RSAConference2019

San Francisco | March 4–8 | Moscone Center

SESSION ID: IDY-W10

No More Firewalls! How Zero Trust Networks are Reshaping Cyber Security

Matt Soseman

Security Architect
Microsoft
@SosemanMatt
http://aka.ms/MattsBlog

Session Objectives

- Understand what Zero Trust is and why it is important.
- Understand how identity, device health and trustworthiness contribute to overall security posture.
- Learn considerations for automated access to resources via device and identity conditions.
- Discover how to apply these conditions to line of business SaaS apps or on-premises web apps.

RSAConference2019

The challenge with perimeter-based networks…

It was a walled garden (castle/moat approach)

- Perimeter-based networks operate on the assumption that all systems (and users) within a network can be trusted.
- Not able to accommodate modern work styles such as Bring Your Own Device (BYOD) and Bring Your Own Cloud (BYOC)
- Attacker can compromise single endpoint within trusted boundary and quickly expand foothold across entire network.

Users cannot be trusted! (Neither can the network!)

4%

Of end-users will click on anything[1]

28%

of attacks involved inside actors[1]

17%

Of breaches had errors as casual events[1]

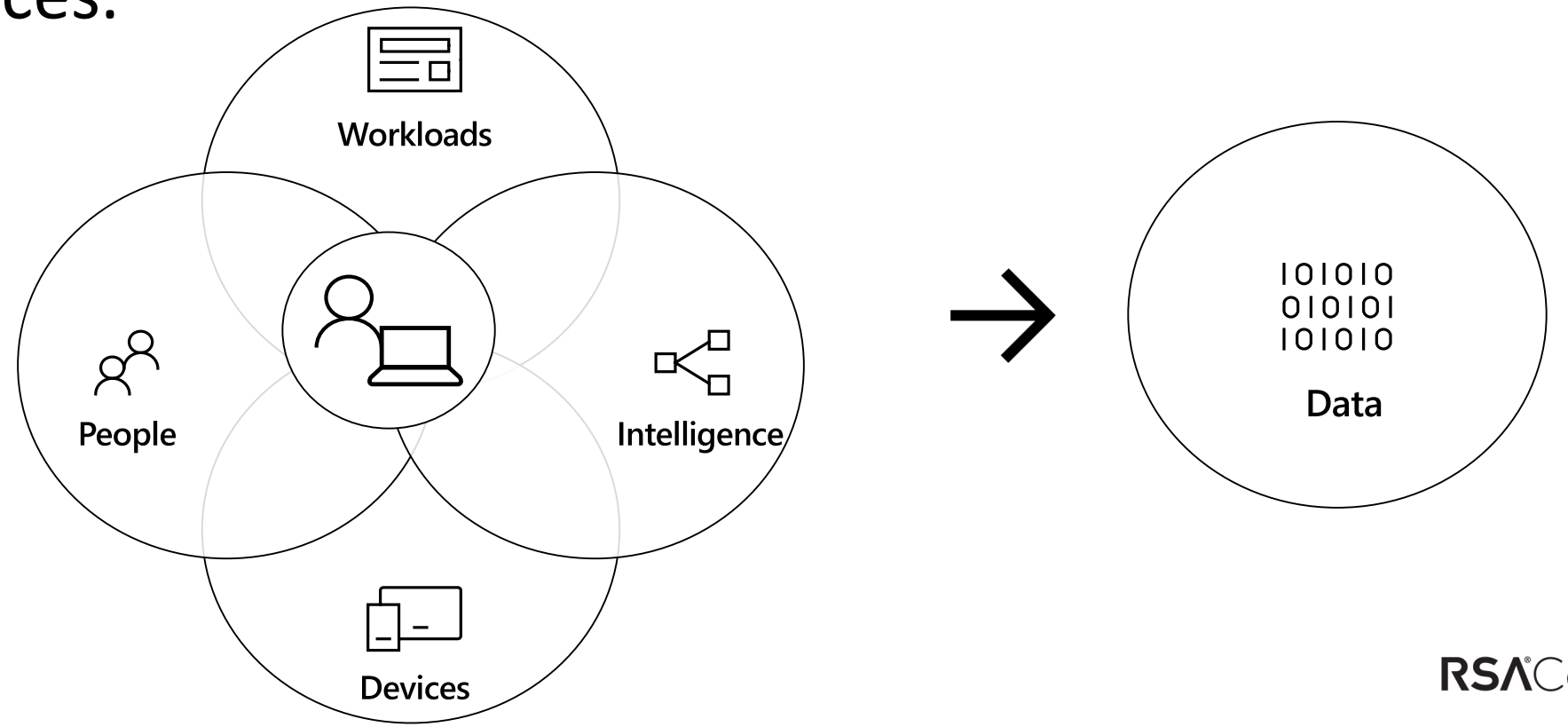
1. Verizon DBIR Report 2018 https://enterprise.verizon.com/resources/reports/dbir/

RSAConference2019

Zero Trust to the rescue!

What is a Zero Trust network?

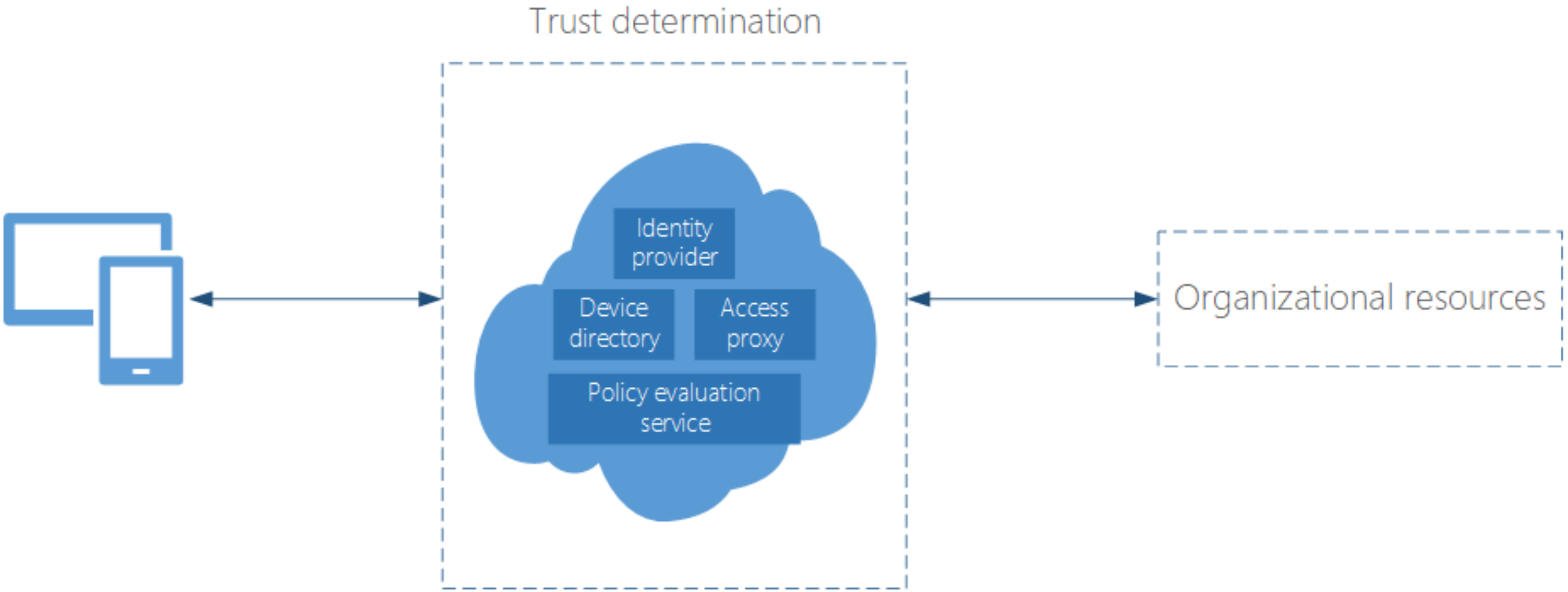
- Eliminates the concept of trust based on network location within a perimeter.
- Leverages device and user trust claims to gate access to data and resources.



What comprises a Zero Trust network?

- Identity provider to keep track of users and user-related information.
- Device directory to maintain a list of devices that have access to corporate resources, along with their corresponding device information (e.g., type of device, integrity etc.)
- Policy evaluation service to determine if a user or device conforms to the policy set forth by security admins
- Access proxy that utilizes the above signals to grant or deny access to an organizational resource
- Anomaly detection and machine learning

Example: Basic components of a Zero Trust network model



Benefits of a Zero Trust model

- Allow conditional access to certain resources while restricting access to high-value resources on managed/compliant devices.
- Prevent network access and lateral movement using stolen credentials and compromised device.
- Enables users to be more productive by working however they want, where they want, when they want.

RSAConference2019

Designing a Zero Trust architecture

Approach: Start with asking questions

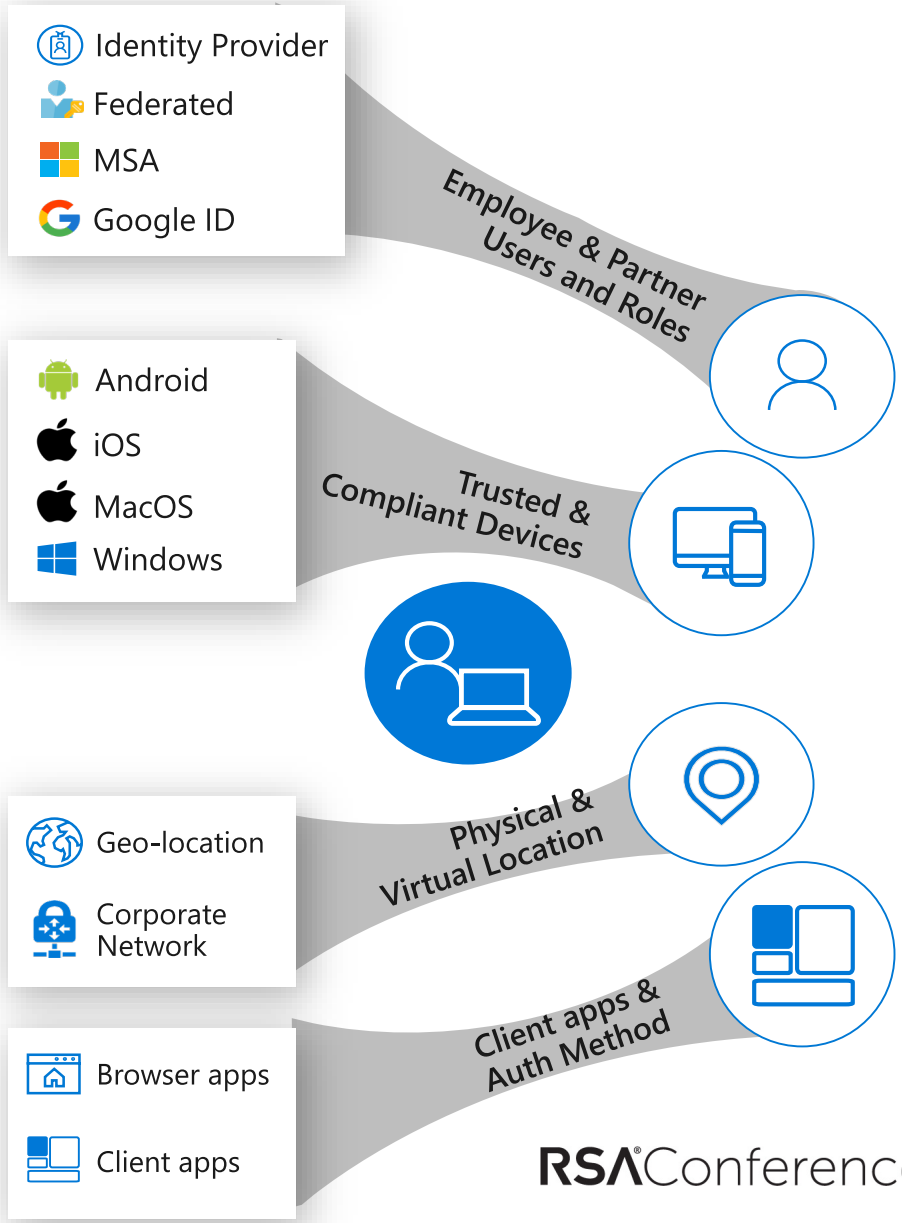
Who are your users? What apps are they trying to access? How are they doing it? Why are they doing it that way?

What conditions are required to access a corporate resource?

What controls are required based on the condition?

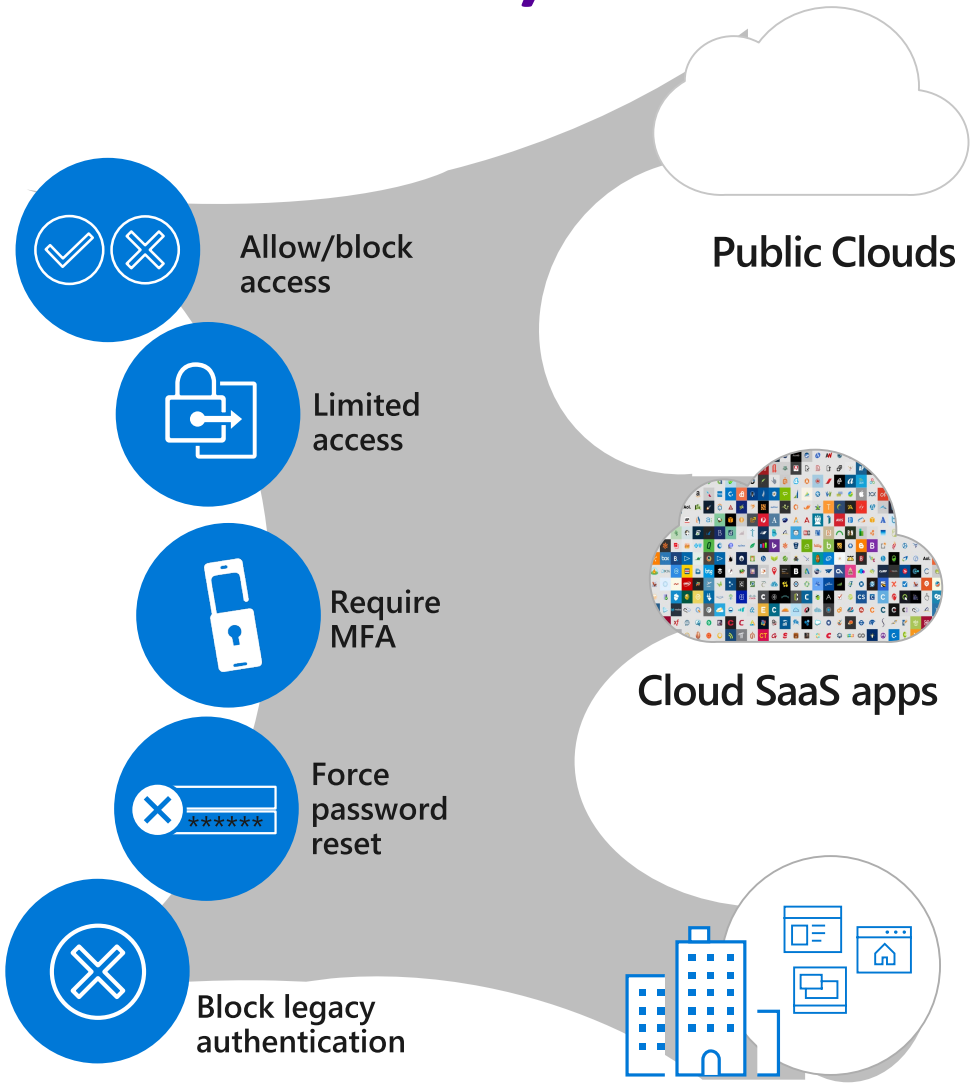
Consider an approach based on set of conditions

- What is the user's role and group membership?
- What is the device health and compliance state?
- What is the SaaS, on-prem or mobile app being accessed?
- What is the user's physical location?
- What is the time of sign-in?
- What is the sign-in risk of the user's identity? (i.e. probability it isn't authorized by the identity owner)
- What is the user risk? (i.e. probability a bad actor has compromised the account?

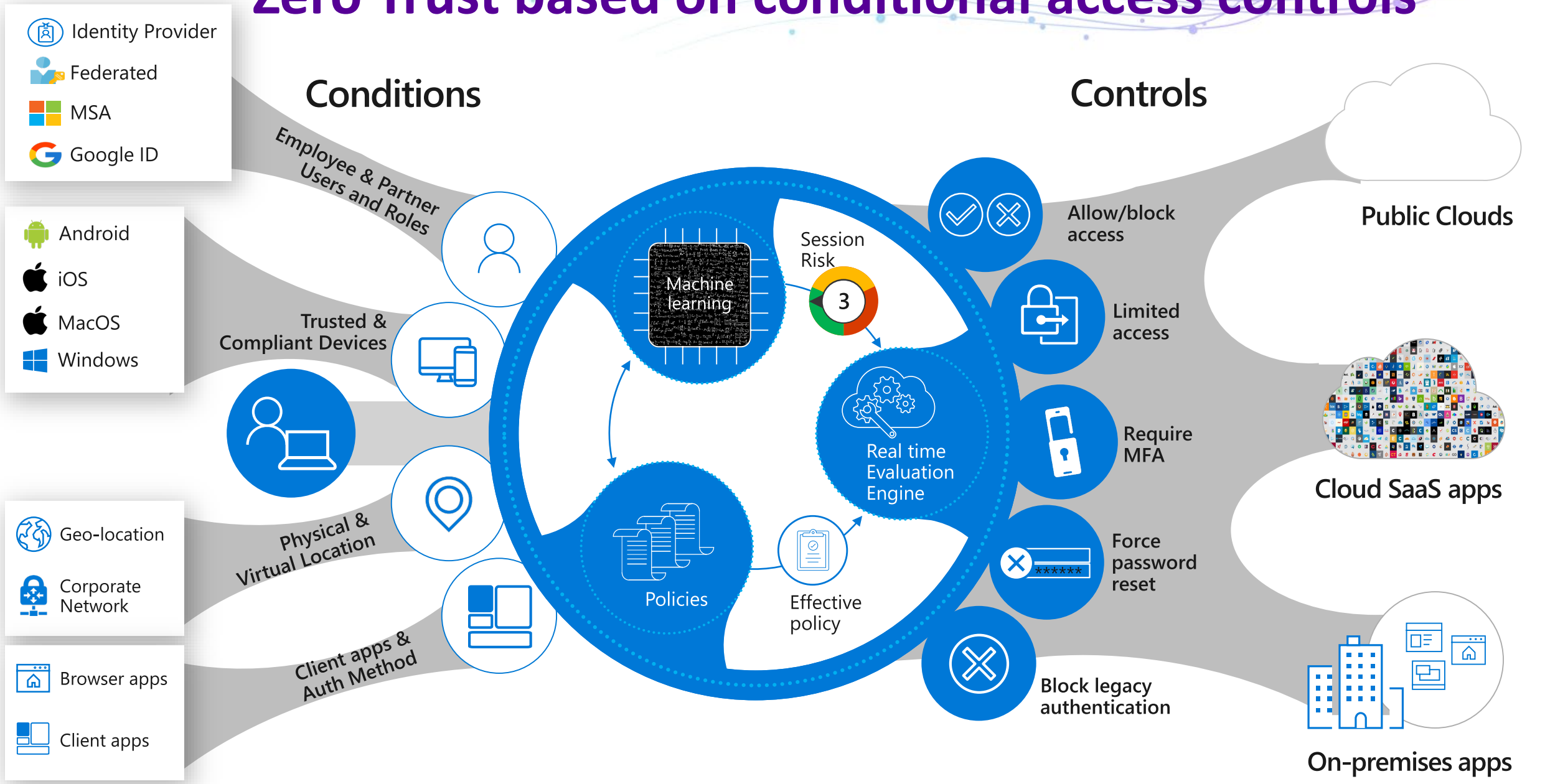


Followed by a set of controls (if/then statement)

- Allow/deny access
- Require MFA
- Force password reset
- Control session access to the app (i.e. allow read but not download, etc)

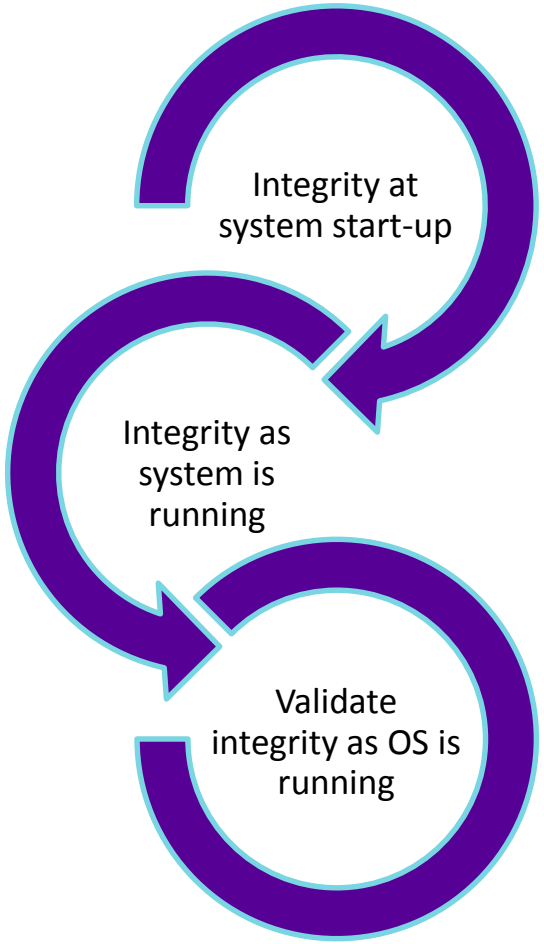


Zero Trust based on conditional access controls

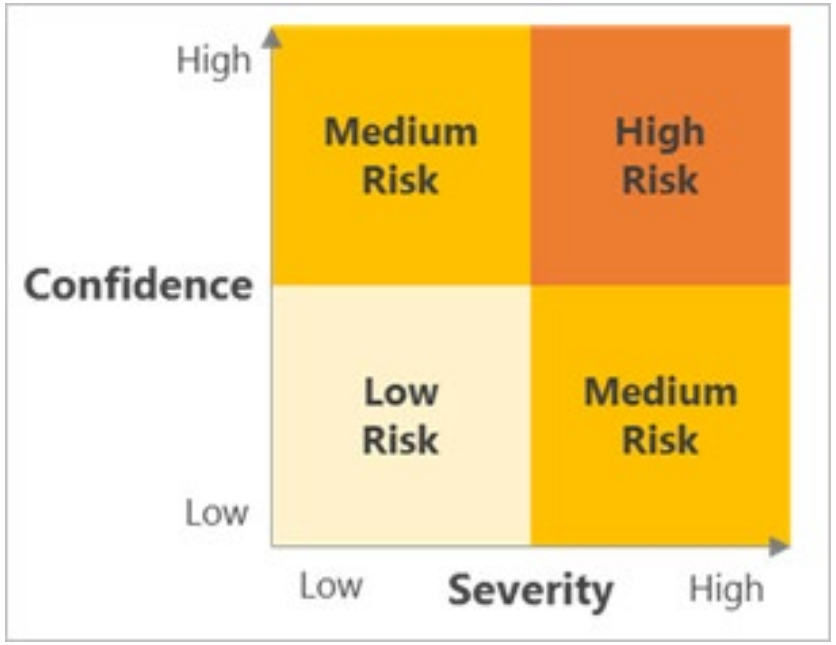


Device Health Conditions

- Determine the machine risk level (i.e. is it compromised by malware, Pass-the-Hash (PtH), etc)
- Determine the system integrity and posture (i.e. hardware-rooted boot-time and runtime checks)
- Integrity checks:
  - Drivers
  - Kernel
  - Firmware
  - Peripheral firmware
  - Antimalware driver code
- Verify boot state of machine
- Compliance policy checks (i.e. is an OS security setting missing/not configured?)



Identity Conditions



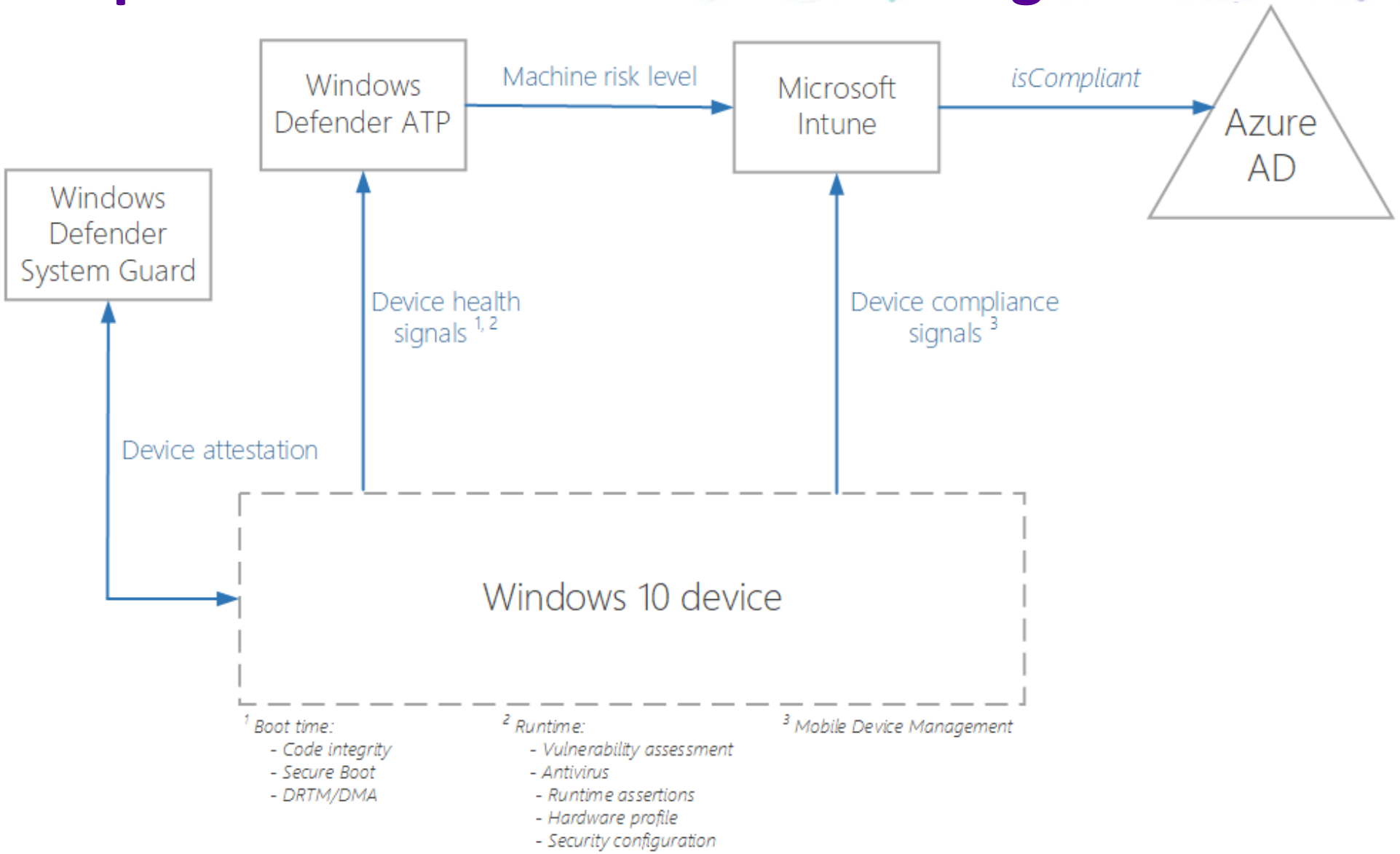
What is the user's risk level?

- Is the sign in coming from:
  - A known botnet IP address?
  - An anonymous IP address?
  - Unauthorized browser? (i.e. Tor)
  - An unfamiliar location?
  - Impossible travel to atypical locations?
- Is the sign in suspicious?
  - High number of failed attempts across multiple accounts over a short period of time
  - Matches traffic patterns of IP addresses used by attackers
- Are the user's credentials (username/password pair) leaked?
  - Up for sale on the dark web / black sites

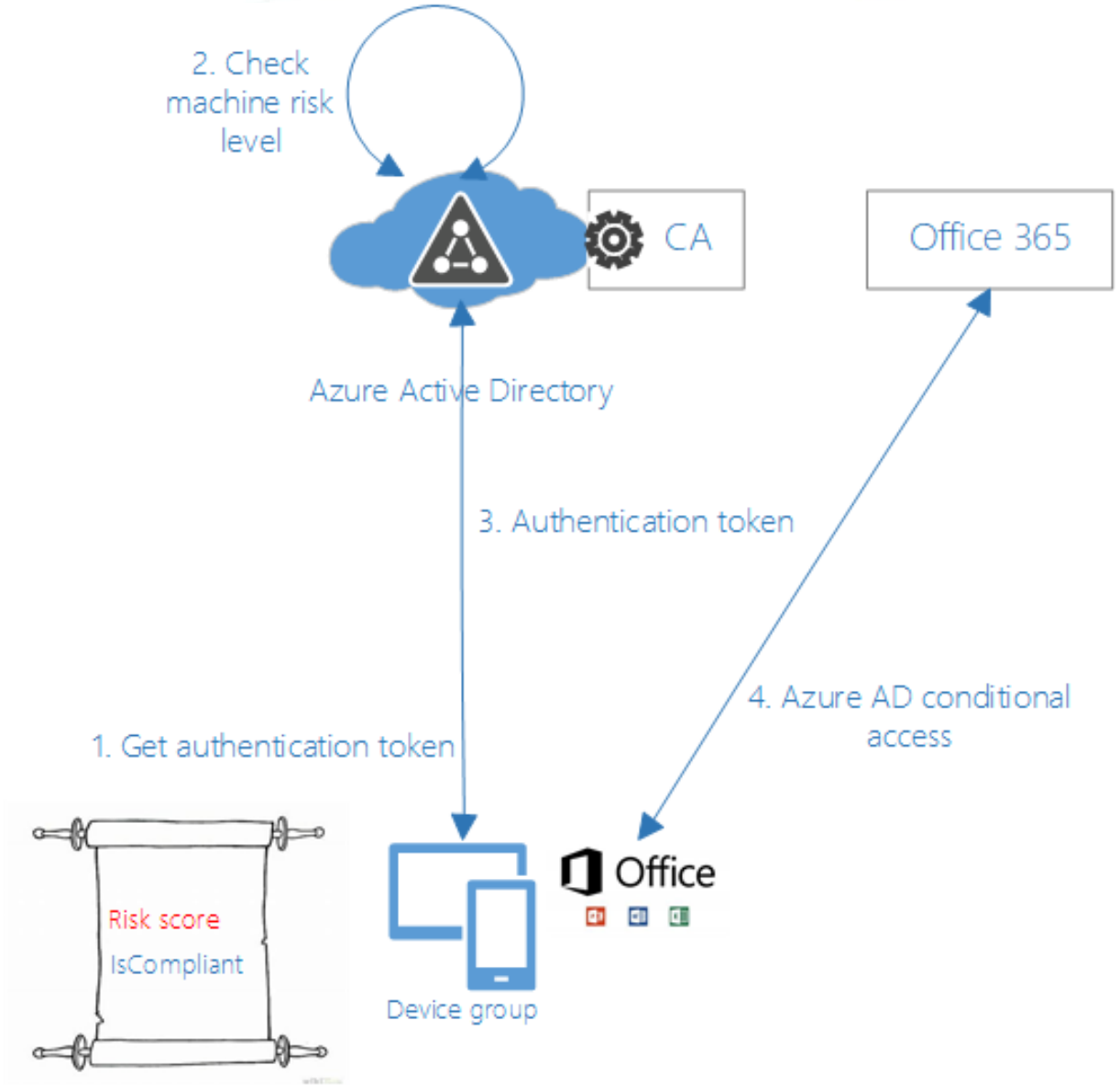
RSAConference2019

Example Zero Trust Architectures

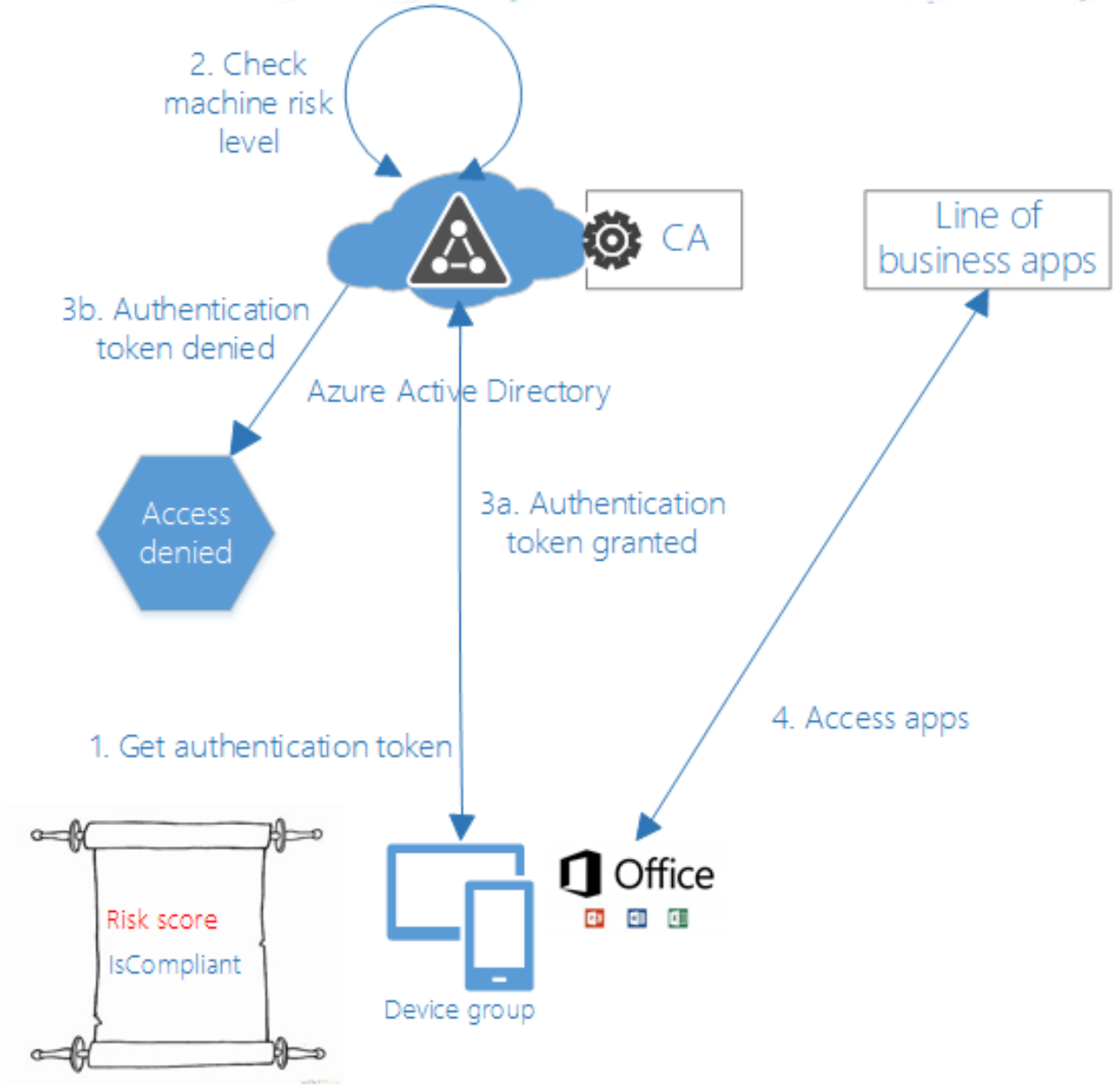
Example Zero Trust architecture using conditional access



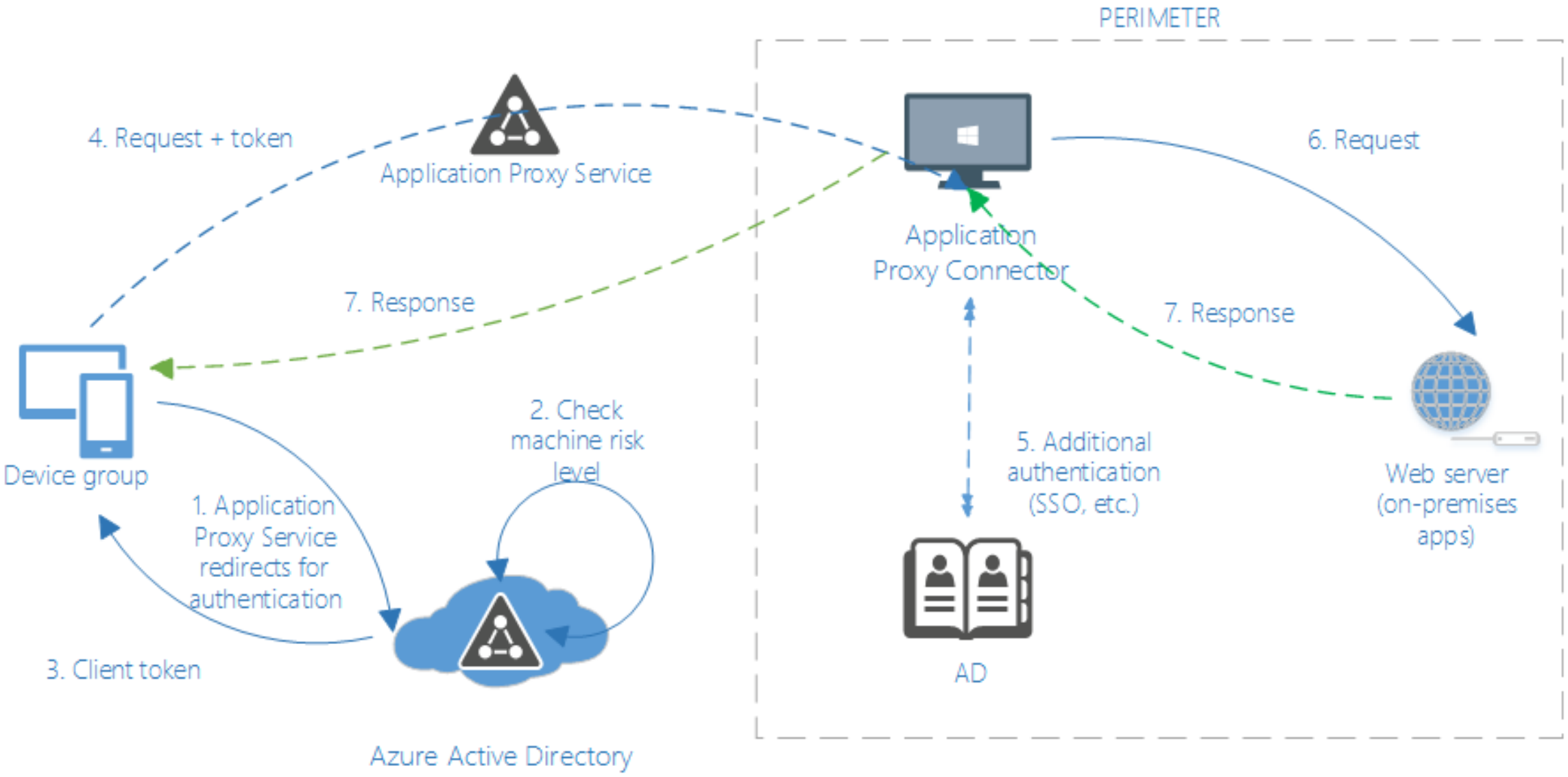
Example Zero Trust data flow using Azure AD to Office 365 or SaaS apps



Example Zero Trust data flow using Azure AD to line of business apps



Example Zero Trust data flow for on-premises web apps



Operations in a Zero Trust model

- Automatic gating to applications is key.
- Automatic remediation based on device health (not rely on user intervention).
- Monitoring for policy violations (signal from the noise).
- Prioritizing alerts correlated with sensitive data access.
- Reporting on state of Identity, Device, SaaS app and data.

Making it real with demos

- Demonstrate how a Zero Trust model behaves in the real world using key scenarios
- Tying the key Zero Trust components together with conditional access policies
- See example reports of policy violations
- Understand the user experience in a Zero Trust model

RSAConference2019

Demo

Challenge with Multi-Factor Authentication, w/ Apple Watch and Terms of Use to an app

RSAConference2019

Demo

Denying a compromised identity access to an app using a Tor Browser and anonymous IP address

RSAConference2019

Demo

Deny access to app using legacy authentication (i.e. POP3,NTLM,etc)

RSAConference2019

Demo

Limiting and auditing session access from a non-managed device (i.e. prevent download from app or apply DLP to downloaded files)

RSAConference2019

Demo

Only allow managed and compliant devices to access applications with option to enroll

RSAConference2019

Demo

Deny access to applications when device is not compliant (i.e. a policy is violated)

RSAConference2019

Demo

Deny access to applications when device is compromised by a threat

RSAConference2019

Demo

Deny access to sensitive data based on identity or device health

RSAConference2019

Demo

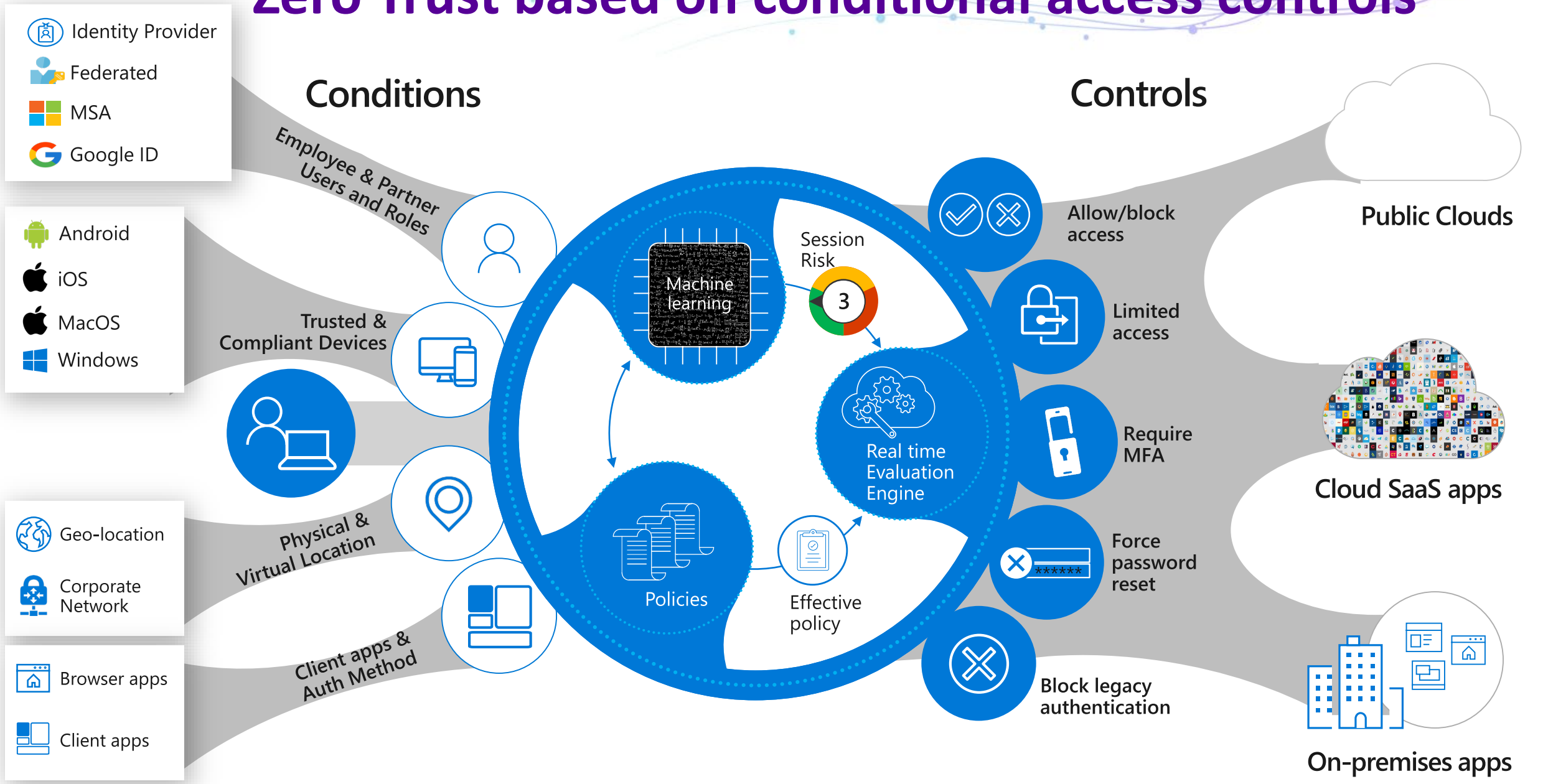
Govern data access on unmanaged device by protecting data in the managed app

RSAConference2019

Demo

Monitoring and operations in a Zero Trust model – Tracking data across identity and devices

Zero Trust based on conditional access controls



Key Takeaways

- Networks that fail to evolve from traditional defenses are vulnerable to breaches. We must assume breach.
- Zero Trust *can* enable new business outcomes that were not possible before.
- Technology has evolved to now make these scenarios possible, and you may already own it.
- Consider an "*if-this-then-that*" automated approach to Zero Trust.
- Identity is everything, make it the control plane.

Apply what you have learned today

Apply what you have learned today – detailed view (take a photo of this slide!)

- Next week you should:
  - Download this deck.
  - Understand what “zero trust controls” your identity solution provides.
  - Discover what products in your environment can integrate with your identity solution to help you create a zero trust story for your organization. (i.e. firewall, VPN, MDM, EDR, DLP, etc)
- In the first three months following this presentation you should:
  - Build a persona profile (set of conditions) required for your end users with an understanding of who they are, where they are going, and what they want.
    - i.e. The state of the identity (verified or compromised), what types of devices they are using, from which locations, and to what applications.
  - Identify what controls are required to respond to those specific conditions
    - i.e. If accessing an app (e.g. SharePoint or G-Suite) from an untrusted device, do I need to challenge with multi-factor authentication? Or require to first enroll the device into MDM/Domain *then* allow access? If the identity is compromised and credentials in public, block access.
- Within six months to one year you should:
  - Identify two “zero trust” controls from above to conduct a production proof of concept. Develop a test plan to effectively test controls. Gather datapoints and effectiveness of policies. Fine tune if needed.
  - Consider a limited production pilot with group of “friendlies” (business users). Study their behavior, gather feedback/datapoints, and understand if/how the policies impact their productivity. Fine tune if needed.
  - Develop an architecture and project plan to roll out those two controls out to the organization with a roadmap of future controls. **Become a rockstar.**