RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **ZT-M06**

What We Learned Implementing Zero Trust Security at Microsoft

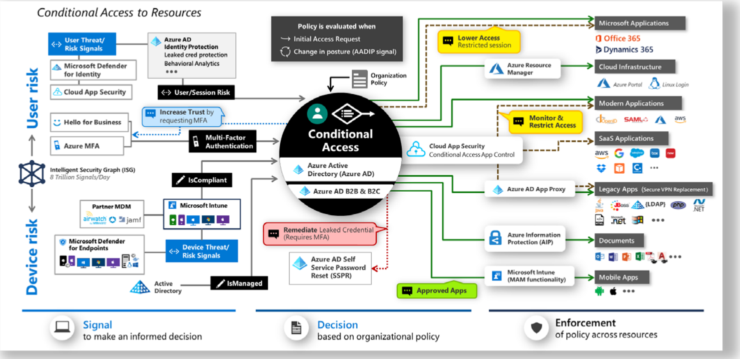
Carmichael Patton

Principal Security Architect
Microsoft – Digital Security & Resiliency
@Xanlythe

Yulia Evgrafova

Senior Service Engineer
Microsoft – Digital Security & Resiliency

Zero Trust can seem…


Conditional Access to Resources
User risk
Device risk
User Threat/ Risk Signals
Azure AD Identity Protection
Leaked cred protection
Behavioral Analytics
•••
Microsoft Defender for Identity
Cloud App Security
User/Session Risk
Increase Trust by requesting MFA
Hello for Business
Azure MFA
Multi-Factor Authentication
Intelligent Security Graph (ISG)
8 Trillion Signals/Day
IsCompliant
Partner MDM
airwatch
jamf
Microsoft Intune
Microsoft Defender for Endpoints
Device Threat/ Risk Signals
Active Directory
IsManaged
Policy is evaluated when
Initial Access Request
Change in posture (AADIP signal)
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
Azure Resource Manager
Monitor & Restrict Access
Cloud App Security
Conditional Access App Control
Azure AD App Proxy
Azure Information Protection (AIP)
Microsoft Intune (MAM functionality)
Approved Apps
Microsoft Applications
Office 365
Dynamics 365
Cloud Infrastructure
Azure Portal
Linux Login
Modern Applications
OpenID
SAML
aws
SaaS Applications
aws
•••
Legacy Apps (Secure VPN Replacement)
Java
JBoss
(LDAP)
php
.NET
.net
•••
Documents
•••
Mobile Apps
•••
Signal
to make an informed decision
Decision
based on organizational policy
Enforcement
of policy across resources

okta

paloalto NETWORKS

cisco

Gartner

BeyondCorp

FORRESTER

Is Zero Trust for me?

How do we start?

Who do we use?

…big

everything from devices to network security

…noisy

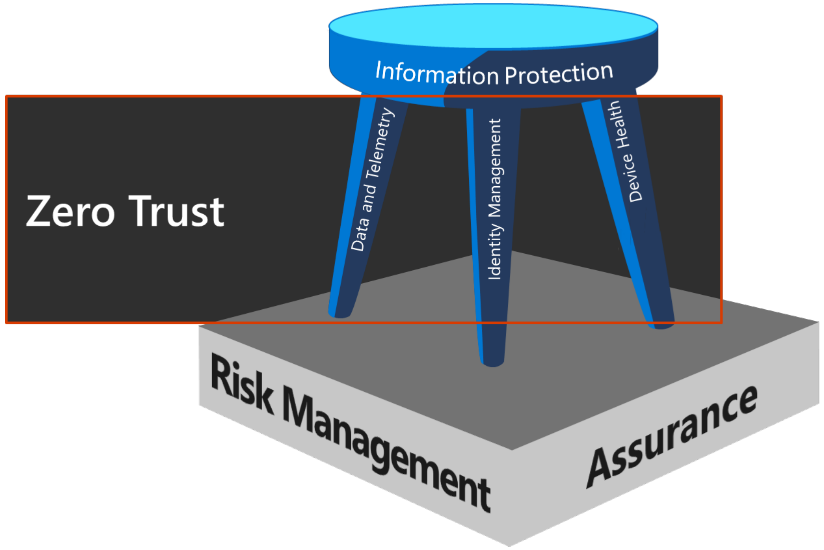
Every firm and analyst has their own definition

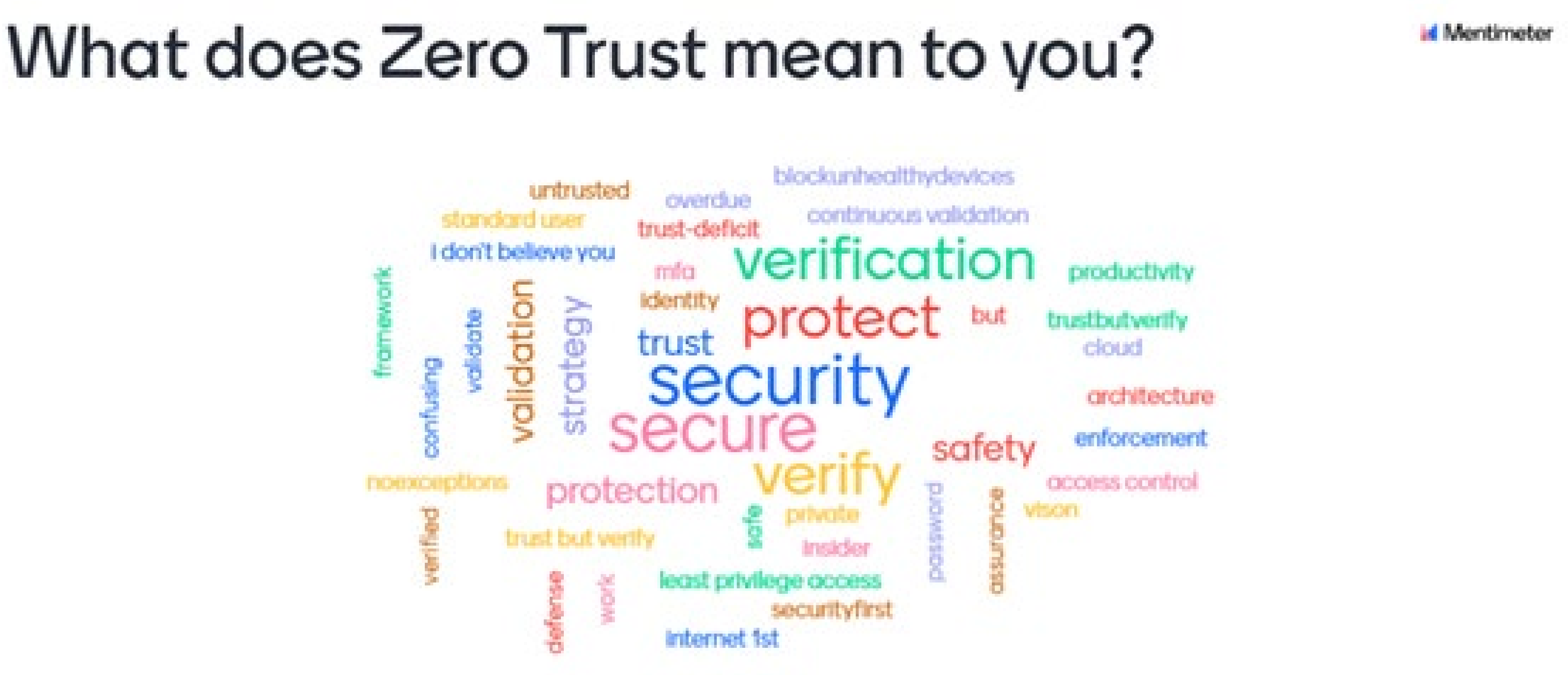
…confusing

Zero Trust journey looks different for everyone

Zero Trust is actually simple:

“In order to trust, you must first verify”





What does Zero Trust mean to you?

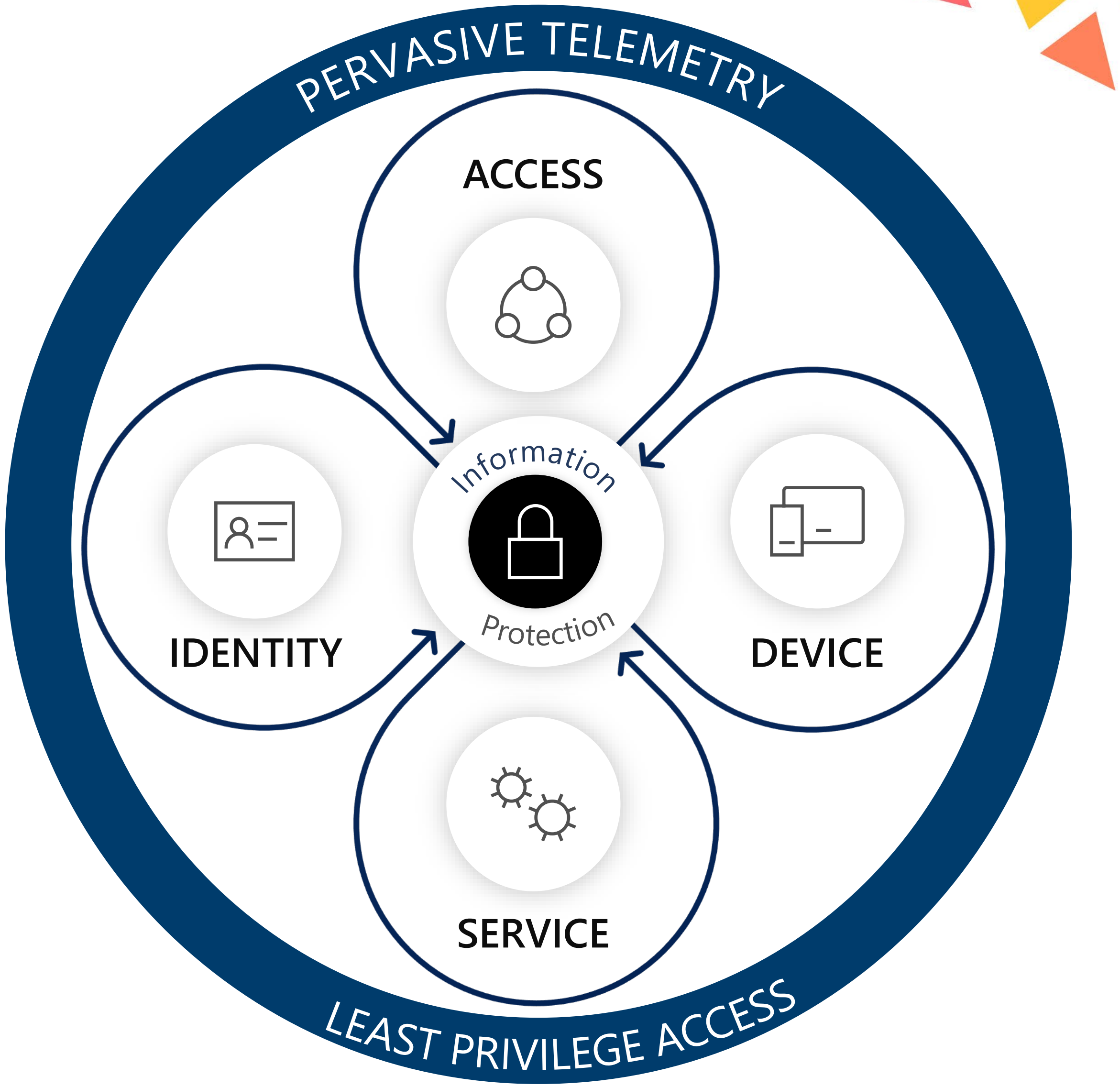
Mentimeter

blockunhealthydevices
untrusted
overdue
standard user
continuous validation
trust-deficit
i don't believe you
verification
productivity
mfa
framework
validation
strategy
identity
protect
but
trustbutverify
validate
trust
cloud
confusing
security
architecture
secure
safety
enforcement
noexceptions
protection
verify
access control
safe
private
password
assurance
vison
verified
trust but verify
insider
least privilege access
defense
work
securityfirst
internet 1st

Presenter's Company Logo – replace or delete on master slide

Zero Trust

- **Identity** – identities are validated and healthy
- **Device** - devices are validated to be managed and healthy
- **Service -** Services, resources, and connections enforce identity and health requirements.
- **Access** – Network access is routed based on user role and device
- **Least privilege access** – limiting access to only the applications, services, and infrastructure required to perform job function
- **Pervasive telemetry** – understanding your environments, measuring risk reduction, and enabling artificial intelligence for anomaly detection



Zero Trust benefits everyone

Increases security

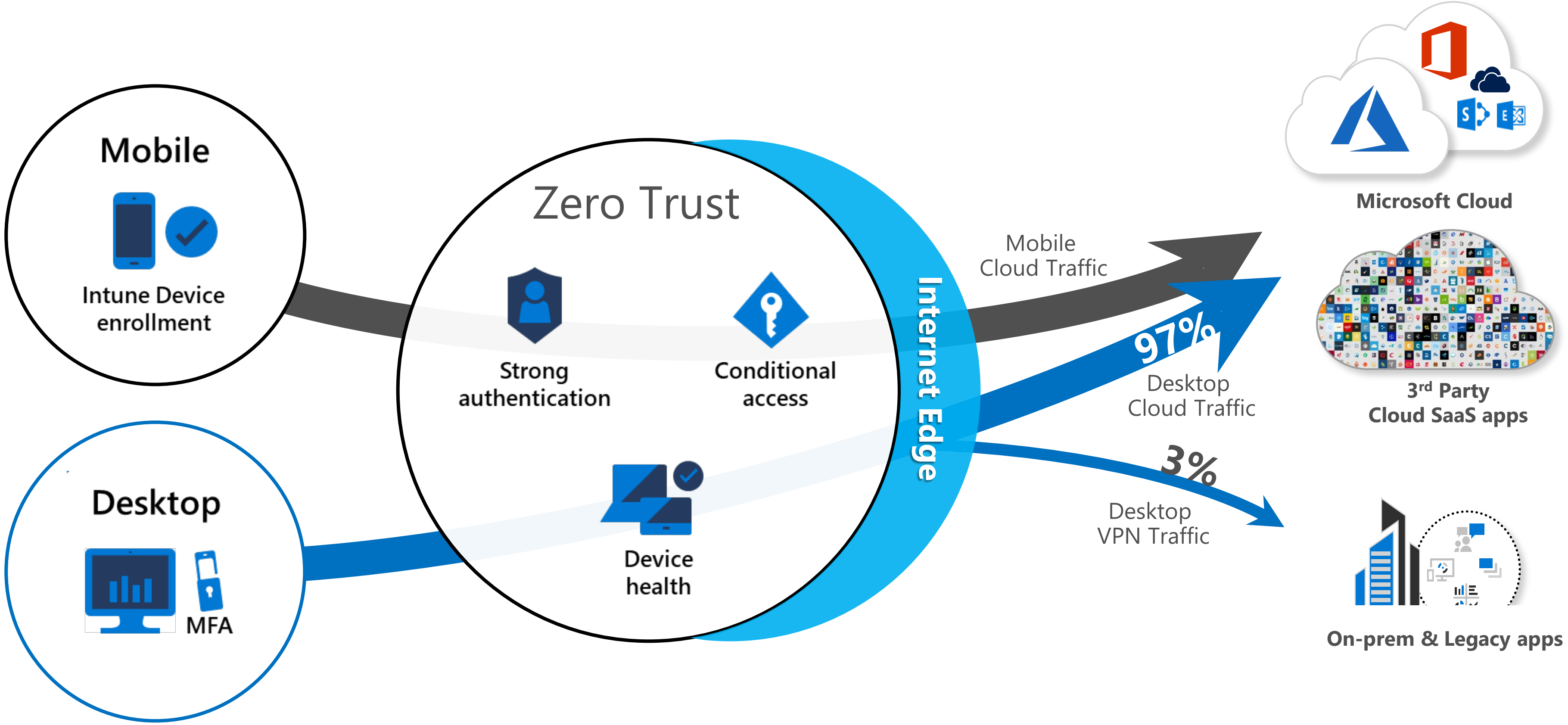
1. Reduce risk of compromised users & endpoints
   - Deny access from unmanaged/unhealthy devices
   - Reduce VPN usage / attack surface
2. Improves security visibility
   - No blind spots for remote devices
   - Centralized view of risk, policy exceptions, and access requests
   - Deep insight into device risk and user session activity
3. Provide access only where needed
   - Network segmentation
   - Minimize lateral movement

Increases productivity

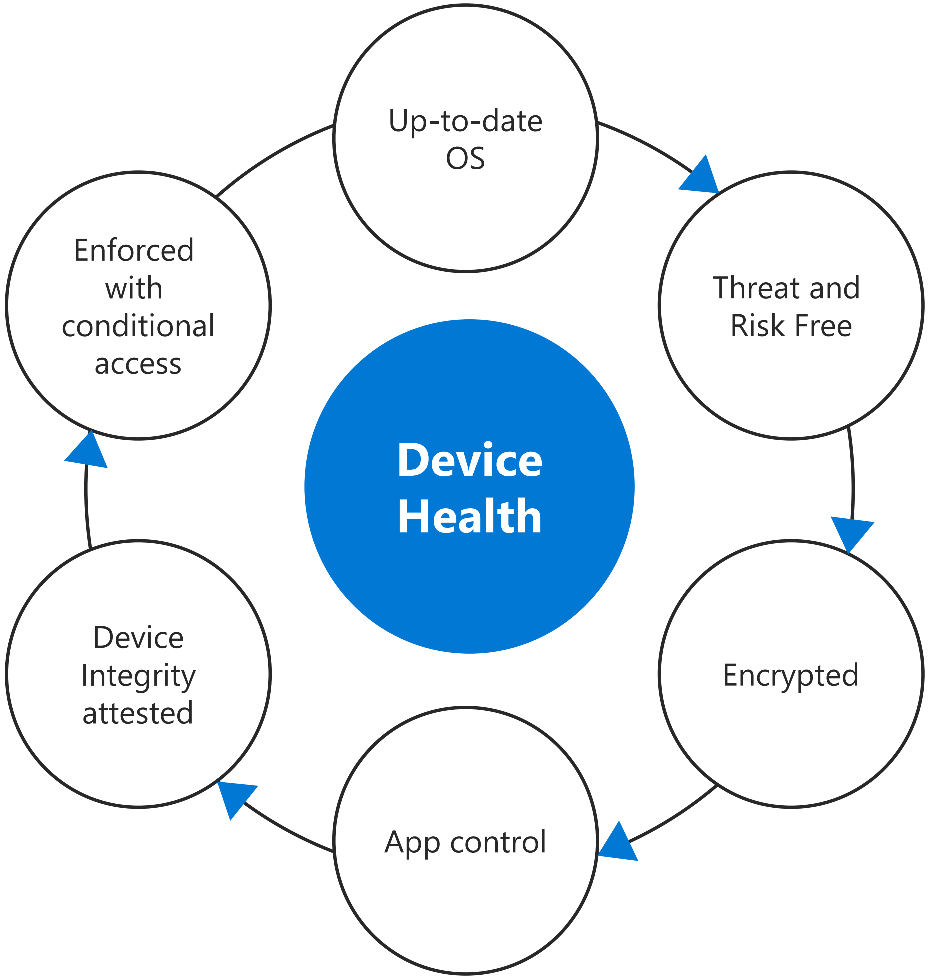
1. Can work anywhere you want
   - Internet is the default network
   - Apps & Data available anywhere
2. Single Sign On (SSO) across enterprise apps and services
   - Sign in once
3. Users guided into a compliant state:
   - Prompt to increase trust (e.g. MFA)
   - Limited access to apps/data
   - Guided steps to enroll devices
   - Virtualization for unmanaged devices

Increase security and productivity from “Password-Less" authentication

Zero Trust Access Model



What makes a healthy device?



Unmanaged devices are a powerful entry point for attackers and present a high risk to the enterprise

Core Scenarios

Scenario 1: All authentication to resources requires modern multi factor authentication

Scenario 2: Employees can enroll devices into a modern management system which guarantees the health of the device to control access to company resources

Scenario 3: Segmented networks built to support the required workloads

Scenario 4: Employees and business guests have a method to access corporate resources when not using a managed device

Scenario 5: Applications and services built with mechanisms that enforce device health check

Implementation goals of Zero Trust @Microsoft 2022+

IDENTITY	• Strong Identity is verified • Access to applications and data limited to minimum required to perform job function
DEVICE	• Client device health is enforced • Unmanaged devices and non-FTE have alternative access methods to resources • Users do not have administrative permissions on client devices
ACCESS	• Reduce dependency on CorpNet • Network Access Controls are enforced
SERVICE	• Applications and services enforcing conditional access
TELEMETRY	• Derive compliance & security state of Zero Trust controls, at enterprise scale to determine controls, policies and actions needed
EXPERIENCE	• Tell the right story to the appropriate internal audiences • Showcase the Microsoft implementation as a Zero Trust model for the industry • Leverage telemetry to measure user experience • Provide visibility into the overall state and progress of the Zero Trust implementation

Zero Trust Progress

Pre-Zero Trust

- ✗ Device management not required
- ✗ Single factor authentication to resources
- ✓ Capability to enforce strong identity exists
- ✓ Data classification and Information protection

Verify Identity

- ✓ SAW enforcement for admin access scenarios
- ✓ Migration from on-prem AD to AAD identities through O365 Migration.
- ✓ 100% of user accounts enforcing MFA

Verify Device

- ✓ 100% of Windows, iOS , Android & MAC devices are under management and enforcement
- ✓ All new devices defaulting to AADJ via Autopilot
- ✓ Device health enforcement in progress

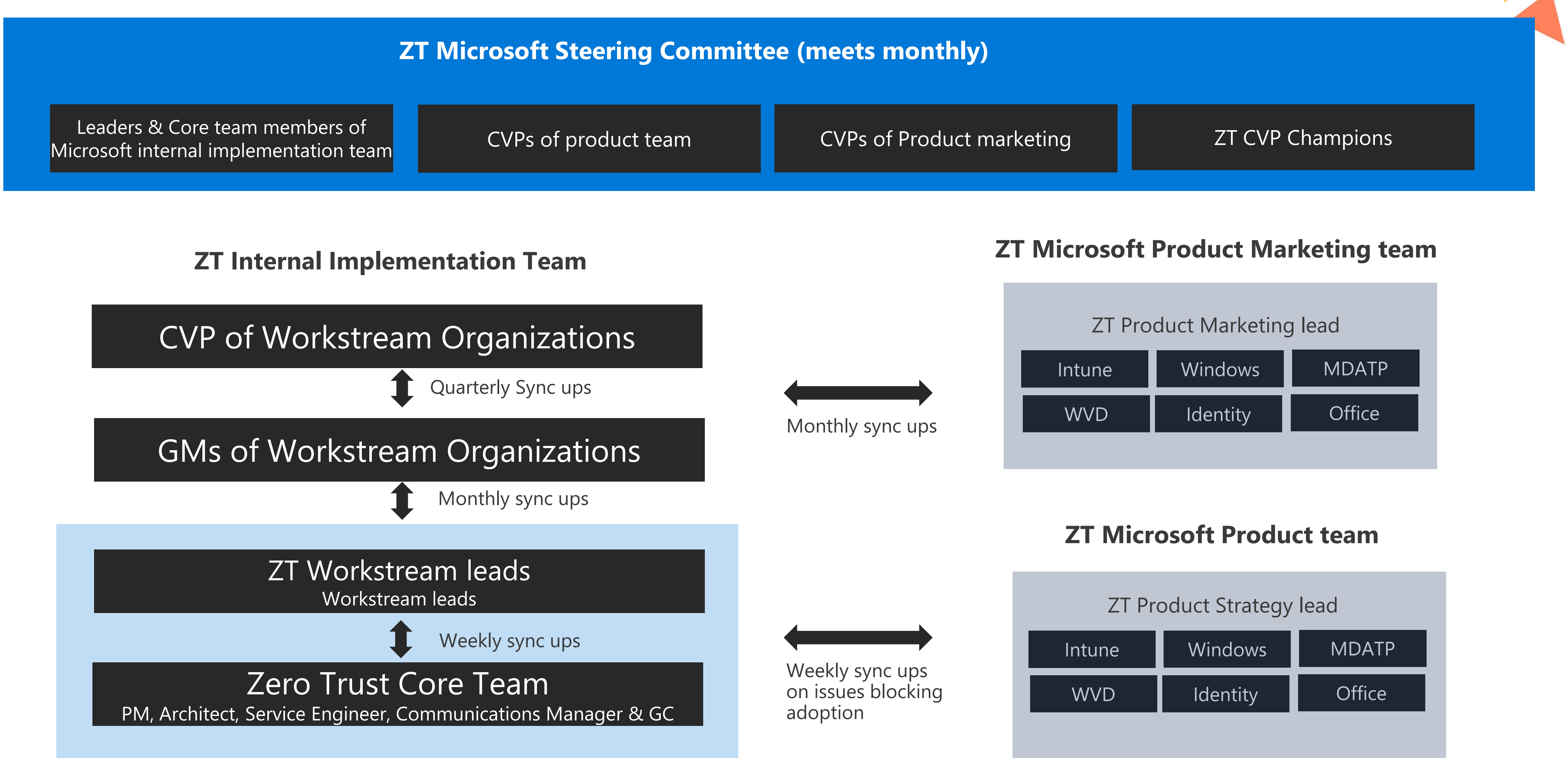
Verify Access

- ✓ Internet available as default in all MSFT office locations in progress
- ✓ Corpnet dependent telemetry created
- ✓ Network segmentation infrastructure creation

Verify Services

- ✓ Applications & Services accessible directly from Internet in progress
- ✓ MFA enforced for O365 access

Programmatic Overview



ZT Microsoft Steering Committee (meets monthly)

- Leaders & Core team members of Microsoft internal implementation team
- CVPs of product team
- CVPs of Product marketing
- ZT CVP Champions

ZT Internal Implementation Team

CVP of Workstream Organizations

Quarterly Sync ups

GMs of Workstream Organizations

Monthly sync ups

ZT Workstream leads
Workstream leads

Weekly sync ups

Zero Trust Core Team
PM, Architect, Service Engineer, Communications Manager & GC

Monthly sync ups

Weekly sync ups on issues blocking adoption

ZT Microsoft Product Marketing team

ZT Product Marketing lead

Intune	Windows	MDATP
WVD	Identity	Office

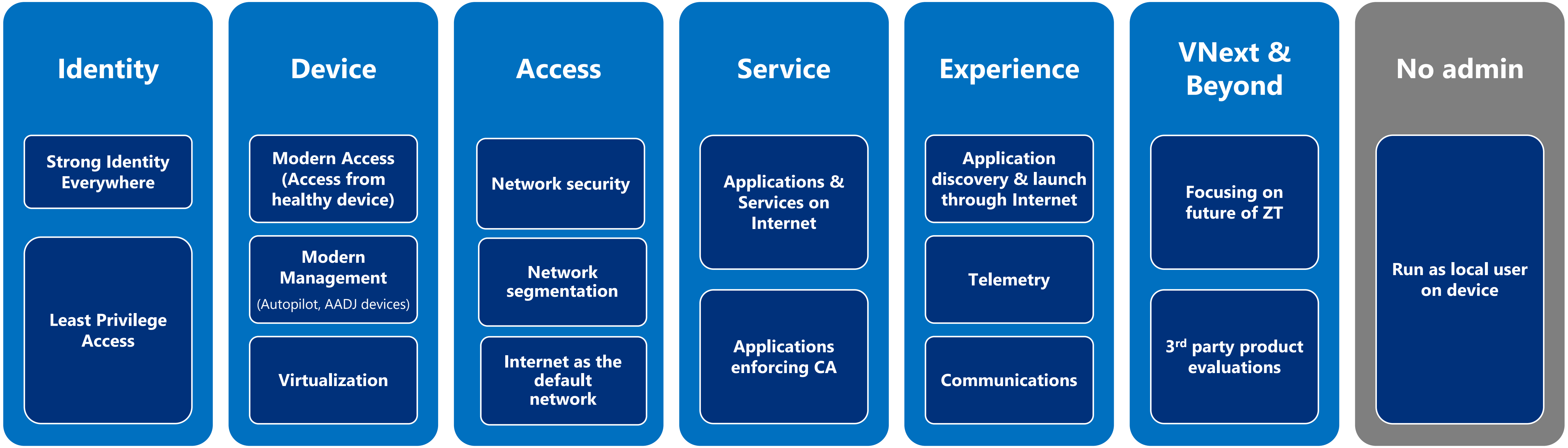
ZT Microsoft Product team

ZT Product Strategy lead

Intune	Windows	MDATP
WVD	Identity	Office

Managing the Zero Trust implementation

- Scenarios-> Goals->Workstreams owned by various sub-organizations
- Resulted in multiple programs reporting under ZT
- Zero Trust is company-wide effort



Identity
- Strong Identity Everywhere
- Least Privilege Access

Device
- Modern Access (Access from healthy device)
- Modern Management (Autopilot, AADJ devices)
- Virtualization

Access
- Network security
- Network segmentation
- Internet as the default network

Service
- Applications & Services on Internet
- Applications enforcing CA

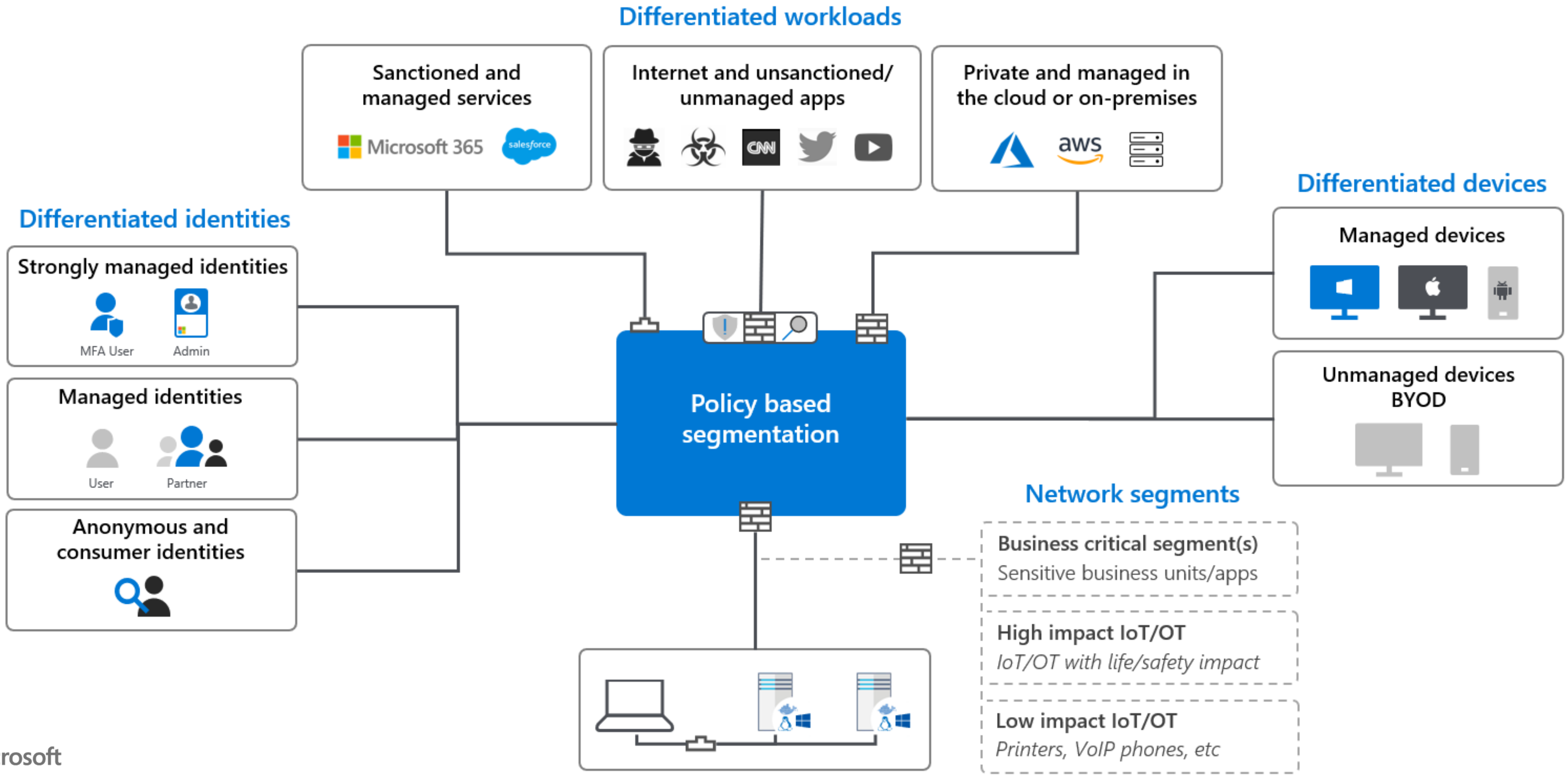
Experience
- Application discovery & launch through Internet
- Telemetry
- Communications

VNext & Beyond
- Focusing on future of ZT
- 3rd party product evaluations

No admin
- Run as local user on device

Future Goal

Zero Trust- Network segmentation transformation



Differentiated workloads

Sanctioned and managed services

Internet and unsanctioned/ unmanaged apps

Private and managed in the cloud or on-premises

Differentiated identities

Strongly managed identities

Managed identities

Anonymous and consumer identities

Policy based segmentation

Differentiated devices

Managed devices

Unmanaged devices BYOD

Network segments

Business critical segment(s)
Sensitive business units/apps

High impact IoT/OT
IoT/OT with life/safety impact

Low impact IoT/OT
Printers, VoIP phones, etc

Key Considerations

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. Run pilots and ringed roll-outs. Slow and steady wins the race.
6. Migrate your users to the Internet and monitor VPN traffic to understand internal dependencies.
7. Focus on user experience as it is critical to employee productivity and moral. Without adoption, your program will not be a success.
8. Communication is key….bring your employees on the journey with you!
9. Assign performance indicators and goals for all workstreams and elements… including employee sentiment.

We want to hear from you!

✓ Read about how we are implementing a Zero Trust Model at Microsoft at aka.ms/ZTatMSFT

✓ Stay connected with us and send feedback to MSZT@Microsoft.com