Microsoft

De-FUD'ing Zero Trust : Hype vs Reality

Abbas Kudrati

APAC Lead Chief Cybersecurity Advisor
Microsoft APAC
@askudrati
https://aka.ms/abbas

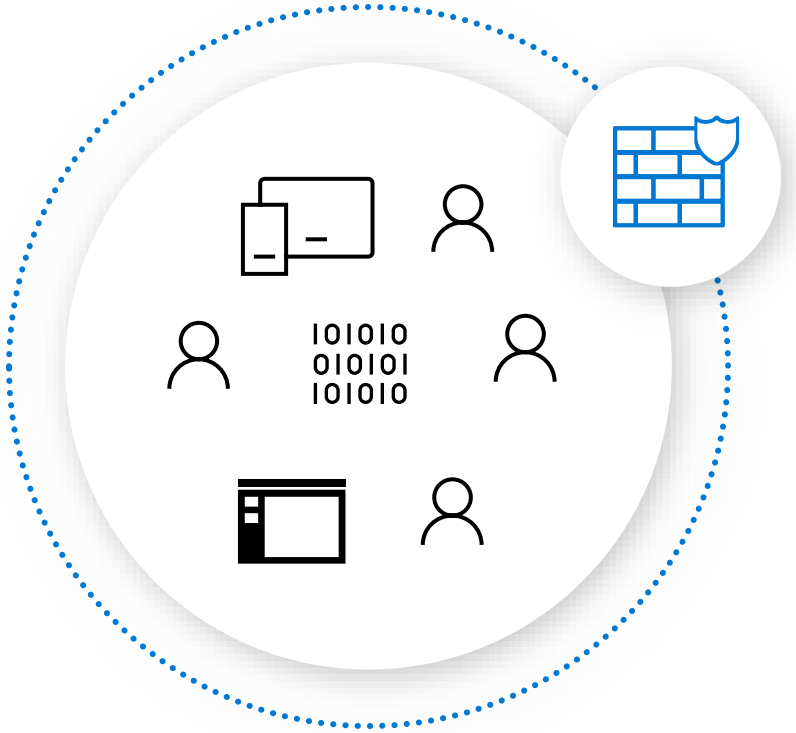
About me

"You join Microsoft, not to be cool
but to make others cool"
Satya Nadella

- **Cybersecurity practitioner and CISO with 23 years of experience in Information / Cybersecurity.**
- **Part time Cybersecurity Professor with Deakin and LaTrobe University in Melbourne, Australia.**
- **Expertise in Zero Trust, Cybersecurity Strategy, Security Operations, Risk, Compliance, Cloud Security and Architecture**

1990s:
Employees work exclusively in a corporate office

Traditional Model



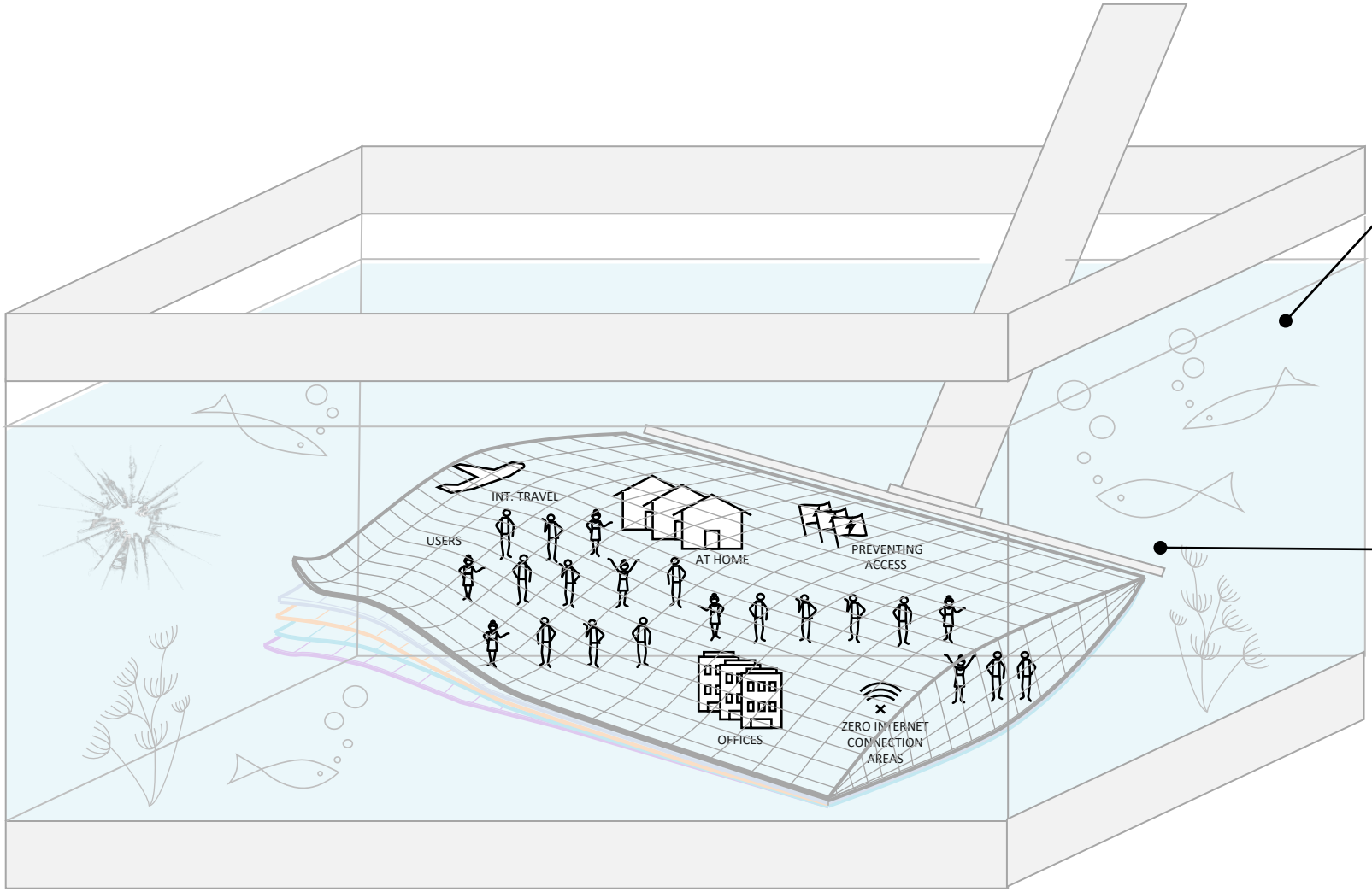
Users, devices, apps, and data protected behind a network firewall

By 1995:

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

The situation many Enterprises face today

One net that covers security needs, inside the fish tank...



Big walls around the Corporate Network

Security net on top of everything

- **Inhibiting user mobility**
- **Preventing Collaboration**
- **Reducing Productivity**
- **Breaches could be a disaster**

Realities of Perimeter-Based Networks

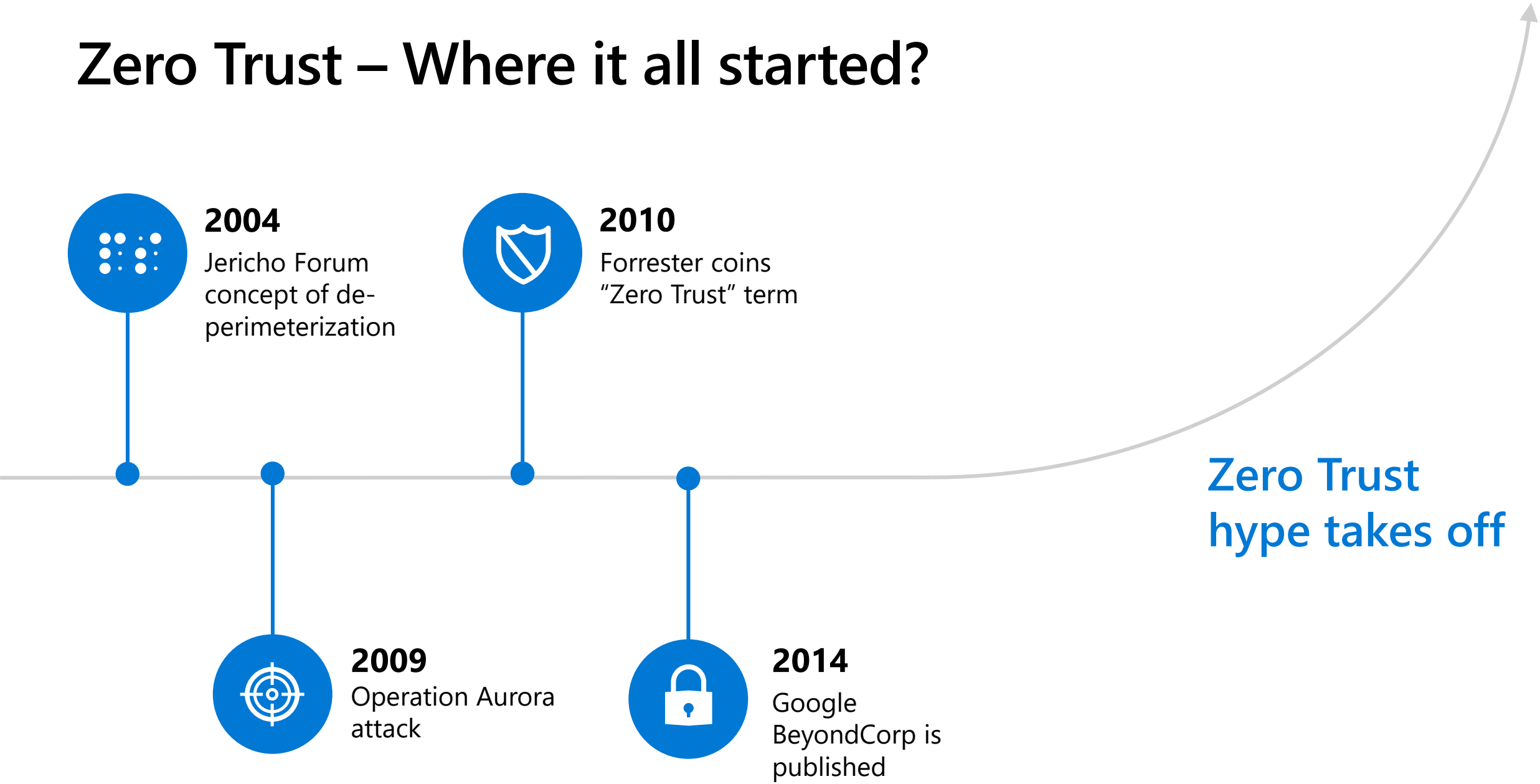
Perimeter-based networks only trust users ***inside*** a network

Single **point of attack** can threaten the entire network

Security teams and end user IT teams often use ***separate and disjointed*** tools and strategy

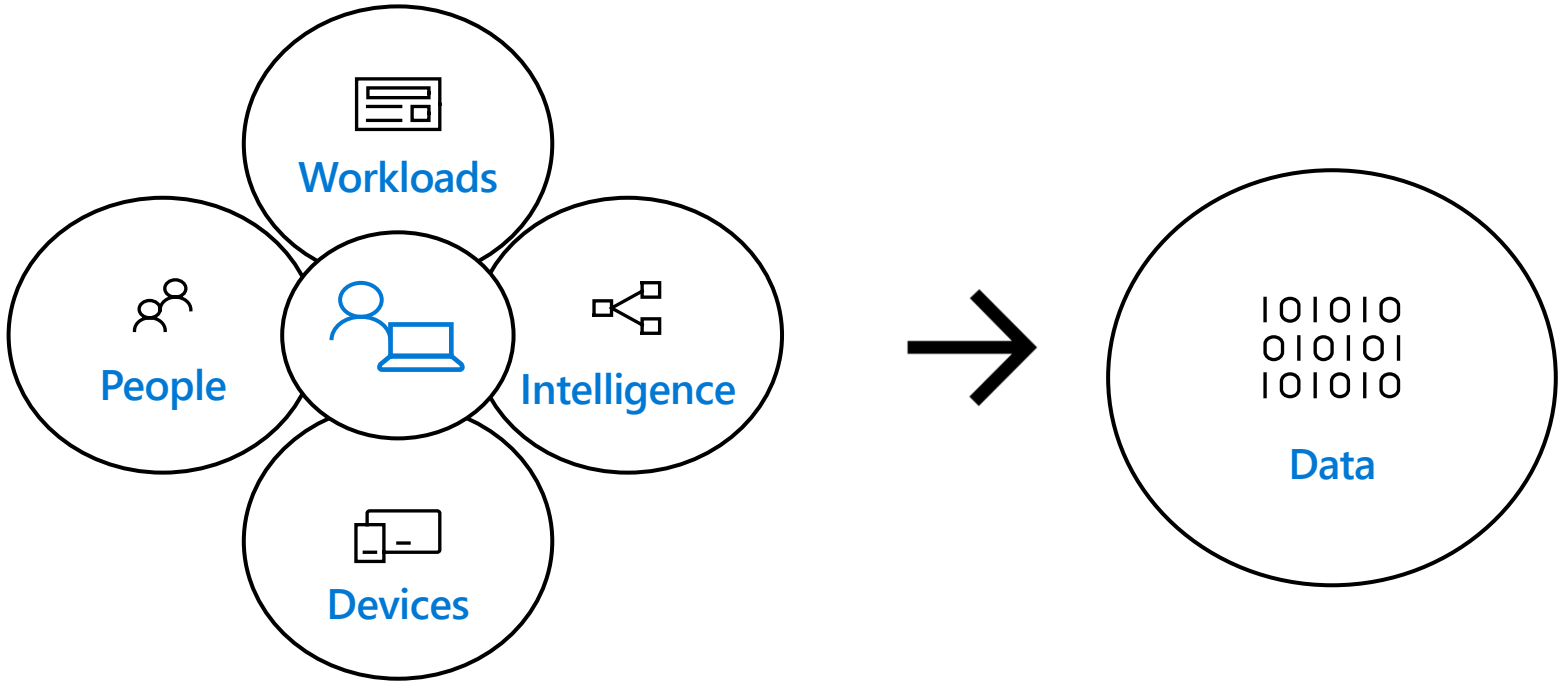
A modern approach is needed

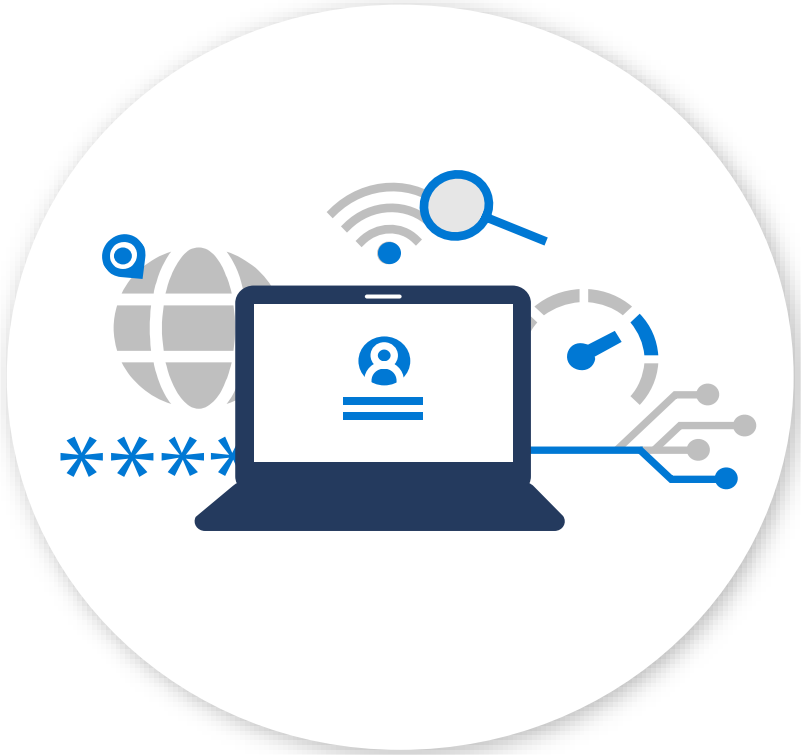
Zero Trust – Where it all started?



What is a Zero Trust Model?

- An approach to security which treats every access attempt as if it's originating from an untrusted network.
- Eliminates the concept of trust based on network location within a perimeter.
- Leverages device and user trust claims to gate access to data and resources.





Benefits of a Zero Trust model

Use conditional access to ensure high-value resources are accessible only from compliant devices.

Prevent network access and lateral movement using stolen credentials or a compromised device.

Enables users to be more productive by working how they want, where they want, and when they want.

Zero Trust is a mindset

- One of the biggest benefits of Zero Trust is a change in mindset
- An approach to security which treats every access attempt as if it's originating from an untrusted network =
- An approach to security which assumes pervasive risk
- How do we behave in an environment of pervasive risk?

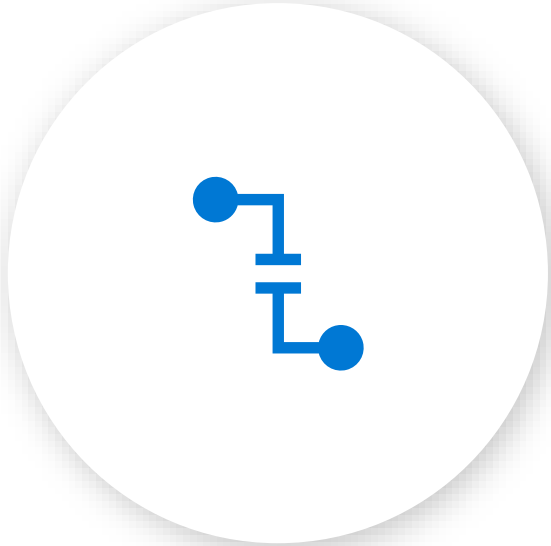
The Zero Trust Mindset

- Don’t accept complacency
- Assume all resources are on the open internet
- Trust no single source
- Breach containment
- Standards are security
- There aren’t enough humans

Principles of Zero Trust

~~Trust but~~
Verify explicitly

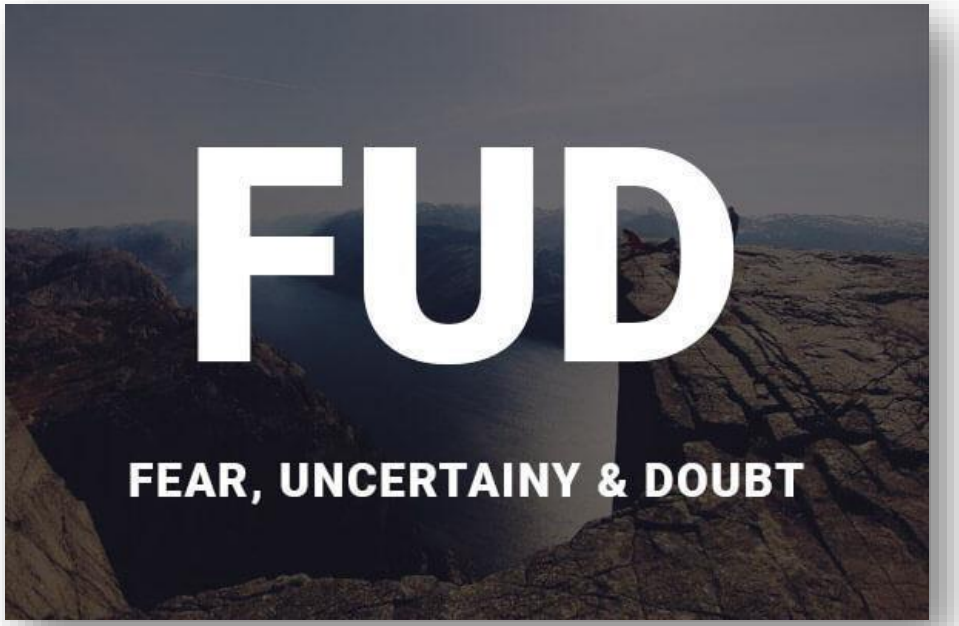
Use least privilege access



Assume breach

De-FUD'ing Zero Trust

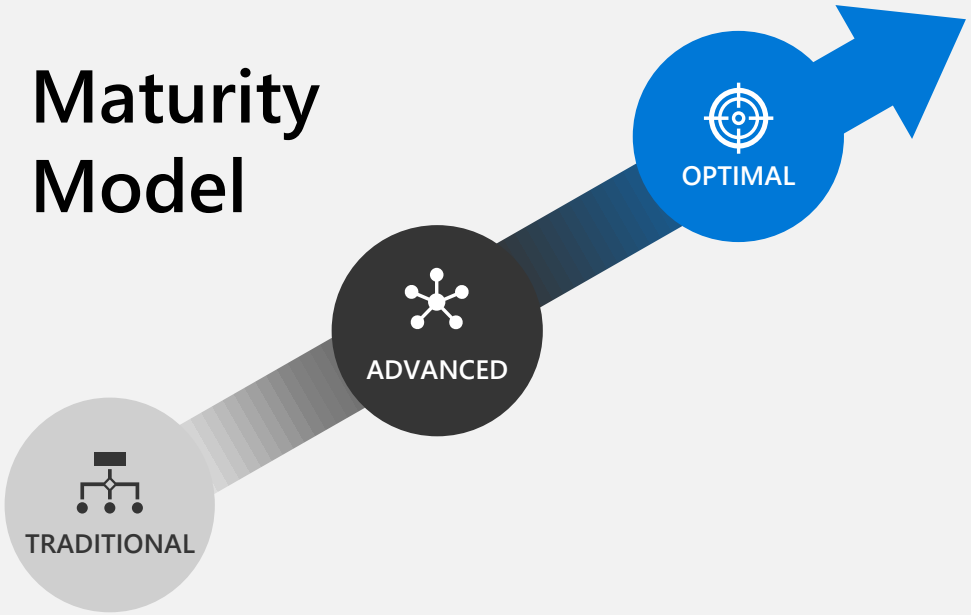
- Literal
- An Adjective
- For Sale
- Instant
- A Destination
- One Size Fits All
- A Revolution



How do I start ?

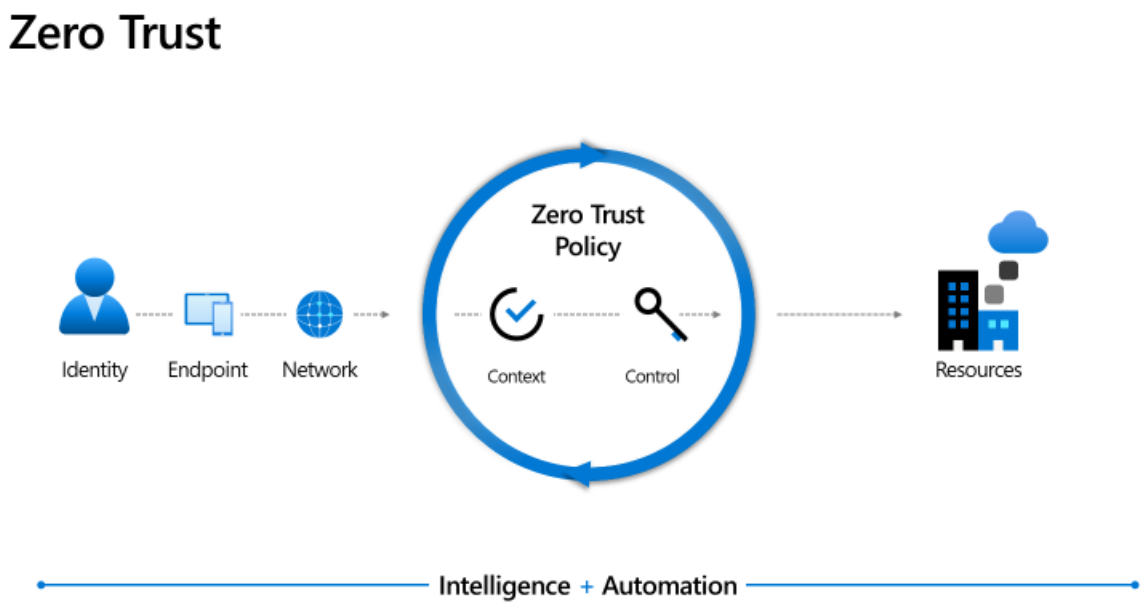
Making Zero Trust a reality

- Do you grok Zero Trust?
- Have you established a v-team with your stakeholders?
- Do you know where you want to arrive?
- Do you know where you are at today?
- Do you have buy-in from C-level to bridge that gap?



Download today at
aka.ms/ztmodel

Zero Trust networking maturity model



Traditional	Advanced	Optimal
Few network security perimeters and flat open network	cloud micro-perimeters with some micro-segmentation	ingress/egress cloud micro-perimeters and deeper micro-segmentation
Minimal threat protection and static traffic filtering	Cloud native filtering and protection for known threats	ML-based threat protection and filtering with context-based signals
Internal traffic is not encrypted	User to app internal traffic is encrypted	All traffic is encrypted
Many ingress/egress	Fully distributed	

Microsoft has rich set of cloud native services designed to help you move to zero trust model

Learn more about zero trust networking at https://www.microsoft.com/security/blog/2020/06/15/zero-trust-part-1-networking/
https://www.microsoft.com/en-us/security/zero-trust

Critical elements

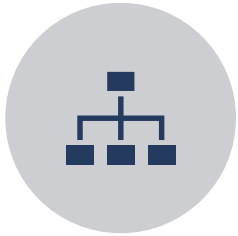
VERIFY IDENTITY.

VERIFY DEVICES.

PROTECT DATA.

HARDEN APPLICATIONS

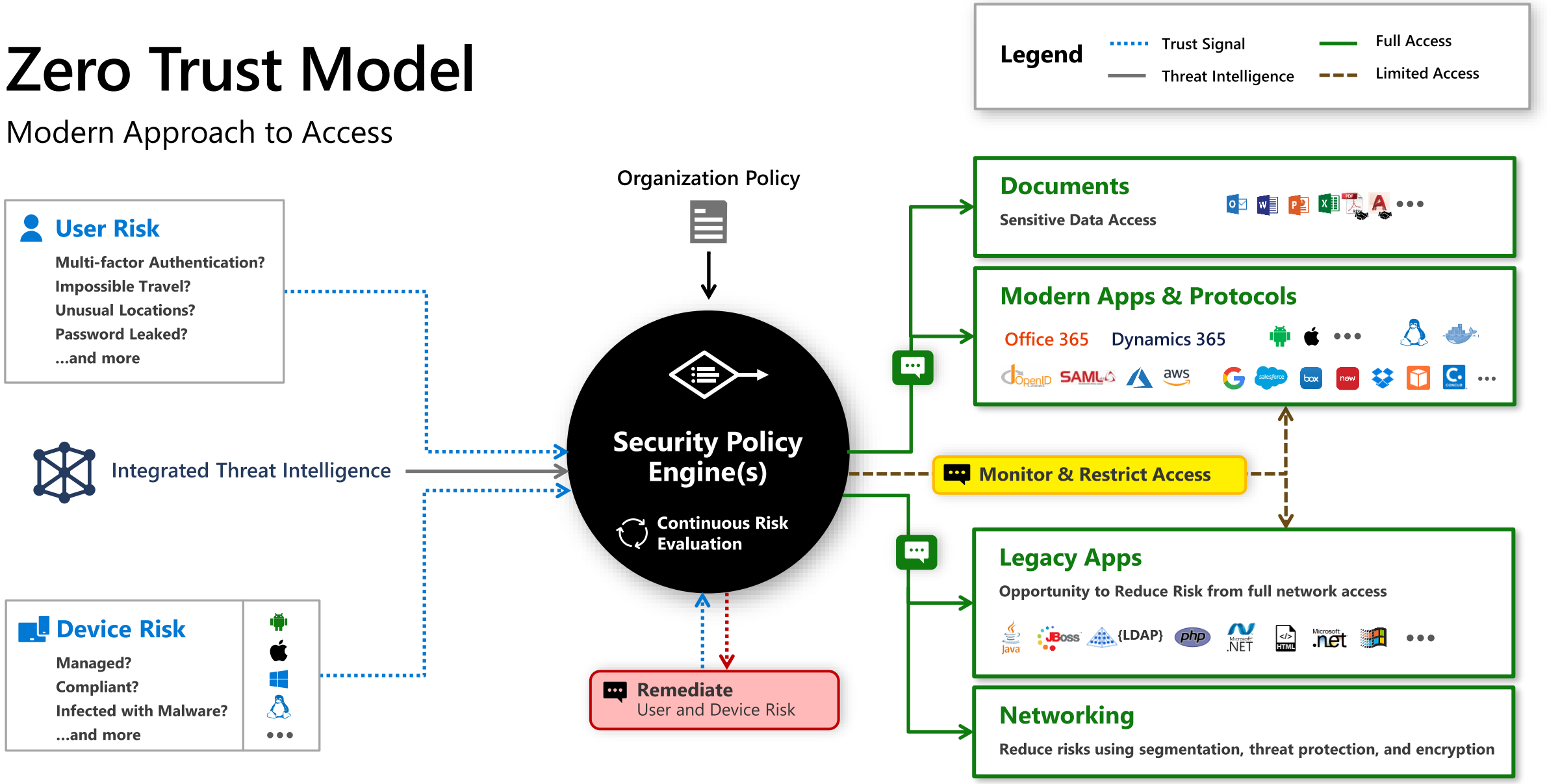
PROTECT INFRASTRUCTURE



GOVERN NETWORKS.

Zero Trust Model

Modern Approach to Access

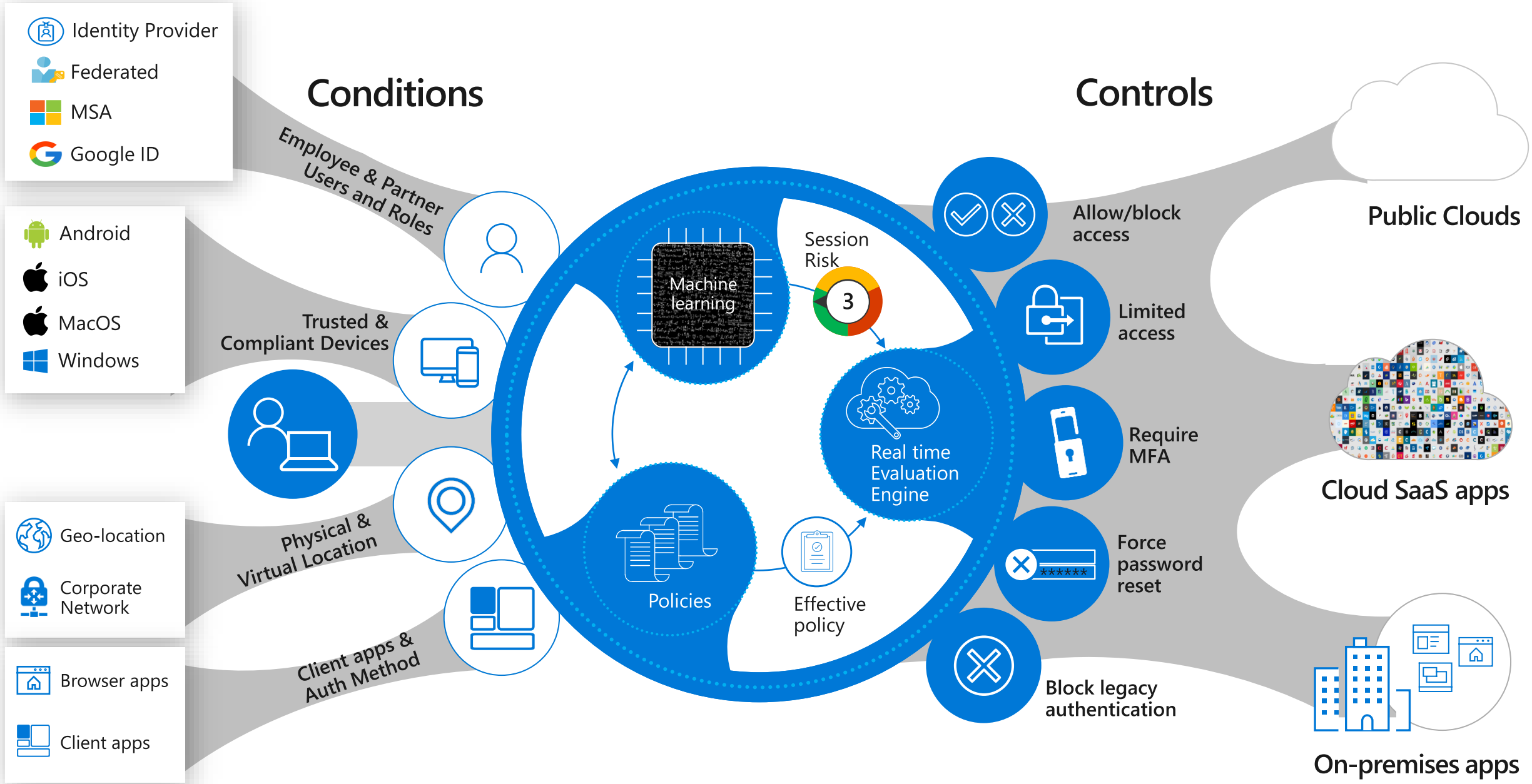


Signal
to make an informed decision

Decision
based on organizational policy

Enforcement
of policy across resources

Zero Trust based on conditional access controls



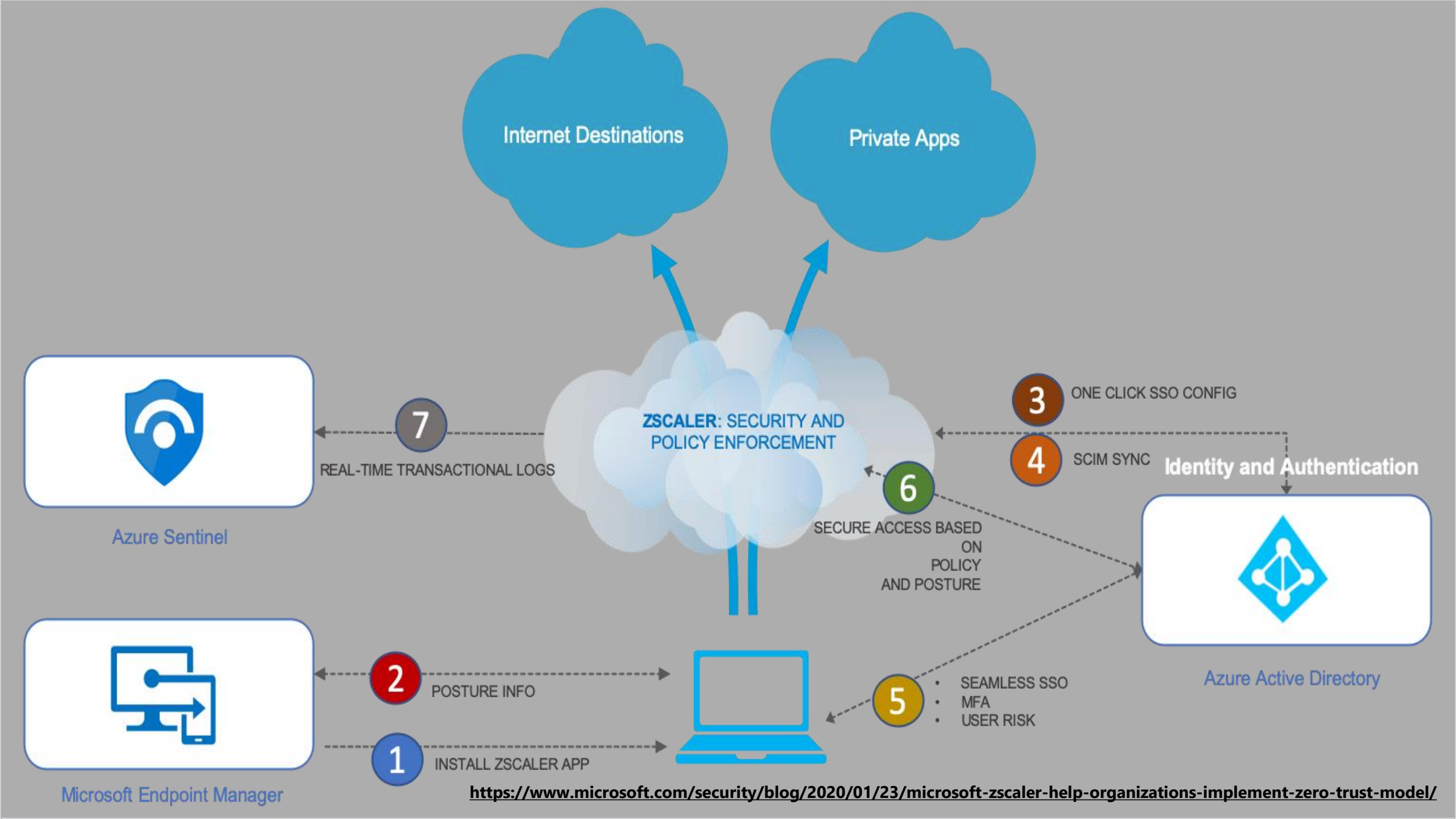
Facilitates direct-to-internet, optimizing applications like Office 365

Zscaler is the only Microsoft qualified security vendor for Office 365

Microsoft Recommendation	1 Egress network connections locally	2 Avoid network hairpins for mobile users	3 Differentiate Office 365 Traffic	4 No SSL Inspection
zscaler Solution	Enable local breakouts Peering key datacenters	Direct access to Office 365 – no VPN backhaul - Local DNS	Seamless Mgmt & traffic prioritization over YouTube / internet traffic	Whitelist Office 365 Traffic

"I'm thrilled to see some of the largest enterprises including Sandvik, Siemens, and GE use **Zscaler and Microsoft to deliver fast and direct access to Office 365**, as well as applications running on Azure.

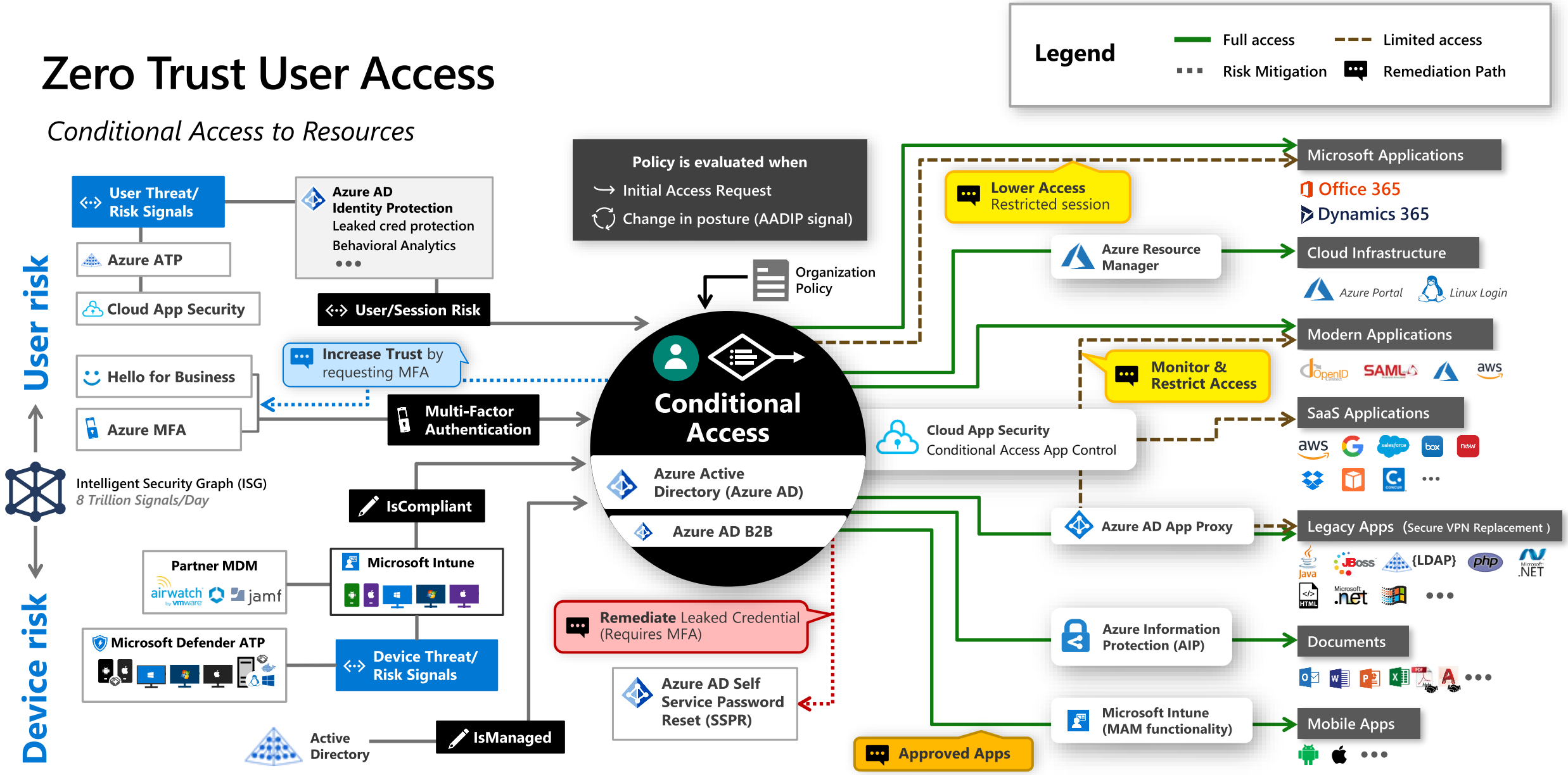
https://www.microsoft.com/en-us/videoplayer/embed/RE3YvKj?autoplay=true



https://www.microsoft.com/security/blog/2020/01/23/microsoft-zscaler-help-organizations-implement-zero-trust-model/

Zero Trust User Access

Conditional Access to Resources



Signal
to make an informed decision

Decision
based on organizational policy

Enforcement
of policy across resources

microsoft.com/en-us/security/business/zero-trust

Apps | Somax Sports - Rev... | Facebook | Video: Flexibility Fo... | Starting With Manu... | Advanced Security... | HP Probook 4520s... | Animated PowerPoi... | DMOZ - Computers... | Mind Maps ... | Privacy Victoria - O...

Microsoft | Security Solutions Products Operations & Intelligence Partners Resources Trust Center All Microsoft

aka.ms/Zero-Trust

Enable a remote workforce by embracing Zero Trust security

Support your employees working remotely by providing more secure access to corporate resources through continuous assessment and intent-based policies.

Watch now

Read maturity model paper

Zero Trust assessment tool

Assess your Zero Trust maturity stage to determine where your organization is and how to move to the next stage.

Take the assessment >

Zero Trust maturity model assessment

Assess your Zero Trust maturity stage (Traditional, Advanced or Optimal) to determine where your organization currently stands. This assessment will give you recommendations on how to progress to the next stage.

Identities

Verify and secure every identity with strong authentication across your entire digital estate.

Get started >

Devices

Gain visibility into devices accessing the network and ensure compliance and health status before granting access.

Get started >

Applications

Discover Shadow IT and control access with real-time analytics and monitoring.

Get started >

Infrastructure

Employ real-time threat detection, automatically block and flag risks, and employ least privilege access principles.

Get started >

Data

Classify, label, and protect data with end-to-end encryption.

Get started >

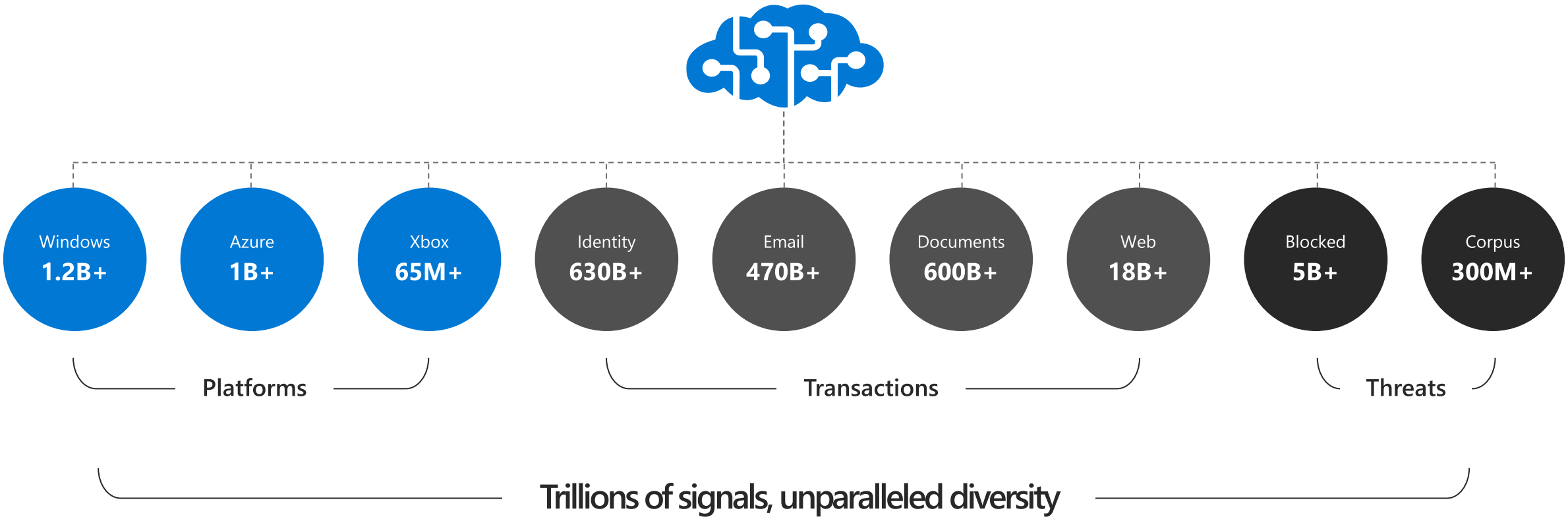
Network

Encrypt all internal communications, limit access by policy, and employ microsegmentation and real-time threat detection.

Get started >

Learning Resources

Microsoft's unique vantage point on security



Microsoft Security—a leader in 5 Gartner magic quadrants

Access Management

Cloud Access Security Brokers

Enterprise Information Archiving

Endpoint Protection Platforms

Unified Endpoint Management Tools

*Gartner "Magic Quadrant for Access Management," by Michael Kelley, Abhyuday Data, Henrique, Teixeira, August 2019
*Gartner "Magic Quadrant for Cloud Access Security Brokers," by Steve Riley, Craig Lawson, October 2019
*Gartner "Magic Quadrant for Enterprise Information Archiving," by Julian Tirsu, Michael Hoech, November 2019
*Gartner "Magic Quadrant for Endpoint Protection Platforms," by Peter Firstbrook, Dionisio Zumerle, Prateek Bhajanka, Lawrence Pingree, Paul Webber, August 2019
*Gartner "Magic Quadrant for Unified Endpoint Management Tools," by Chris Silva, Manjunath Bhat, Rich Doheny, Rob Smith, August 2019

Learning Resources

Chief Information Security Officer (CISO) Workshop Training LINK

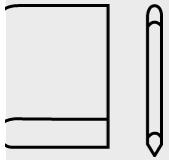
Microsoft security architecture training

PPT YouTube

Microsoft Exams Learning Resources

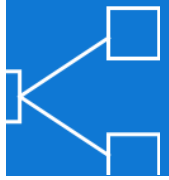
(LINK)

Microsoft Cloud Training Events LINK



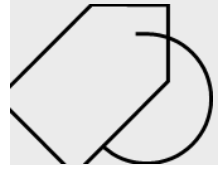
My Collections of scripts and ppts

aka.ms/abbas



Zero Trust Model

LINK



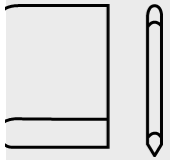
Best support for your enterprise need

Kubernetes 101 Docs
aka.ms/LearnAKS

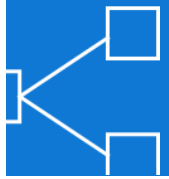
Best practices
aka.ms/aks/bestpractices

Hear from experts
aka.ms/k8s/lightboard

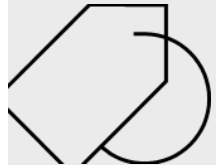
Case studies
aka.ms/aks/casestudy



Microservices architecture
aka.ms/aks/microservices



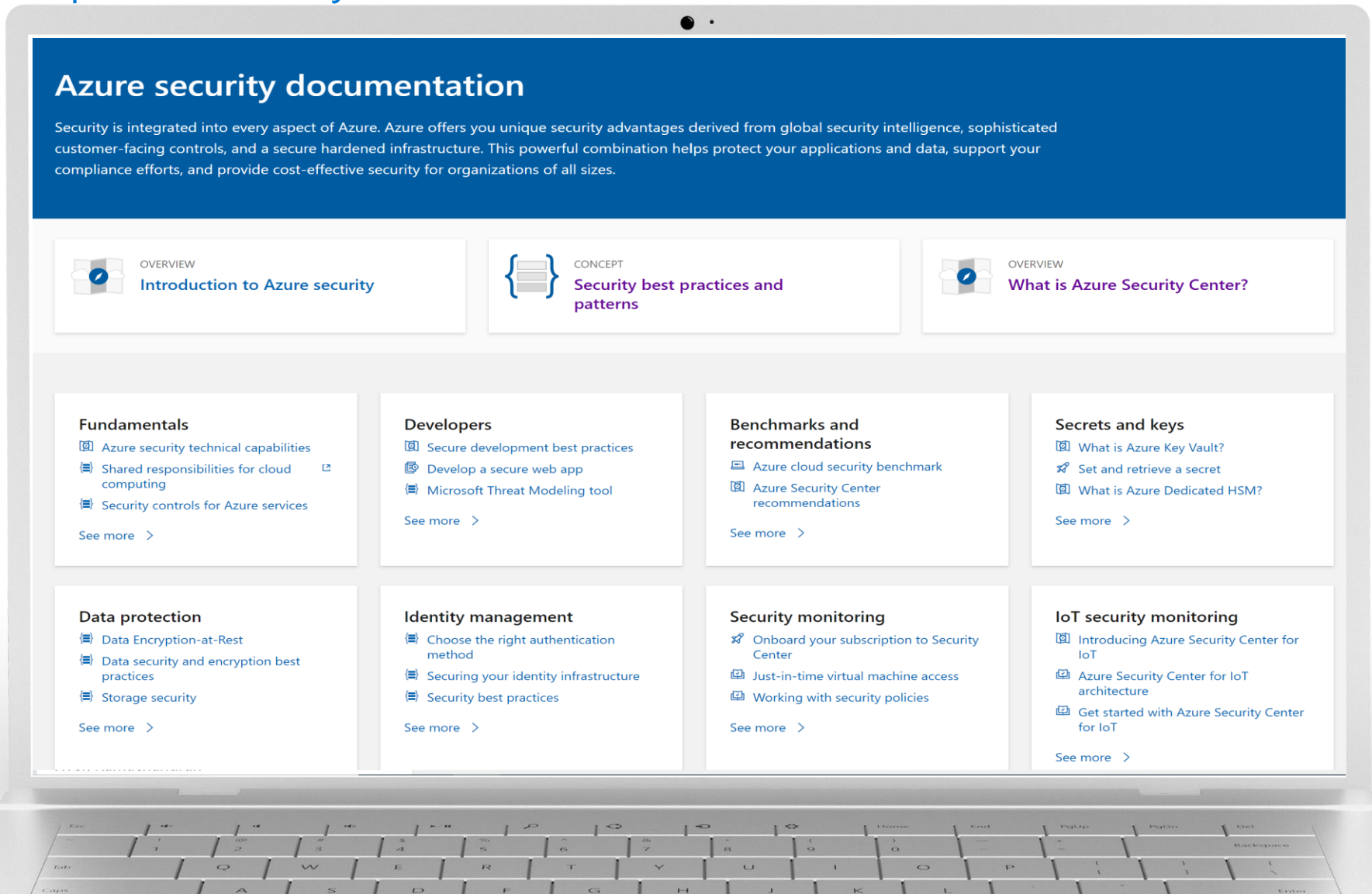
Try for free
aka.ms/aks/trial



Feedback on the roadmap? Tell us at https://aka.ms/aks/feedback

Azure Security Documentation

https://aka.ms/MyASIS



Azure Security Documentation Site has extensive information on security topics

Microsoft

Microsoft Certifications

Microsoft Certifications are the industry's premier credentials for professional technologies.

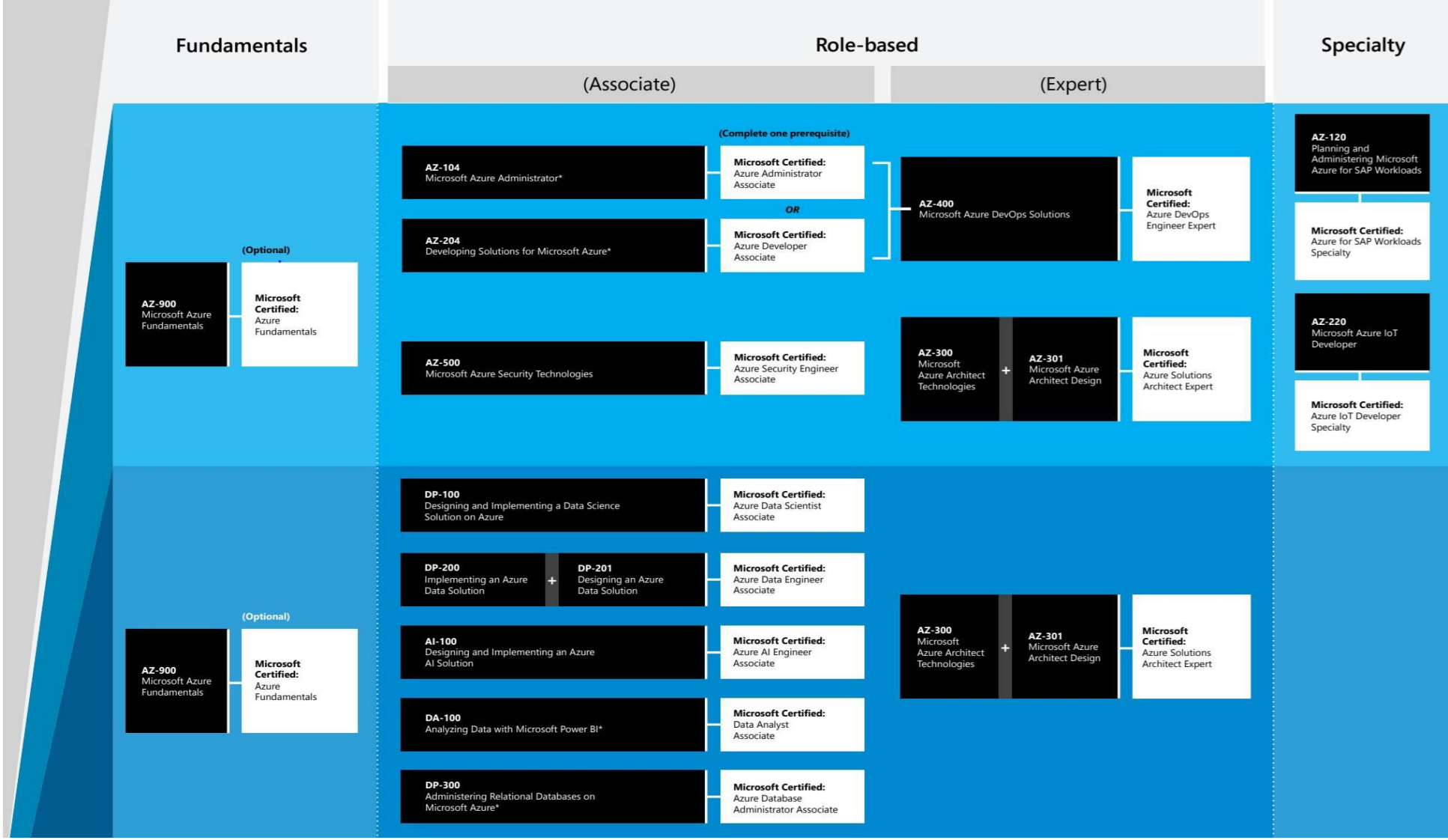
Certification types:

Fundamentals validates foundational understanding of Microsoft technologies and is optional for getting started.

Role-based validates technical skills required to perform industry job-roles on Microsoft platforms and technologies.

Specialty validates deep technical skills and ability managing industry solutions, including third-party solutions, on or with Microsoft platforms.

Learn more at Microsoft.com/Certifications



[Tips and Tricks for getting your Microsoft Certification]

[How to pick the right Azure Exam Certification Path]

[EXAM PREP: AZ-500 | Microsoft Azure Security Technologies]

Q&A

Abbas Kudrati
https://aka.ms/abbas
@askudrati