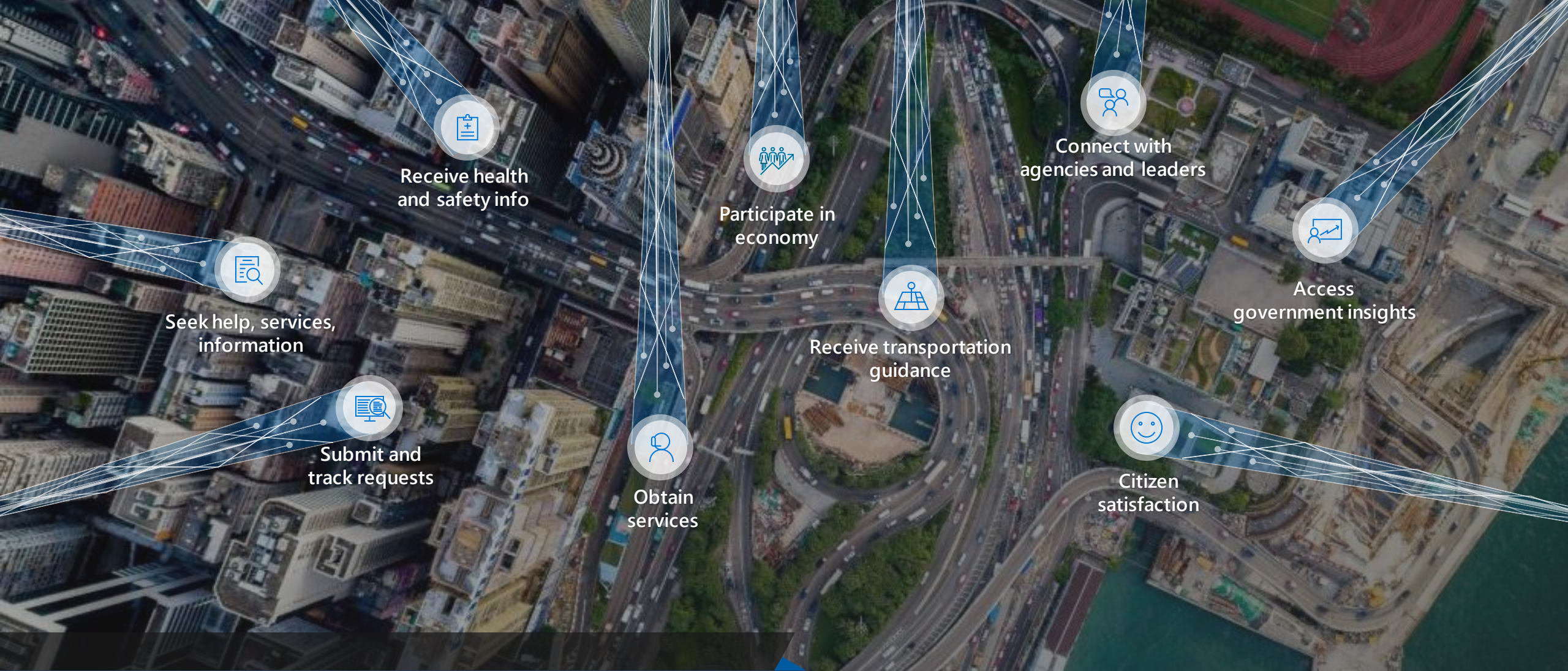




Why Zero Trust?

Dan Craytor, Ph.D.
CTO – US Public Sector
danc@microsoft.com





Receive health and safety info

Participate in economy

Connect with agencies and leaders

Access government insights

Seek help, services, information

Receive transportation guidance

Citizen satisfaction

Submit and track requests

Obtain services

THE DIGITAL ERA IS HERE

What does this mean to you?

“ Every company is a software company. You have to start thinking and operating like a digital company. It’s no longer just about procuring one solution and deploying one. It’s really you, yourself, thinking of your own future as a digital company. ”
– Satya Nadella, Microsoft CEO

Today's technology is fueling widespread disruption

Public governments will begin processing citizen services in real-time, leveraging better customer intelligence and **robotic process automation**

By 2023, 25% of

By 2023, **at least 80%** of government services require authentication

19% of all citizens have a physical or cognitive disability

More than **1 billion people** worldwide experience some form of disability. And **70%** of those with disabilities—**estimated 70% have invisible disabilities.**

In 2019 12.7% cyber attacks were against public admin, defense, social sec and **9.5%** to human health and social work

generated **1.5 quintillion bytes of data daily** in 2018, and that number continues to rise

And the most likely threat is phishing

300% increase in identity attacks over the past year.



Phishing

23M

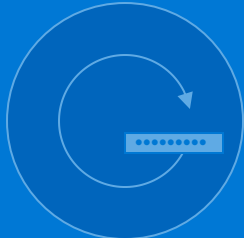
high risk enterprise sign-in attempts detected in **March 2018**



Password Spray

350K

compromised accounts detected in **April 2018**



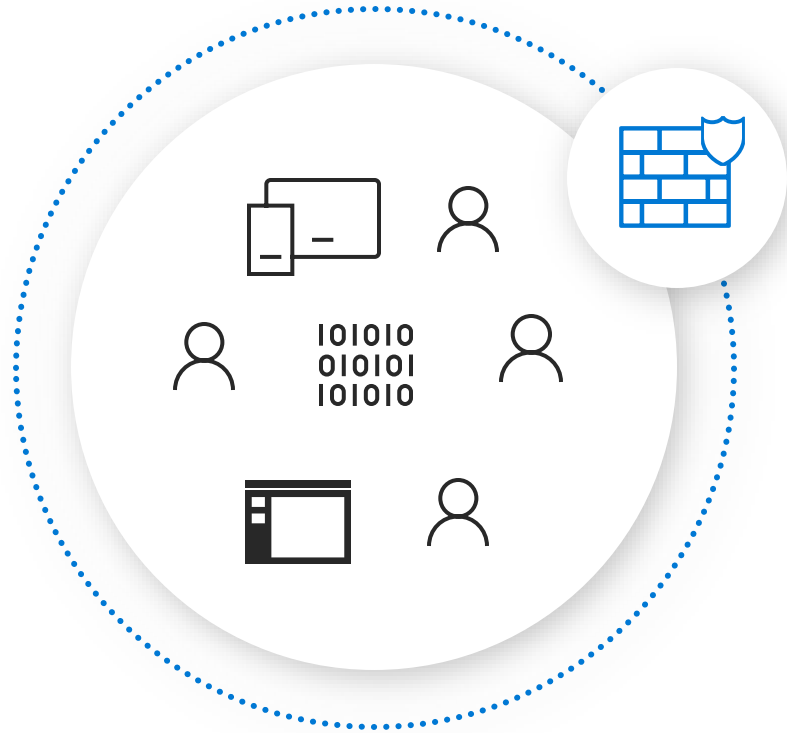
Breach Replay

4.6B

attacker-driven sign-ins detected in **May 2018**

A Little History!

Traditional Model



Users, devices, apps, and data
protected behind a network firewall



By 1995:

Most networks are connected
by VPN and Internet replacing
WANs – Firewalls and VPN
dominate security conversation

PROTECT

across all endpoints, from sensors to the datacenter



DETECT

using targeted signals, behavioral monitoring, and machine learning

RESPOND

closing the gap between discovery and action

Old World vs. New World

Users are employees



Employees, partners, & customers

Corporate managed devices



Bring your own devices

On-premises apps



Explosion of cloud apps

Corp network and firewall



Perimeter-less

Local packet tracking and logs


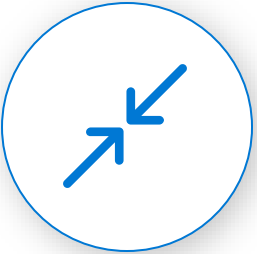
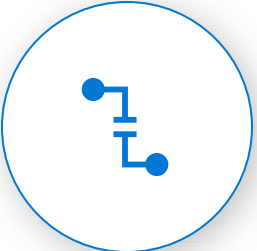


Explosion of signal

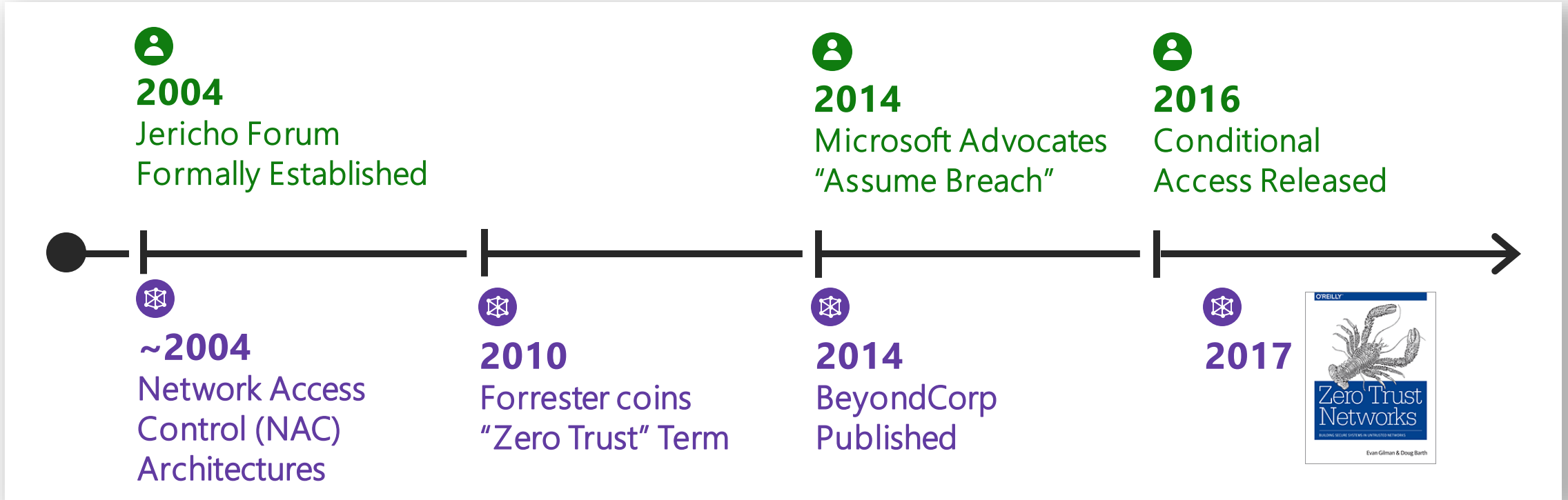
New World

- Employees, partners, & customers
- Bring your own devices
- Explosion of cloud apps
- Perimeter-less
- Explosion of signal

New Security Paradigm

-  Identity is the firewall
-  Devices are the perimeter
-  Assume breach

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



Slow mainstream adoption for both network identity models:



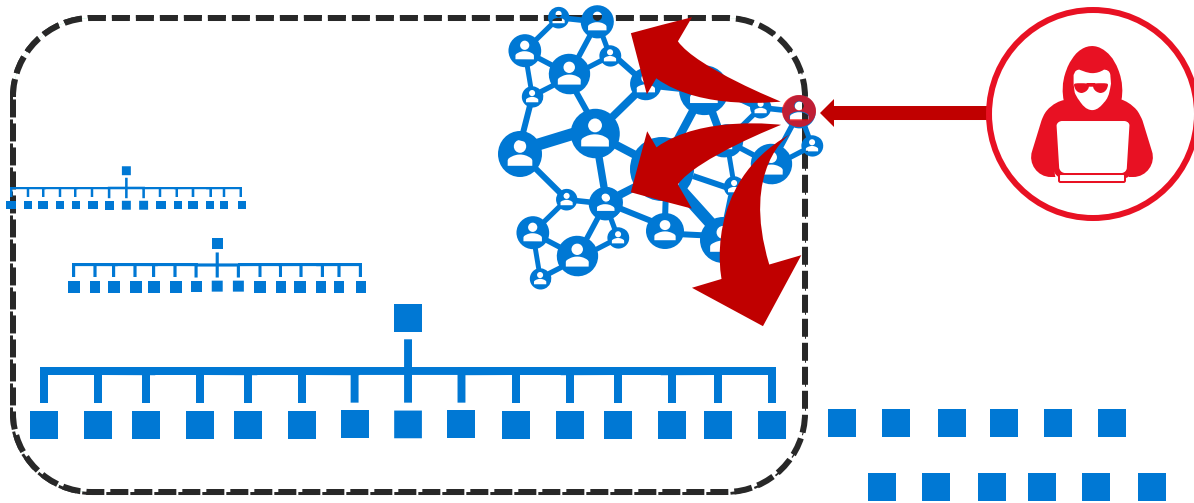
Network – Expensive and challenging to implement
Google's BeyondTrust success is rarely replicated



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

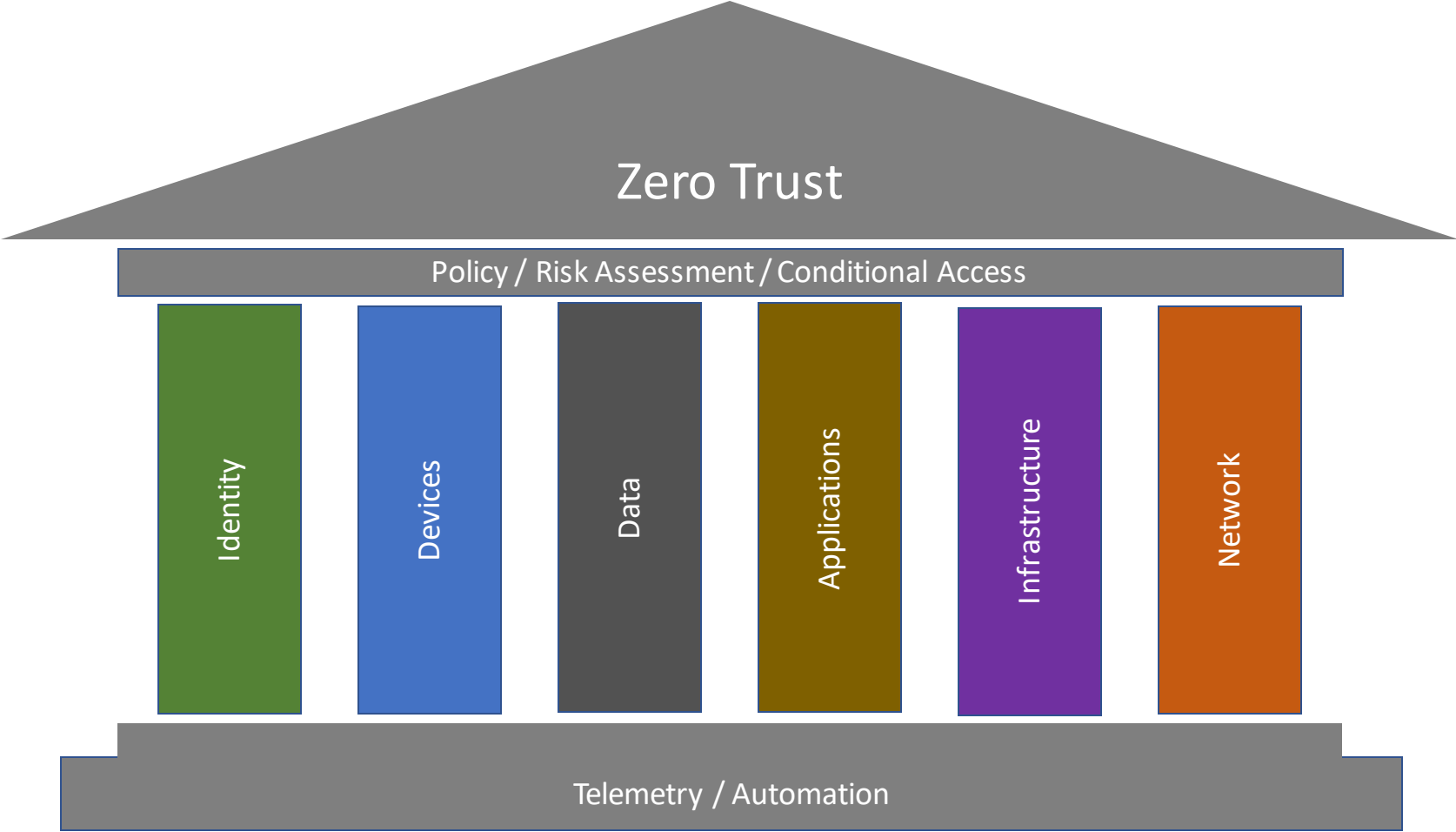
Why are we having a Zero Trust conversation?

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. **Attackers shift to identity attacks**
 - Phishing and credential theft
 - Security teams often overwhelmed
4. **Assets increasingly leave network**
 - BYOD, WFH, Mobile, and SaaS

How is our approach different?



This is your journey



NIST Definition of Zero Trust



“Zero trust (ZT) is the term for an **evolving set of cybersecurity paradigms** that move network defenses from static, network-based perimeters to **focus on users, assets, and resources.**”

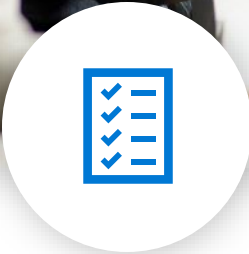


“Zero trust assumes there is **no implicit trust granted to assets or user accounts** based solely on their physical or network location.”

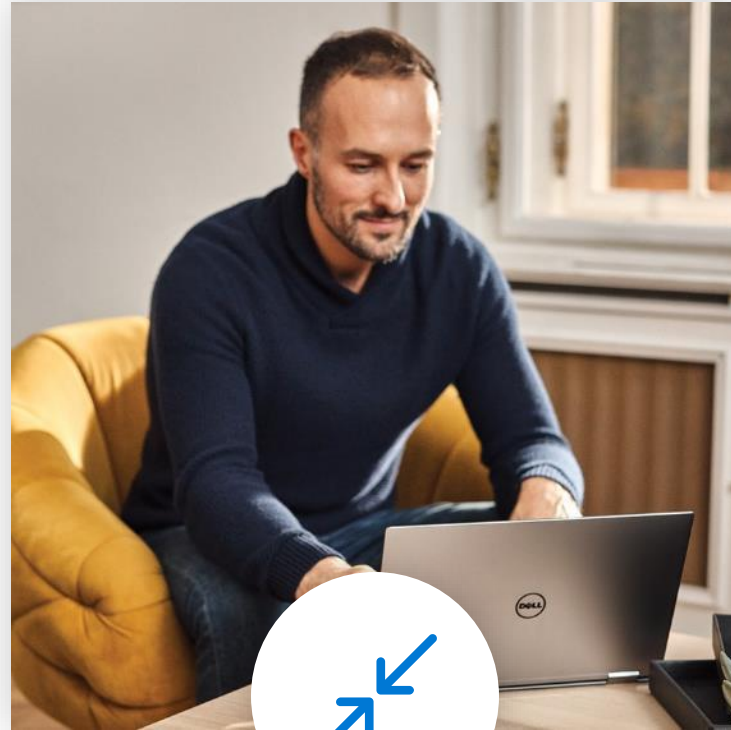


“Zero trust **focuses on protecting resources, not network segments,** as the network location is no longer seen as the prime component to the security posture of the resource.”

Zero Trust Principles (industry lessons learned)



Explicit verification

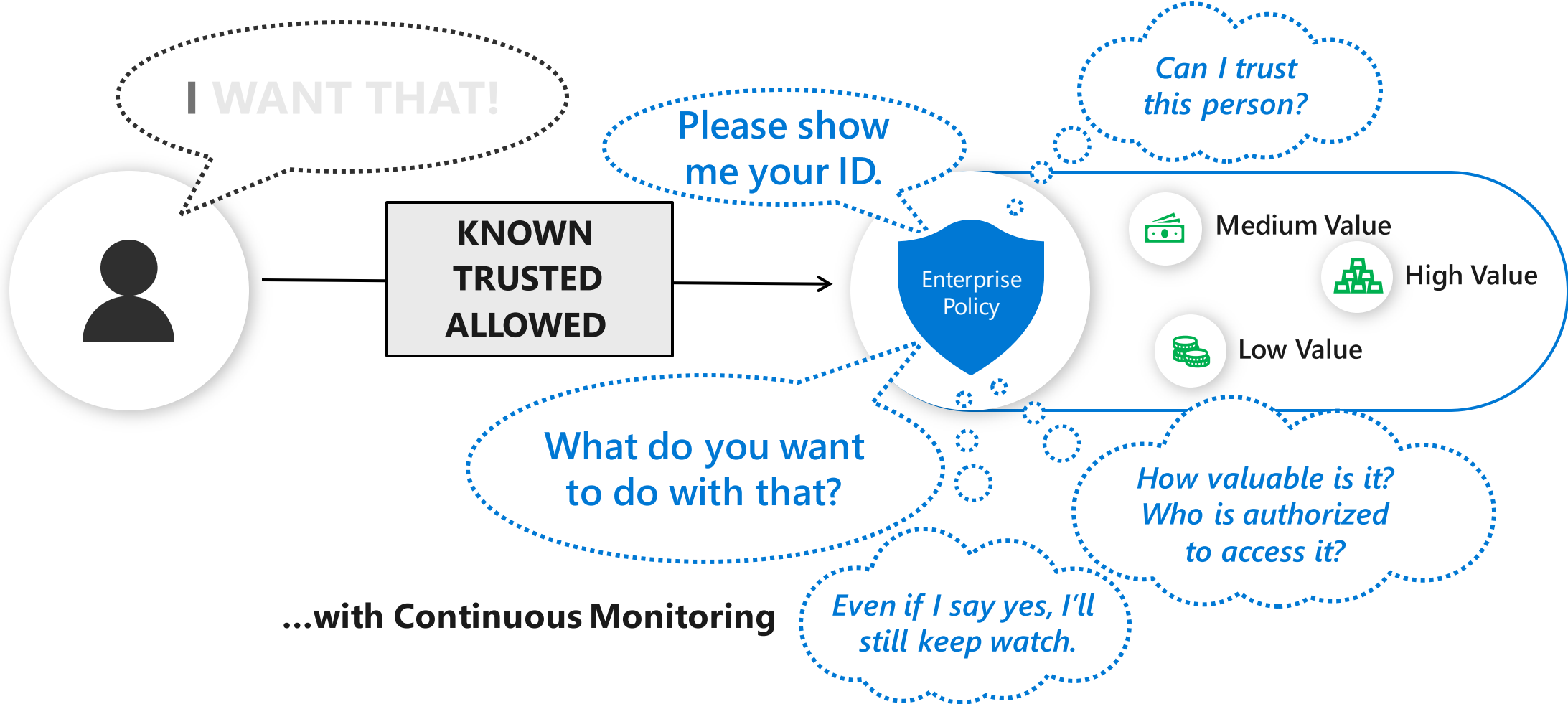


Least privilege access

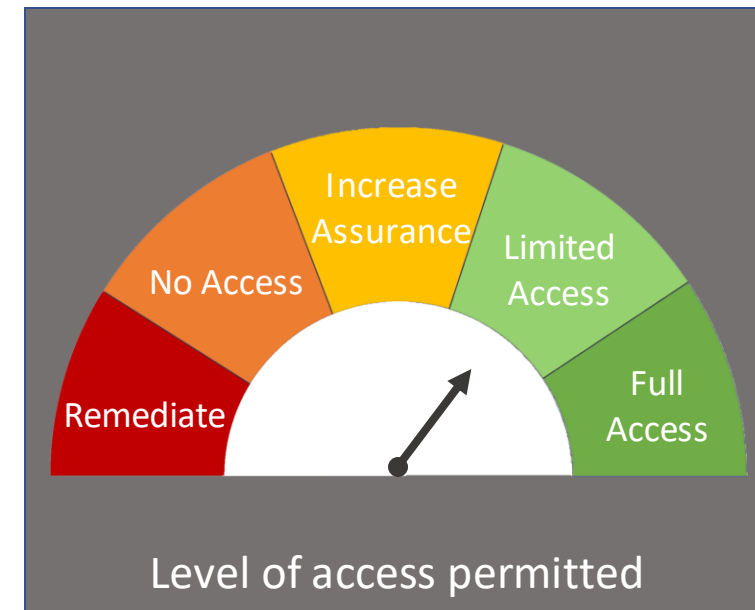
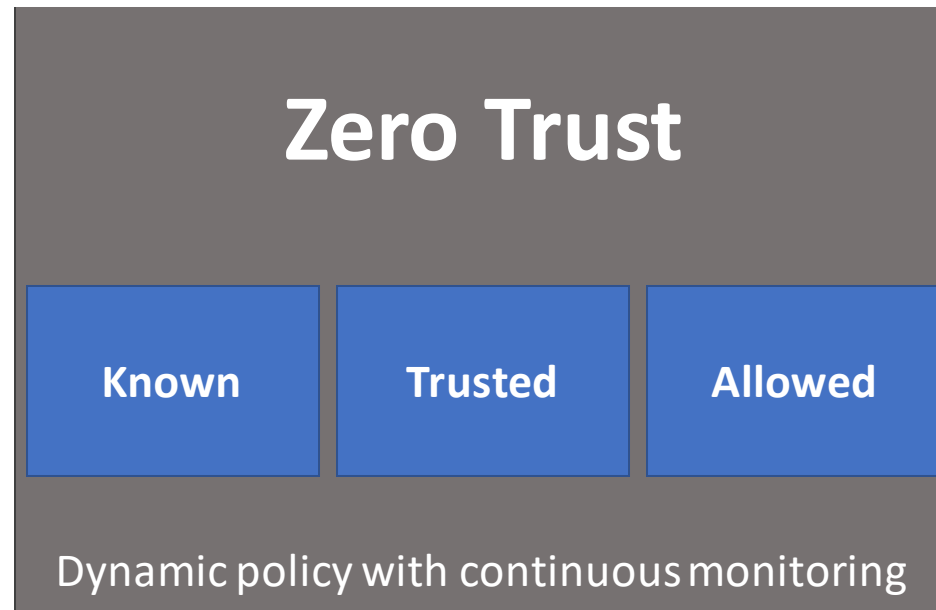
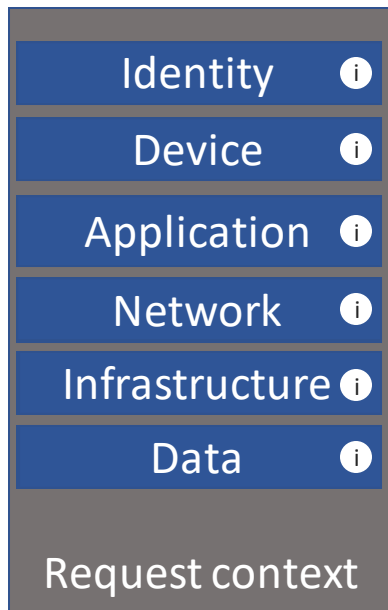
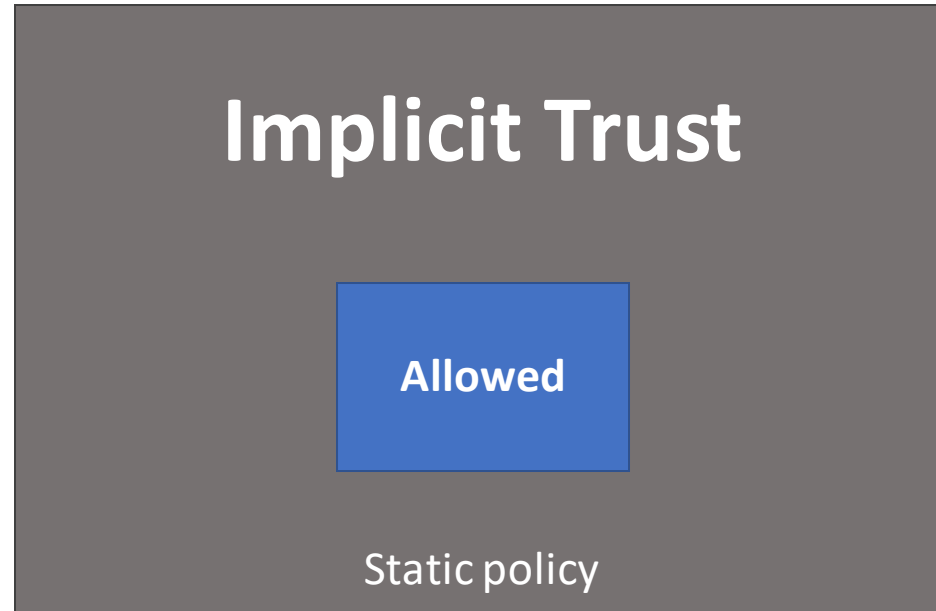
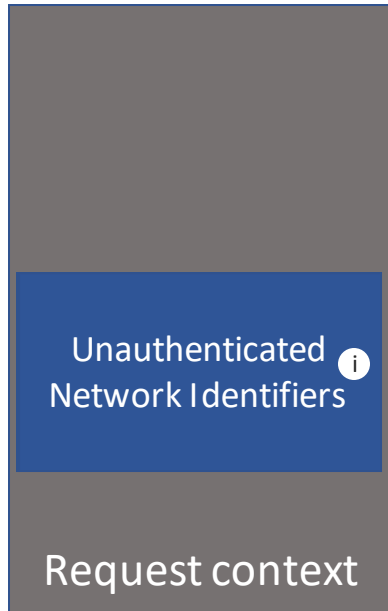


Assume breach

How Zero Trust works



Moving from Implicit Trust to Zero Trust



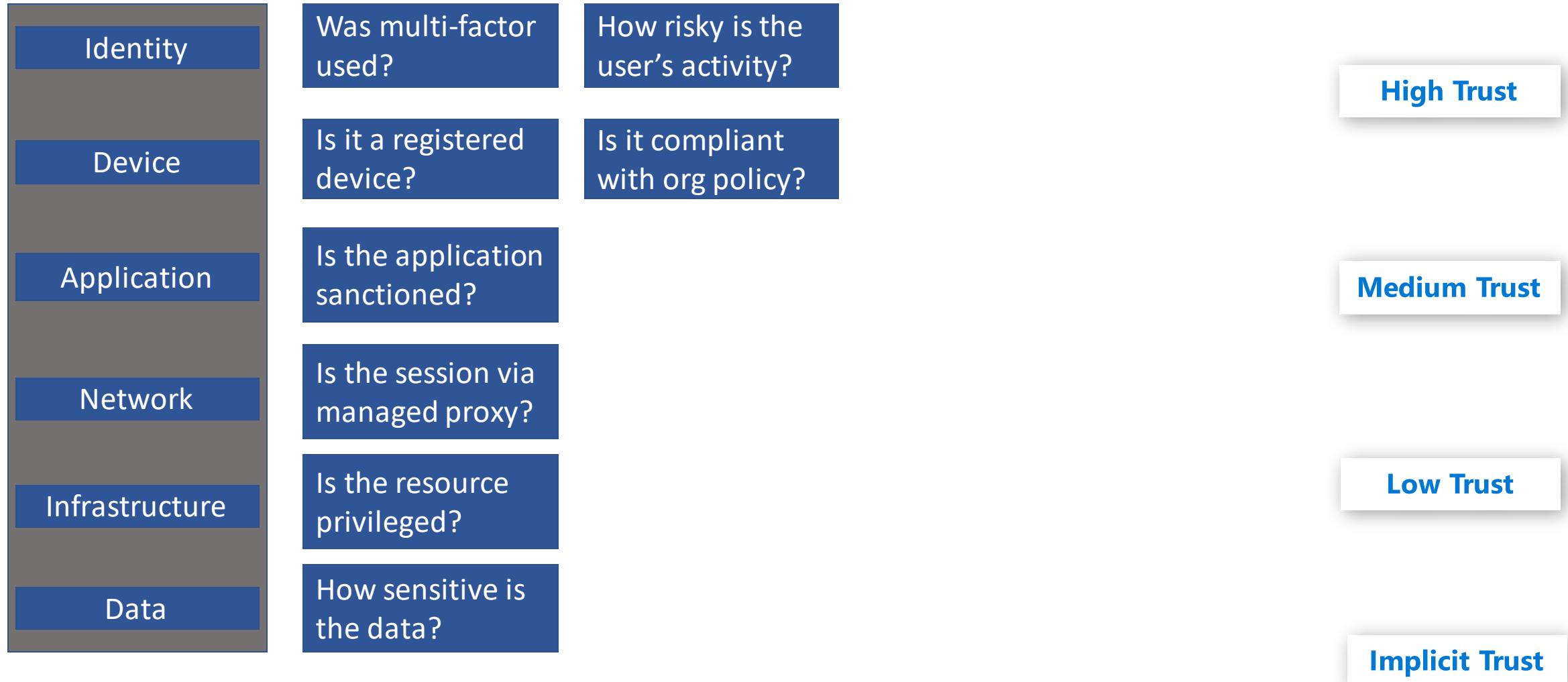
Building Trust

Resource 1 Policy ⓘ

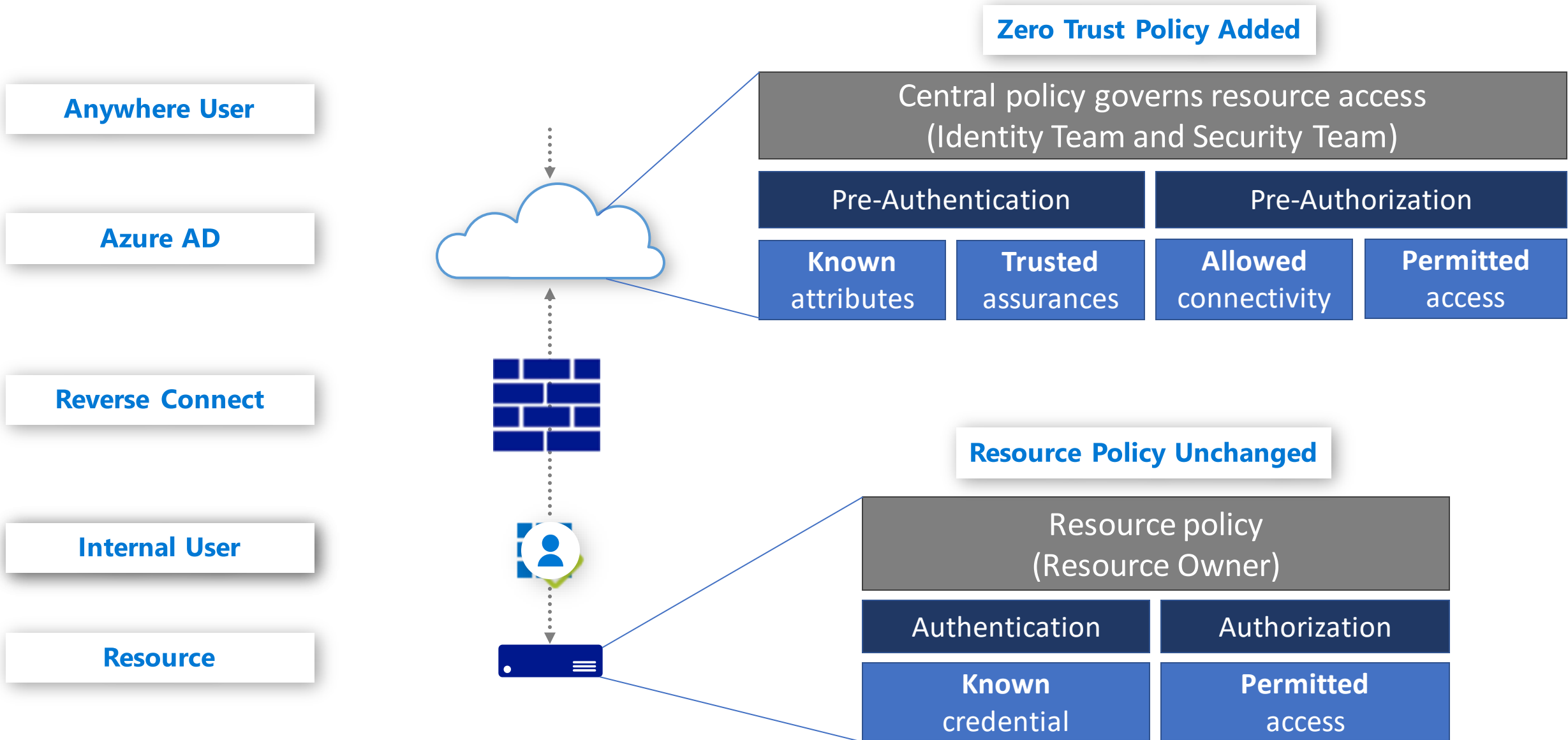
Resource 2 Policy ⓘ

Resource 3 Policy ⓘ

Choose attributes and assurances from across the six pillars to achieve necessary trust for each resource



Scenario: Beyond VPN - Layer in Zero Trust with Secure Hybrid Access



Consistent Zero Trust User Experience Enterprise-Wide



Zero Trust Benefits

across security and productivity



Increases security

1. Reduce risk of compromised users & endpoints
 - Remove user endpoints from enterprise network
 - Reduce VPN usage / attack surface
2. Improve security visibility
 - No blind spots for remote devices
 - Centralized monitoring of risk, policy exceptions, and access requests
 - Contextual evidence of device risk and user session activity
3. Increase control of cloud environments
 - Application approval and session control
 - Automated policy enforcement

Increases productivity

1. Increase mission agility and flexibility
 - Enables secure work from anywhere
 - With any device
2. Consistent user experience
 - Seamless Single Sign On (SSO) experience across enterprise apps and services
3. Improve “access denied” experience
 - Limited access to apps/data
 - Increase assurance with MFA, device registration, or vulnerability resolution
 - Remediation of compromised entities

Better security and user experience from “Password-Less” authentication

Zero Trust Maturity Model (1 of 2)

Identities



Traditional

- On-premises identity provider is in use
- No SSO is present between cloud and on premises apps
- Visibility into identity risk is very limited

Advanced

- Cloud identity federates with on-premises system
- Conditional access policies gate access and provide remediation actions
- Analytics improve visibility

Optimal

- Passwordless authentication is enabled
- User, device, location, and behavior is analyzed in real time to determine risk and deliver ongoing protection

Devices



- Devices are domain joined and managed with solutions like Group Policy Object or Config Manager
- Devices are required to be on network to access data

- Devices are registered with cloud identity provider
- Access only granted to cloud managed & compliant devices
- DLP policies are enforced for BYO and corporate devices

- Endpoint threat detection is used to monitor device risk
- Access control is gated on device risk for both corporate and BYO devices

Apps



- On-premises apps are accessed through physical networks or VPN
- Some critical cloud apps are accessible to users

- On-premises apps are internet-facing and cloud apps are configured with SSO
- Cloud Shadow IT risk is assessed; critical apps are monitored and controlled

- All apps are available using least privilege access with continuous verification
- Dynamic control is in place for all apps with in-session monitoring and response

Zero Trust Maturity Model (2 of 2)

Infrastructure



Network



Data



Traditional

- Permissions are managed manually across environments
- Configuration management of VMs and servers on which workloads are running

- Few network security perimeters and flat open network
- Minimal threat protection and static traffic filtering
- Internal traffic is not encrypted

- Access is governed by perimeter control, not data sensitivity
- Sensitivity labels are applied manually, with inconsistent data classification

Advanced

- Workloads are monitored and alerted for abnormal behavior
- Every workload is assigned app identity
- Human access to resources requires Just-In-Time

- Many ingress/egress cloud micro-perimeters with some micro-segmentation
- Cloud native filtering and protection for known threats
- User to app internal traffic is encrypted

- Data is classified and labeled via regex/keyword methods
- Access decisions are governed by encryption

Optimal

- Unauthorized deployments are blocked with alerts
- Granular visibility and access control are available across all workloads
- User and resource access is segmented for each workload

- Fully distributed ingress/egress cloud micro-perimeters and deeper micro-segmentation
- ML-based threat protection and filtering with context-based signals
- All traffic is encrypted

- Classification is augmented by smart machine learning models
- Access decisions are governed by a cloud security policy engine
- DLP policies secure sharing with encryption and tracking

Next Steps



Learn more about our vision for Zero Trust at microsoft.com/security/blog/zero-trust/



Develop a cyber migration strategy with Zero Trust principles



Begin with a small environment or single resource as a proving ground. Advance the respective strategic priorities across the enterprise



Enable secure connectivity paths that do not rely on implicit trust. Increase assurance with centralized policy and continuous risk monitoring



Continually evaluate mission alignment and threat agility to adjust cyber strategy



Connect with your Microsoft representative about scheduling an envisioning workshop

Thursday 11am: Brian La Macchia

Cryptography - Quantum Computing

Thank you – Open Q&A

Have more questions, lets connect!

Maria Groh

Account Exec

maria.groh@microsoft.com

Chris Schraf

Sr Specialist

chris.schraf@microsoft.com

Dan Craytor

CTO

danc@microsoft.com