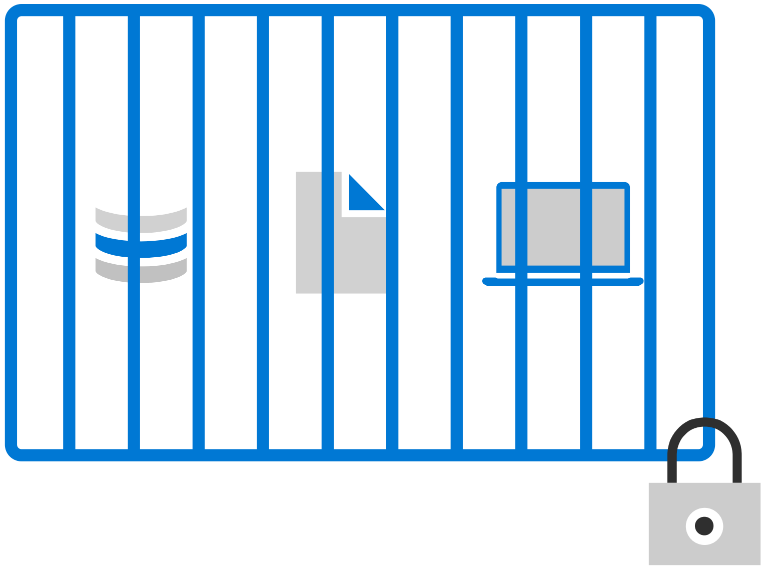
Microsoft Security

Strengthening Security Foundation with Zero Trust
零信任強化資訊保安基礎

Kevin Liu, CISSP, CEH, ITIL
Security and Modern Work Technical Specialist

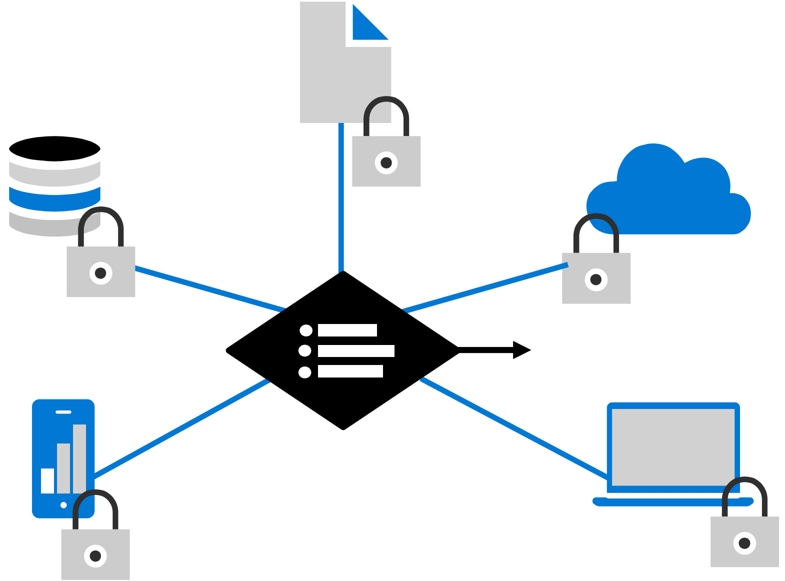
Secure assets where they are with Zero Trust

Simplify security and make it more effective



Classic Approach

Restrict everything to a 'secure' network

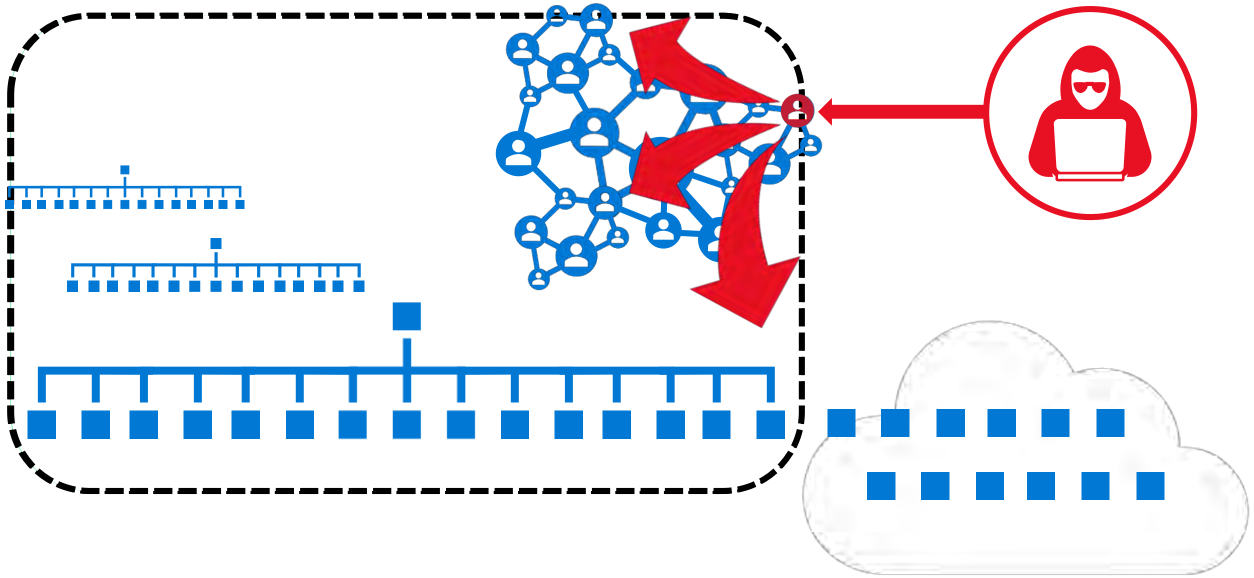


Zero Trust

Protect assets anywhere with central policy

Why Zero Trust is important?

Keep **Assets** away from **Attackers**



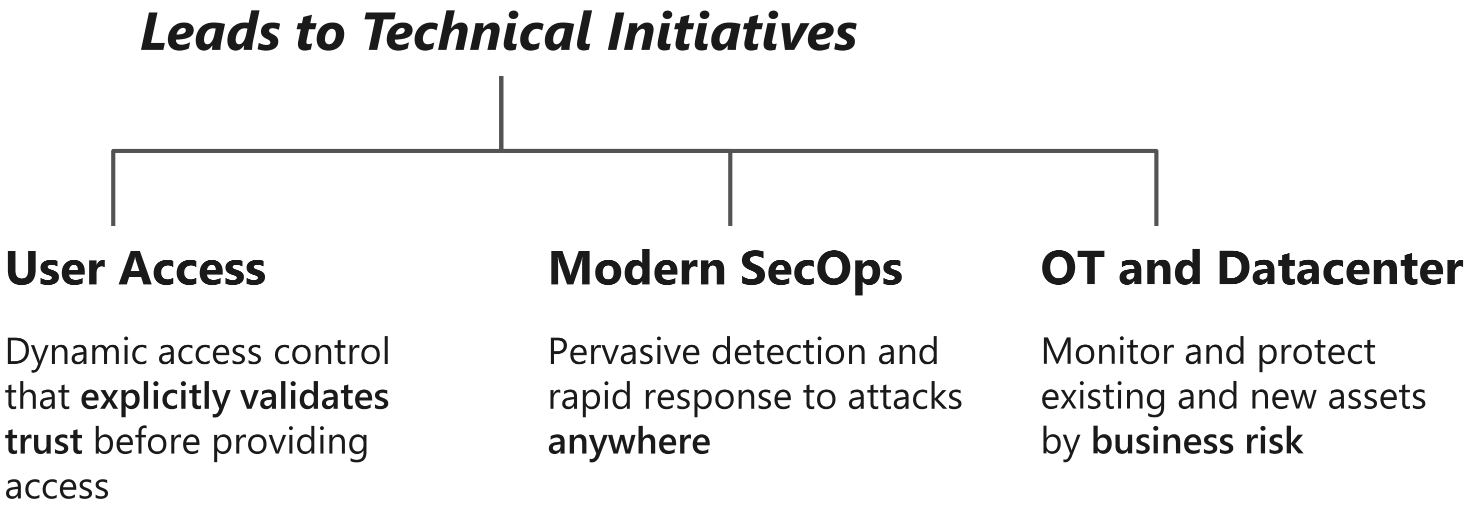
1. **IT Security is Complex**
   - Many Devices, Users, & Connections
2. **“Trusted network” security strategy**
   - Initial attacks were network based
   - *Seemingly* simple and economical
   - Accepted lower security within the network
3. **Assets increasingly leave the network**
   - BYOD, WFH,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

Zero Trust

- ● Simplify
- ● Integrate
- ● Automate
- ● Consolidate

Security Strategy for

- **business assets** (data, applications, devices)
- **everywhere** (private & public networks)



Leads to Technical Initiatives

User Access

Dynamic access control that **explicitly validates trust** before providing access

Modern SecOps

Pervasive detection and rapid response to attacks **anywhere**

OT and Datacenter

Monitor and protect existing and new assets by **business risk**

Increases security

Increases productivity

Microsoft Zero Trust Principles

Guidance for technical architecture

Verify explicitly

Always validate all available data points including

- User identity and location
- Device health
- Service or workload context
- Data classification
- Anomalies

Use least privilege access

To help secure both data and productivity, limit user access using

- Just-in-**time** (JIT)
- Just-**enough**-access (JEA)
- Risk-based **adaptive** polices
- Data protection against **out of band** vectors

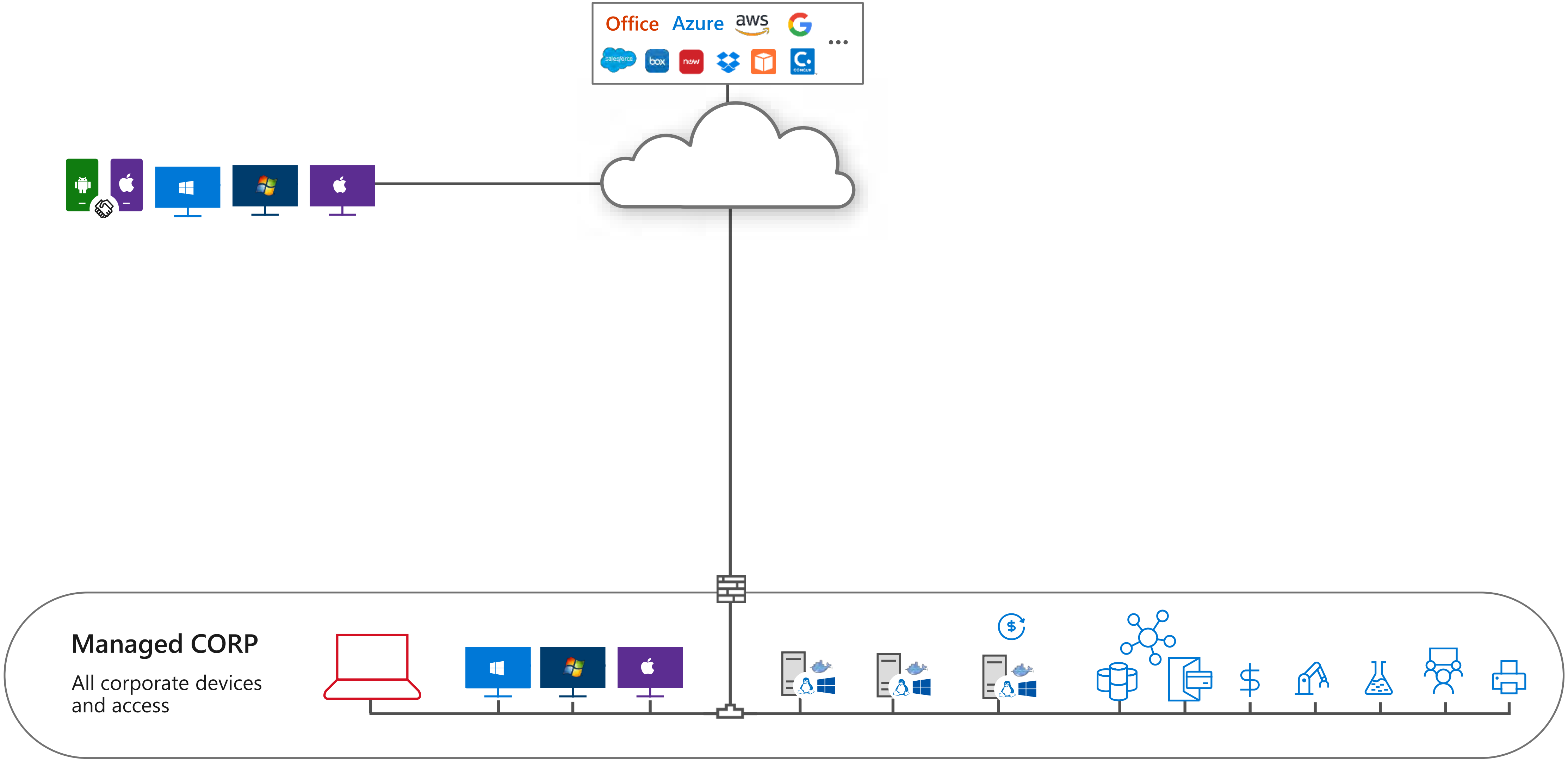
Assume breach

Minimize blast radius for breaches and prevent lateral movement by

- **Segmenting access** by network, user, devices, and app awareness.
- **Encrypting** all sessions end to end.
- **Use analytics** for threat detection, posture visibility and improving defenses

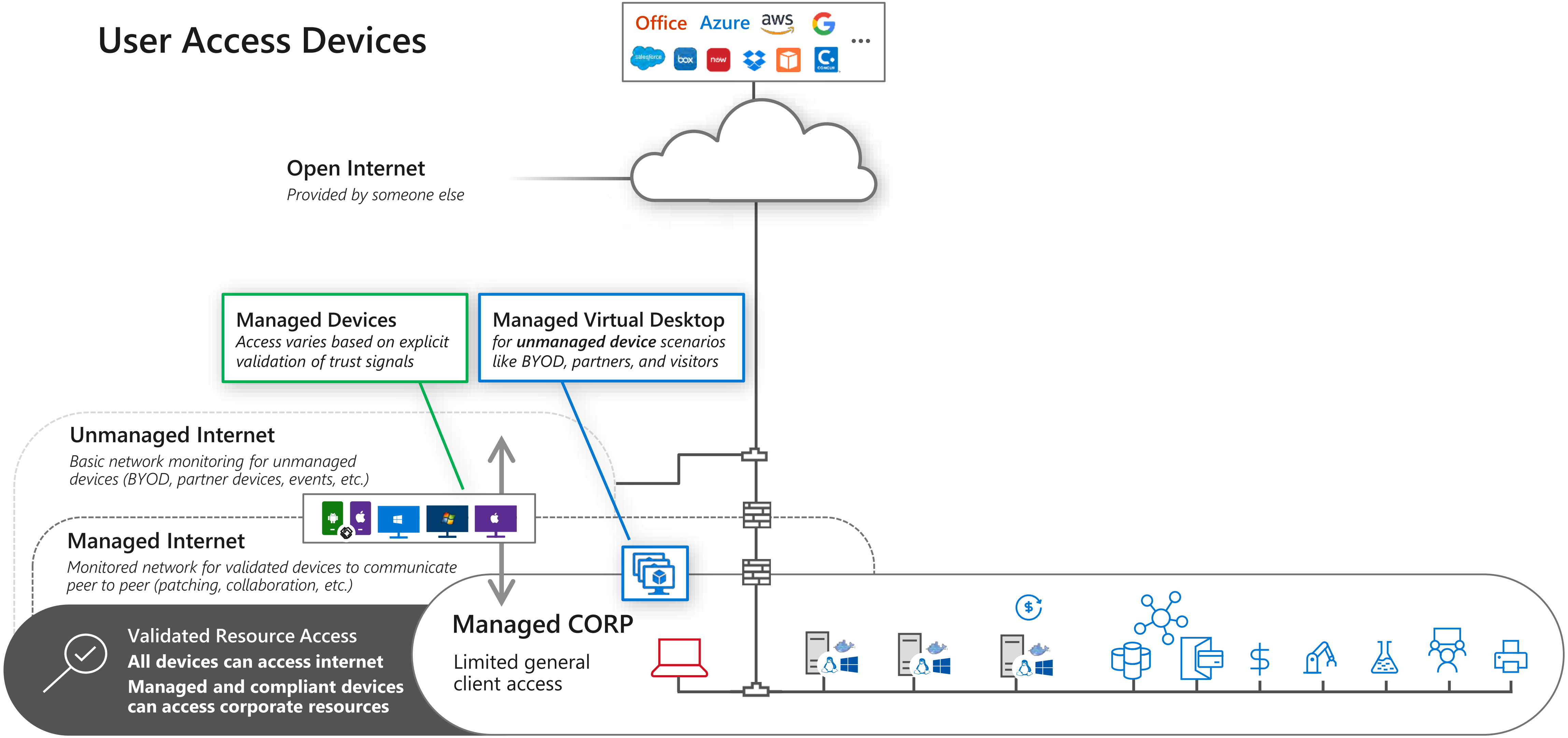
MENU

Typical ‘Flat’ Network



Zero Trust – Client Security Transformation

User Access Devices



Open Internet
Provided by someone else

Managed Devices
Access varies based on explicit validation of trust signals

Managed Virtual Desktop
*for **unmanaged device** scenarios like BYOD, partners, and visitors*

Unmanaged Internet
Basic network monitoring for unmanaged devices (BYOD, partner devices, events, etc.)

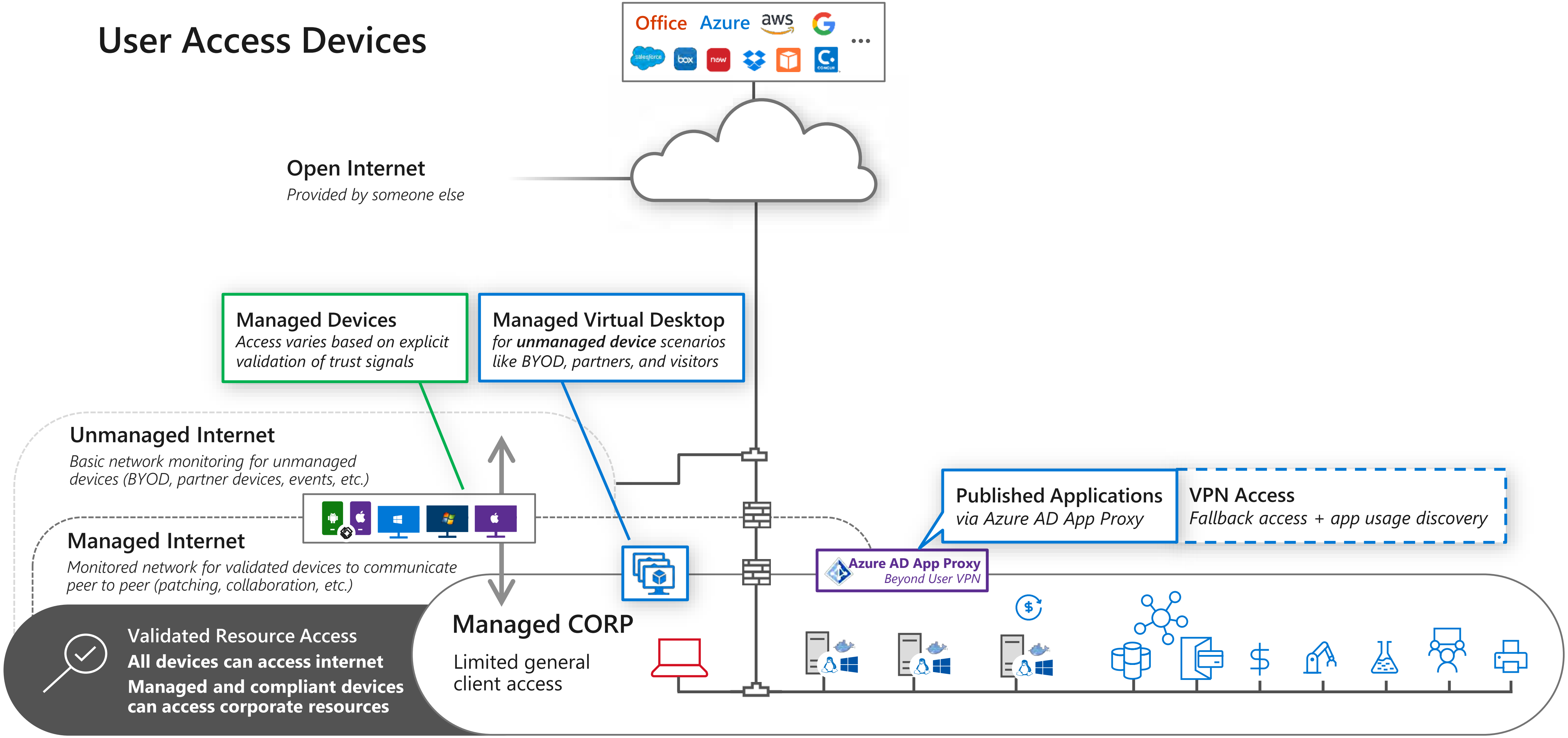
Managed Internet
Monitored network for validated devices to communicate peer to peer (patching, collaboration, etc.)

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 & multi-cloud environments

Zero Trust – App Access for Clients



User Access Devices

Open Internet
Provided by someone else

Managed Devices
Access varies based on explicit validation of trust signals

Managed Virtual Desktop
*for **unmanaged device** scenarios like BYOD, partners, and visitors*

Unmanaged Internet
Basic network monitoring for unmanaged devices (BYOD, partner devices, events, etc.)

Managed Internet
Monitored network for validated devices to communicate peer to peer (patching, collaboration, etc.)

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

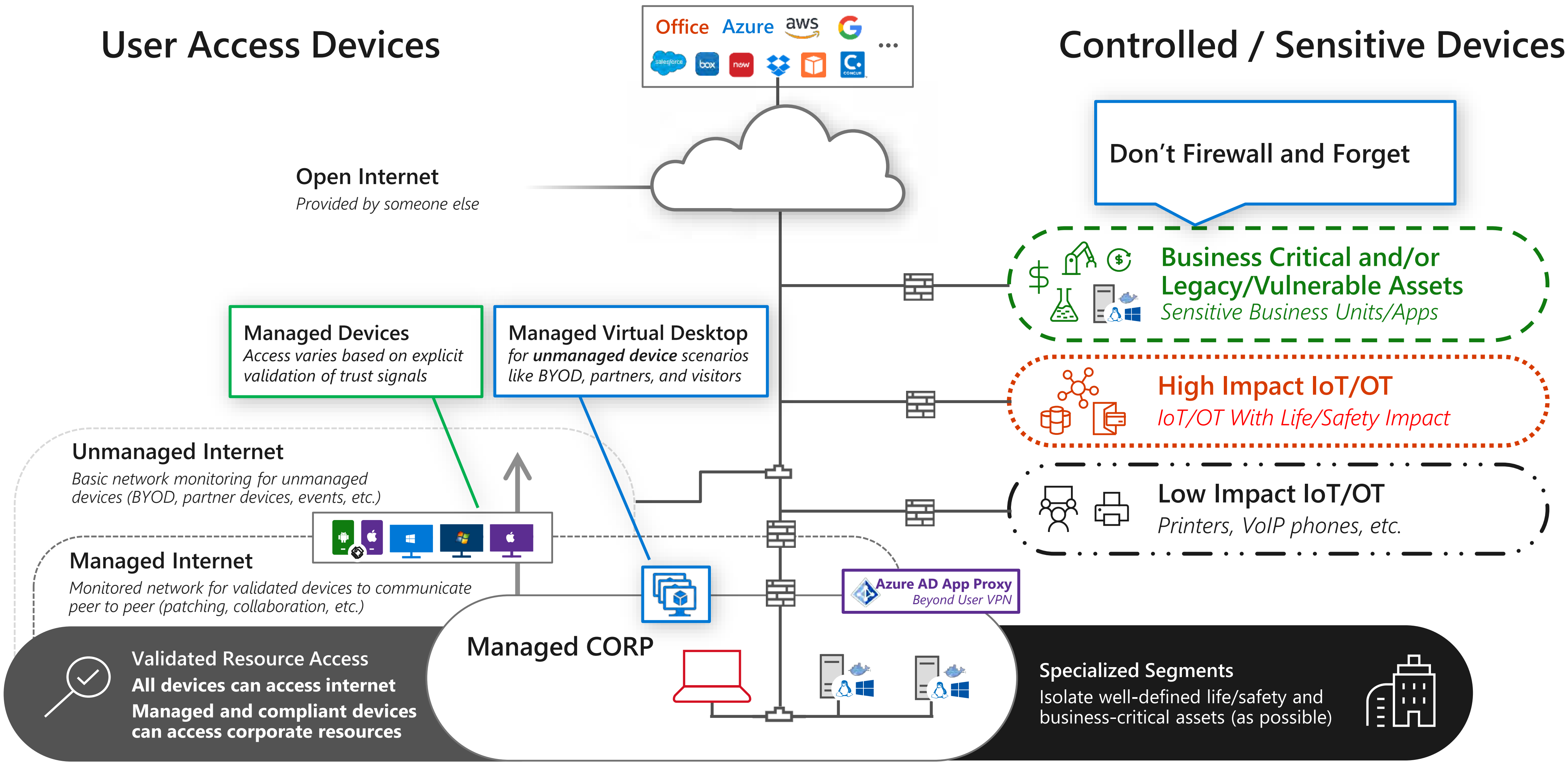
Managed CORP
Limited general client access

Published Applications
via Azure AD App Proxy

VPN Access
Fallback access + app usage discovery

Spans on-premises & multi-cloud environments

Zero Trust – Network Segment Transformation



User Access Devices

Controlled / Sensitive Devices

Open Internet
Provided by someone else

Don't Firewall and Forget

Business Critical and/or Legacy/Vulnerable Assets
Sensitive Business Units/Apps

High Impact IoT/OT
IoT/OT With Life/Safety Impact

Low Impact IoT/OT
Printers, VoIP phones, etc.

Managed Devices
Access varies based on explicit validation of trust signals

Managed Virtual Desktop
*for **unmanaged device** scenarios like BYOD, partners, and visitors*

Unmanaged Internet
Basic network monitoring for unmanaged devices (BYOD, partner devices, events, etc.)

Managed Internet
Monitored network for validated devices to communicate peer to peer (patching, collaboration, etc.)

Azure AD App Proxy
Beyond User VPN

Managed CORP

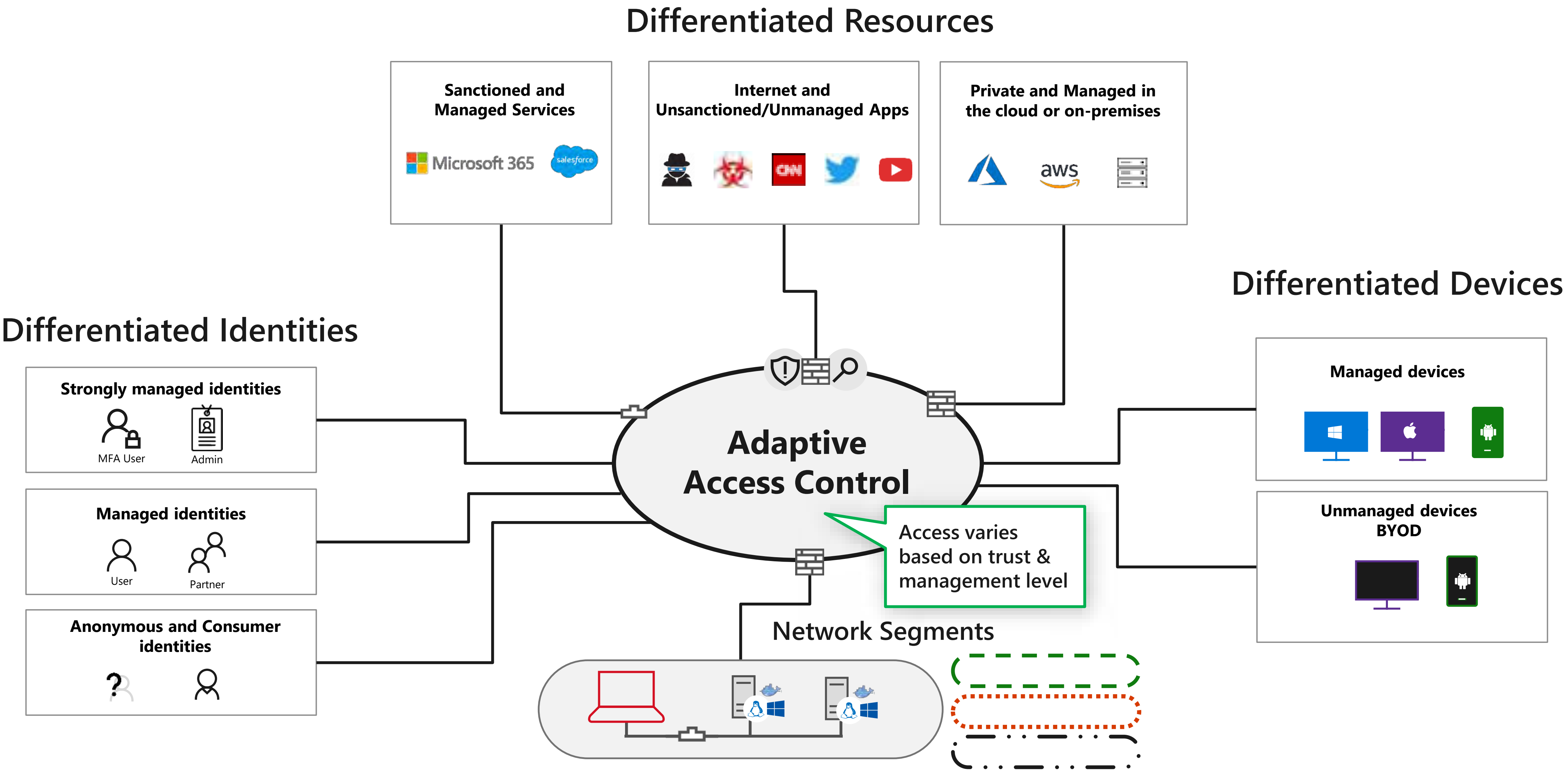
Validated Resource Access
All devices can access internet
Managed and compliant devices can access corporate resources

Specialized Segments
Isolate well-defined life/safety and business-critical assets (as possible)

Spans on-premises & multi-cloud environments

Full Zero Trust End State

Bringing the best of both worlds



Differentiated Resources
Sanctioned and Managed Services
Microsoft 365
salesforce
Internet and Unsanctioned/Unmanaged Apps
CNN
Private and Managed in the cloud or on-premises
aws
Differentiated Identities
Strongly managed identities
MFA User
Admin
Managed identities
User
Partner
Anonymous and Consumer identities
?
Adaptive Access Control
Access varies based on trust & management level
Network Segments
Differentiated Devices
Managed devices
Unmanaged devices BYOD

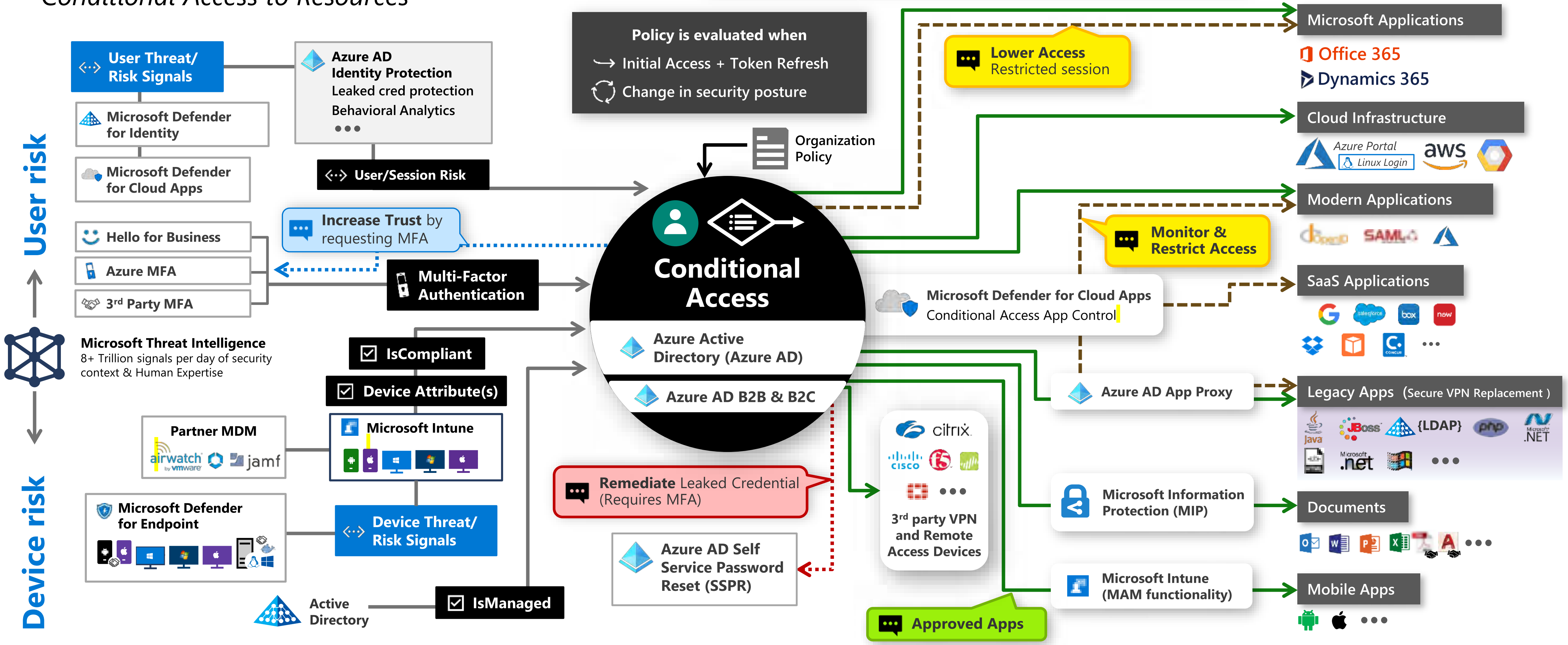
Zero Trust User Access

Conditional Access to Resources

Legend

- Full access
- Limited access
- Risk Mitigation
- Remediation Path

Microsoft



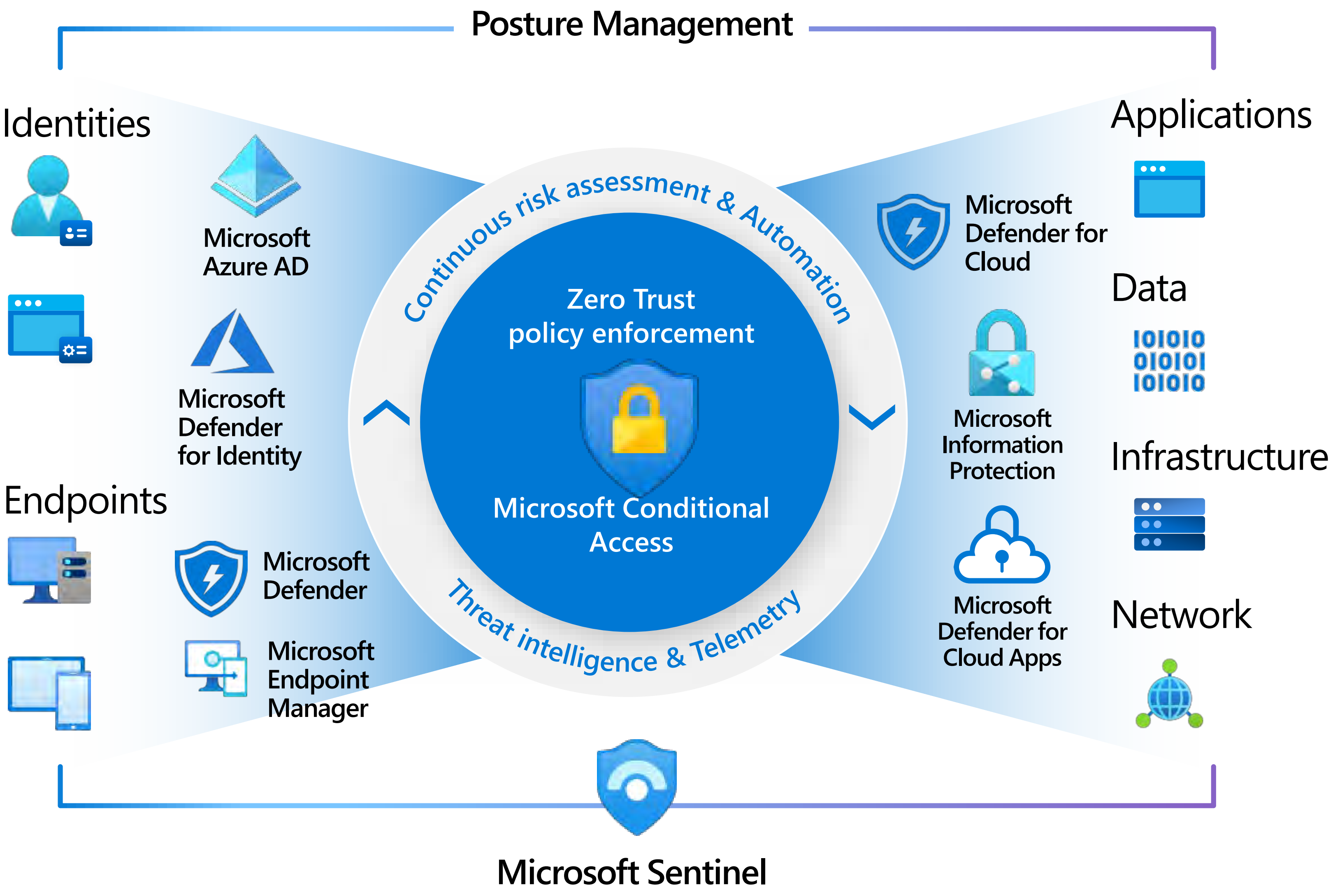
User risk
User Threat/ Risk Signals
Microsoft Defender for Identity
Microsoft Defender for Cloud Apps
Azure AD Identity Protection
Leaked cred protection
Behavioral Analytics
•••
User/Session Risk
Hello for Business
Azure MFA
3rd Party MFA
Increase Trust by requesting MFA
Multi-Factor Authentication
Microsoft Threat Intelligence
8+ Trillion signals per day of security context & Human Expertise
Device risk
IsCompliant
Device Attribute(s)
Partner MDM
airwatch by vmware
jamf
Microsoft Intune
Microsoft Defender for Endpoint
Device Threat/ Risk Signals
Active Directory
IsManaged
Policy is evaluated when
Initial Access + Token Refresh
Change in security posture
Organization Policy
Conditional Access
Azure Active Directory (Azure AD)
Azure AD B2B & B2C
Remediate Leaked Credential (Requires MFA)
Azure AD Self Service Password Reset (SSPR)
Lower Access Restricted session
Monitor & Restrict Access
Microsoft Defender for Cloud Apps
Conditional Access App Control
Azure AD App Proxy
citrix
cisco
•••
3rd party VPN and Remote Access Devices
Microsoft Information Protection (MIP)
Microsoft Intune (MAM functionality)
Approved Apps
Microsoft Applications
Office 365
Dynamics 365
Cloud Infrastructure
Azure Portal
Linux Login
aws
Modern Applications
SAML
SaaS Applications
salesforce
box
now
•••
Legacy Apps (Secure VPN Replacement)
Java
JBoss
{LDAP}
php
.NET
Microsoft .net
•••
Documents
•••
Mobile Apps
•••

Signal
to make an informed decision

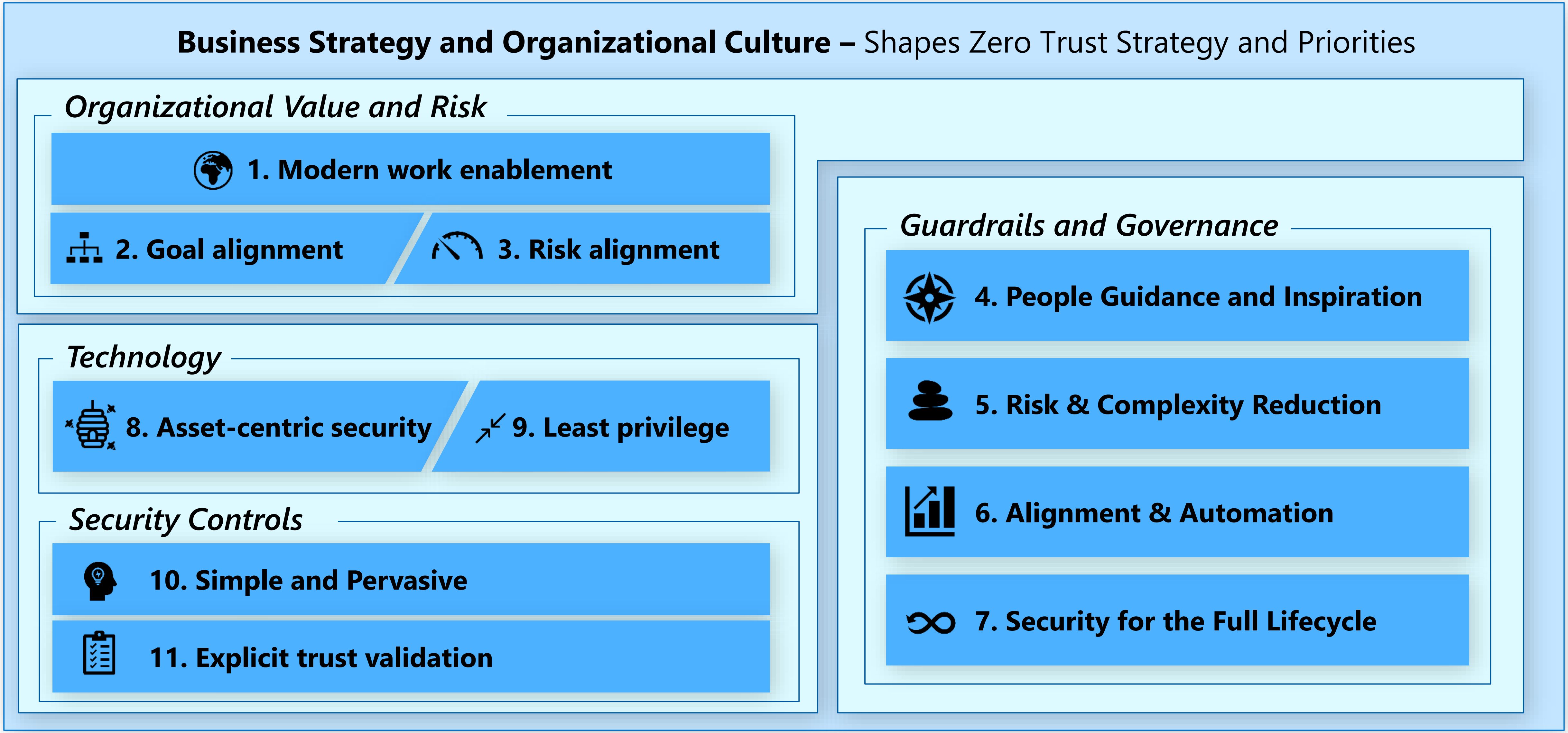
Decision
based on organizational policy

Enforcement
of policy across resources

Microsoft Zero Trust Capabilities


Posture Management
Identities
Microsoft Azure AD
Microsoft Defender for Identity
Endpoints
Microsoft Defender
Microsoft Endpoint Manager
Continuous risk assessment & Automation
Zero Trust policy enforcement
Microsoft Conditional Access
Threat intelligence & Telemetry
Applications
Microsoft Defender for Cloud
Data
Microsoft Information Protection
Infrastructure
Microsoft Defender for Cloud Apps
Network
Microsoft Sentinel

Zero Trust Core Principles



Business Strategy and Organizational Culture – Shapes Zero Trust Strategy and Priorities

Organizational Value and Risk

- **1. Modern work enablement**
- **2. Goal alignment**
- **3. Risk alignment**

Guardrails and Governance

- **4. People Guidance and Inspiration**
- **5. Risk & Complexity Reduction**
- **6. Alignment & Automation**
- **7. Security for the Full Lifecycle**

Technology

- **8. Asset-centric security**
- **9. Least privilege**

Security Controls

- **10. Simple and Pervasive**
- **11. Explicit trust validation**

Microsoft Security

Product categories

Identity	Security	Compliance	Privacy	Management
Microsoft **Entra**	Microsoft **Defender** Microsoft **Sentinel**	Microsoft **Purview**	Microsoft **Priva**	Microsoft **Endpoint Manager**

Microsoft Security

Thank you!

http://aka.ms/security