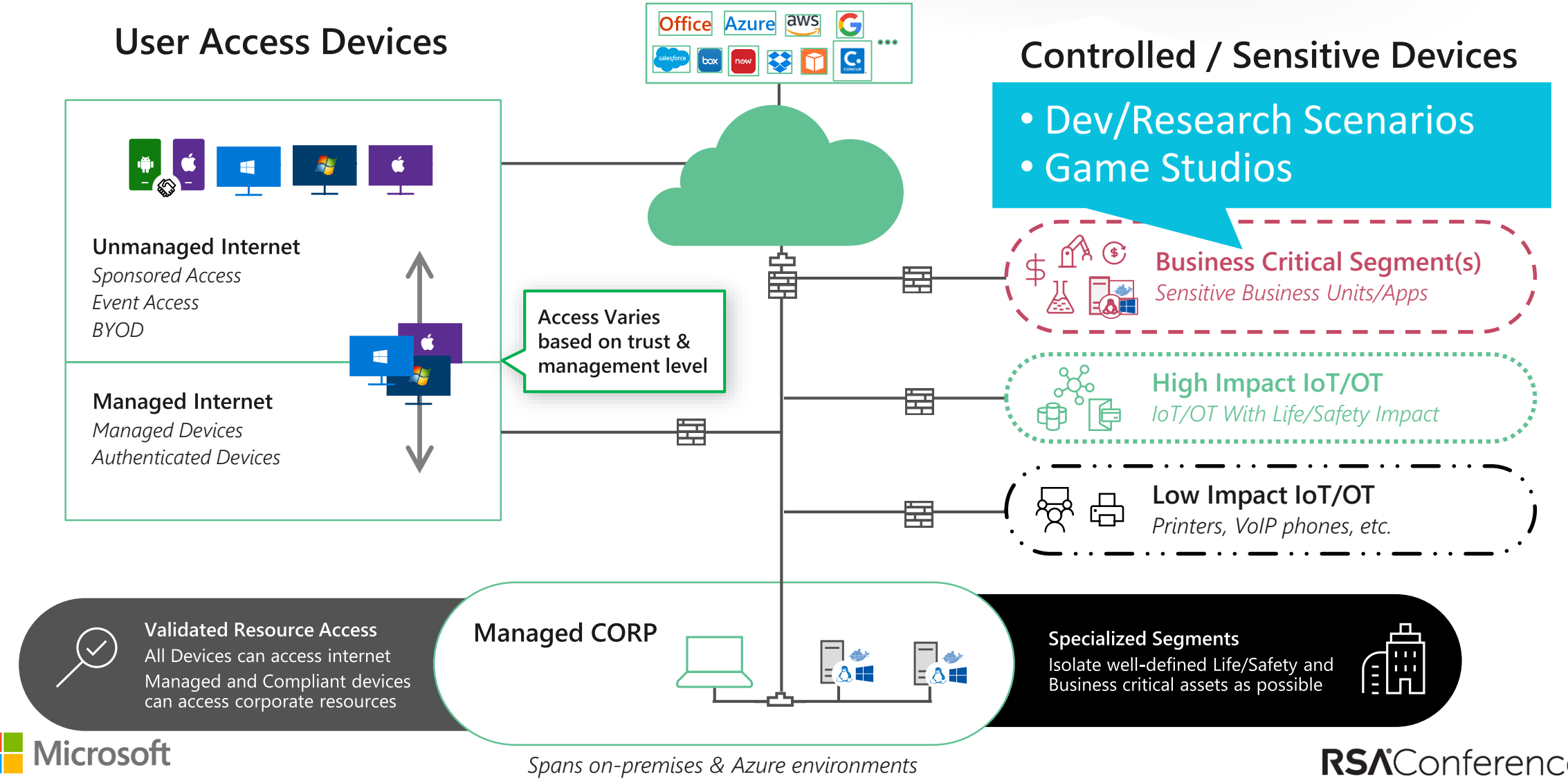


Zero Trust – Client Security Transformation



Spans on-premises & Azure environments

Zero Trust – Network Segment Transformation



Key Considerations in getting started

1. Collect **telemetry** and evaluate **risks**, and then set **goals**.
2. Get to modern identity and MFA - **Onboard to AAD.**
3. For CA enforcement, focus on top **used applications** to ensure maximum coverage.
4. Start with **simple policies** for device health enforcement such as device lock or password complexity.
5. Determine your **network connectivity strategy**

To Learn more

Aka.ms/ZeroTrust

1. Maturity Model White paper
2. Microsoft Implementation of Zero trust
3. Zero Trust Assessment tool

Good luck with your Journey!