Microsoft

Zero Trust Network Architecture: Security built for the modern world

Abbas Kudrati
Chief Cybersecurity Advisor
Cybersecurity Solutions Group
Microsoft AU, Asia
Abbas.Kudrati@Microsoft.com
https://aka.ms/abbas
@askudrati

Current roles:

- **Chief Cybersecurity Advisor** – Microsoft Asia
- **Industry Professor – Deakin University**
- **Professor of Practice in Cyber Security** – LaTrobe University
- **Executive Advisory Board Member – Cyber Security** – Deakin University, LaTrobe University and 6Clicks
- **Global Threat Advisory Board Member** – EC-Council ASPAC

Previous roles (last 6):

- KPMG Australia : **CISO**
- Public Transport Victoria : **CISO**
- National Bank of Kuwait : Dy **CISO**
- eGovernment Authority – Bahrain: **CISO**
- Ernst & Young – Bahrain : **Manager Cyber Advisory**
- KPMG Kuwait, Bahrain Qatar : **Sr, Consultant**

Awards & Accolades:

- **2019 "Top Cybersecurity Advisor for APJ" Microsoft**
- **2018 "Best Security Professional"** ISACA Oceanic CACS
- **2018 "CISO 100 Award"** by CISO Council, UAE
- **2017** SPLUNK **"Boss of the SOC "BOTS"** Winner for Melbourne region
- **2015** Australian **"CISO of the year"** finalist
- **2014** Middle East **"IT Governance Professional of year"**
- **2011** Middle East **"Security Strategist of year"**

Professional Certificates & Qualifications:

1. Certified Chief Information Security Officer **(C|CISO)**
2. Certified Information Security Manager **(CISM)**
3. Certified in Cloud Security Knowledge **(CCSK)**
4. Certified Information System Auditor **(CISA)**
5. **Certified Cybersecurity Practitioner (CSX-P)**
6. Certified in Governance of Information Technology
7. Certified Block Chain Expert **(CBE)**
8. Certified Ethical Hacker **(C|CEH)**
9. Certified Computer Forensic Hacking Investigator
10. TOGAF 8 Certified Enterprise Architect **(TOGAF CEA)**
11. **COBIT 5** Foundation Certified
12. **ISO 27001: 2005** Lead Auditor
13. **PRINCE 2** Practitioner and Foundation Certified
14. ITIL Foundation Certified **(ITIL)**
15. EC Council Disaster Recovery Professional **(E|DRP)**
16. SABSA Foundation Certified
17. **Microsoft Certified Azure Foundation**
18. **Microsoft Certified M365 Foundation**
19. Microsoft Certified Systems Engineer+ Security
20. **Cisco Certified Network Associate** (CCNA)
21. GNIIT Diploma in Systems Management
22. Bachelor of Commerce – Accounting and Auditing

Unpredictable change

The information security landscape is transforming in ways most organizations couldn't have predicted even five years ago. The complexity of the modern workplace is overwhelming the capabilities of traditional security strategies and tools.

Remote work

1.87 billion workers, nearly half of the global workforce, will be mobile workers by **2022**

Personal devices

64% of employees now use personal devices for work purposes

Third-party services

28% increase in cloud and SaaS threats over the last year alone[1]

Cyber attacks

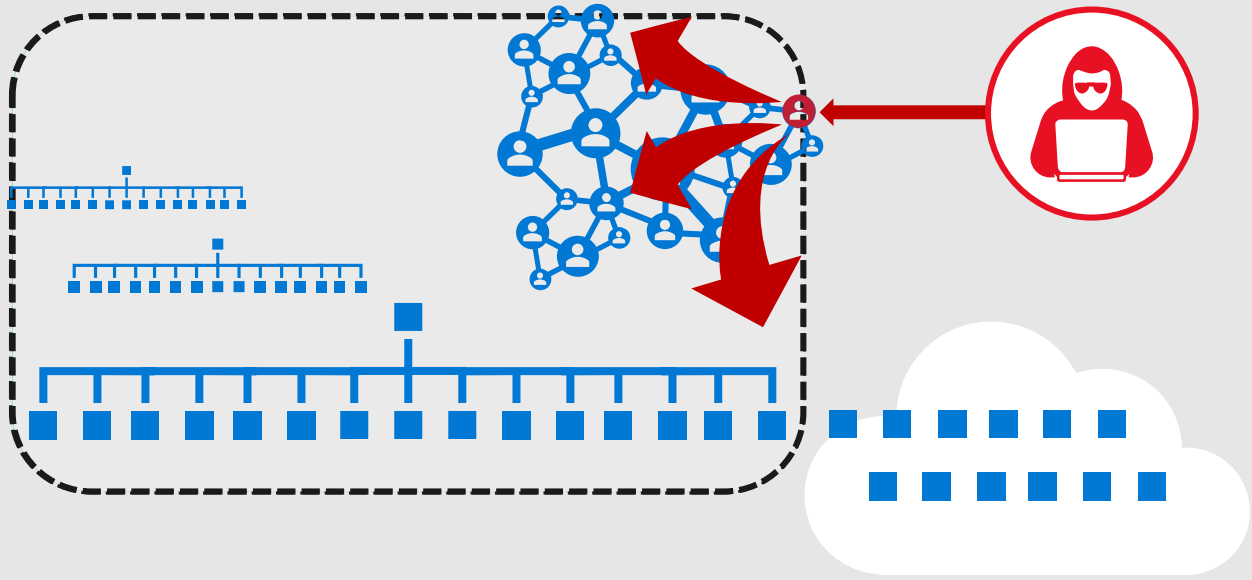
11% increase in cyberattacks in the last year, **67%** over the last five years[2]

Privacy & compliance

Organizations are bombarded by more than **200** updates a day from more than **75** regulatory bodies around the world.

Why are we having a Zero Trust conversation?

Access Control: Keep **Assets** away from **Attackers**



1. **IT Security is Complex**
   - Many Devices, Users, & Connections
2. **"Trusted network" security strategy**
   - Initial attacks were network based
   - *Seemingly* simple and economical
   - Accepted lower security within network
3. **Assets increasingly leave network**
   - BYOD, WFH, Mobile, and SaaS
4. **Attackers shift to identity attacks**
   - Phishing and credential theft
   - Security teams often overwhelmed

This "Zero Trust" idea has been evolving for a while

2004
Jericho Forum Formally Established

~2004
Network Access Control (NAC) Architectures

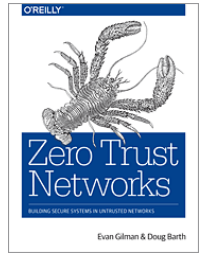
2010
Forrester coins "Zero Trust" Term

2014
Microsoft Advocates "Assume Breach"

2014
BeyondCorp Published

2016
Conditional Access Released

2017



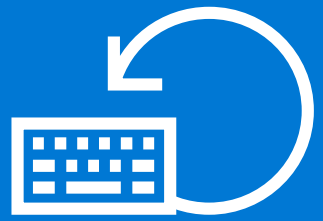
Ongoing
Passwordless Initiative

Slow mainstream adoption for both network identity models:

Network – Expensive and challenging to implement
Google's BeyondTrust success is rarely replicated

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

Trends and challenges



Attackers using identity to bypass network controls

Phishing allow attackers to impersonate valid user Identities

Credential theft allows attackers to expand access by impersonating identities

Passwords aren't enough to protect identities

Single factor authentication (Passwords) without context isn't enough assurance

Attacks on credentials circumvent software assurances (without hardware isolation)

Identities being used outside network

Cloud, Mobile, and IoT assets are frequently beyond reach of enterprise firewalls

Identity and Access controls are inconsistent on different cloud services and devices

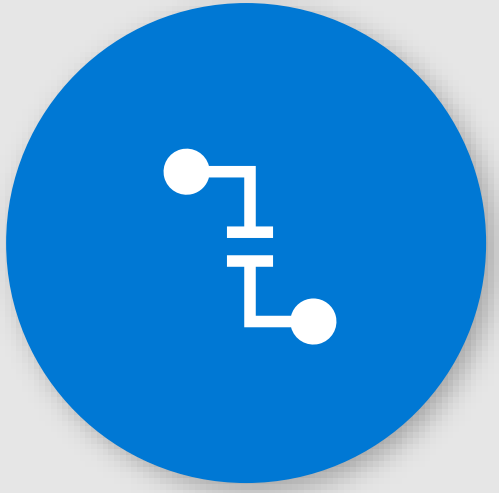
Zero Trust Principles

Verify Explicitly

Always authenticate and authorize based on all available data points, including user identity, location, device health, data classification, and anomalies.

Least Privilege

Minimize user access with Just-In-Time and Just-Enough Access (JIT/JEA), risk-based adaptive polices, and data protection which protects data and productivity.

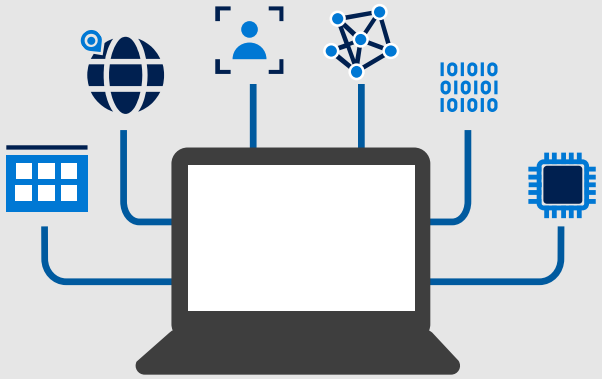


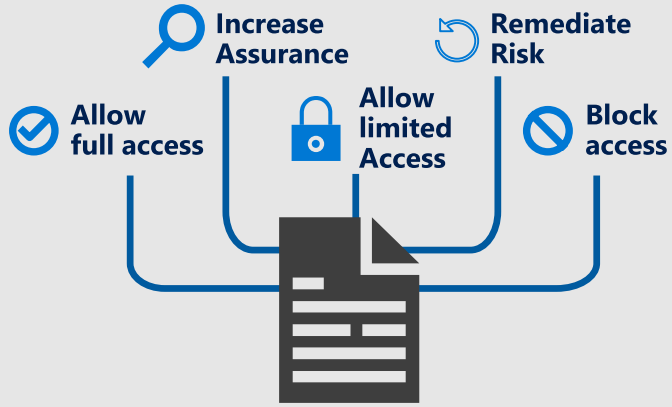
Assume Breach

Minimize scope of breach damage and prevent lateral movement by segmenting access via network, user, devices and application awareness. Verify all sessions are encrypted end to end. Use analytics to get visibility and drive threat detection.

Zero Trust Access Control Strategy

Never Trust. Always verify.





Signal

to make an informed decision

Device Risk
- Device Management
- Threat Detection
- and more…

User Risk
- Multi-factor Authentication
- Behavior Analytics
- and more…

Decision

based on organization's policy

Apply to inbound requests

Re-evaluate during session

Enforcement

of policy across resources

Modern Applications
SaaS Applications
Legacy Applications
And more…

Approach: Start with asking questions

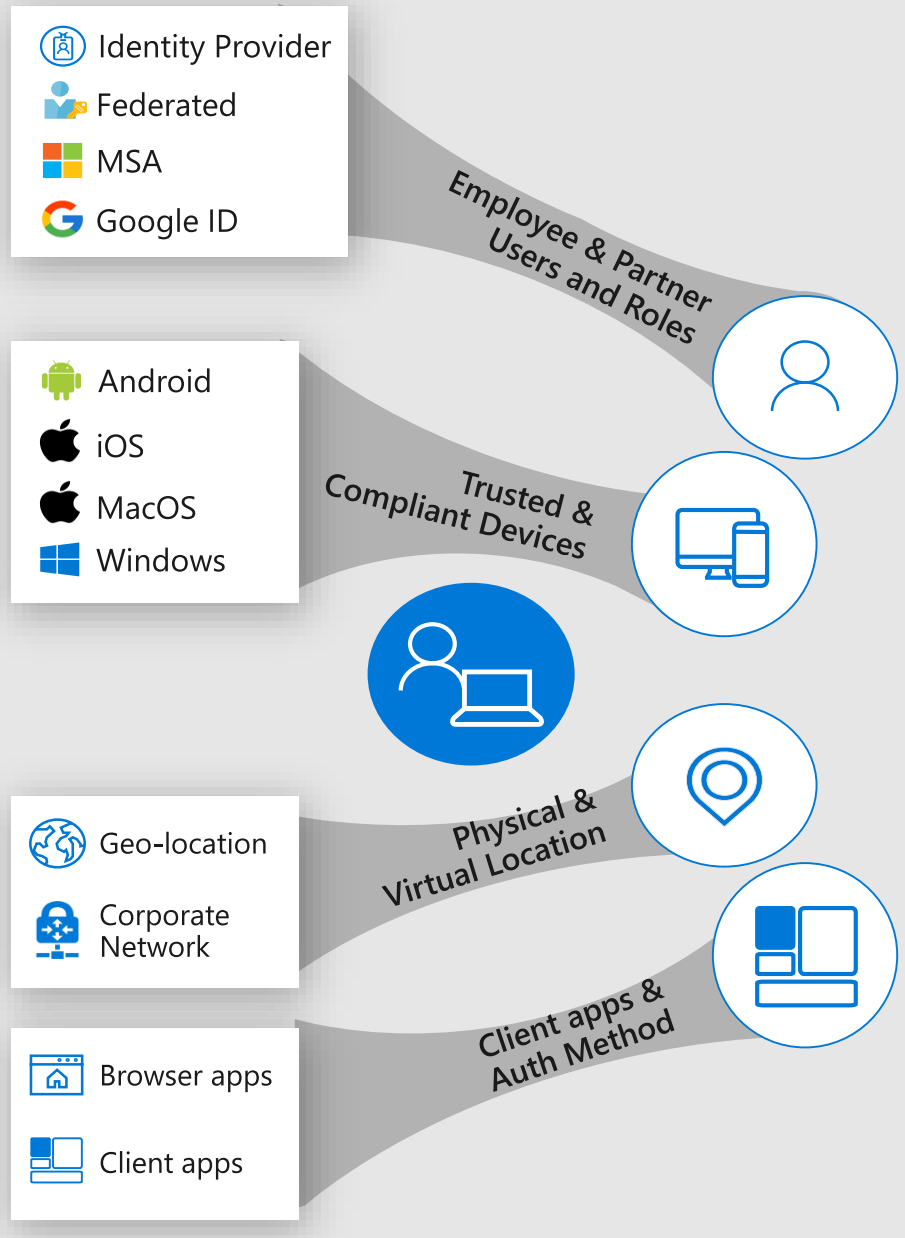
Who are your users? What apps are they trying to access? How are they doing it? Why are they doing it that way?

What conditions are required to access a corporate resource?

What controls are required based on the condition?

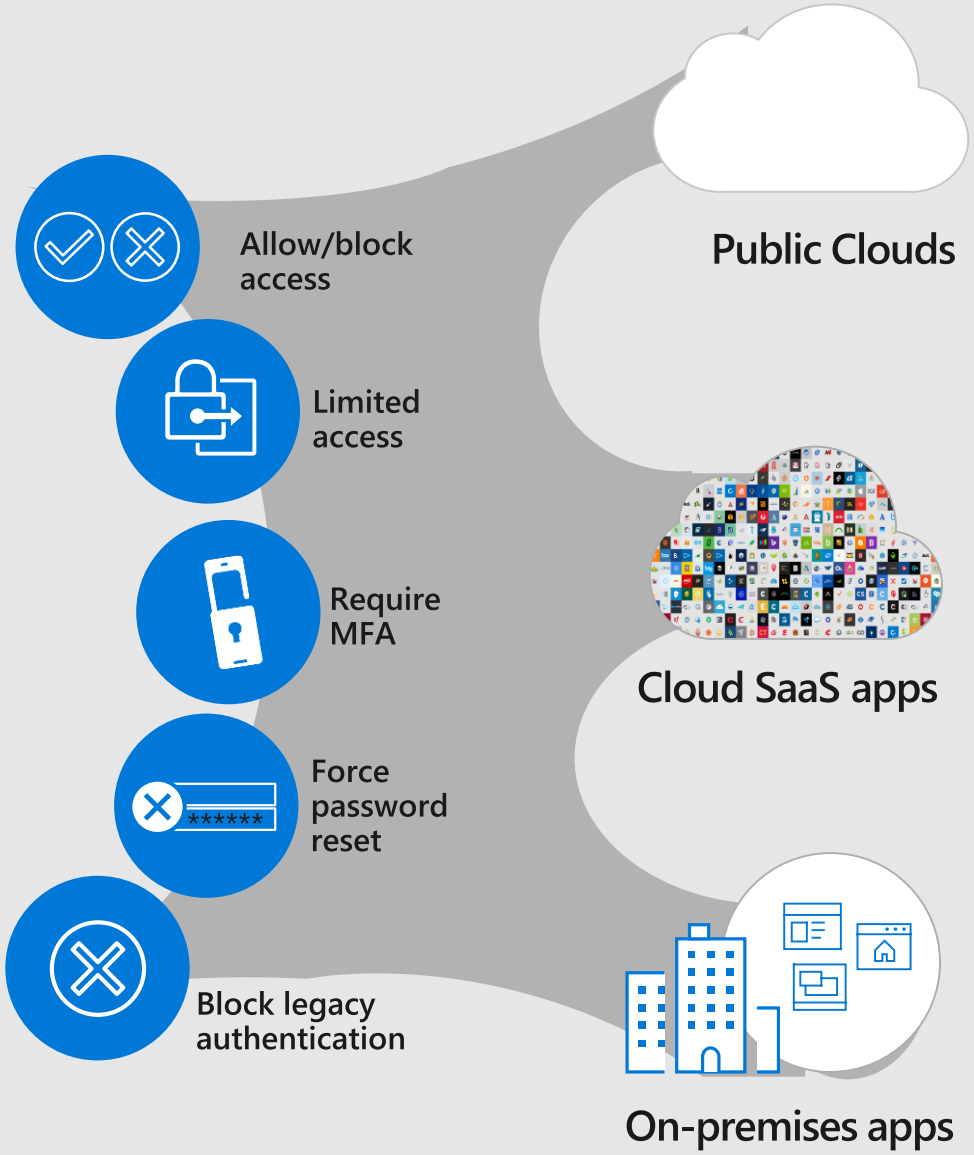
Consider an approach based on set of conditions

- 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?

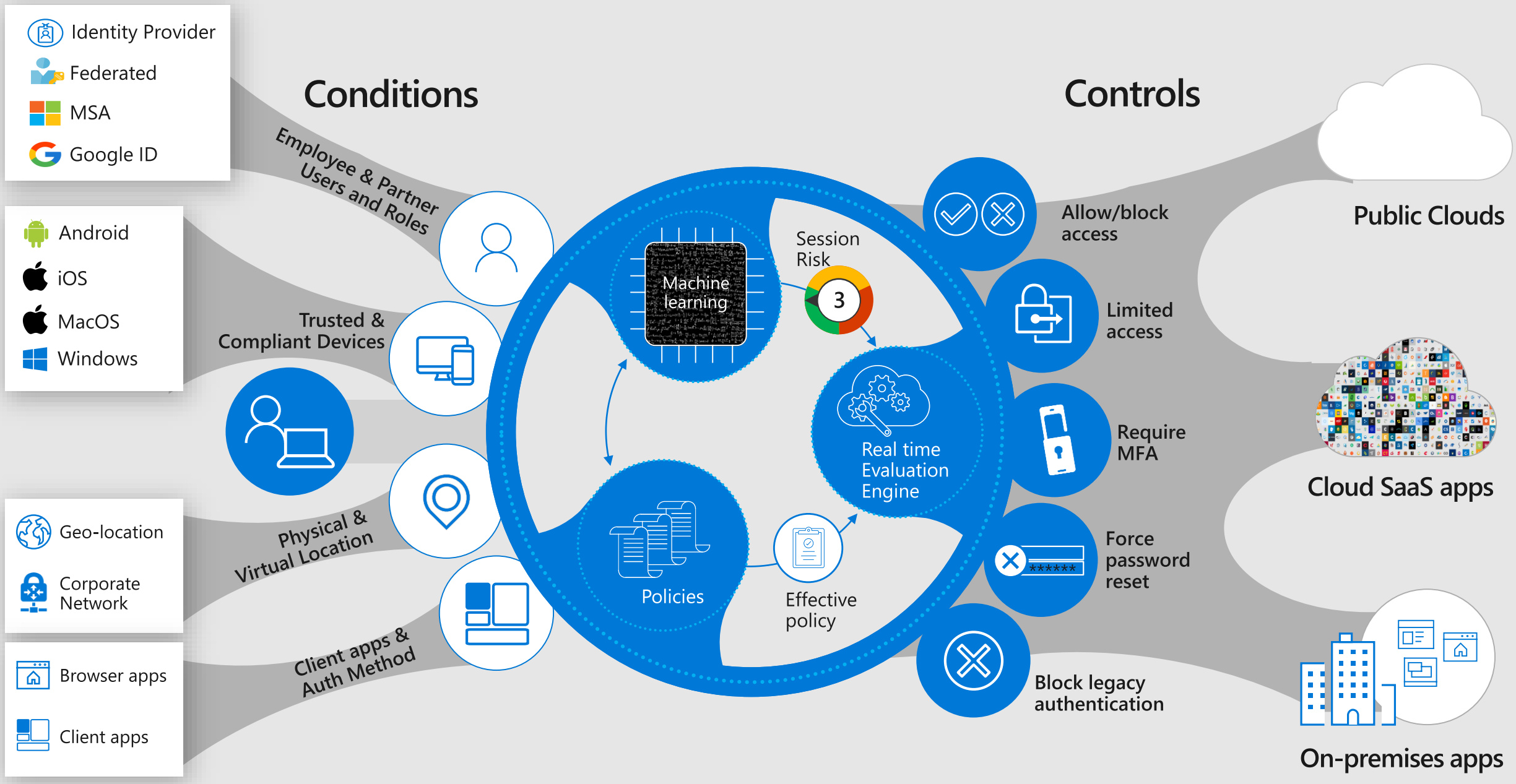


Followed by a set of controls (if/then statement)

- 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's Recommended Zero Trust Priorities

Do the most important stuff first

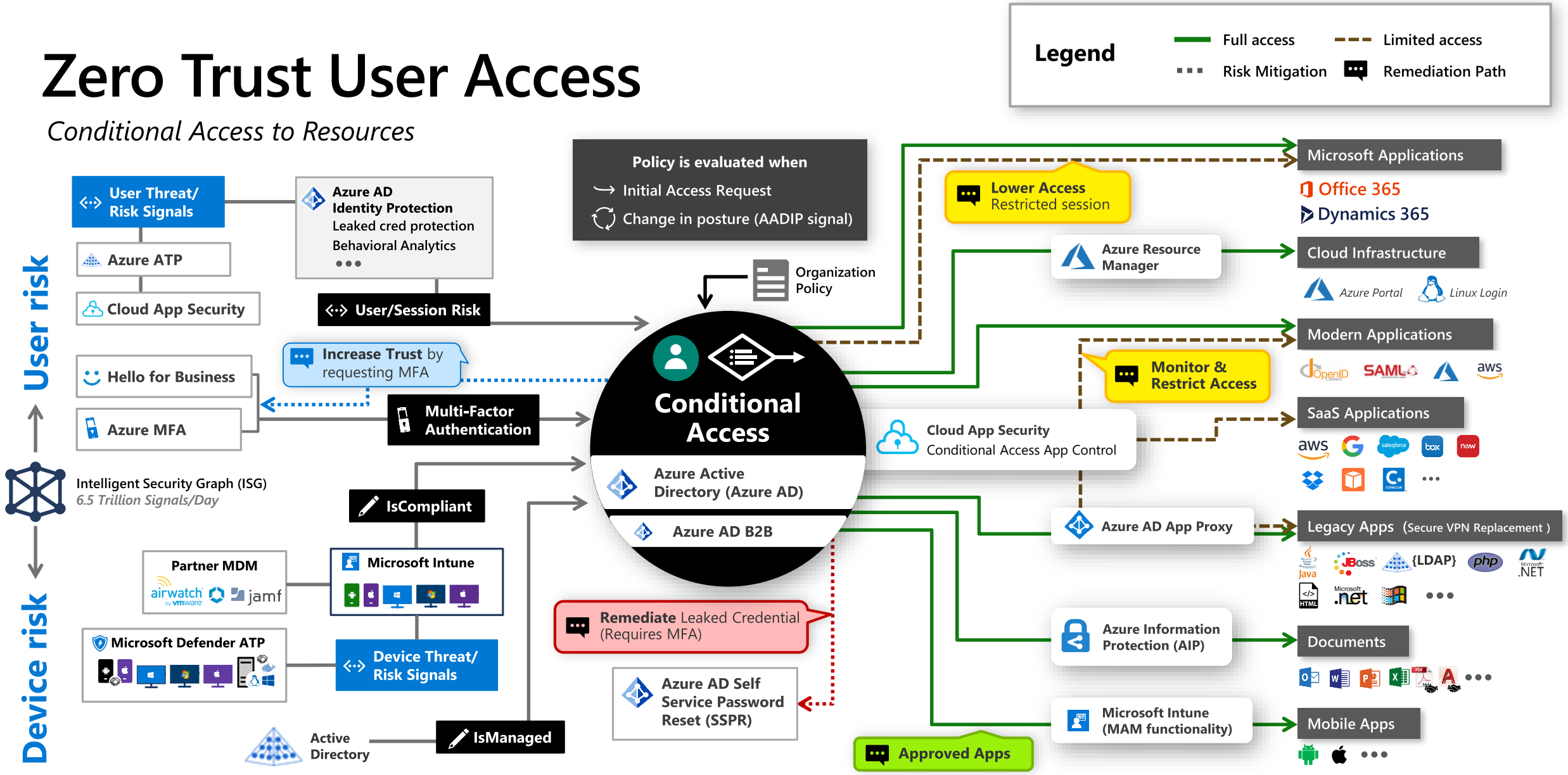
1. **Align segmentation strategy & teams** by unifying network, identity, app, etc. into a single enterprise segmentation strategy (as you migrate to Azure)

2. **Build identity-based perimeter** to protect modern ***and*** legacy enterprise assets

3. **Refine network perimeter** using microsegmentation (if required for residual risk)

Zero Trust User Access

Conditional Access to Resources



Signal
to make an informed decision

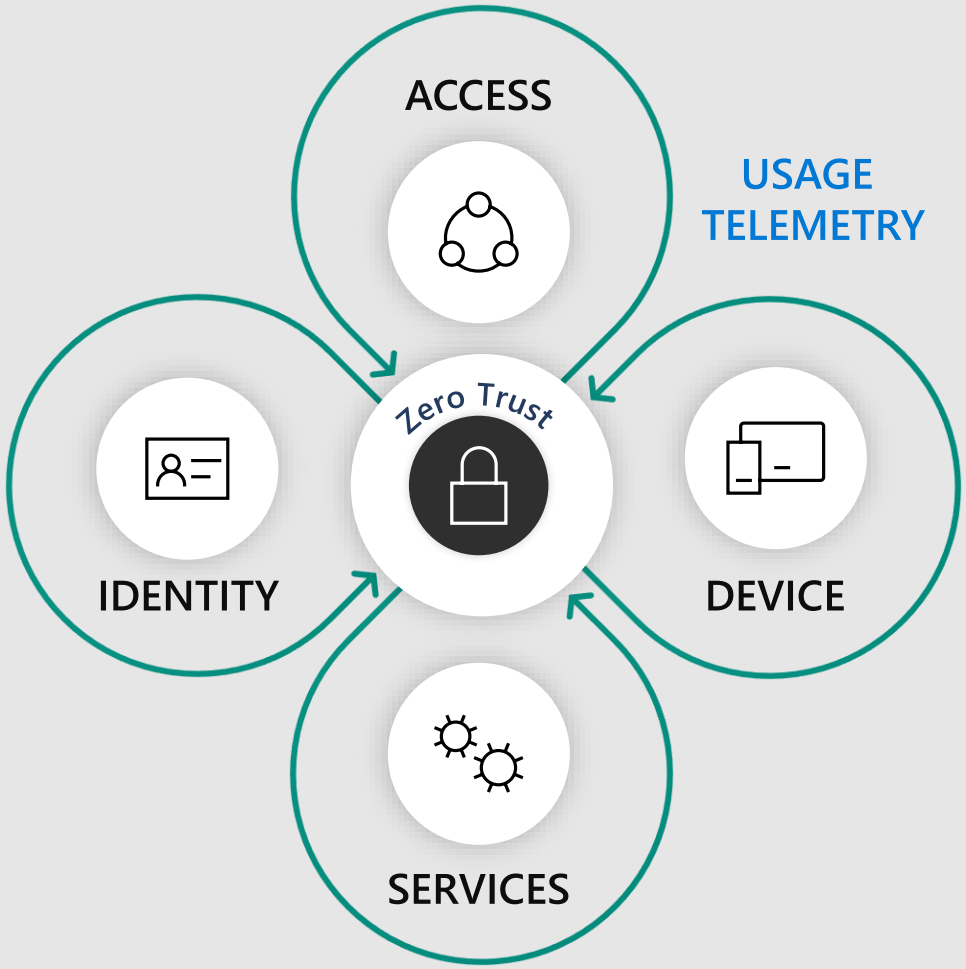
Decision
based on organizational policy

Enforcement
of policy across resources

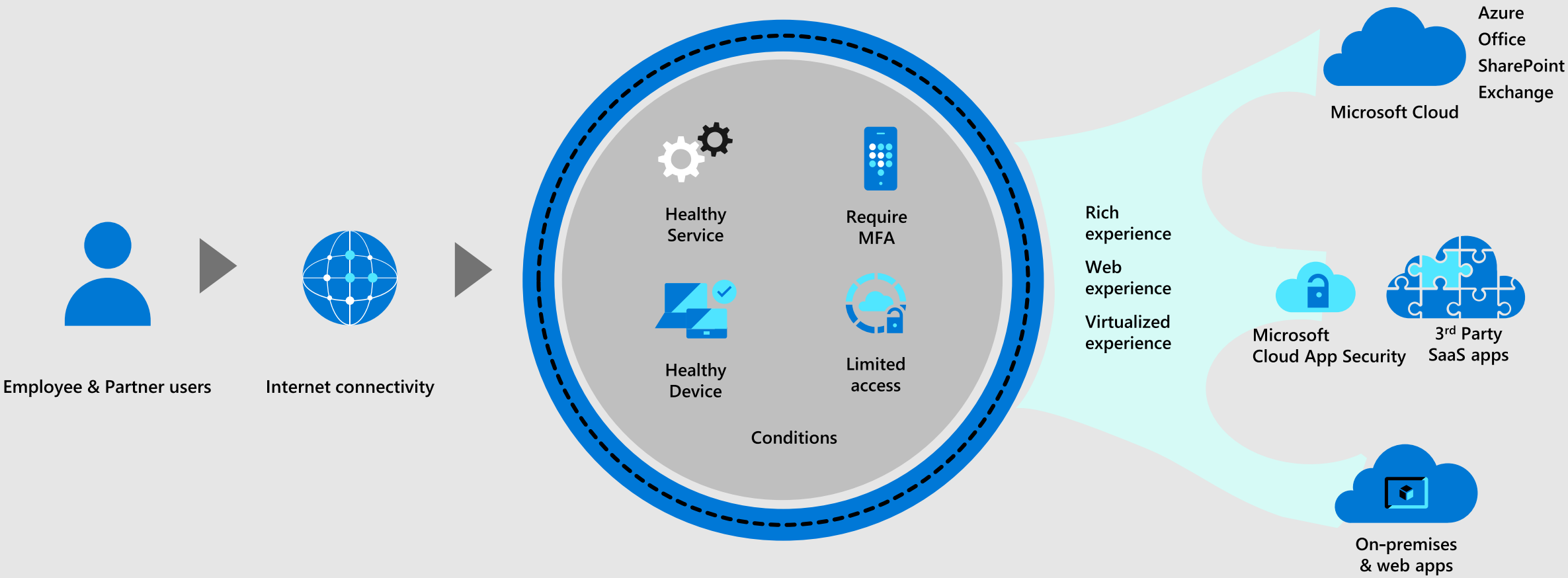
How Microsoft achieved “Zero Trust”?

“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 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

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 **(Distant Future)**

User and Access Telemetry

Key Takeaways

- Networks that fail to evolve from traditional defenses are vulnerable to breaches. We must assume breach.
- Zero Trust *can* enable new business outcomes that were not possible before.
- Technology has evolved to now make these scenarios possible, and you may already own it.
- Consider an "*if-this-then-that*" automated approach to Zero Trust.
- Identity is everything, make it the control plane.

Next step : How to get started

Next week you should:

- Understand what “zero trust controls” your identity solution provides.
- Discover what products in your environment can integrate with your identity solution to help you create a zero trust story for your organization. (i.e. firewall, VPN, MDM, EDR, DLP, etc).

Next step : How to get started

In the first three months you should:

- Build a persona profile (set of conditions) required for your end users with an understanding of who they are, where they are going, and what they want.
  - i.e. The state of the identity (verified or compromised), what types of devices they are using, from which locations, and to what applications.

- Identify what controls are required to respond to those specific conditions
  - i.e. If accessing an app (e.g. SharePoint or G-Suite) from an untrusted device, do I need to challenge with multi-factor authentication? Or require to first enroll the device into MDM/Domain *then* allow access? If the identity is compromised and credentials in public, block access.

Next step : How to get started

Within six months to one year you should:

- Identify two “zero trust” controls from above to conduct a production proof of concept. Develop a test plan to effectively test controls. Gather datapoints and effectiveness of policies. Fine tune if needed.
- Consider a limited production pilot with group of “friendlies” (business users). Study their behavior, gather feedback/datapoints, and understand if/how the policies impact their productivity. Fine tune if needed.
- Develop an architecture and project plan to roll out those two controls out to the organization with a roadmap of future controls. **Become a rockstar.**

Microsoft Zero Trust Readiness

Priority	Zero Trust Networking components	Microsoft Product
Foundational components	Device Management	Azure AD + Intune + Windows + ATP
	User/Group Inventory	Azure AD
	User & Device/Group management	Azure AD
	Device health checking	Azure AD + Intune + Windows
	Removal of corpnet access (Wired Port Security)	Windows+ Intune
	Policy Language & Access Decision Engine	AAD conditional access
Core expectations	Access Proxy	Azure App Proxy
Guests and non-managed scenarios	Access for non-managed devices	Windows VD & Office
Desirable for simplified user experience	User experience – Application Discovery	AAD Access Panel + Company Portal+ Bing for work+ TBD
	User experience – Application Launch	Power Apps + Desktop+ Web + TBD

Q&A