

Trust No One

What is Zero Trust?

June 29, 2023

Presented by:

Mike Reams

Practice Director, Security &
Cloud Infrastructure

BENNETT ADELSON

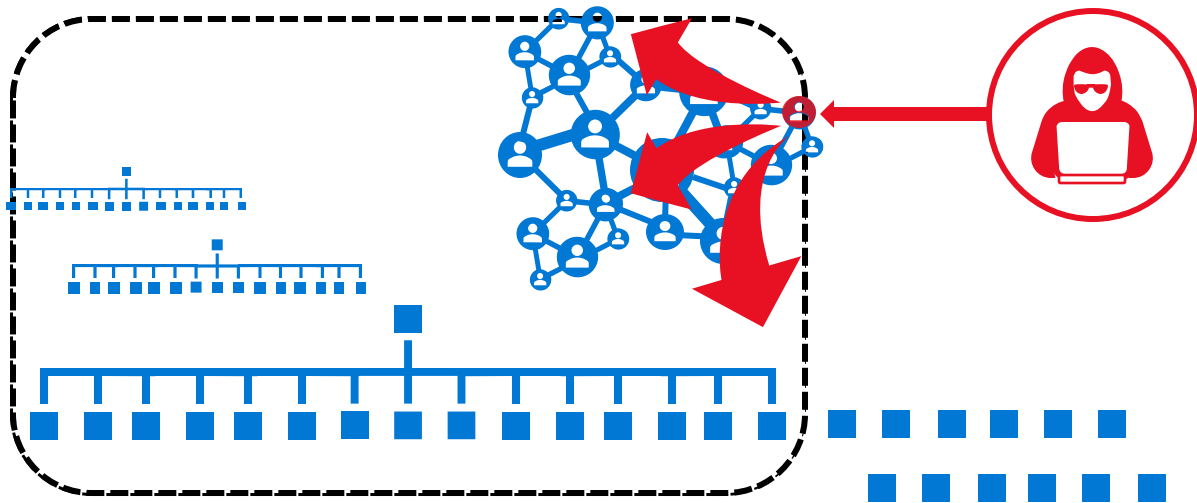


Agenda

- ✓ Why The Conversation?
- ✓ Security Challenges
- ✓ What is Zero Trust?
- ✓ Capabilities Overview
- ✓ Zero-Trust Approach
- ✓ Q&A

Why Are We Having A Zero Trust Conversation?

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



- 1. IT Security is Complex**
 - Many Devices, Users, & Connections
 - Hybrid Disconnected Workforce
- 2. Disrupted “Walled Trusted Network” model**

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

What Is Zero-Trust?



Zero trust security is a security model that assumes all users, devices, and networks inside and outside an organization's perimeter are untrusted and must be verified prior to granting access.

The concept of zero-trust networking has been around a decade; however, we have seen its popularity in industry discussions grow exponentially in the last few years.

Key Zero Trust Principles

Guidance for Technical Architecture



Verify Explicitly

Always validate all available data points including:

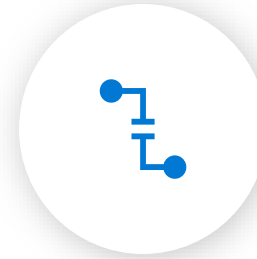
- User identity and location
- Device health
- Service or workload context
- Data classification
- Anomalies



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** policies
- Data protection against **out of band** vectors



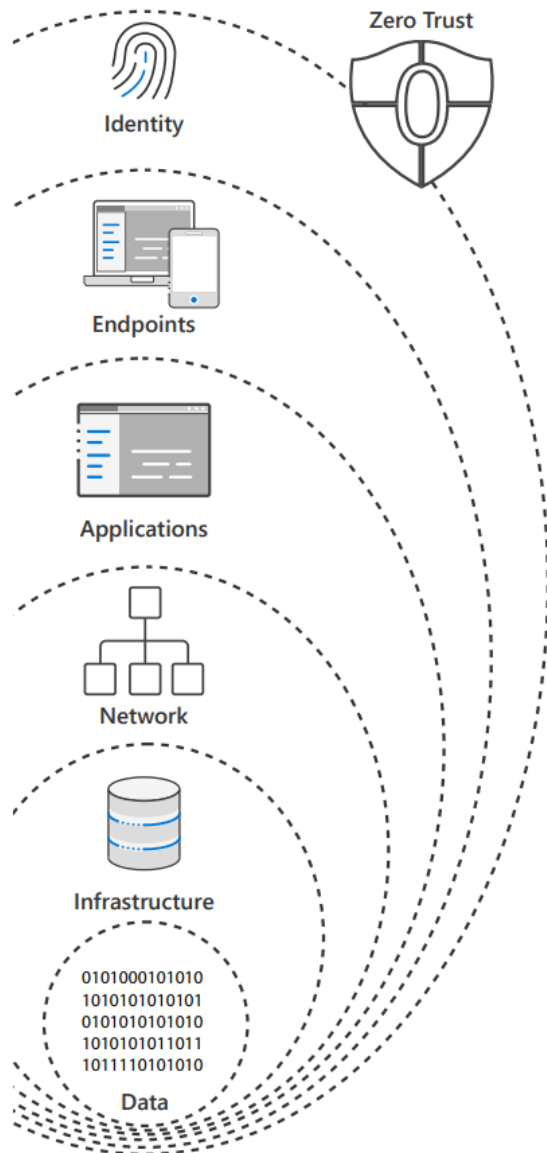
Assume Breach

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 encryption, communication channels, and data at rest.
- **Use analytics** for threat detection, posture visibility and improving defenses.

Zero Trust Areas of Defense

Zero Trust security layers



Identity

Zero Trust starts with **identity**, verifying that only the people, devices and processes that have been granted access to your resources can access them.

Endpoints

Next comes assessing the security compliance of device **endpoints** - the hardware accessing your data - including the IoT systems on the edge.

Applications

This oversight applies to your **applications** too, whether local or in the Cloud, as the software-level entry points to your information.

Network

Next, there are protections at the **network** layer for access to resources - especially those within your corporate perimeter.

Infrastructure

Followed by the **infrastructure** hosting your data on-premises and in the cloud. This can be physical or virtual, including containers and micro-services and the underlying operating systems and firmware.

Data

And finally, protection of the **data** itself across your files and content, as well as structured and unstructured data wherever it resides

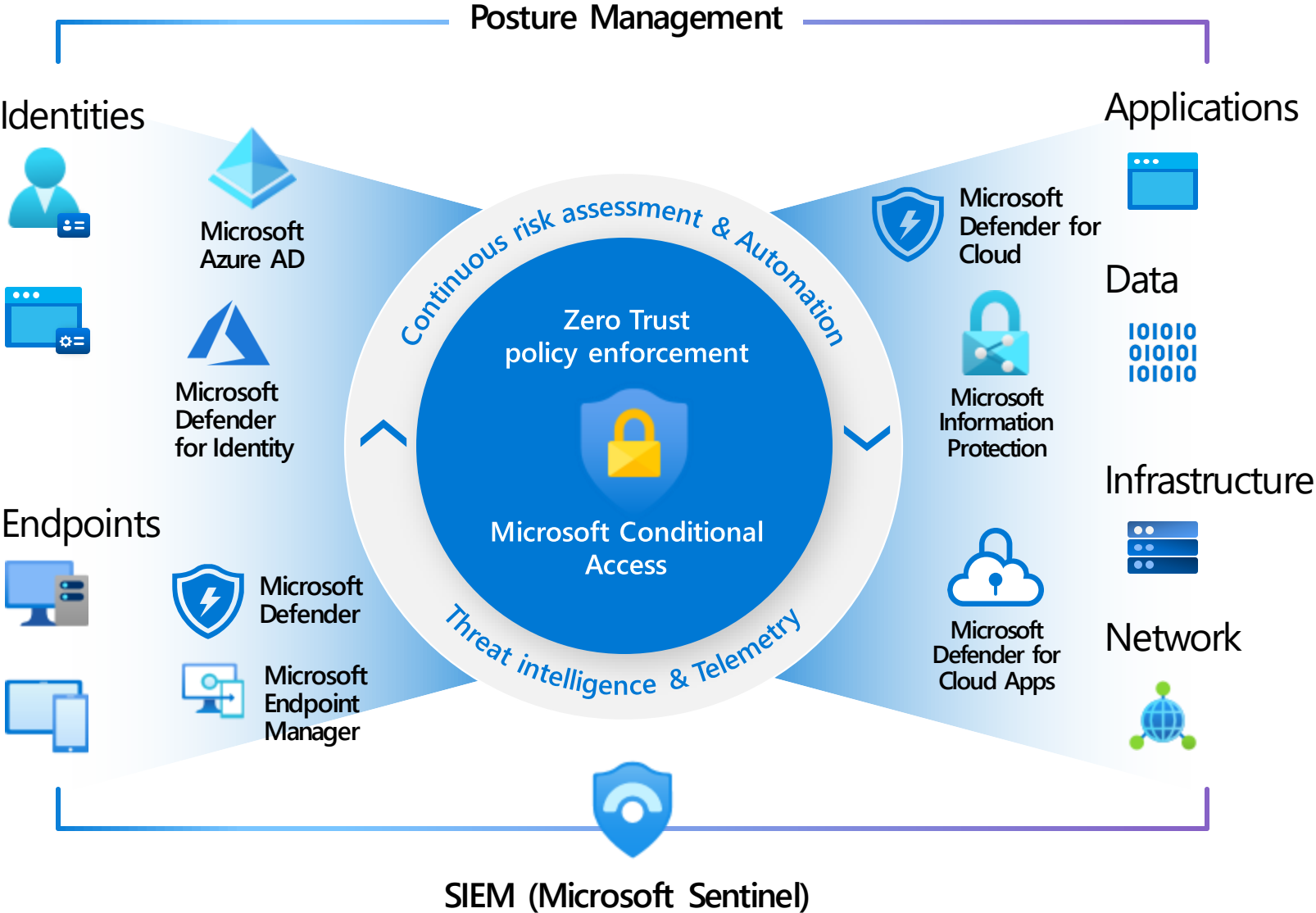
Zero Trust approach advocates protection at each layer

Microsoft Zero Trust Capabilities

Use Least Privilege Access

Verify Explicitly

Assume Breach



Cross-cloud and Cross-Platform

Comprehensive Security, Compliance and Identity capabilities that integrate with your existing solutions

Industry Partnerships

NIST / CIS / The Open Group / Others Microsoft Intelligent Security Association Solution Integration and MDR/MSSP Partners CERTs / ISACs / Others Law Enforcement ...



Microsoft Security, Compliance, and Identity Capabilities

🛡️ Threat Intelligence – 8+ Trillion signals per day of security context

Access Control

Identity and Network

Modern Security Operations

Rapid Resolution with XDR, SIEM, SOAR, UEBA and more

Asset Protection

Information Protection and App Security / DevSecOps

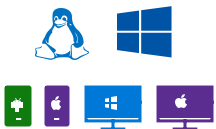
Technical Governance

Risk Visibility, Scoring, and Policy Enforcement

People Security – User Education/Empowerment and Insider Threats



Endpoints & Devices



Software as a Service (SaaS)



Hybrid Infrastructure – IaaS, PaaS, On-Premises



IoT Devices



Operational Technology (OT)

Security Operations [Center] (SOC) – Reduce attacker time/opportunity to impact business

Multi-Cloud and Cross-Platform Technology

Secure the enterprise you have

Microsoft Information Protection and Azure Purview

Discovery, Classify, Protect, and Monitor unstructured data (documents, spreadsheets, files, etc.), structured data (SQL, Databases, etc.) and identify critical risks (Open S3 buckets, SaaS Sharing Risks, etc.)

Identity & Access



Information Protection

Identity Enablement

Access cloud and legacy applications for Enterprise users, Partners (B2B), and Customers/Citizens (B2C)



Azure Active Directory

Identity Security

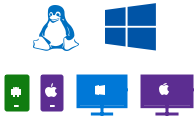
Zero Trust Access Control using Behavioral Analytics, Threat Intelligence, and integration of device and app trust signals

GitHub Advanced Security – Secure development capabilities



Securing components common most enterprise software supply chains

Endpoints & Devices



Microsoft Endpoint Manager
Unified Endpoint Management (UEM)

Software as a Service (SaaS)



Hybrid Infrastructure – IaaS, PaaS, On-Premises



Continuous Cross-Platform Cloud Security Posture Management (CSPM) and Cloud Workload Protection (CWPP)

IoT Devices



Operational Technology (OT)

Security Operations [Center] (SOC)

Microsoft Sentinel – Cloud Native SIEM, SOAR, and UEBA for IT, OT, and IoT

Microsoft 365 Defender

Microsoft Defender - Extended Detection and Response (XDR)

Microsoft Defender for Cloud

Microsoft Defender for IoT

Microsoft Defender for Endpoint Unified Endpoint Security

- Endpoint Detection & Response (EDR)
- Data Loss Protection (DLP)
- Web Content Filtering
- Threat & Vuln Management

Microsoft Defender for Cloud Apps

- App Discovery & Risk Scoring (Shadow IT)
- Threat Detection & Response
- Policy Audit & Enforcement
- Session monitoring & control
- Info Protection & Data Loss Prevention (DLP)

Threat visibility and capabilities tailored to resources

- Threat & Vulnerability Management
- Integrated data classification
- Threat analytics on top attacks
- Advanced Detection & Remediation
- Automated Investigation & Remediation
- Advanced Threat Hunting

XDR for IaaS, PaaS, and On-Premises

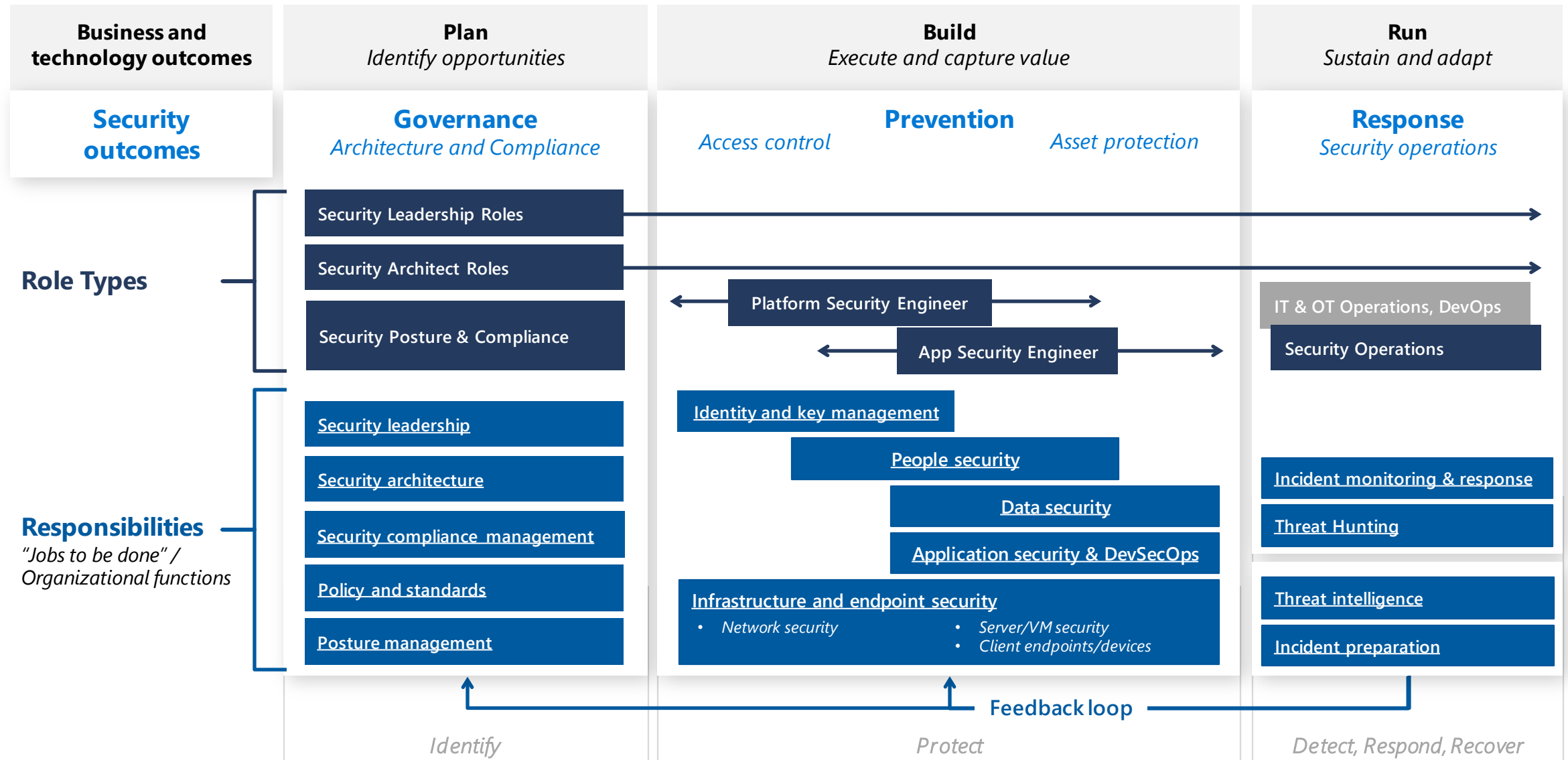
- VMs, Servers, App Environments
- Storage and Databases
- Containers and Orchestration
- and more

- ICS, SCADA, OT
- Internet of Things (IoT)
- Industrial IoT (IIoT)
- Asset & Vulnerability management
- Threat Detection & Response

Azure Arc

Threat Intelligence – 8+ Trillion signals per day of security context

Security Roles and Responsibilities



Zero Trust Rapid Modernization Plan (RaMP)

Prioritizing rapid progress on highest positive impact potential

Roll out to IT Admins first

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


Top Priorities – critical security modernization steps

 **User Access and Productivity**
Zero Trust Foundations

- 1. Explicitly validate trust for all access requests (via Azure AD Conditional Access)**
 - a. User Accounts** - Require Passwordless or MFA for all users + measure risk with threat intelligence & behavior analytics
 - b. Endpoints** - Require device integrity for access (configuration compliance first, then XDR signals)
 - c. Apps** - Enable Azure AD for all SaaS, for VPN authentication, and for legacy apps (on-premises + IaaS) via App Proxy
 - d. Network** - Establish basic traffic filtering and segmentation to isolate business-critical or highly vulnerable resources

 **Data, Compliance & Governance**
Align to business and mission

- 2. Ransomware Recovery Readiness** - Ensure backups are validated, secure, and immutable to enable rapid recovery
- 3. Data** - Discover and protect sensitive data (via Microsoft Info Protection, Defender for Cloud Apps, CA App Control)

 **Modern Security Operations**


- 4. Streamline response** to common attacks with XDR for Endpoint/Email/Identity + Cloud (via M365 & Defender for Cloud)
- 5. Unify Visibility** with modern Security Information and Event Management (SIEM via Microsoft Sentinel)
- 6. Reduce manual effort** - using automated investigation/remediation (SOAR), enforcing alert quality, and threat hunting

As Needed – typically driven by cloud adoption or OT/IoT usage

 **Infrastructure & Development**
Datacenter & DevOps Security

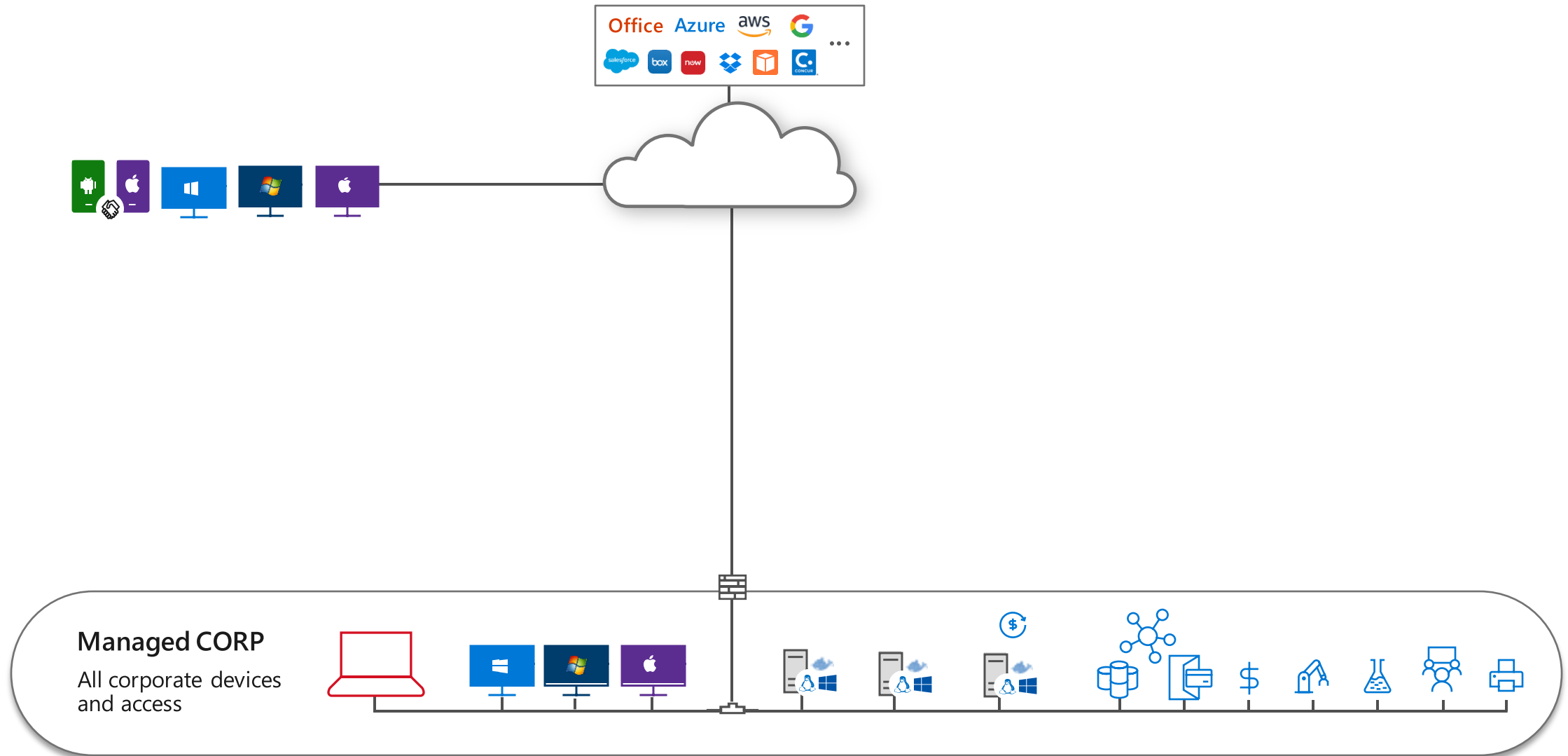
- Security Hygiene** – Rigorously monitor+remediate security configurations, permissions (CIEM), security updates, and more
- Reduce Legacy Risk** – Retire or isolate legacy technology (Unsupported OS/Applications, legacy protocols)
- DevOps Integration** – Integrate infrastructure + development security practices into DevOps with minimal friction
- Microsegmentation** – Additional *identity and network* restrictions (dynamic trust-based and/or static rules)

Align to cloud migration schedule

 **Operational Technology (OT) and Industrial IoT**

- Discover** – Find & classify assets with business critical, life safety, and operational/physical impact (via Defender for IoT)
- Protect** – isolate assets from unneeded internet/production access with static and dynamic controls
- Monitor** – unify threat detection and response processes for OT, IT, and IoT assets (via Microsoft Defender for IoT)

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.)



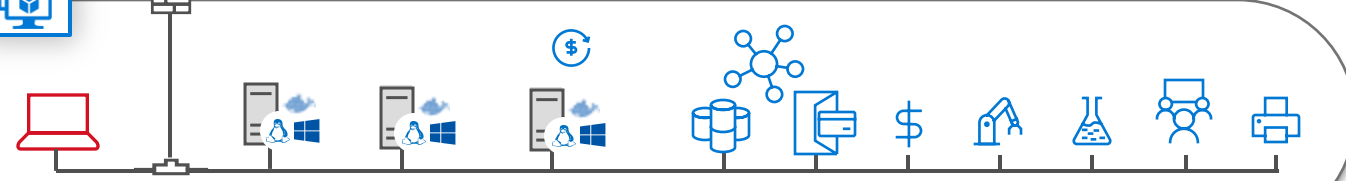
Managed Internet

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

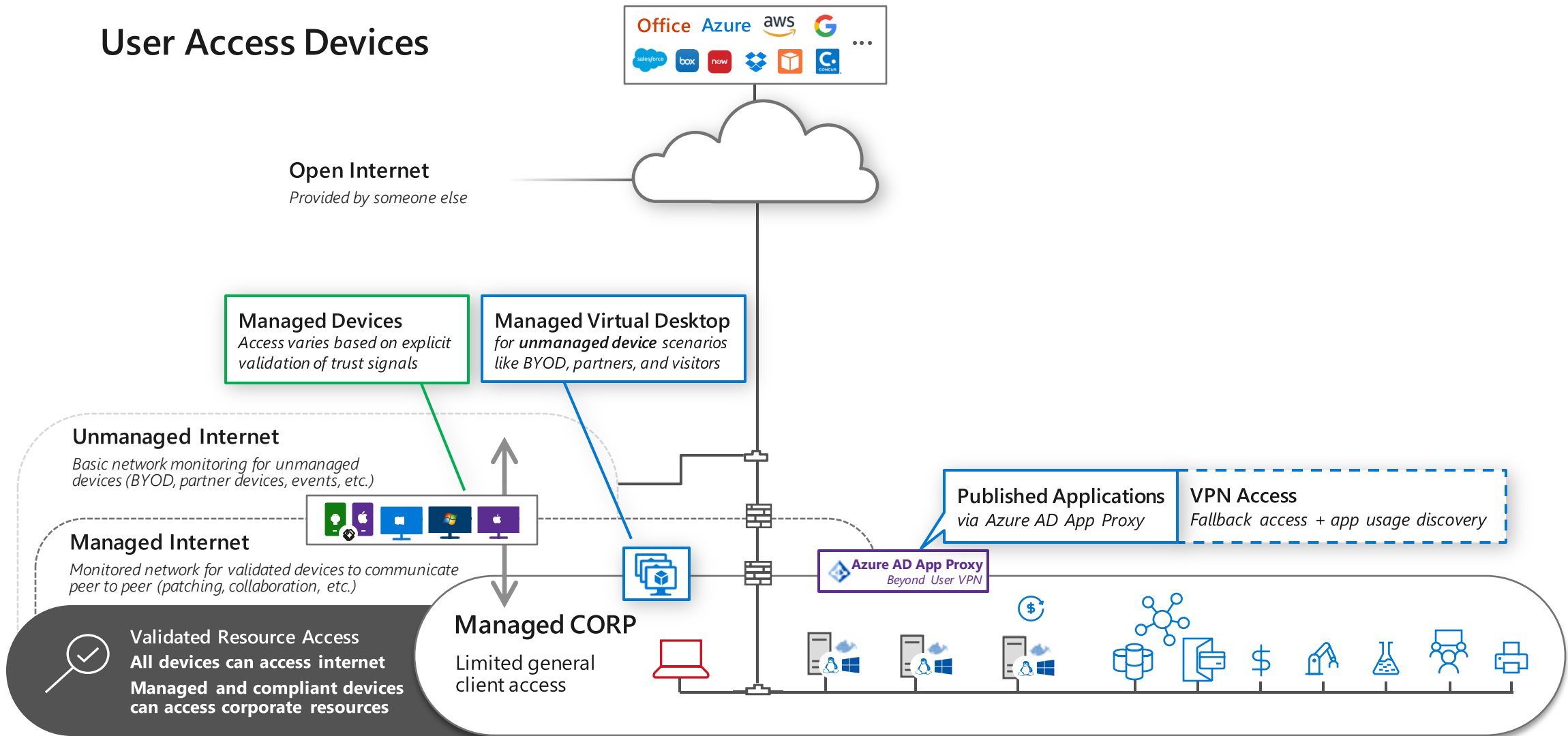
Managed CORP

Limited general client access

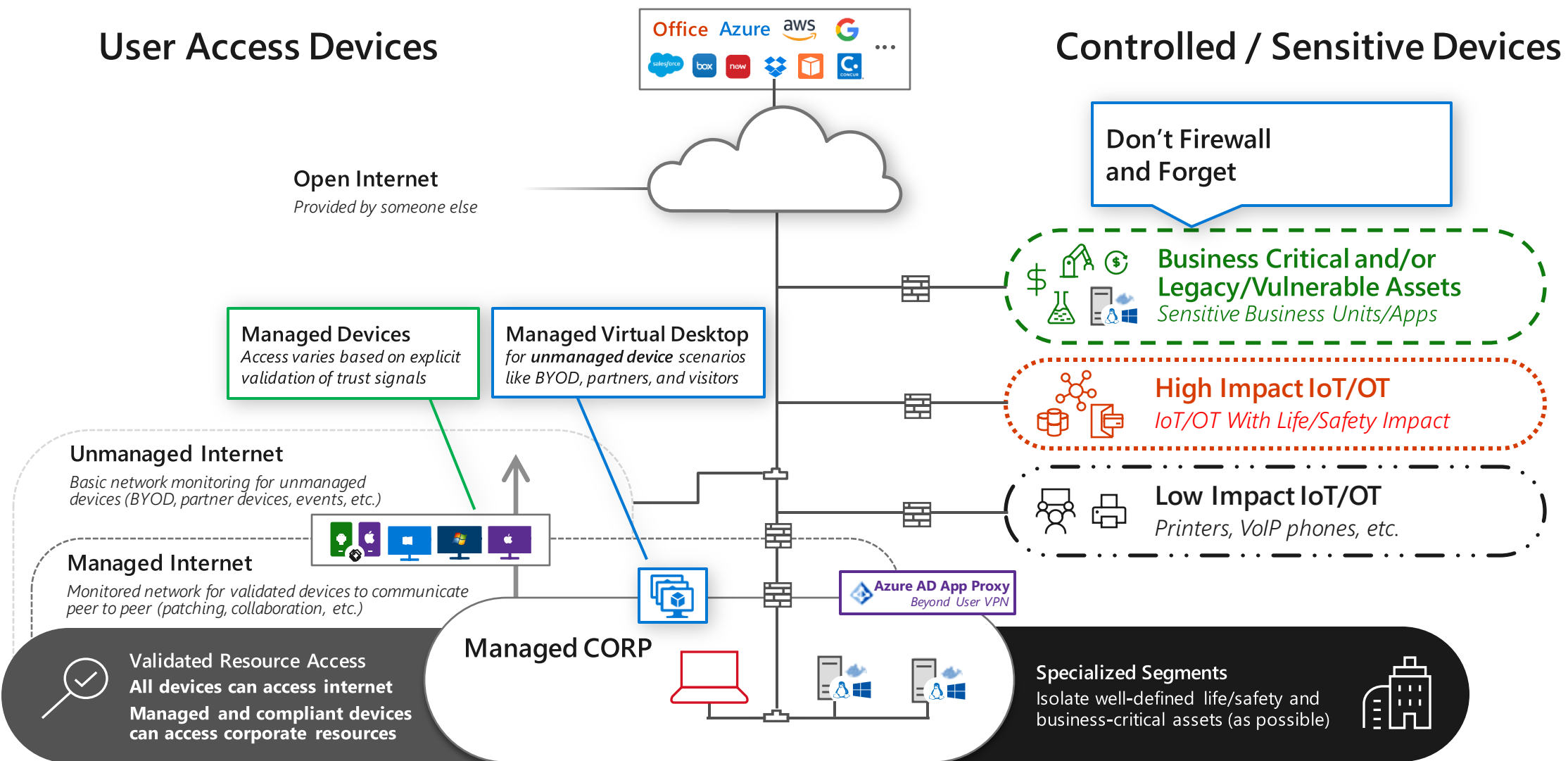


Spans on-premises & multi-cloud environments

Zero Trust – App Access for Clients



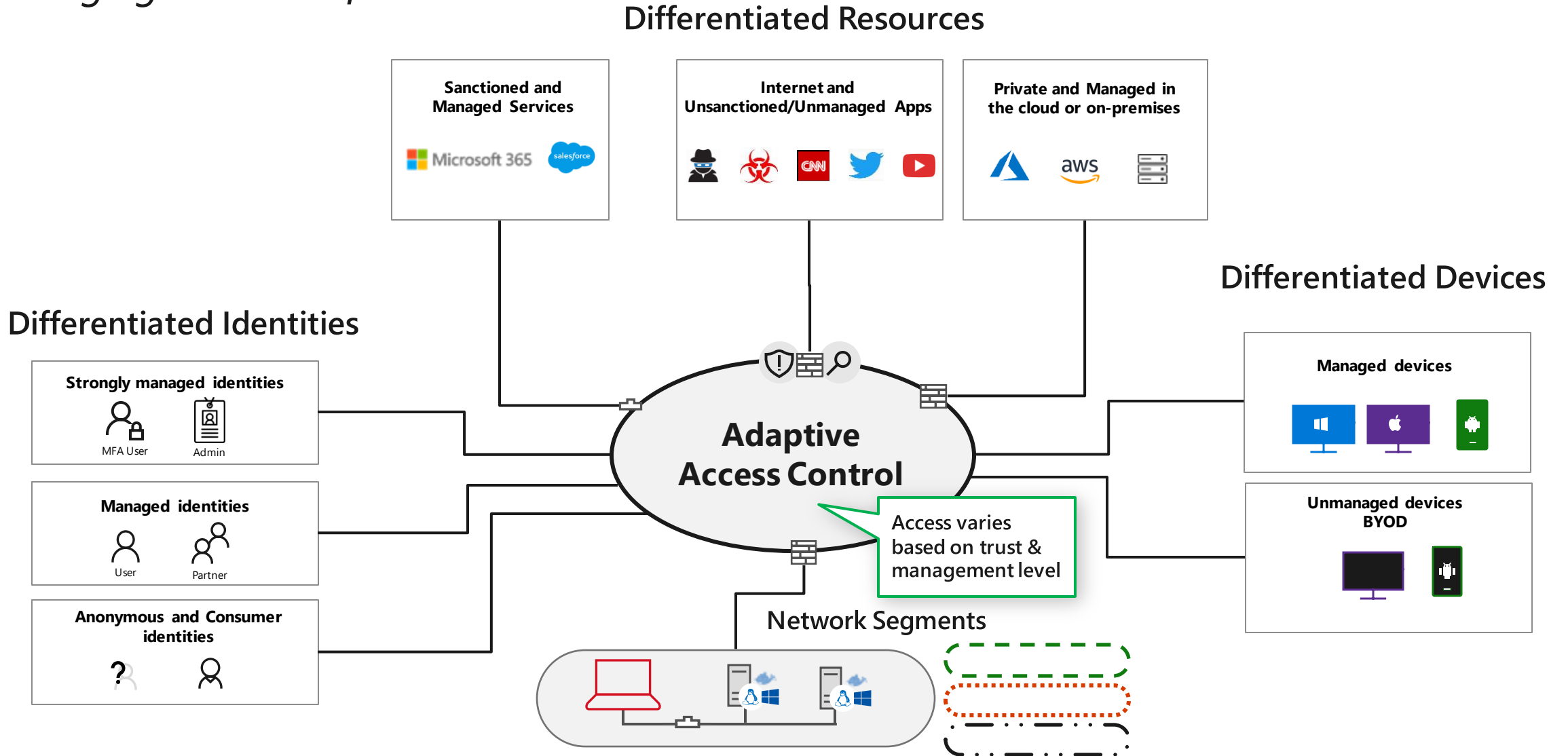
Zero Trust – Network Segment Transformation



Spans on-premises & multi-cloud environments

Full Zero Trust End State

Bringing the best of both worlds



Cloud Security Assessment

Our Baseline Offering

Analysis of an organization's security posture, evaluating vulnerabilities, identity, and compliance risks with remediation recommendations.

BENNETT ADELSON

Customers who are looking to understand their risk of business loss and vulnerabilities to cyberattack - or has become a recent victim.

Scope



Assessment:

- Inventory of hardware & software across the digital estate including all infrastructure server and client instances.



Scope Coverage:

- Azure Security Scoring and Posture Assessment
- Physical and Virtual Environments
- Windows and Linux
- SQL and Windows Server
- Networking, Firewall, and Security Software
- Shadow IT Discovery
- Cloud-based Security configuration



Effort:

- 5 business days

Comprehensive Approach



Data Collection

- Inventory all applicable operating systems, infrastructure, and endpoints collecting hardware, software, and versions deployed
- Collect all end user identity management policies and usage data
- Run O365 secure score and Azure Secure score
- Run Compliance Manager



Analysis

- Review hardware end-of-life and non-cloud compatible versions of operating systems
- Evaluate security risks due to identity control gaps and provide policy guidance
- Analysis of security gaps, vulnerabilities, and recommendations of mitigation by priority of risk impact
- Evaluate the customer security posture with O365 Secure score analysis and Azure Secure score
- Align customer risk analysis based on applicable standards (Zero Trust Framework, or applicable framework)

Deliverables



Insights, analysis, recommendations:

- Executive Summary Review
- Data-driven finding on analysis
- Prioritized risk mitigation recommendations with appropriate Microsoft security solution (M365/Azure)
- Align customer risks identified in Zero Trust Architecture



Most Common Business Cases

- Reduce Cyber Insurance
- Improve Security Posture



Recommendation on Next Steps



Remediation Proposal

- Migration and Deployment Plan
- Effort Estimate

We can help...

Call us to discuss how Bennett Adelson can help accelerate your Zero Trust implementation with best practices, the latest trends, and a framework informed by real-world deployments.

Mike Reams

**Practice Director, Security & Cloud
Infrastructure**

mreams@bennettadelson.com

404-285-4477

Brian Connelly

Senior Solution Sales Executive

bconnelly@bennettadelson.com

216-338-1524

Kevin Karlik

Senior Solution Sales Executive

kkarlik@bennettadelson.com

216-256-6796