Microsoft

Never trust, Always verify

Getting to Zero Trust with Azure Active Directory

Swetha Rai

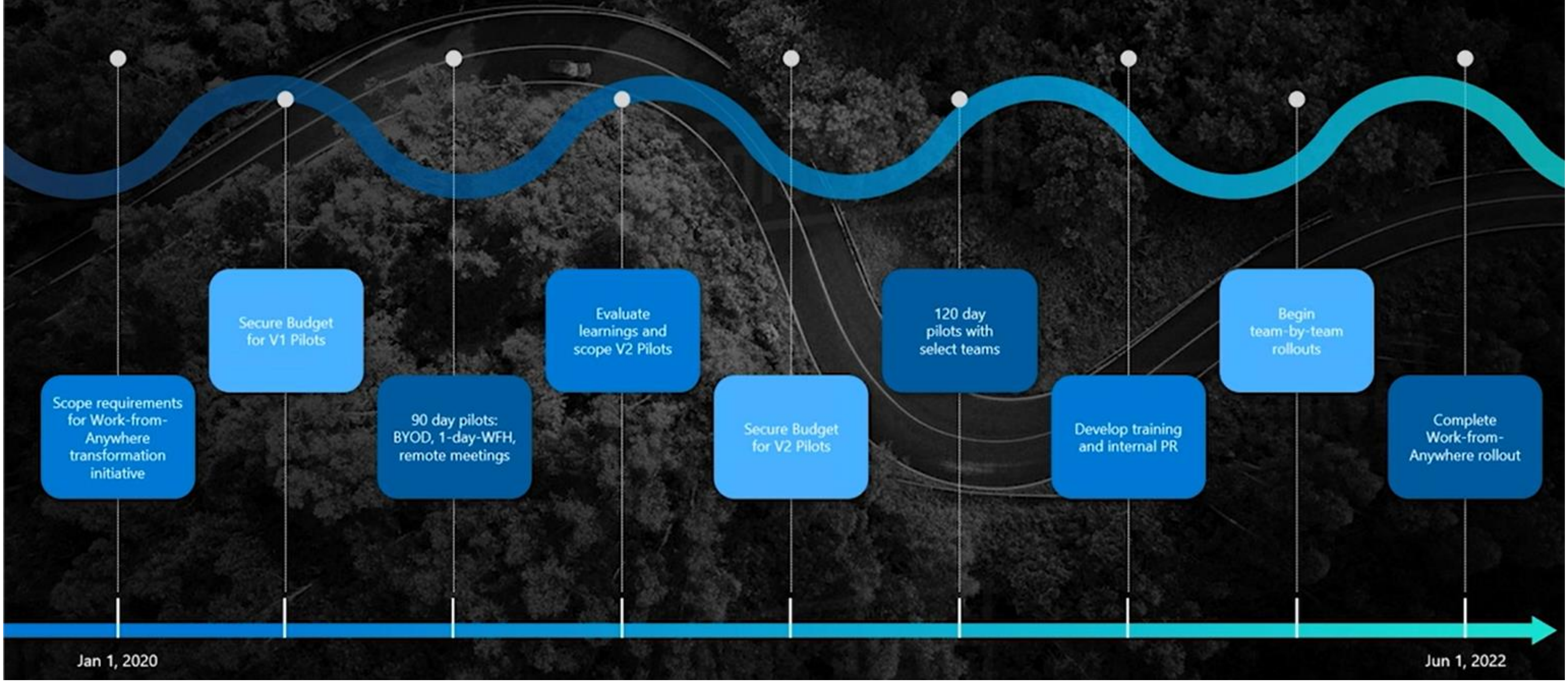
Corissa Koopmans

Program Manager at Microsoft – Azure AD Identity Division

Agenda

- New security model
- Zero Trust implementation
- Components
- Resources
- Q&A

Digital transformation roadmap



Scope requirements for Work-from-Anywhere transformation initiative

Secure Budget for V1 Pilots

90 day pilots: BYOD, 1-day-WFH, remote meetings

Evaluate learnings and scope V2 Pilots

Secure Budget for V2 Pilots

120 day pilots with select teams

Develop training and internal PR

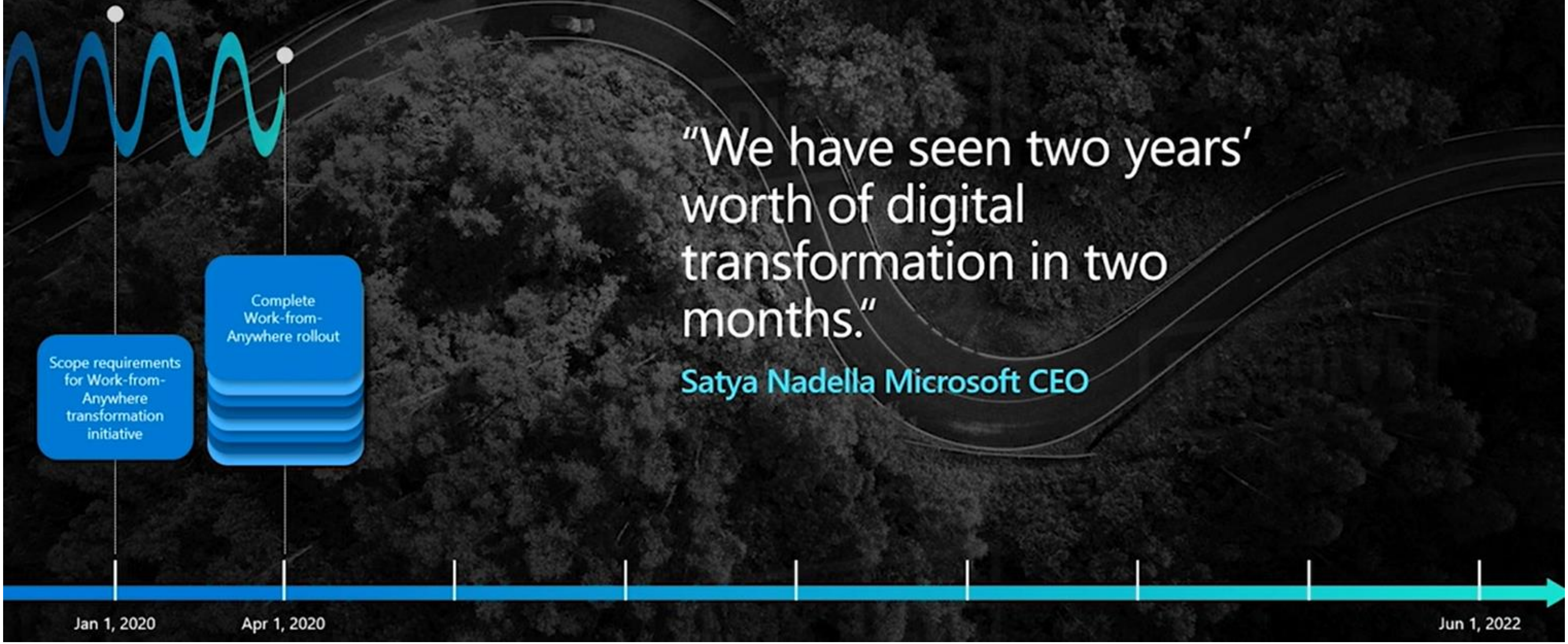
Begin team-by-team rollouts

Complete Work-from-Anywhere rollout

Jan 1, 2020

Jun 1, 2022

Digital transformation roadmap



Scope requirements for Work-from-Anywhere transformation initiative

Complete Work-from-Anywhere rollout

> “We have seen two years’ worth of digital transformation in two months.”
>
> Satya Nadella Microsoft CEO

Then vs Now

Full Control (mostly)

Control Identity

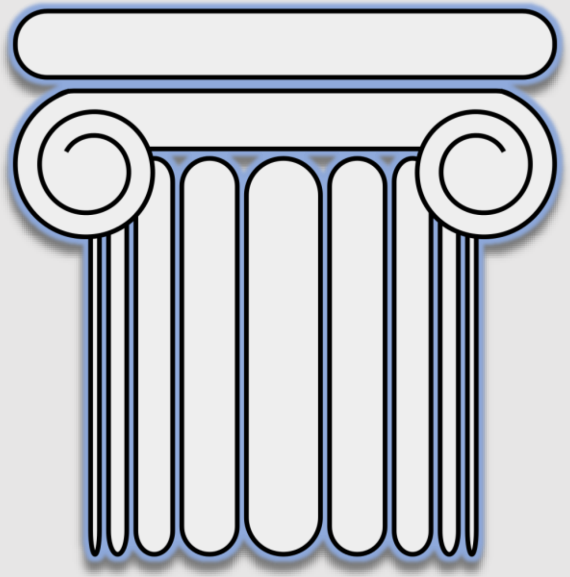
We need a new security model : Zero Trust

“Trust nothing, verify everything”

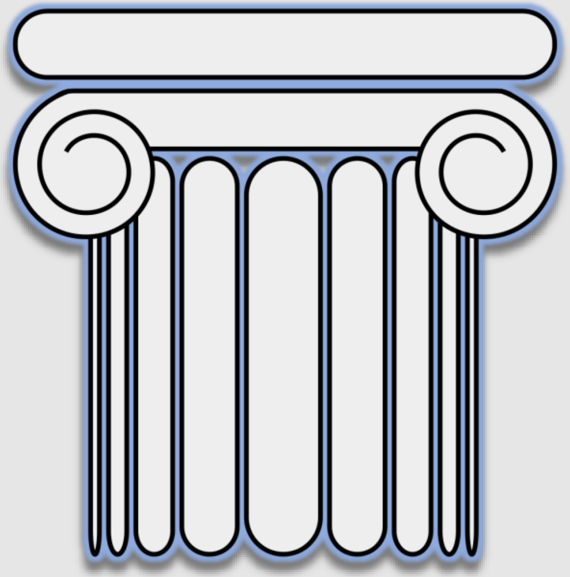
- Built for cloud workloads
- Extends productivity while maximizing security

What even is it…

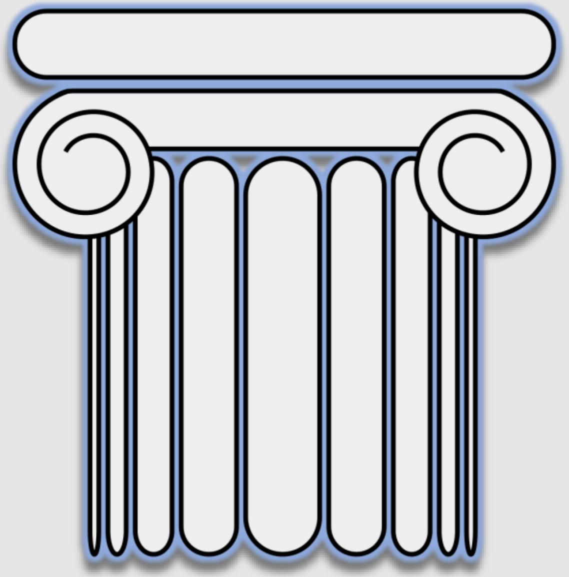
Zero trust mindset…



Verify explicitly

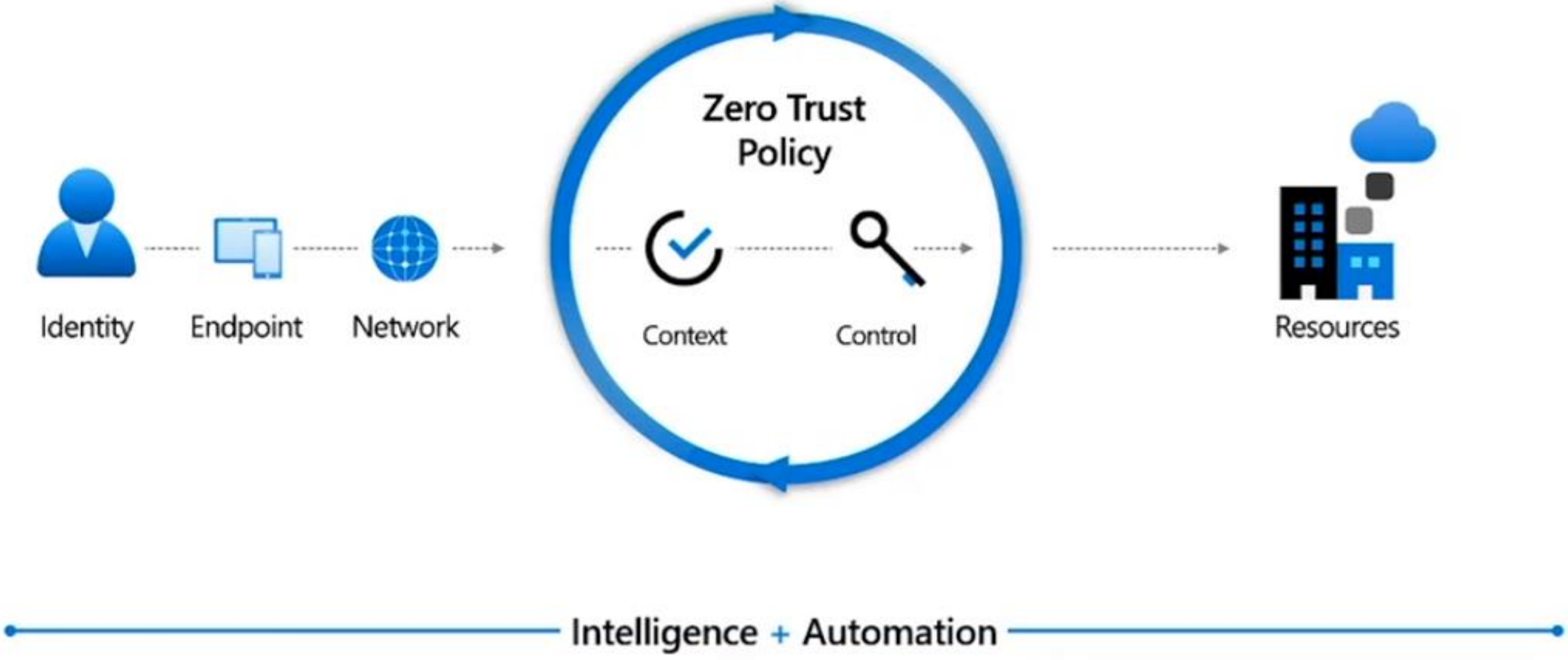


Use least
privileged access



“Assume breach”

Zero Trust


Identity
Endpoint
Network
Zero Trust Policy
Context
Control
Resources
Intelligence + Automation

Build Zero Trust into...

People

Devices

Workloads

Data

Networking

Infrastructure

Identity

People

- ✓ Connect/consolidate all identities.
- ✓ Enable SSO for all apps (SaaS and on-premises)
- ✓ Use strong credentials (MFA, FIDO2, etc)
- ✓ Reduce administrator accounts and implement policies (PIM)
- ✓ Control access with smart policies (Conditional access, Identity Protection)

Microsoft

Demo

Devices

Devices

✓ Ensure devices are known, healthy and compliant

✓ Require endpoint threat detection and anti-malware software on all devices.

✓ Turn on hybrid or Azure AD-join

Microsoft

Demo

Applications & Workloads

Workloads

- ✓ Restrict access to approved mobile apps and configurations (Intune MAM)
- ✓ Replace VPNs with proxy/VDI solutions
- ✓ Discover/monitor “Shadow IT” (MCAS)
- ✓ Gate access based on real-time analytics
- ✓ Limit User Consent to apps from verified publishers and low impact privileges

Microsoft

Demo

Data

101010
010101
101010

Data

- ✓ Move towards data-driven protection
- ✓ Use machine learning to classify and label data
- ✓ Determine access to data based on risk

Microsoft

Demo

Networking

Networking

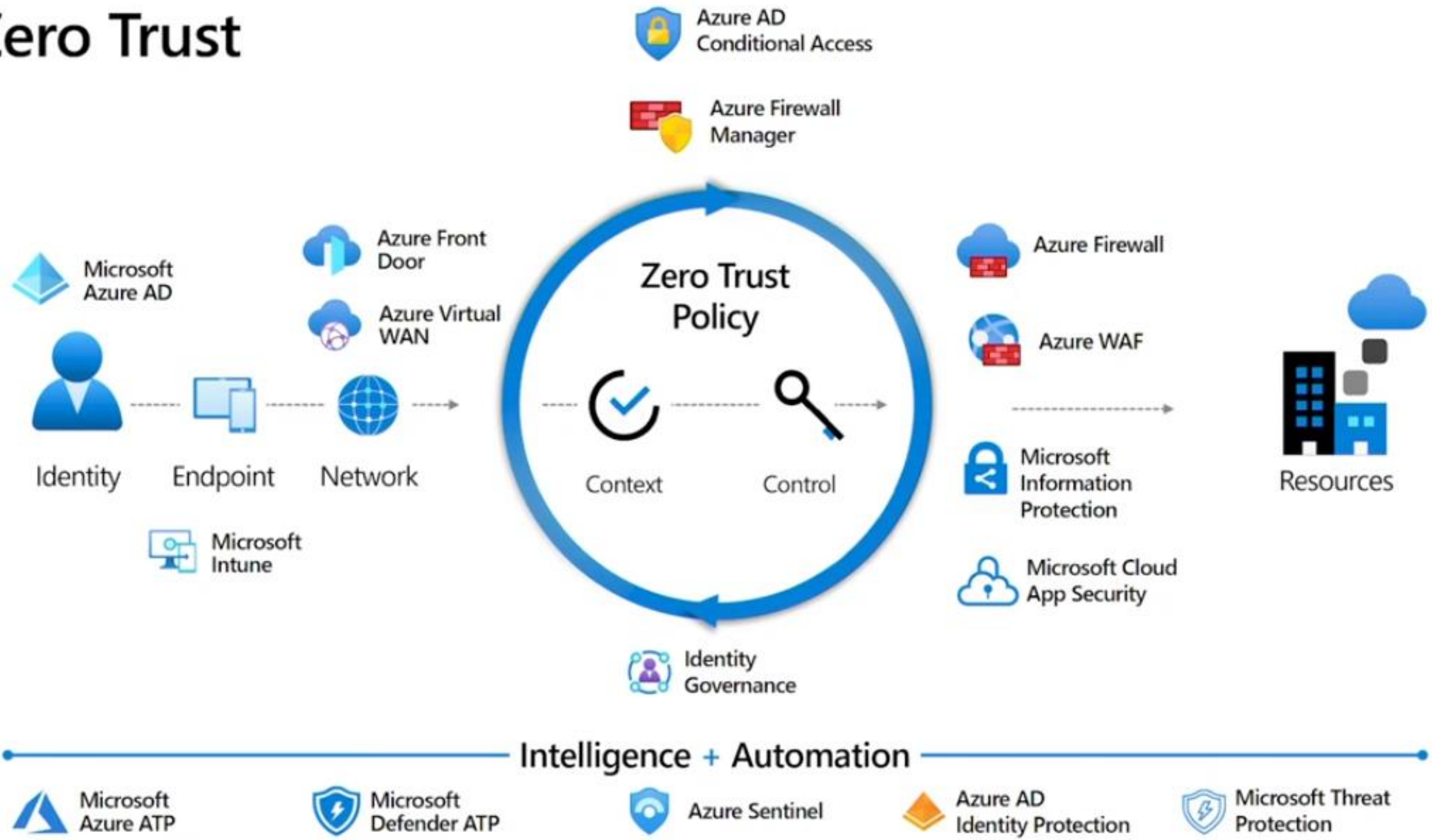
- ✓ Don’t implicitly trust internal networks
- ✓ All sessions should be encrypted
- ✓ Isolate networks and workloads
- ✓ Limit access via policy

Infrastructure

Infrastructure

- ✓ Review the baseline infrastructure deployment objectives
- ✓ Monitor and set up alerts for abnormal behavior
- ✓ Assign every workload an app identity
- ✓ Require Just-In Time access

Zero Trust



Azure AD Conditional Access

Azure Firewall Manager

Microsoft Azure AD

Azure Front Door

Azure Virtual WAN

Identity

Endpoint

Network

Microsoft Intune

Zero Trust Policy

Context

Control

Identity Governance

Azure Firewall

Azure WAF

Microsoft Information Protection

Microsoft Cloud App Security

Resources

Intelligence + Automation

Microsoft Azure ATP

Microsoft Defender ATP

Azure Sentinel

Azure AD Identity Protection

Microsoft Threat Protection

The Payoff

Intelligence

- ✓ Block or change compromised creds
- ✓ MFA challenge session risk
- ✓ Deny access to infected devices
- ✓ Revoke access to documents at risk
- ✓ Automatically defend against emerging threats

Go-Do's

- Deploy strong credentials (MFA/FIDO2/Other)
- Deploy Azure AD Privileged Identity Management
- Review sign-in and audit logs to increase awareness
- Review apps and their permissions in your environment

Resources

- **Zero Trust Deployment Center**
  - aka.ms/ZTGuide
- **Azure AD blog**
  - aka.ms/identityblog
- **Zero Trust Assessment tool**
  - aka.ms/zerotrust
- **Five steps to securing your identity infrastructure**
  - aka.ms/securitysteps
- **Inventory applications and their granted permissions**
  - https://aka.ms/getazureadpermissions

Questions?