Balancing Cybersecurity Risk with “Zero Trust Network Architecture”

Abbas Kudrati

APAC Lead Chief Cybersecurity Advisor, Microsoft

@askudrati

https://aka.ms/abbas

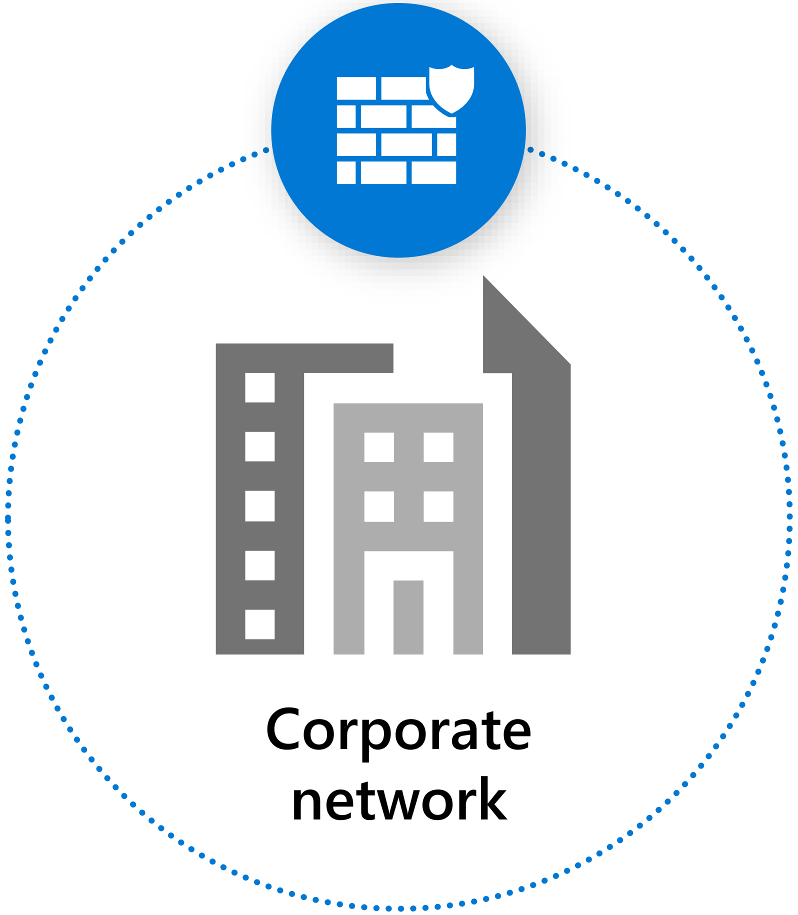
28th Aug 2020

GTACS 2020
GOVERNANCE · TECHNOLOGY AUDIT · CONTROL · SECURITY

ISACA®
Singapore Chapter

Disclaimer: The views and opinions expressed in this presentation are those of the author and do not necessarily reflect the official policy or position of any organization.

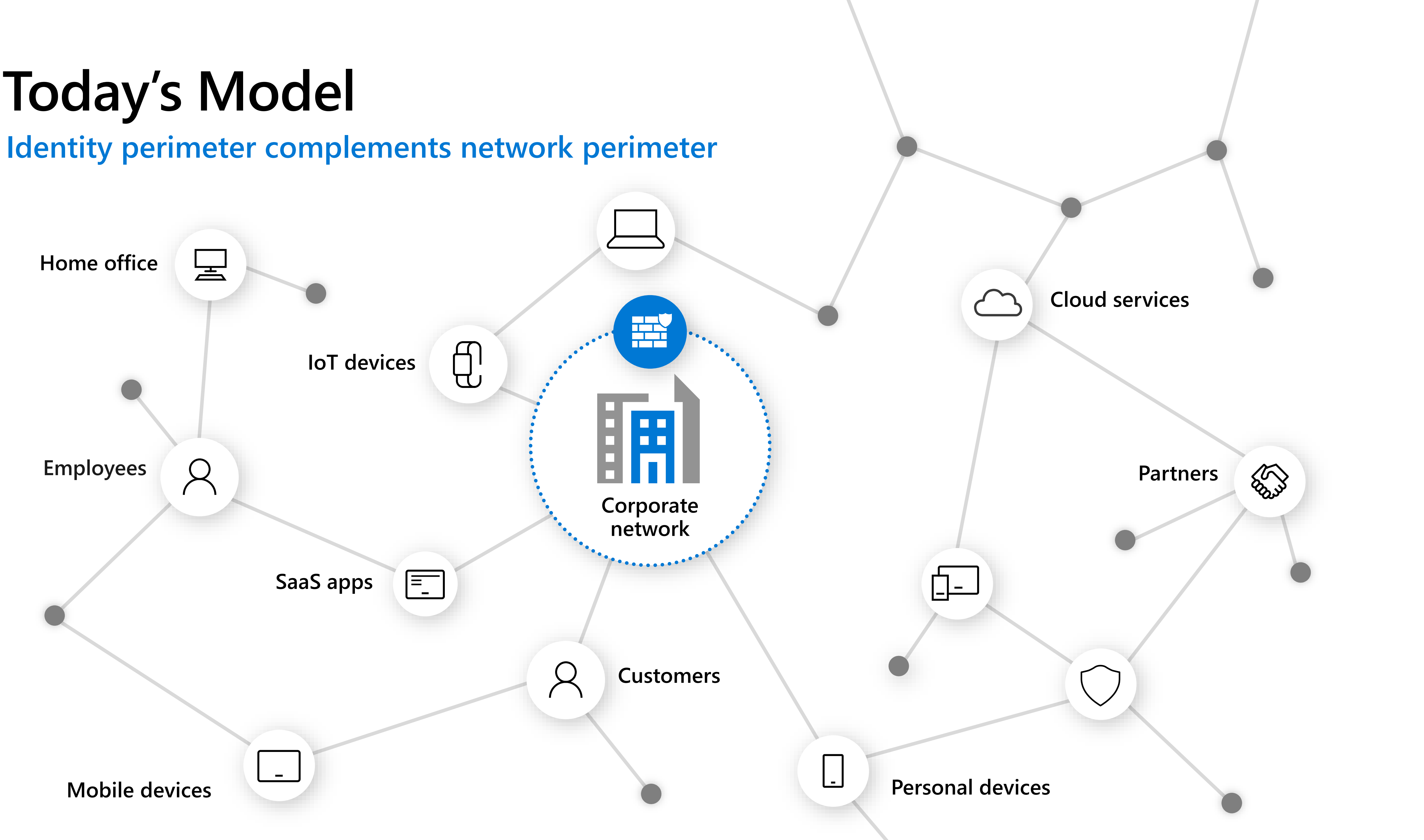
Traditional Model



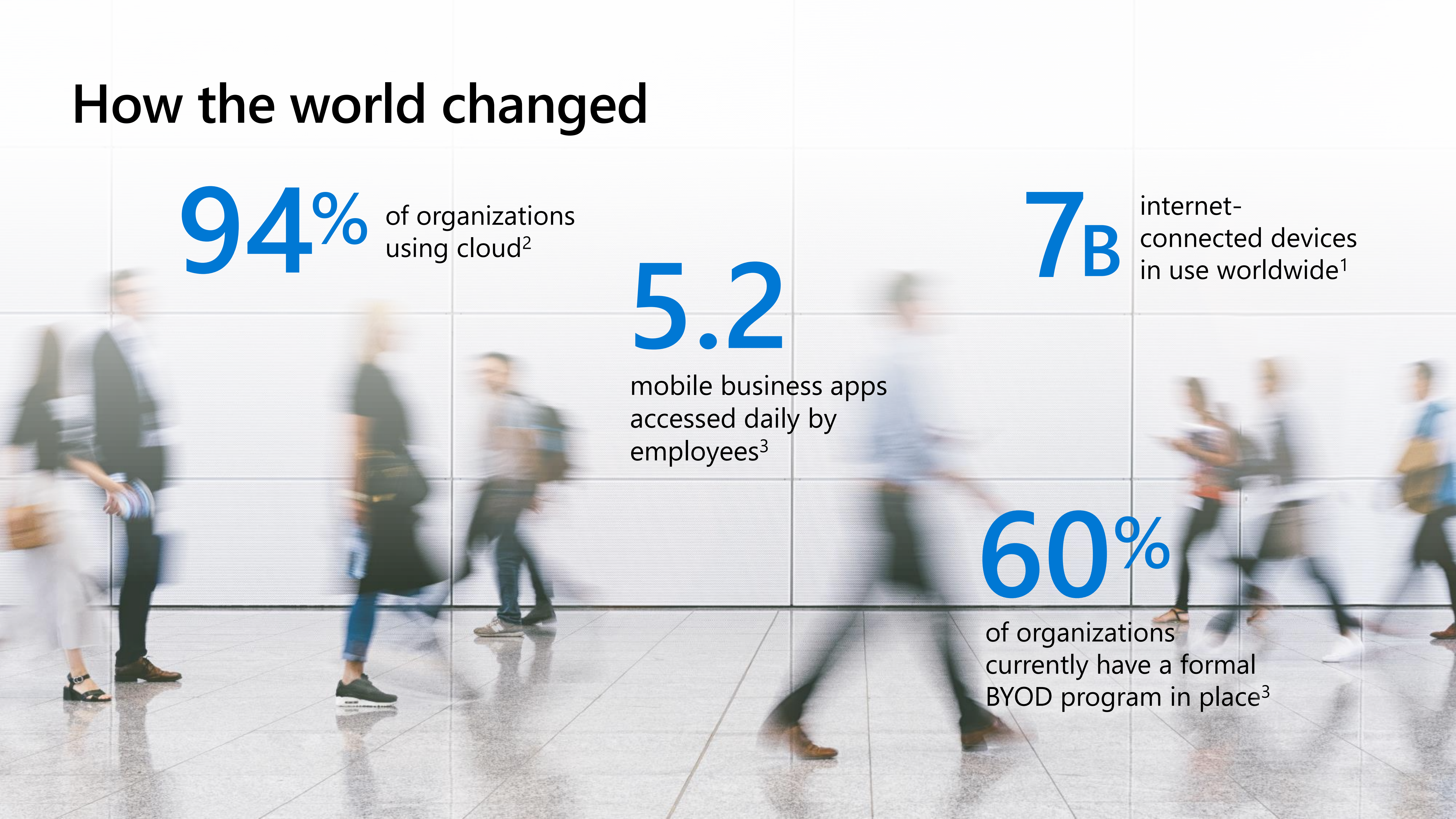
Users, devices, apps, and data protected behind a DMZ/firewall

Today's Model

Identity perimeter complements network perimeter



How the world changed



94% of organizations using cloud[2]

5.2 mobile business apps accessed daily by employees[3]

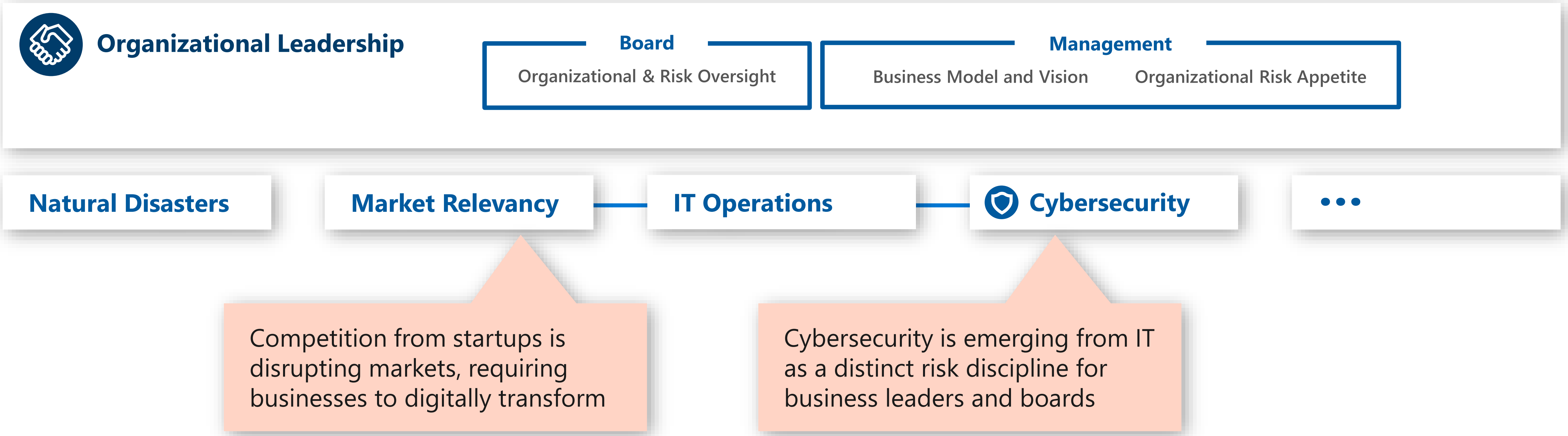
7B internet-connected devices in use worldwide[1]

60% of organizations currently have a formal BYOD program in place[3]

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~~	→	Expanding Perimeters
~~Local packet tracking and logs~~	→	Explosion of signal

Managing organizational risk



Organizational Leadership

Board

Organizational & Risk Oversight

Management

Business Model and Vision

Organizational Risk Appetite

Natural Disasters

Market Relevancy

IT Operations

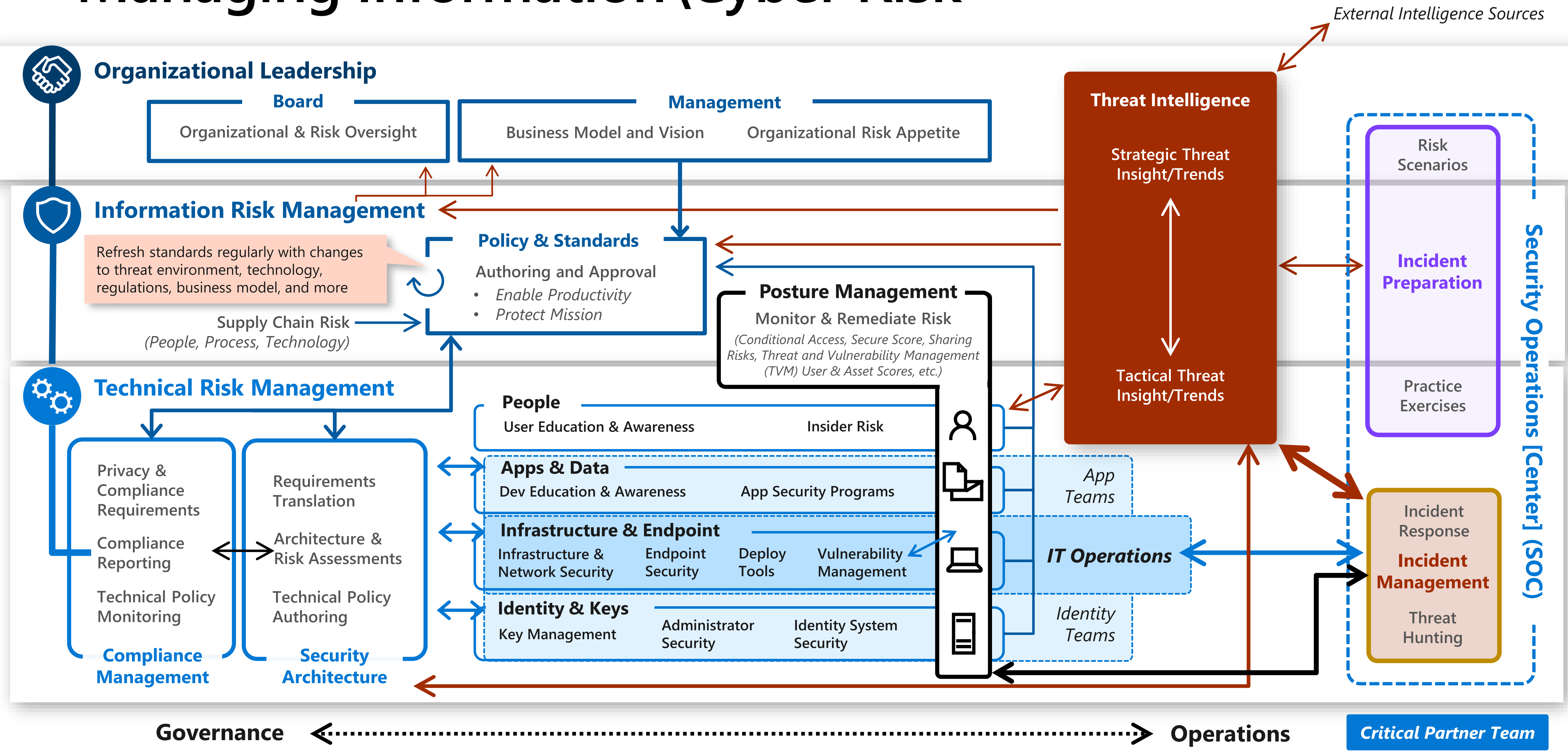
Cybersecurity

•••

Competition from startups is disrupting markets, requiring businesses to digitally transform

Cybersecurity is emerging from IT as a distinct risk discipline for business leaders and boards https://aka.ms/SecurityRoles

Managing Information\Cyber Risk



External Intelligence Sources

Organizational Leadership

Board

Organizational & Risk Oversight

Management

Business Model and Vision

Organizational Risk Appetite

Information Risk Management

Refresh standards regularly with changes to threat environment, technology, regulations, business model, and more

Policy & Standards

Authoring and Approval

- *Enable Productivity*
- *Protect Mission*

Supply Chain Risk *(People, Process, Technology)*

Technical Risk Management

Privacy & Compliance Requirements

Compliance Reporting

Technical Policy Monitoring

Compliance Management

Requirements Translation

Architecture & Risk Assessments

Technical Policy Authoring

Security Architecture

Posture Management

Monitor & Remediate Risk

(Conditional Access, Secure Score, Sharing Risks, Threat and Vulnerability Management (TVM) User & Asset Scores, etc.)

People

User Education & Awareness

Insider Risk

Apps & Data

Dev Education & Awareness

App Security Programs

App Teams

Infrastructure & Endpoint

Infrastructure & Network Security

Endpoint Security

Deploy Tools

Vulnerability Management

IT Operations

Identity & Keys

Key Management

Administrator Security

Identity System Security

Identity Teams

Threat Intelligence

Strategic Threat Insight/Trends

Tactical Threat Insight/Trends

Security Operations [Center] (SOC)

Risk Scenarios

Incident Preparation

Practice Exercises

Incident Response

Incident Management

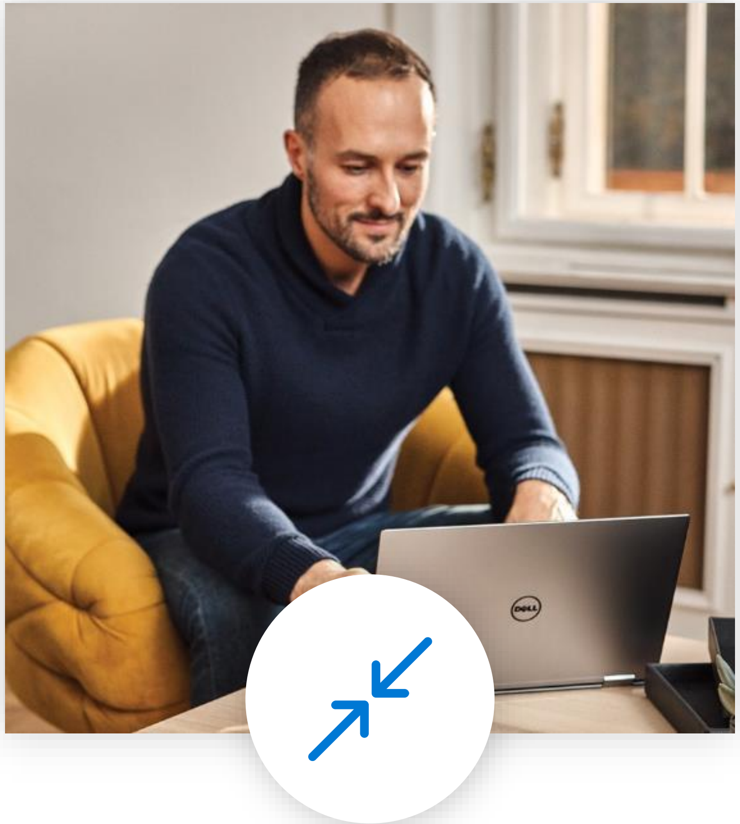
Threat Hunting

Governance ↔ **Operations**

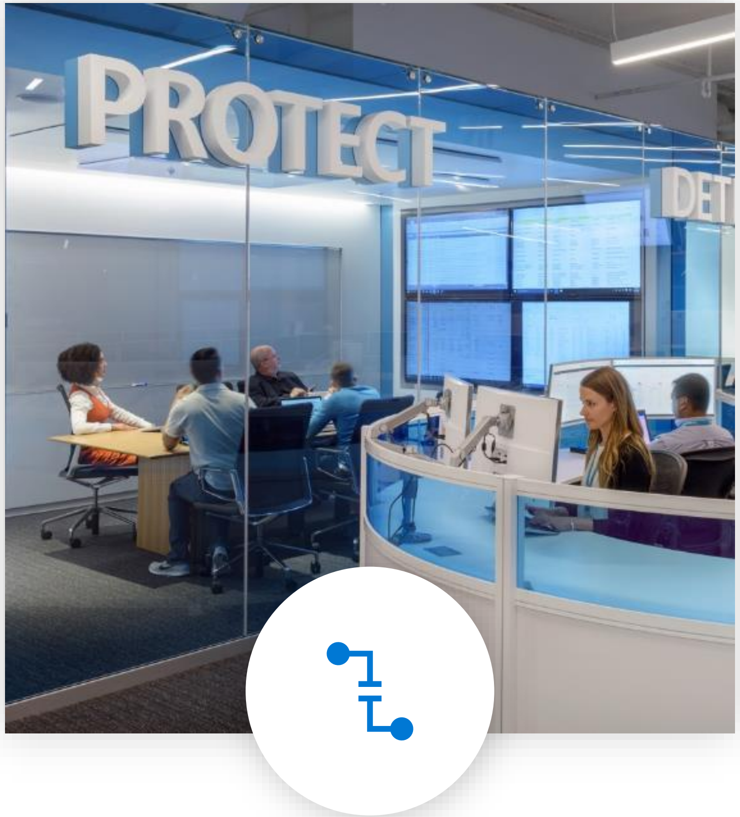
Critical Partner Team

A new reality needs new principles

Verify explicitly

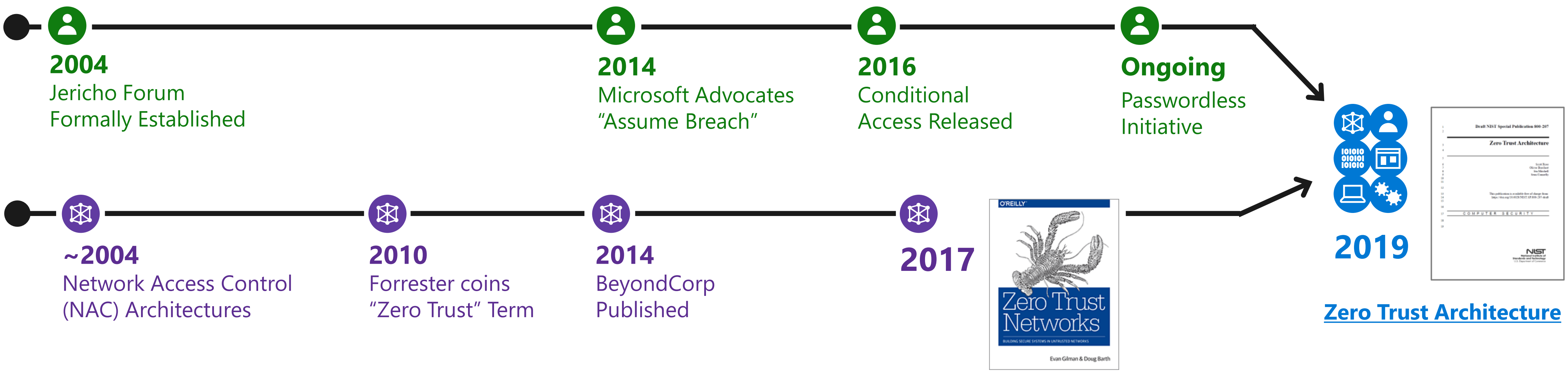


Use least privilege access



Assume breach

“Zero Trust” has been around for a while



2004
Jericho Forum
Formally Established

2014
Microsoft Advocates
“Assume Breach”

2016
Conditional
Access Released

Ongoing
Passwordless
Initiative

~2004
Network Access Control
(NAC) Architectures

2010
Forrester coins
“Zero Trust” Term

2014
BeyondCorp
Published

2017

2019

[Zero Trust Architecture]

Historically slow mainstream adoption for both network & identity models:

Network – Expensive and challenging to implement
Google’s BeyondCorp success is rarely replicated

Identity – Natural resistance to big changes
Security has a deep history/affinity with networking

Increasing consensus on convergence (though still ‘early days’ of this approach)

Zero Trust

Strategy that builds security assurances

- for business data and applications
- on a public or untrusted network.

Leads to

Productivity Security

Policy Driven Access Architecture for Employees & Partners:

1. Explicitly validate trust of access requests
2. Dynamically address insufficient trust

Modern SOC

Pervasive detection & response

1. Deep asset visibility inside & outside the firewall
2. Rapid remediation with automation and integrated workflows

And More

- *Datacenter Access & Isolation Architecture*
- *Internet of Things / Operational Technology*
- *And more…*

Increases security, Reduce risk

Increases productivity

Zero Trust across the digital estate

Identity

Devices

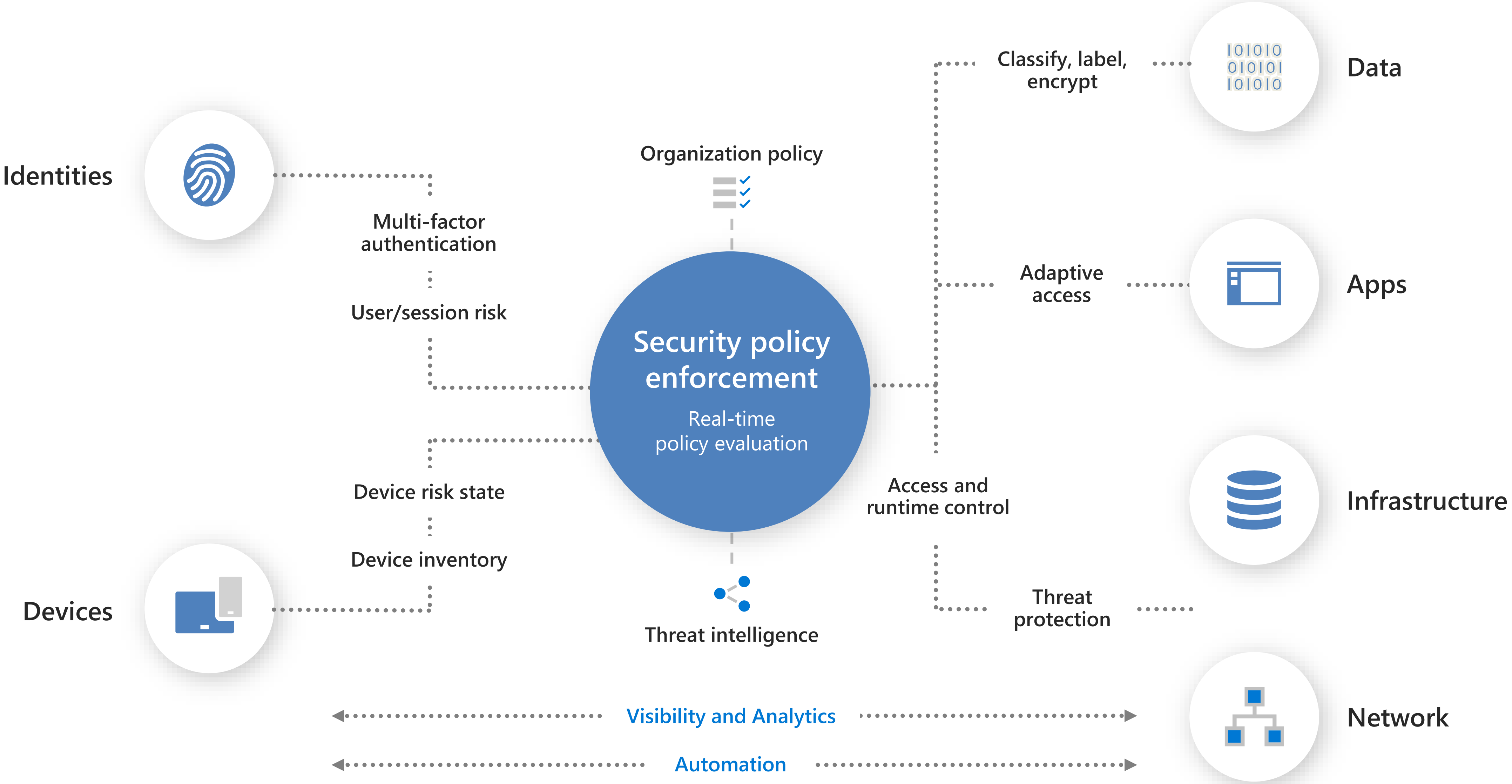
Apps

Infrastructure

Networking

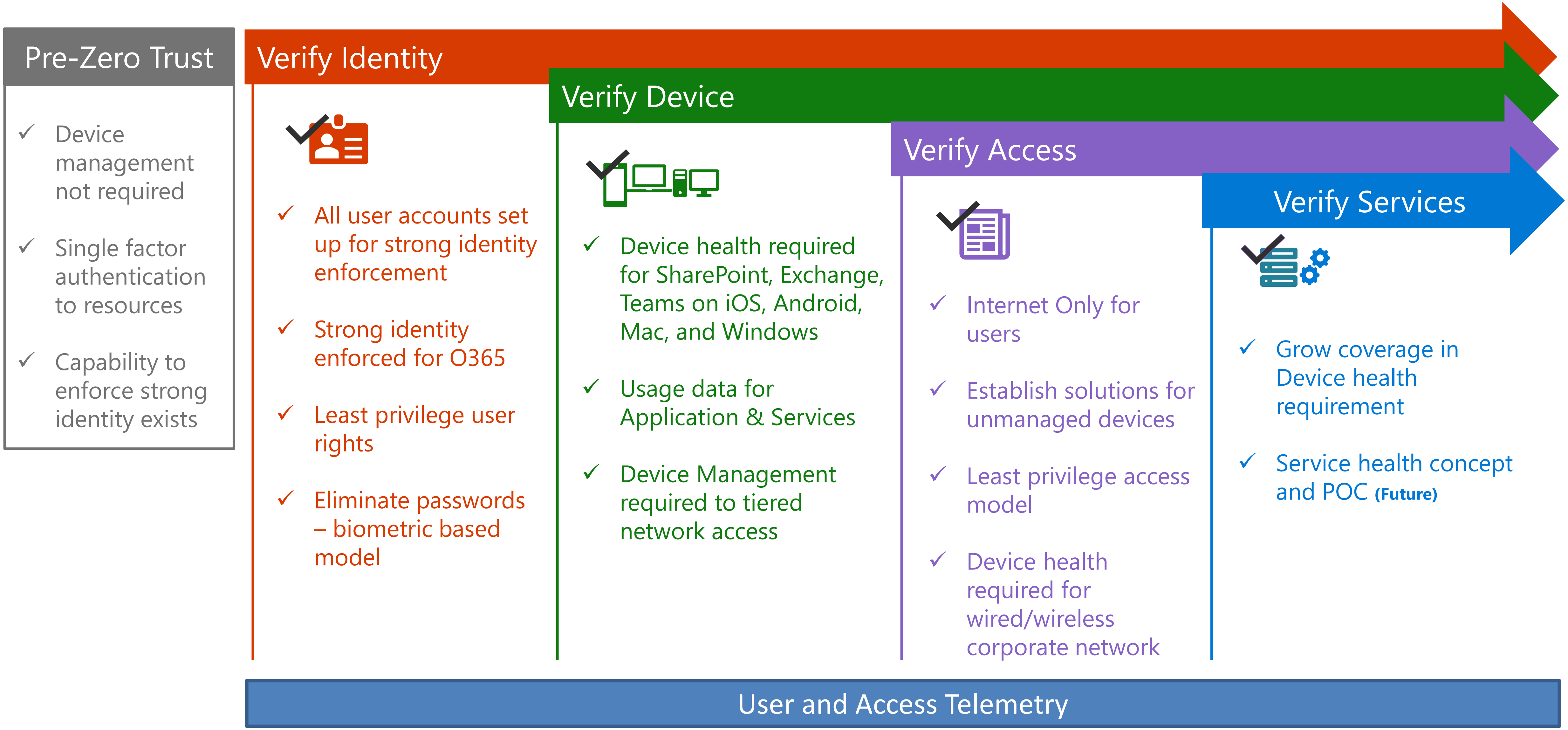
Data

Zero Trust architecture



Case Study: Microsoft

Major phases of Zero Trust Networking



Pre-Zero Trust

- ✓ Device management not required
- ✓ Single factor authentication 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

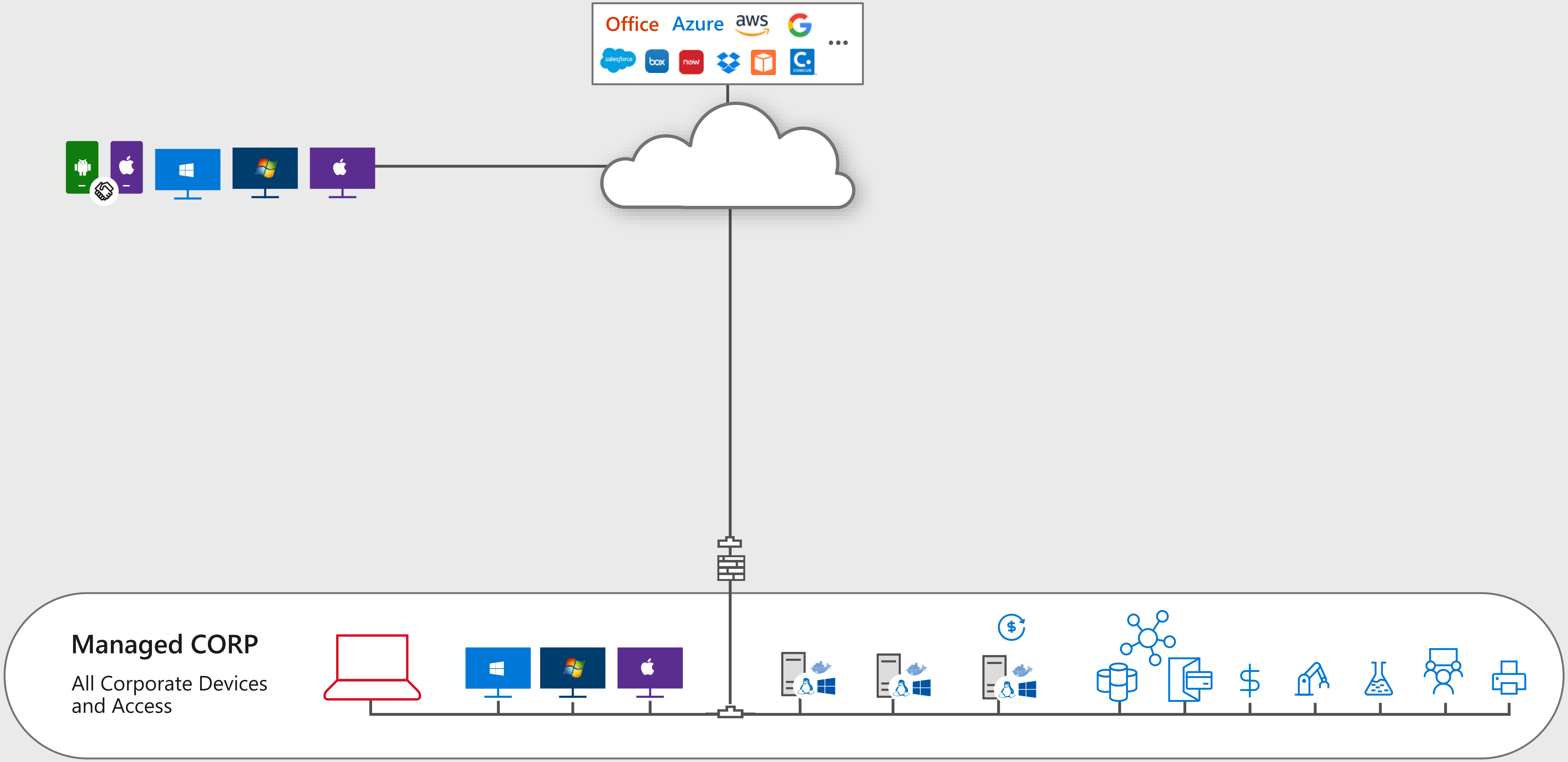
- ✓ Internet Only for users
- ✓ Establish solutions for unmanaged devices
- ✓ Least privilege access model
- ✓ Device health required for wired/wireless corporate network

Verify Services

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

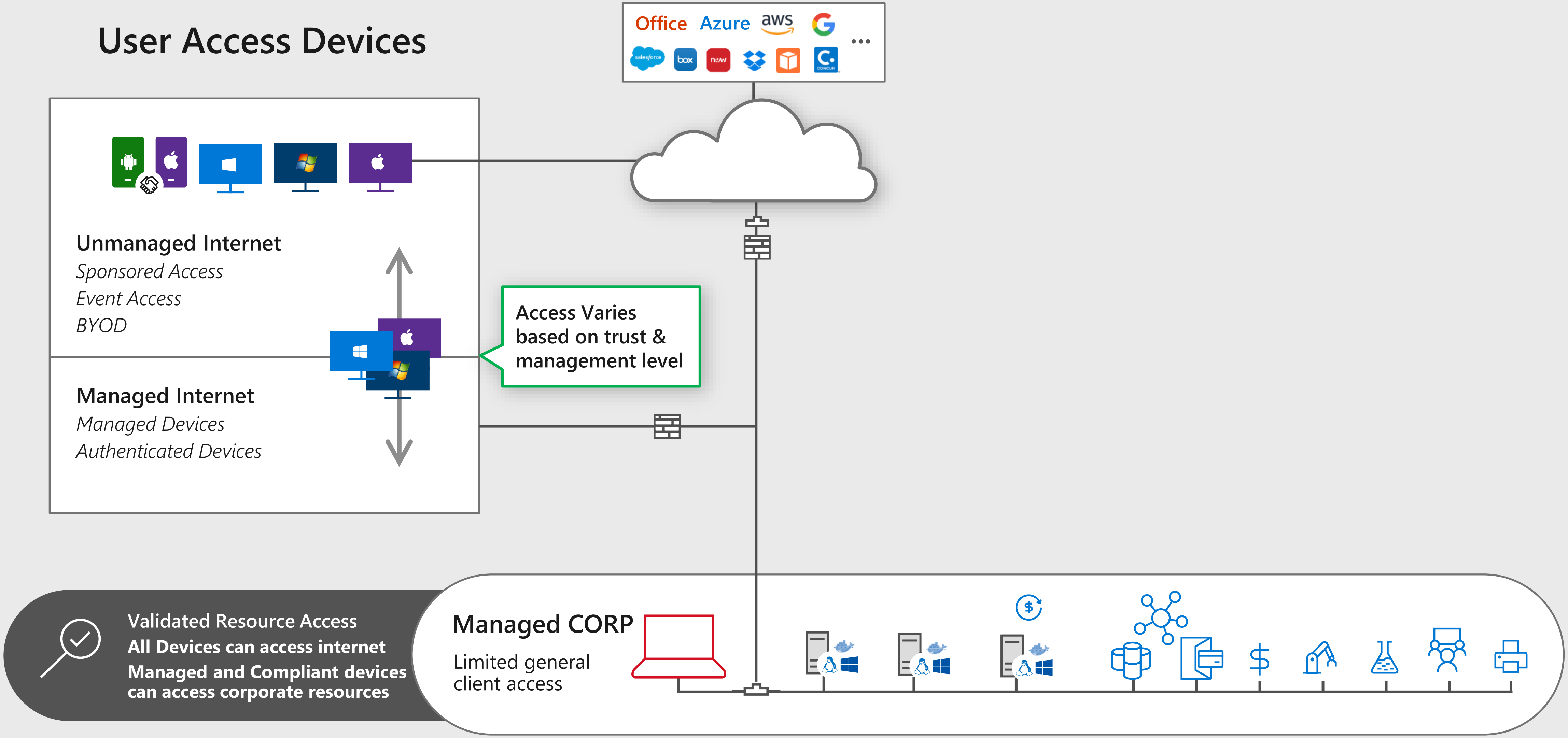
User and Access Telemetry

Typical 'Flat' Network



Zero Trust – Client Security Transformation

User Access Devices



Unmanaged Internet

Sponsored Access

Event Access

BYOD

Managed Internet

Managed Devices

Authenticated Devices

Access Varies based on trust & management level

Validated Resource Access

All Devices can access internet

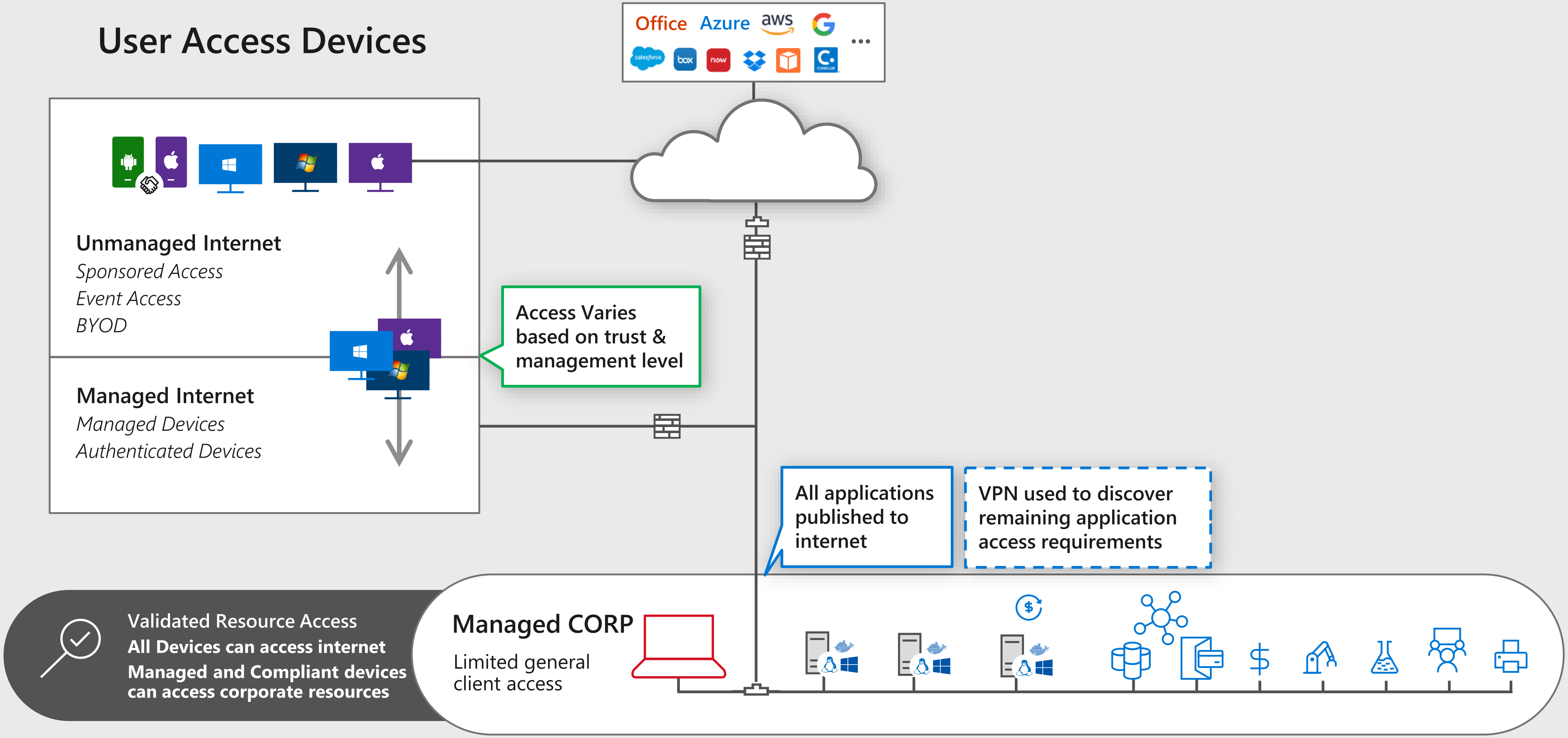
Managed and Compliant devices can access corporate resources

Managed CORP

Limited general client access

Spans on-premises & Azure environments

Zero Trust – Client Security Transformation



User Access Devices

Unmanaged Internet
Sponsored Access
Event Access
BYOD

Managed Internet
Managed Devices
Authenticated Devices

Access Varies based on trust & management level

All applications published to internet

VPN used to discover remaining application access requirements

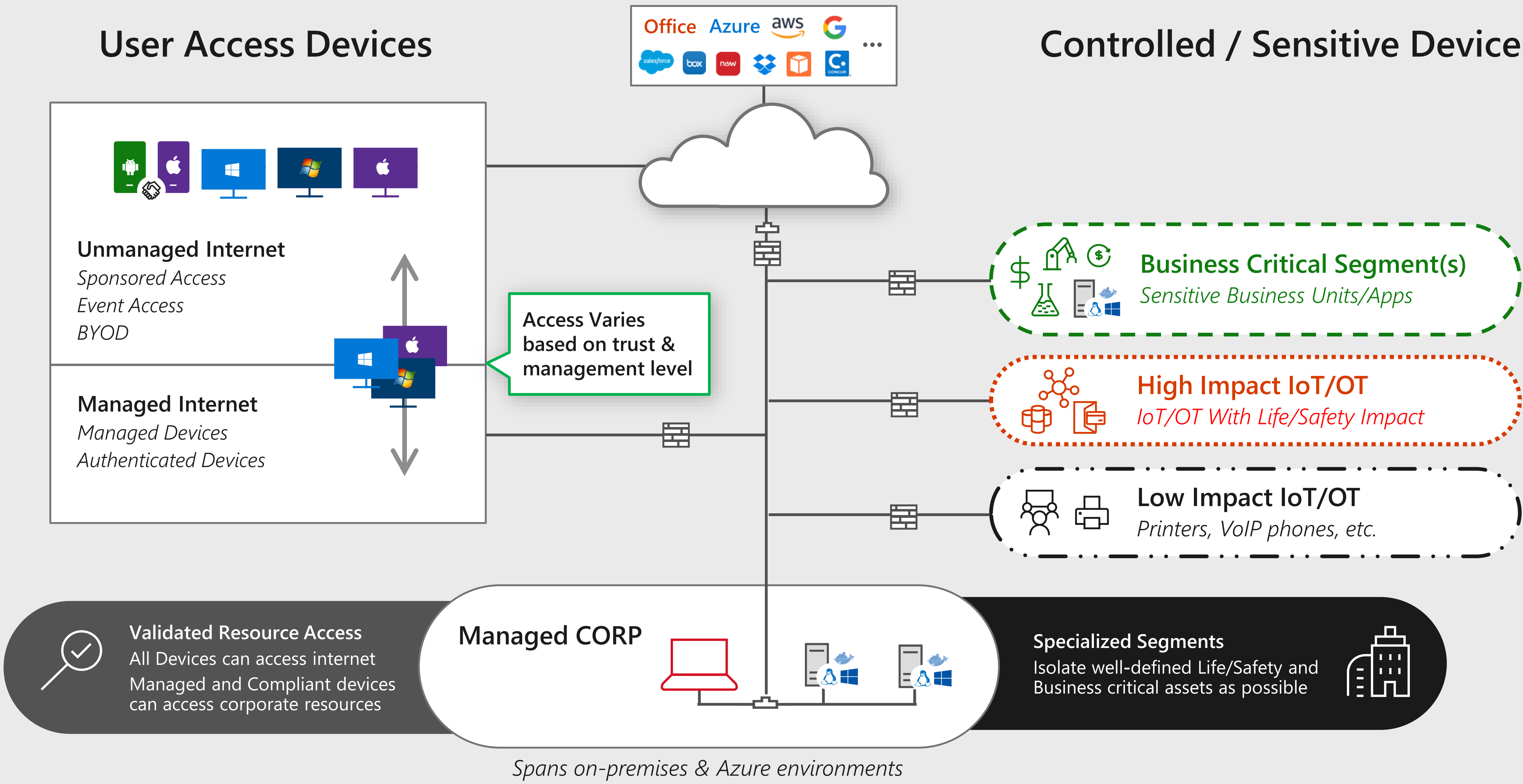
Validated Resource Access
All Devices can access internet
Managed and Compliant devices can access corporate resources

Managed CORP

Limited general client access

Spans on-premises & Azure environments

Zero Trust – Network Segment Transformation

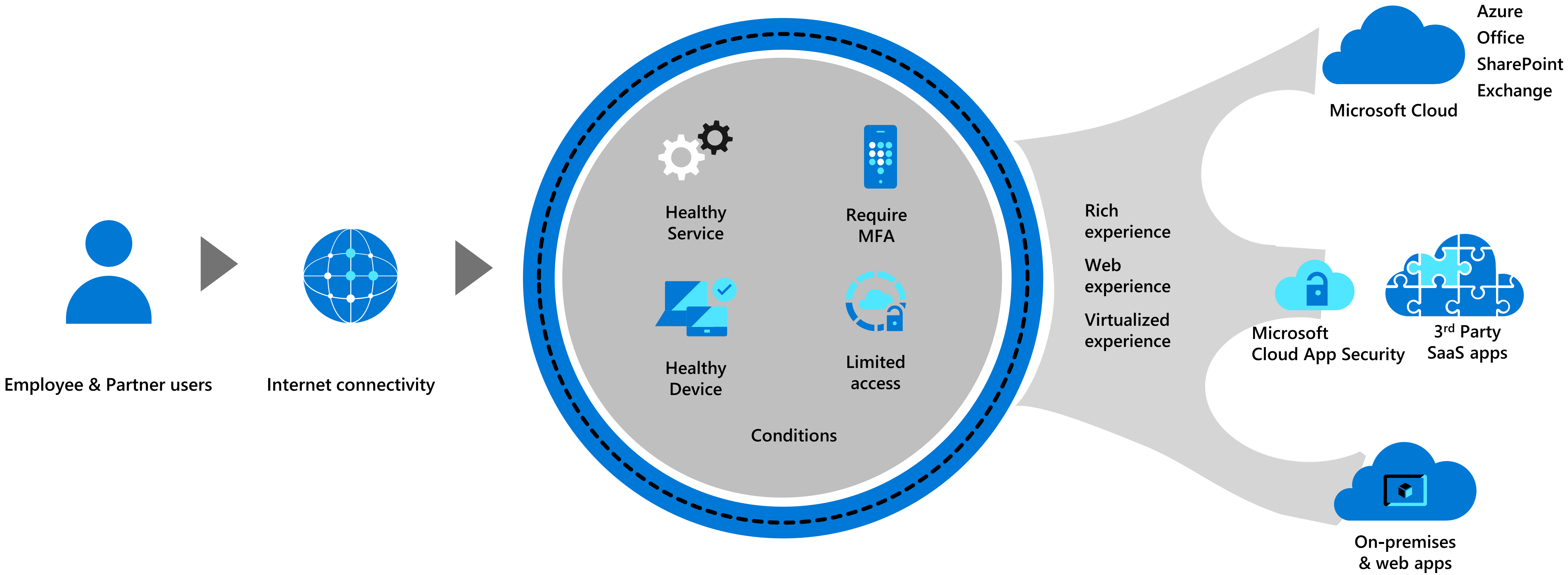


Validated Resource Access
All Devices can access internet
Managed and Compliant devices can access corporate resources

Specialized Segments
Isolate well-defined Life/Safety and Business critical assets as possible

Spans on-premises & Azure environments

Zero Trust Access Model



Productivity Benefits:
50% update time reduction
75% reduction in device issues
2x battery life
Faster device boot times – 75% improvement

Security Benefits:
Elimination of "shadow" VPN & Wireless APs
4x security auths – no user interaction
Reduction of surface area – 42% reduction
No more passwords – Helpdesk call reduction

Zero Trust Benefits

for both security and productivity

Increases security

1. Reduce risk of compromised users & endpoints
   - Remove user endpoints from enterprise network
   - Reduce VPN usage / attack surface
2. Improves security visibility
   - **No blind spots** for remote devices
   - **Centralized view** of risk, policy exceptions, and access requests
   - **Deep insight** into device risk and user session activity

Increases productivity

1. Can work anywhere you want
   - Apps & Data available anywhere
   - Empowers everyone including security
2. Can choose your own device
3. Single Sign On (SSO) across enterprise apps and services
4. Improved "Access Denied" experience:
   - Prompt to increase trust (e.g. MFA)
   - Limited access to apps/data

Better security *and* user experience from "Password-Less" authentication

Key Considerations in getting started

1. **Collect telemetry** and **evaluate risks**, and then **set goals.**

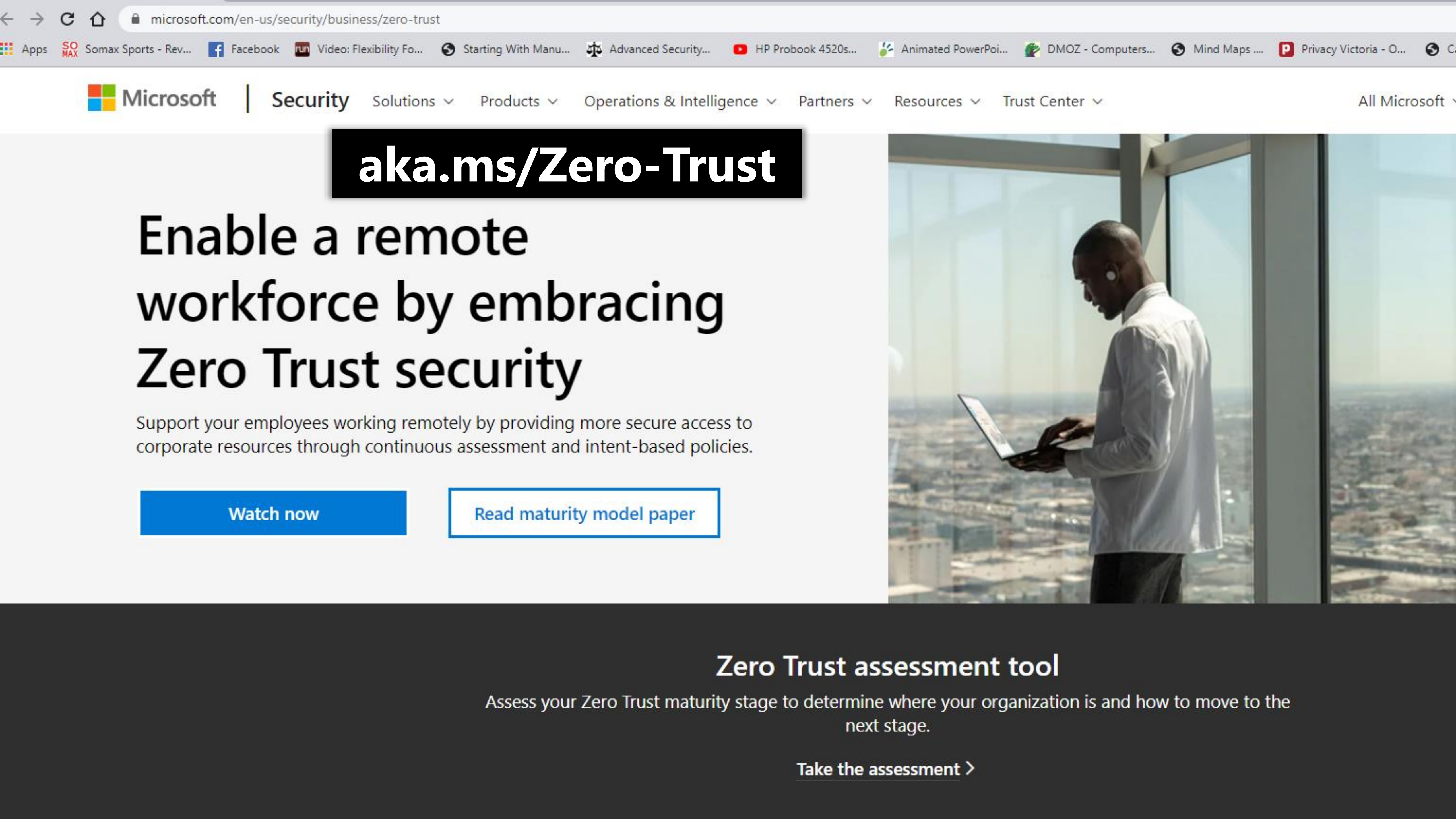
2. Get to modern identity and MFA - **Onboard to AAD.**

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**

aka.ms/Zero-Trust

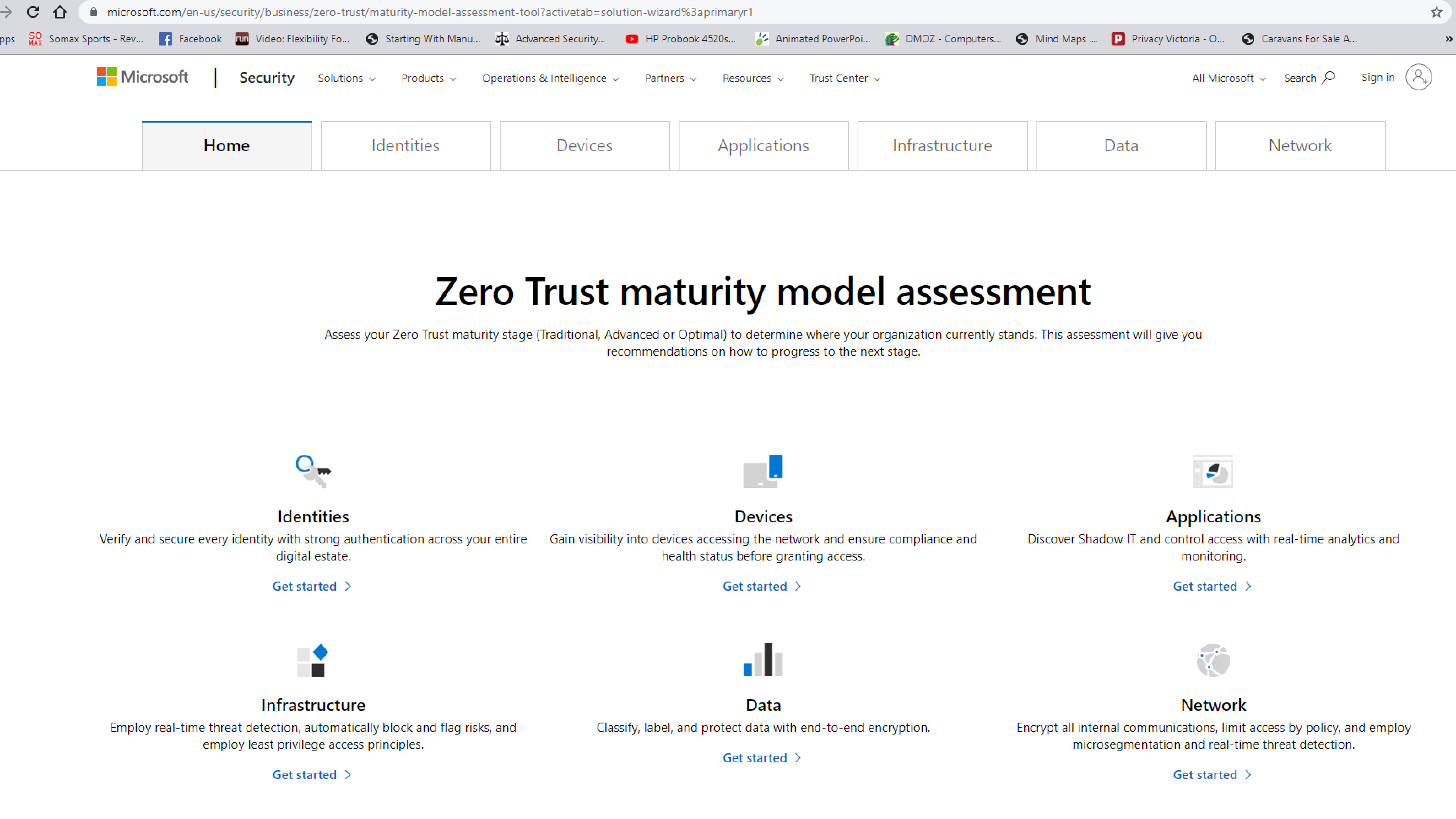


Enable a remote workforce by embracing Zero Trust security

Support your employees working remotely by providing more secure access to corporate resources through continuous assessment and intent-based policies.

Zero Trust assessment tool

Assess your Zero Trust maturity stage to determine where your organization is and how to move to the next stage.



Zero Trust maturity model assessment

Assess your Zero Trust maturity stage (Traditional, Advanced or Optimal) to determine where your organization currently stands. This assessment will give you recommendations on how to progress to the next stage.

Identities

Verify and secure every identity with strong authentication across your entire digital estate.

Get started >

Devices

Gain visibility into devices accessing the network and ensure compliance and health status before granting access.

Get started >

Applications

Discover Shadow IT and control access with real-time analytics and monitoring.

Get started >

Infrastructure

Employ real-time threat detection, automatically block and flag risks, and employ least privilege access principles.

Get started >

Data

Classify, label, and protect data with end-to-end encryption.

Get started >

Network

Encrypt all internal communications, limit access by policy, and employ microsegmentation and real-time threat detection.

Get started >

GTACS 2020

GOVERNANCE • TECHNOLOGY AUDIT • CONTROL • SECURITY

ISACA®

Singapore Chapter