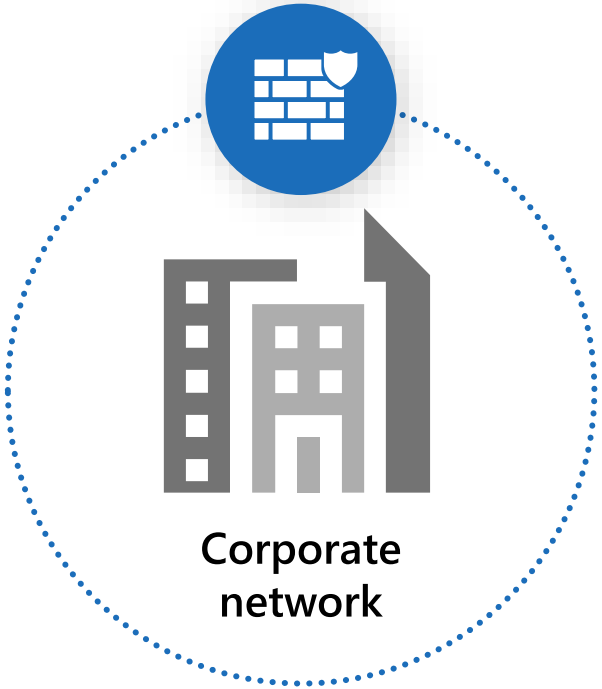
Implementing a Zero Trust Security Model

Abbas Kudrati | Microsoft

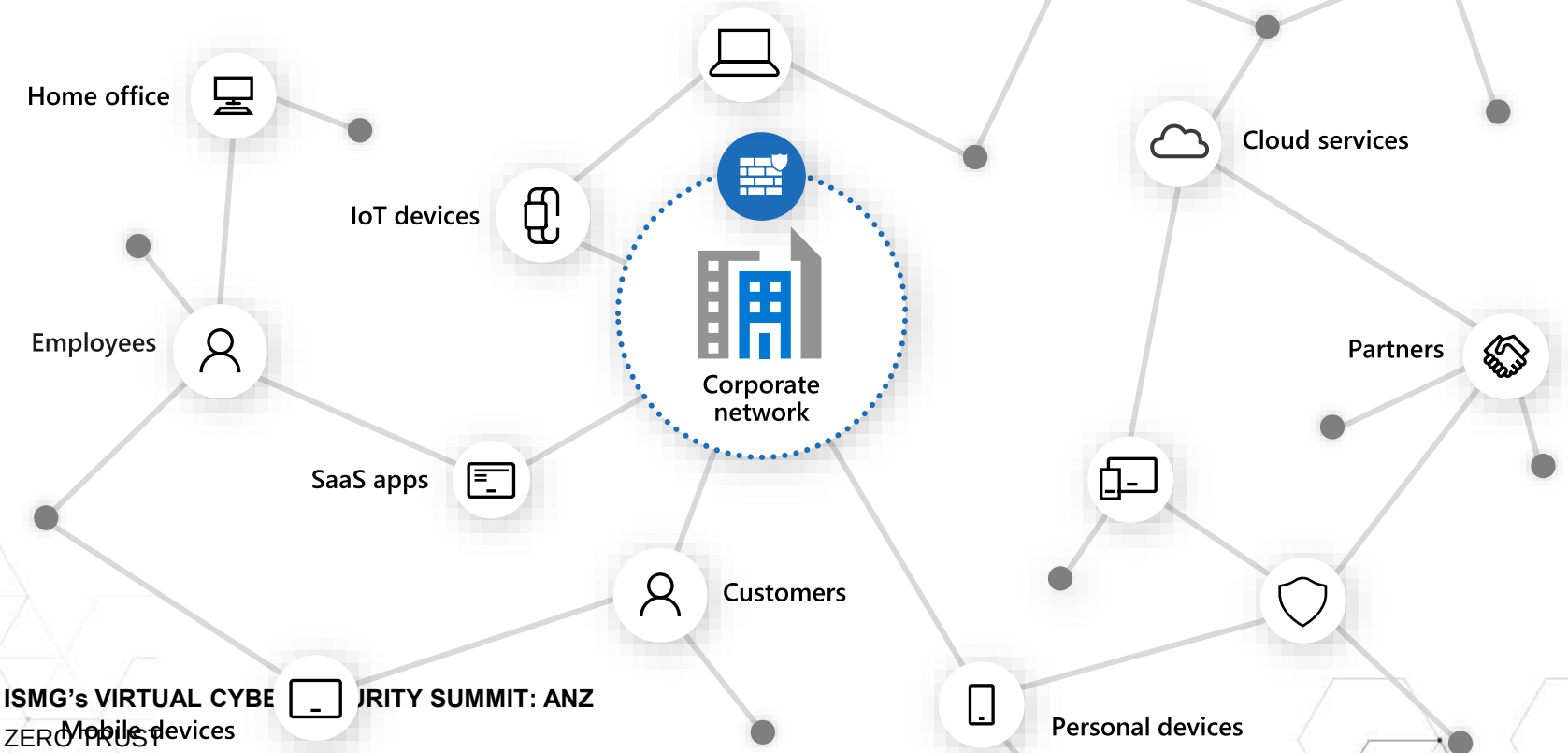
Traditional Model



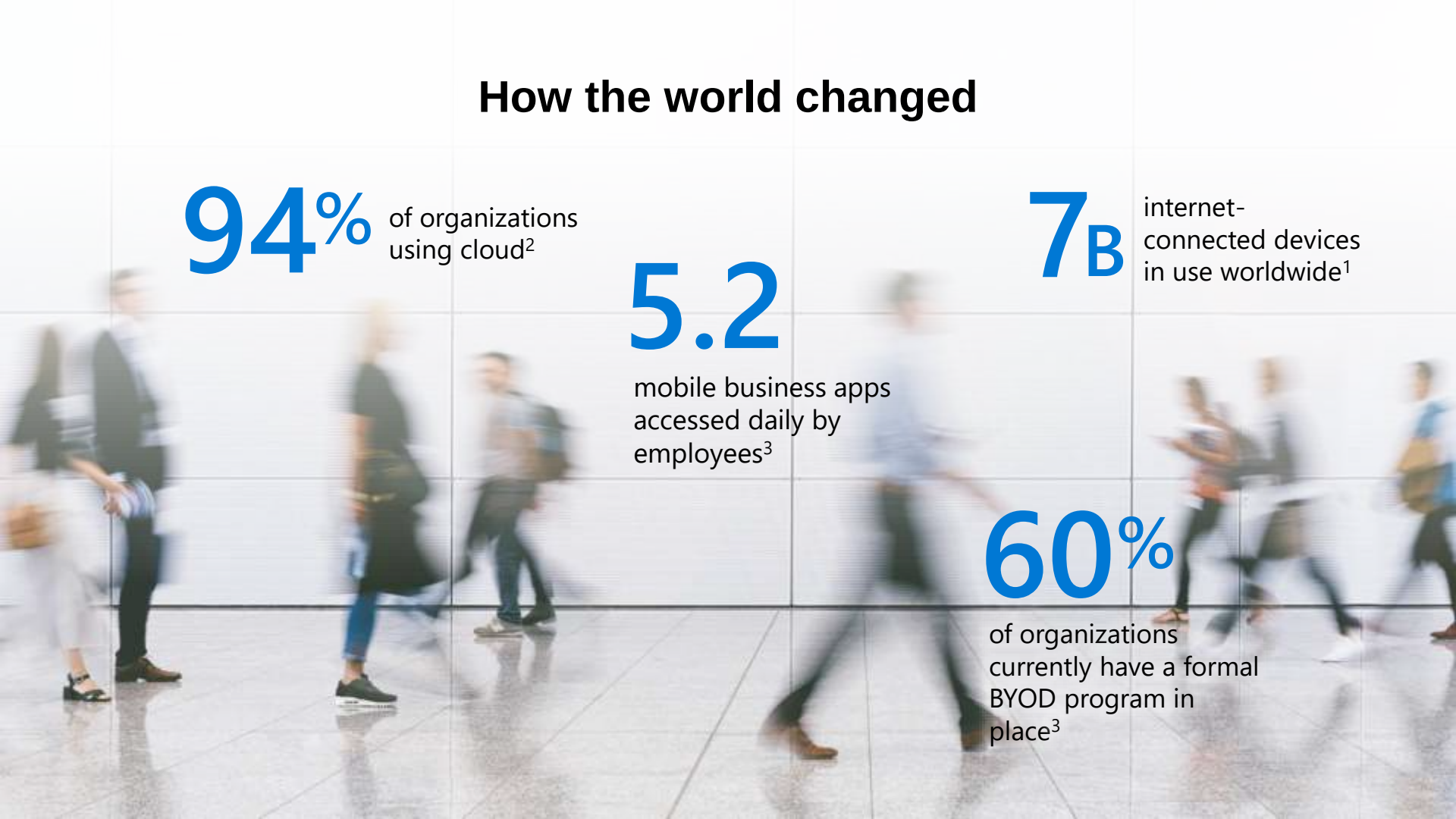
Users, devices, apps, and data protected behind a DMZ/firewall

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]

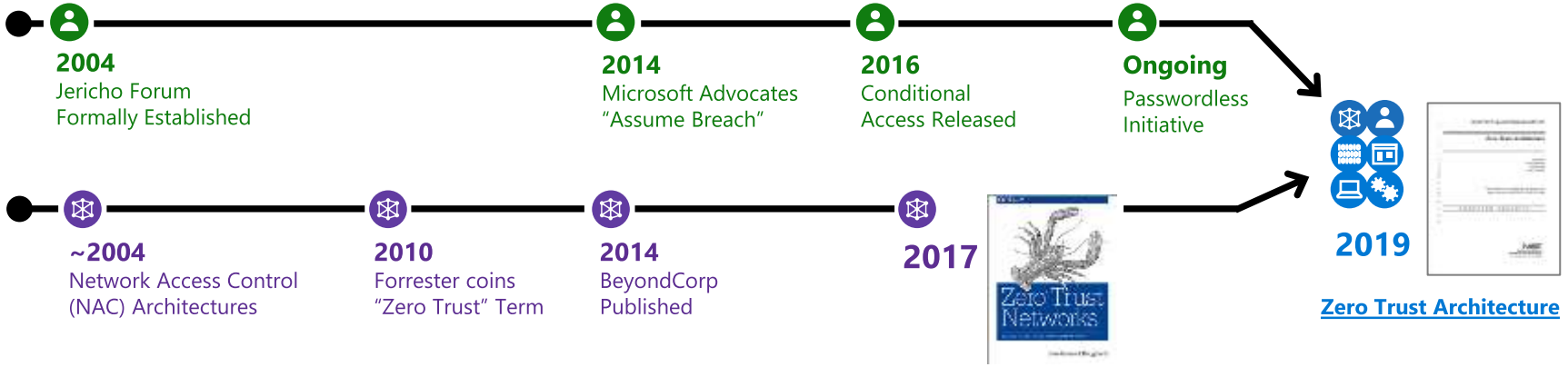
Old World vs. New World

~~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

Zero Trust

An integrated approach to securing access with adaptive controls and continuous verification across your entire digital estate

“Zero Trust” has been around for a while



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

Converged approach gaining significant momentum (though still ‘early days’ of this approach)

Zero Trust

Security strategy – Treat every access attempt as if it's originating from an untrusted network.

Leads to

Access Architecture
uses policy to:

1. **Explicitly validate trustworthiness**
2. **Dynamically address insufficient trust:**
   - Increase trust
   - Limit access
   - Block access

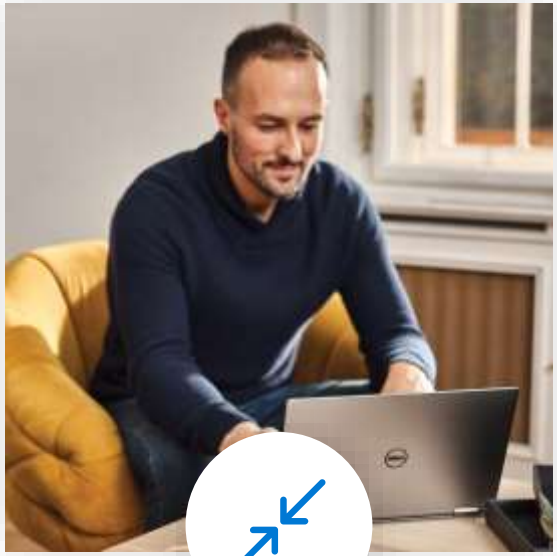
Mobility & Choice
to enable productivity

1. **Can work anywhere**
   - Applications & Data available anywhere
   - Security protections work anywhere
2. **Users can choose any device type**

Increases both security *and* productivity

A new reality needs new principles

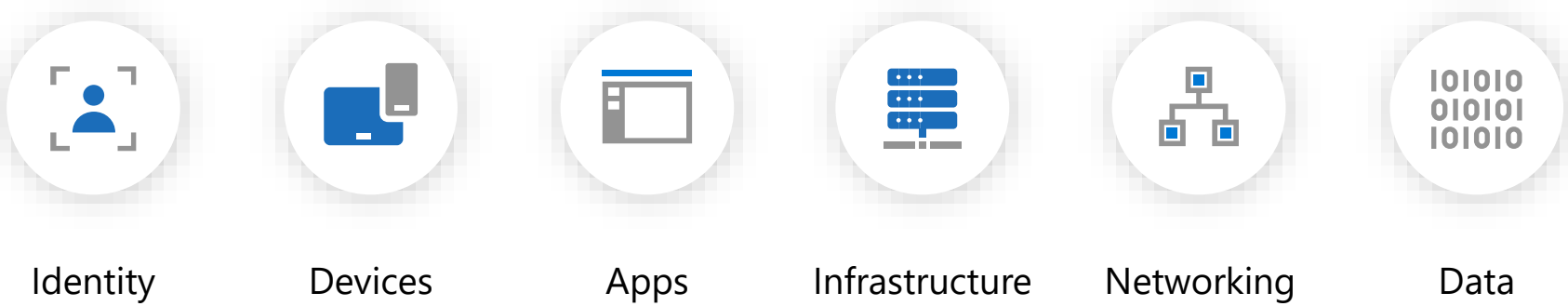
Verify explicitly



Use least privilege access

Assume breach

Zero Trust across the digital estate



Approach: Start with asking questions

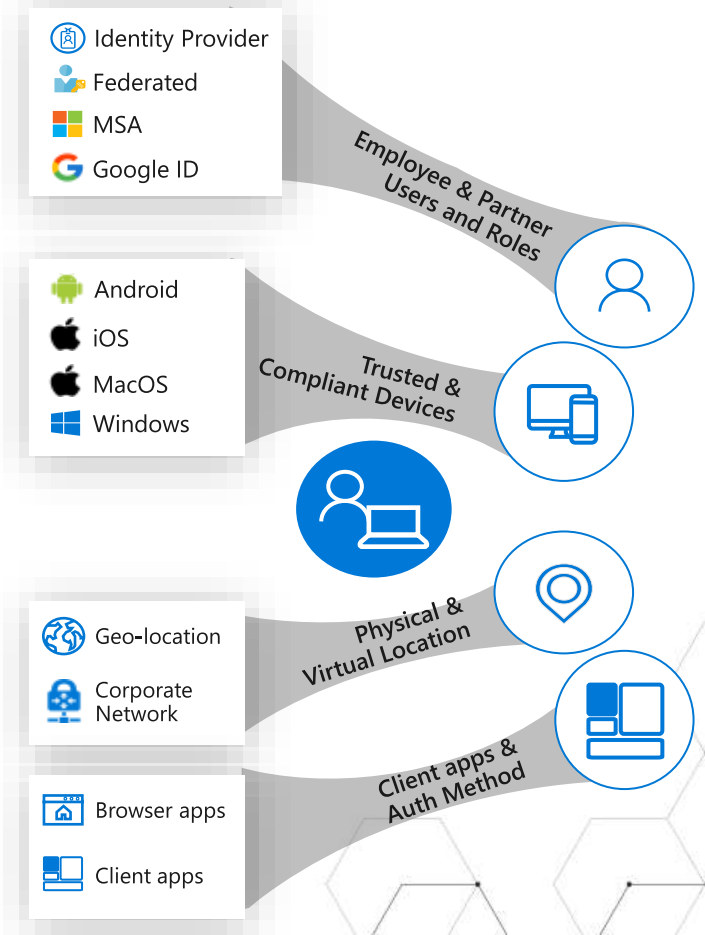
Who are your users? What apps are they trying to access? How are they doing it? Why are they doing it that way?

What conditions are required to access a corporate resource?

What controls are required based on the condition?

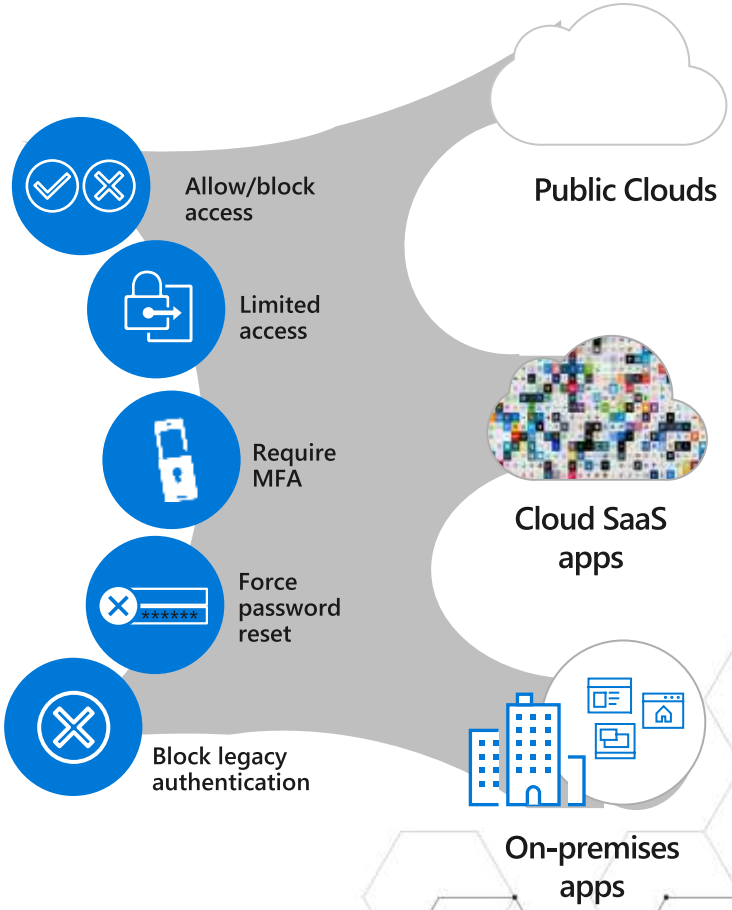
Consider an approach based on set of conditions

- What is the user's role and group membership?
- What is the device health and compliance state?
- What is the SaaS, on-prem or mobile app being accessed?
- What is the user's physical location?
- What is the time of sign-in?
- What is the sign-in risk of the user's identity? (i.e. probability it isn't authorized by the identity owner)
- What is the user risk? (i.e. probability a bad actor has compromised the account?

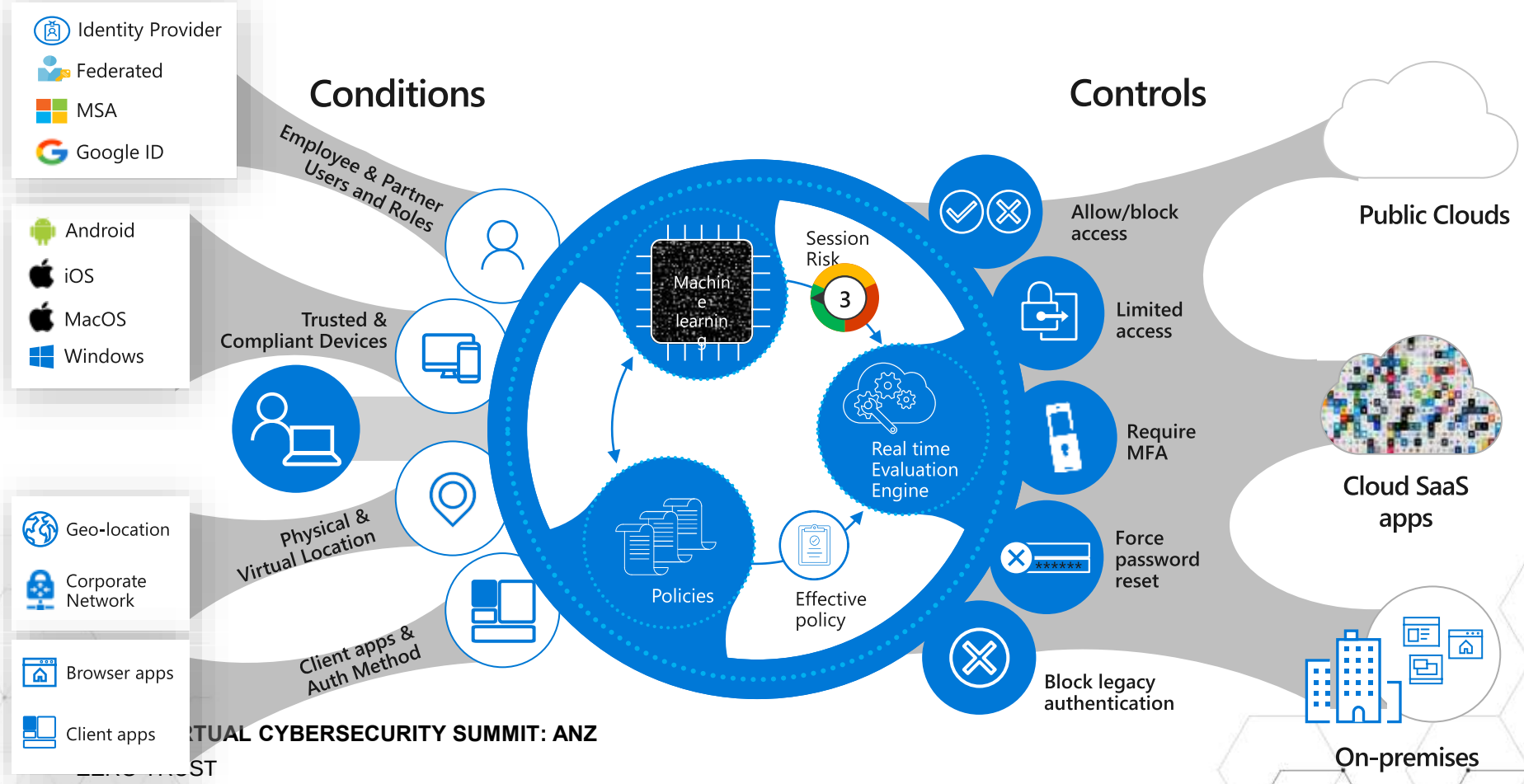


Followed by a set of controls (if/then statement)

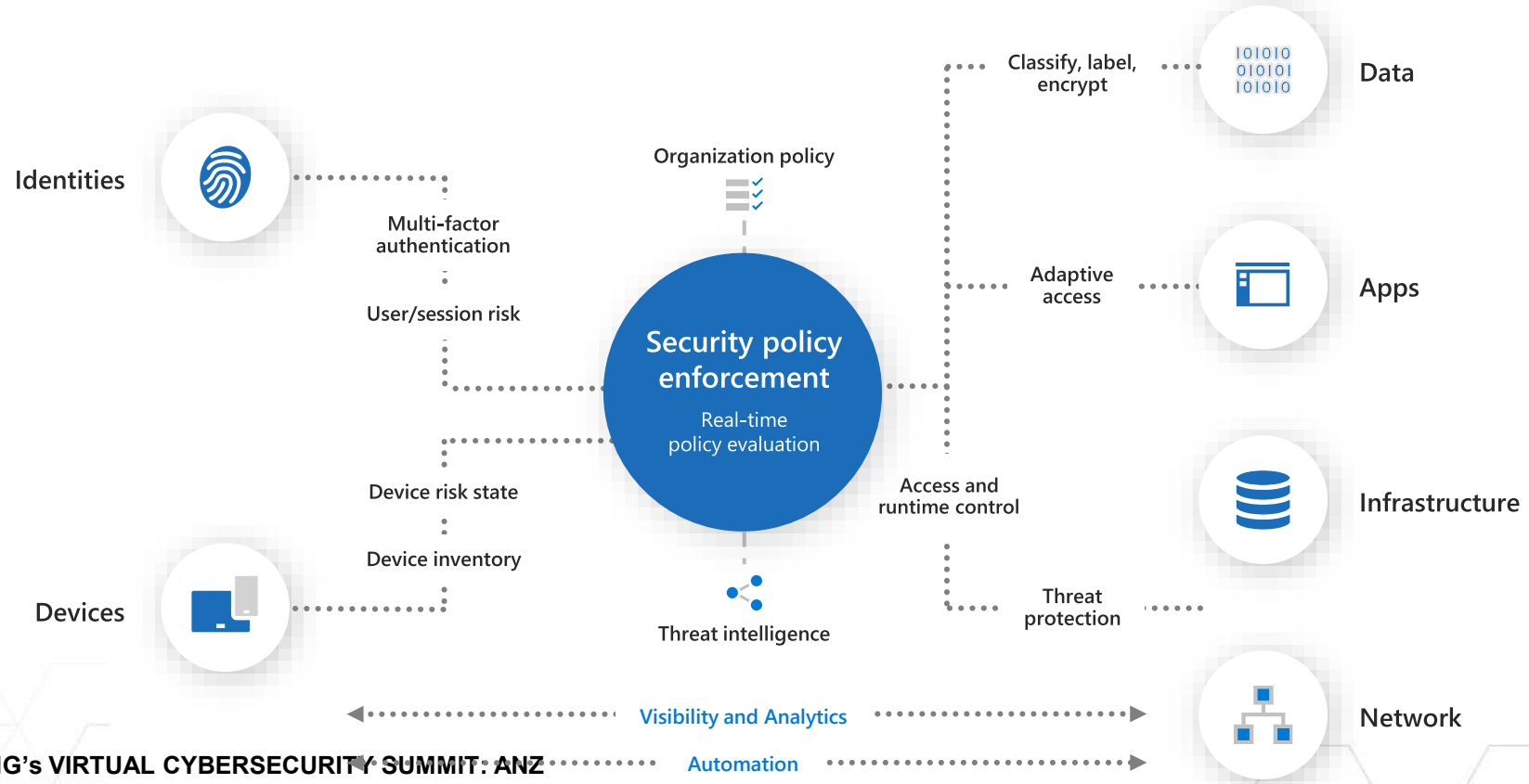
- Allow/deny access
- Require MFA
- Force password reset
- Control session access to the app (i.e. allow read but not download, etc)



Zero Trust based on conditional access controls



Microsoft 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

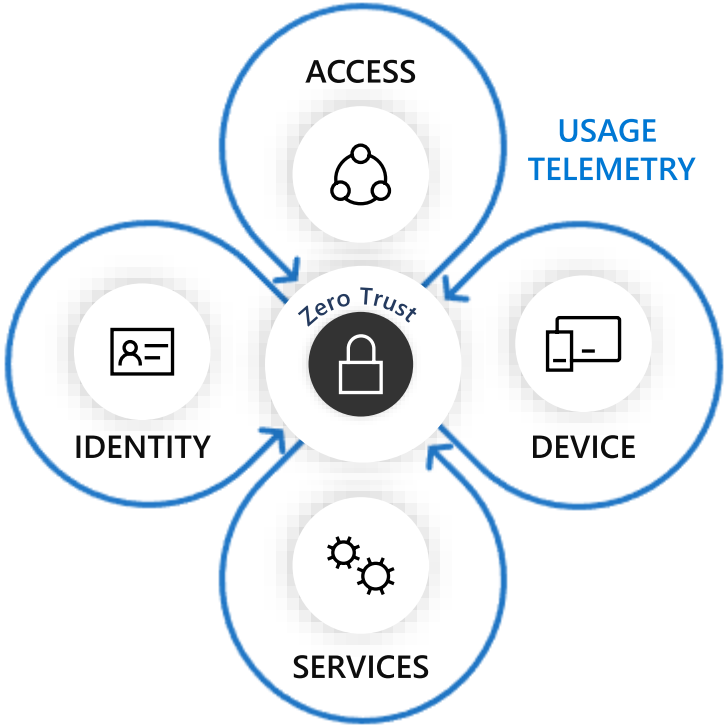
- ✓ Grow coverage in Device health requirement
- ✓ Service health concept and POC **(Future)**

User and Access Telemetry

How Microsoft achieved “Zero Trust”?

“Strong identity + device health + least privilege user access verified with telemetry”

- ✓ Assets are moved from the internal network to the internet… except for the most critical assets
- ✓ Enhanced user experience with Internet First
- ✓ Reduced attack surface of the environment
- ✓ Comprehensive telemetry, artificial intelligence for anomaly detection, service health verification



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

Microsoft's Recommended Zero Trust Priorities

Do the most important stuff first

1. **Align segmentation strategy & teams** by unifying network, identity, app, etc. into a single enterprise segmentation strategy (aligns naturally to Azure/Cloud migration)

2. **Build modern (identity-based) perimeter**

Critical Path

- **User -** Require Passwordless or MFA to access modern applications
- **Device -** Require Device Integrity for Access (critically important step)

Roll out critical path to IT Admins first

- Targeted by Attackers
- High potential impact
- Provide technical feedback

Finish Strategy

- Modernize Apps + Retrofit strong assurances to legacy on-premises assets via App Proxy
- Increase Protection levels for sensitive data (CASB, CA Access Control, AIP)
- Retire legacy authentication protocols (retiring some required for effective MFA)

3. **Refine segmentation and network perimeter**

- Segment assets with business critical, life safety, and operational/physical impact.
- Add microsegementation to further reduce risk (static and/or dynamic trust-based restrictions)
- Retire or isolate legacy computing platforms (Unsupported OS/Applications)

microsoft.com/en-us/security/business/zero-trust

Apps | Somax Sports - Rev... | Facebook | Video: Flexibility Fo... | Starting With Manu... | Advanced Security... | HP Probook 4520s... | Animated PowerPoi... | DMOZ - Computers... | Mind Maps ... | Privacy Victoria - O...

Microsoft | Security Solutions Products Operations & Intelligence Partners Resources Trust Center All Microsoft

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.

Watch now | Read maturity model paper

Zero Trust assessment tool

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

Take the assessment >

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 >

Q&A

aka.ms/zero-trust