Zero Trust Security

Gowdhaman Jothilingam

Topics Covered

- Understand what Zero Trust is and why it is important.
- What comprises a Zero Trust network and how to create architecture
- Conditions and Controls
- Understand how identity, device health
- Benefits of Zero Trust
- Discover how to apply these conditions to line of business SaaS apps or on-premises web apps.
- Examples and Demo (If time permits)

TRADITIONAL MODEL

Trusted Zone

Untrusted Zone

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]

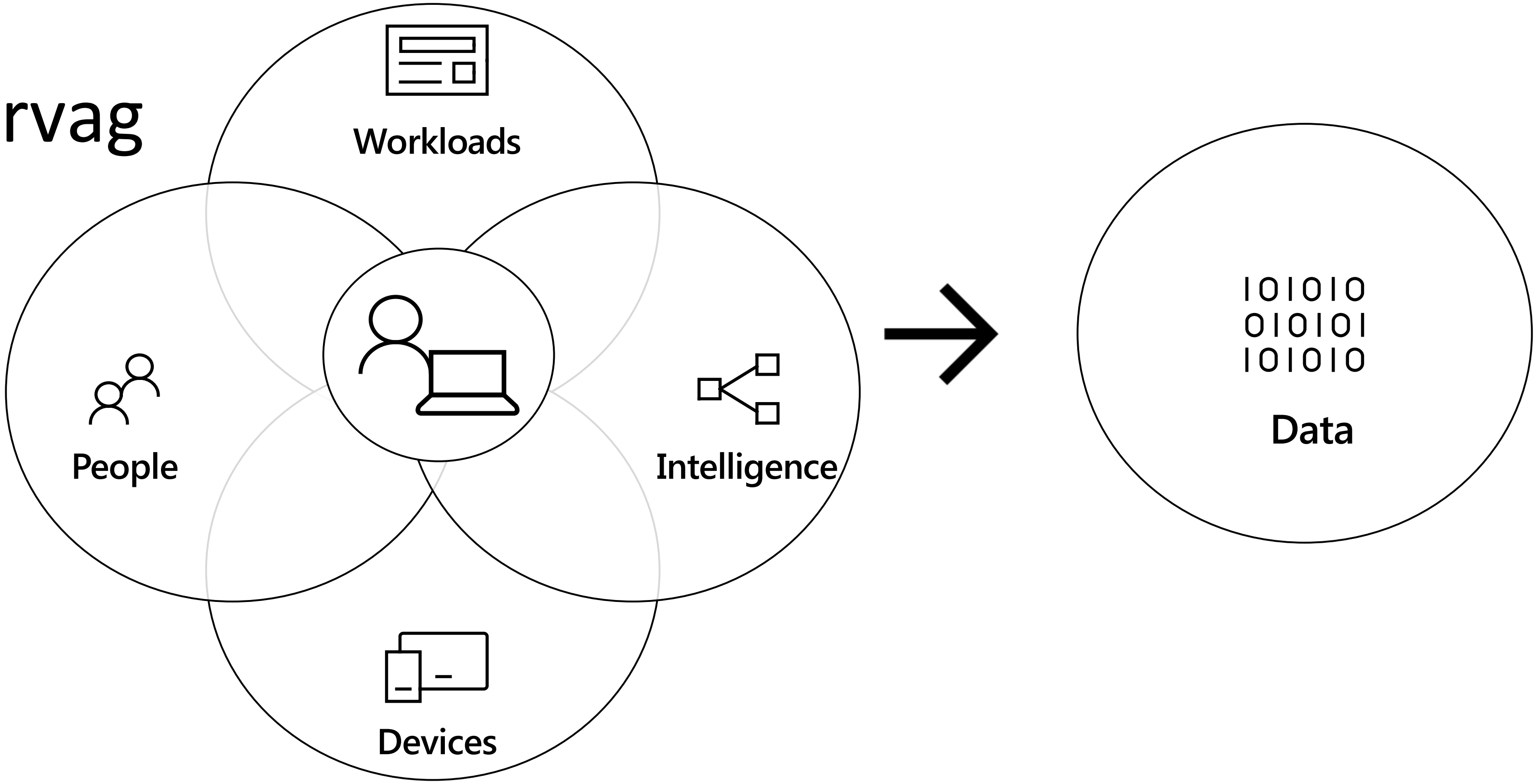
17%

Of breaches had errors as casual events[1]

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

What is a Zero Trust network?

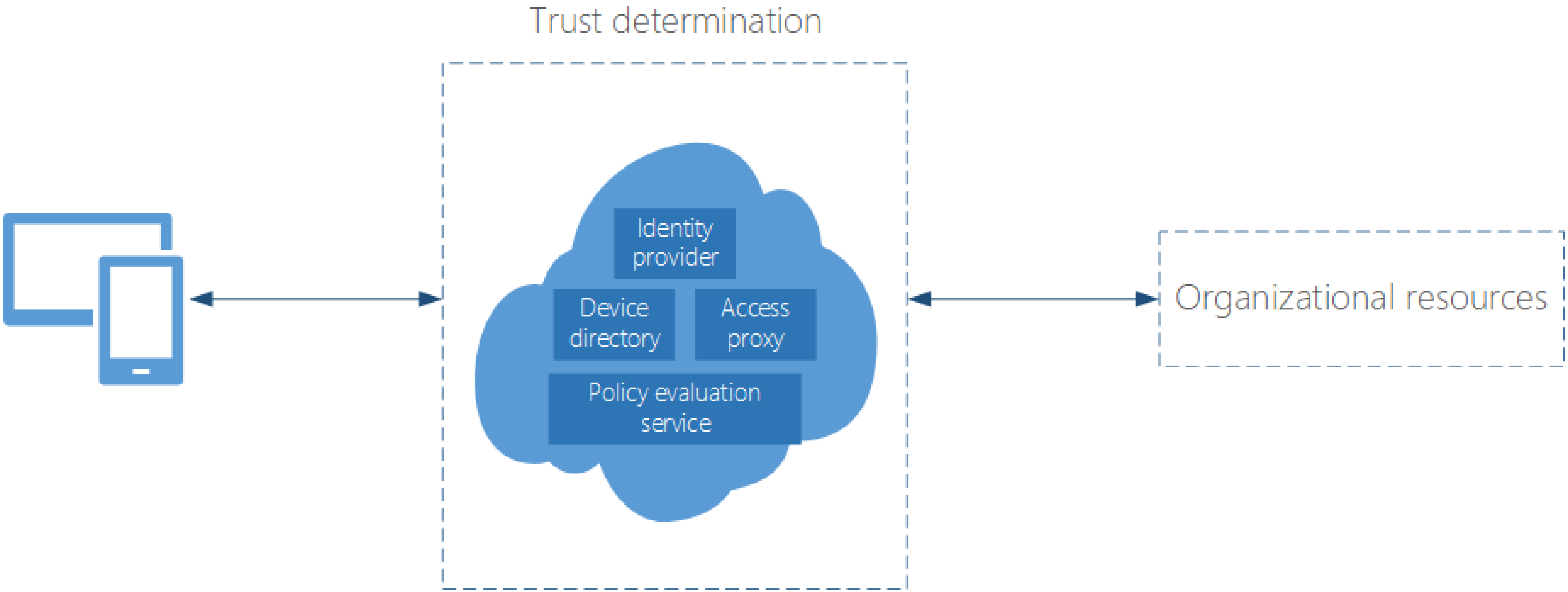
- Eliminates the concept of trust based on network location within a perimeter.
- Leverages device and user trust claims to get access to data and resources.
- John Kindervag



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



Trust determination

Identity provider

Device directory

Access proxy

Policy evaluation service

Organizational resources

Designing a Zero Trust architecture

Approach: Start with asking questions

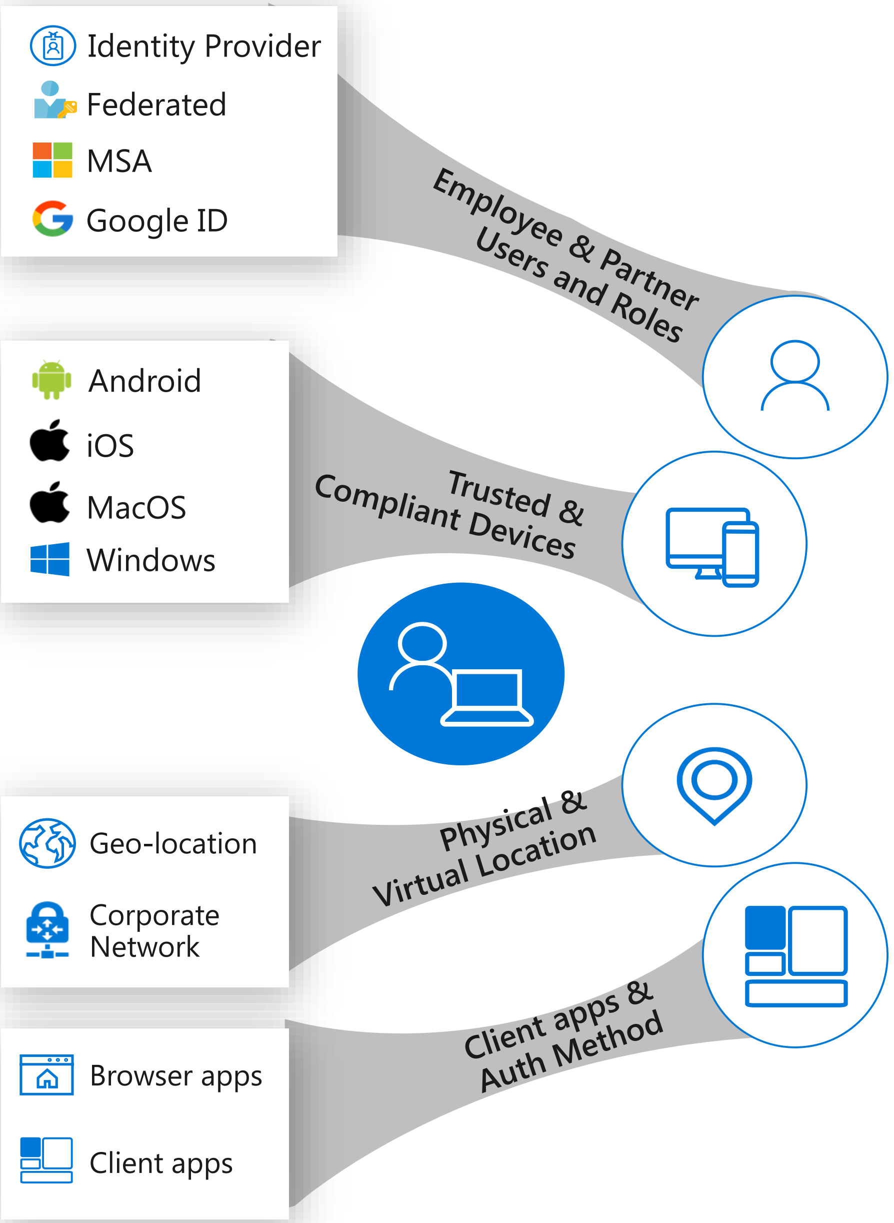
Who are your users? What apps are they trying to access? How are they doing it? Why are they doing it that way?

What conditions are required to access a corporate resource?

What controls are required based on the condition?

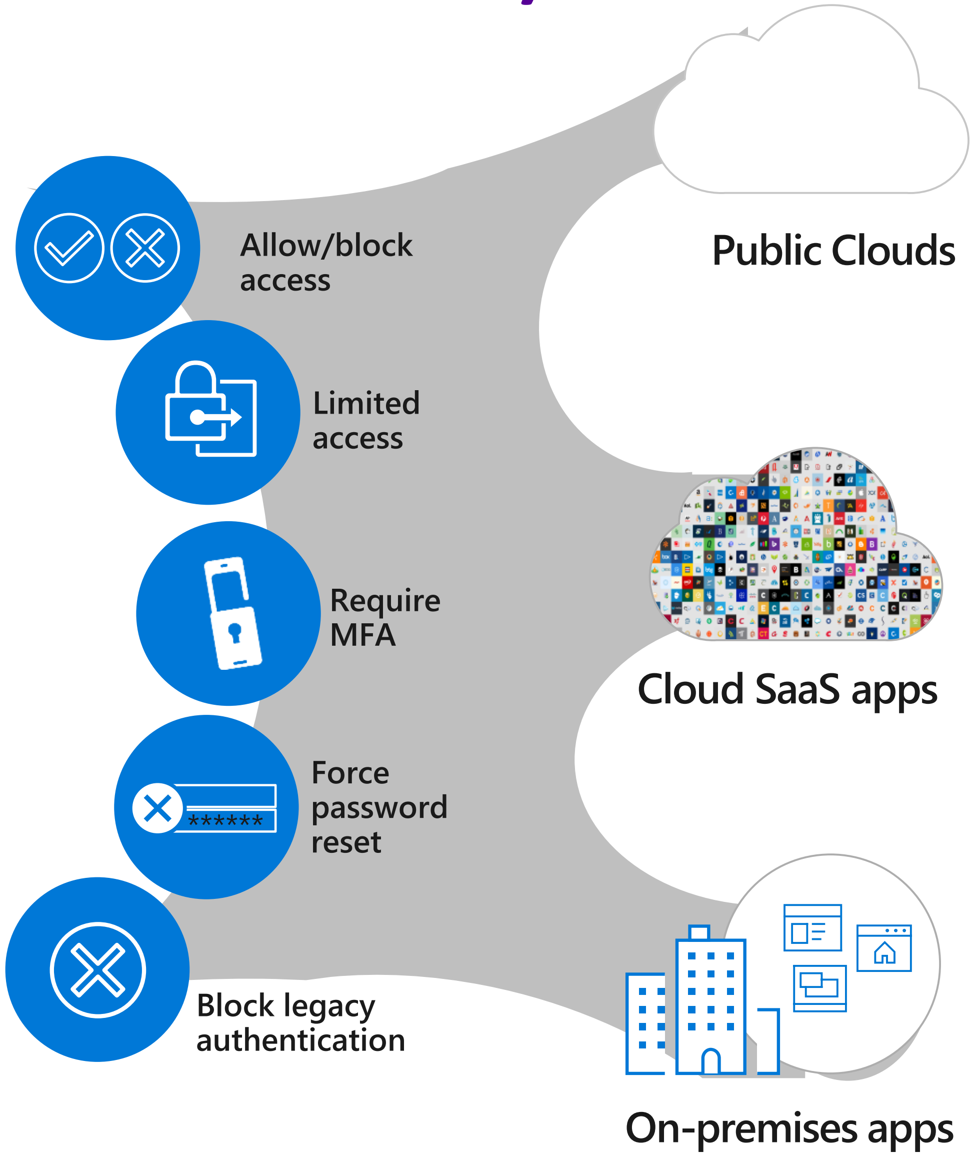
Consider an approach based on set of conditions

- 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?



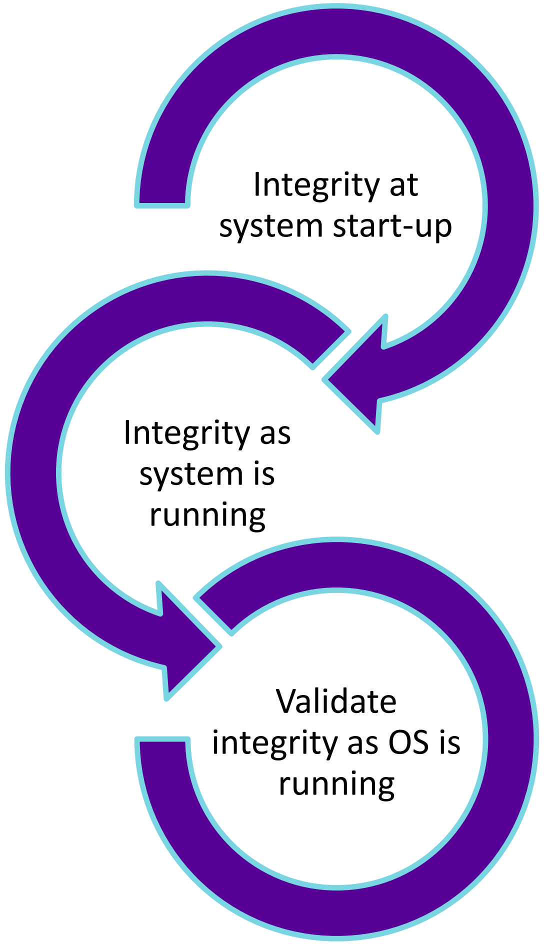
Followed by a set of controls (if/then statement)

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



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?)



Integrity at system start-up

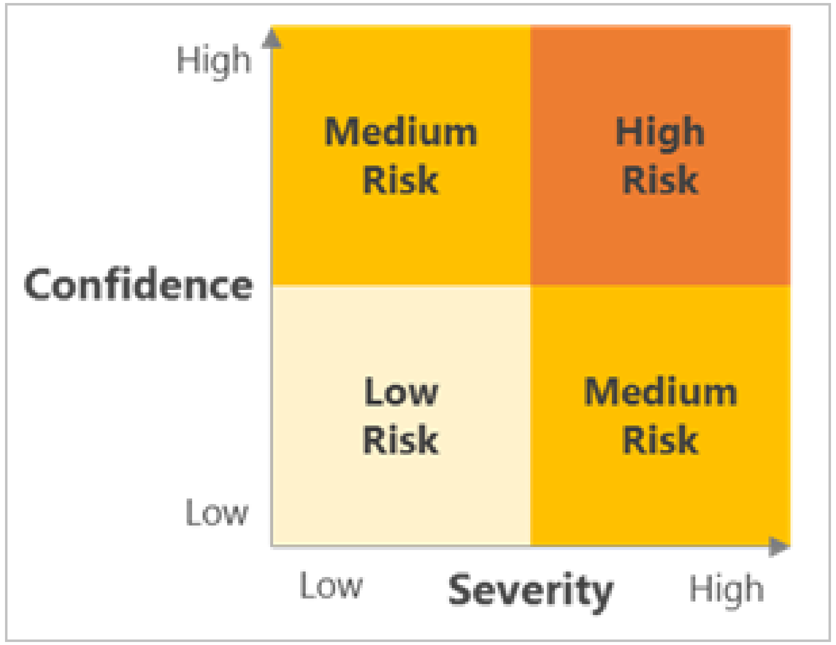
Integrity as system is running

Validate integrity as OS is running

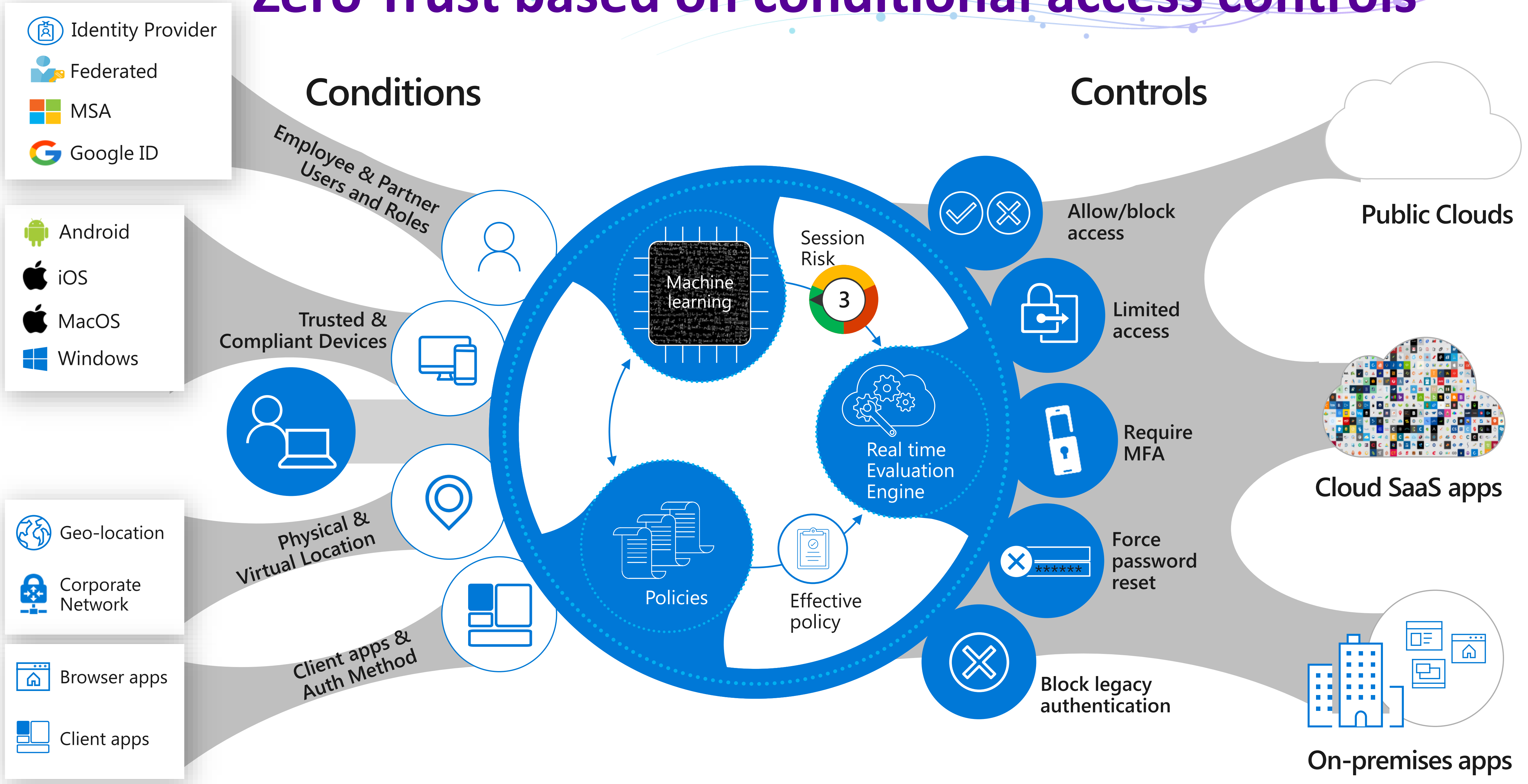
Identity Conditions

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



Zero Trust based on conditional access controls



Identity Provider

Federated

MSA

Google ID

Android

iOS

MacOS

Windows

Geo-location

Corporate Network

Browser apps

Client apps

Conditions

Employee & Partner Users and Roles

Trusted & Compliant Devices

Physical & Virtual Location

Client apps & Auth Method

Machine learning

Session Risk

3

Real time Evaluation Engine

Policies

Effective policy

Controls

Allow/block access

Limited access

Require MFA

Force password reset

******

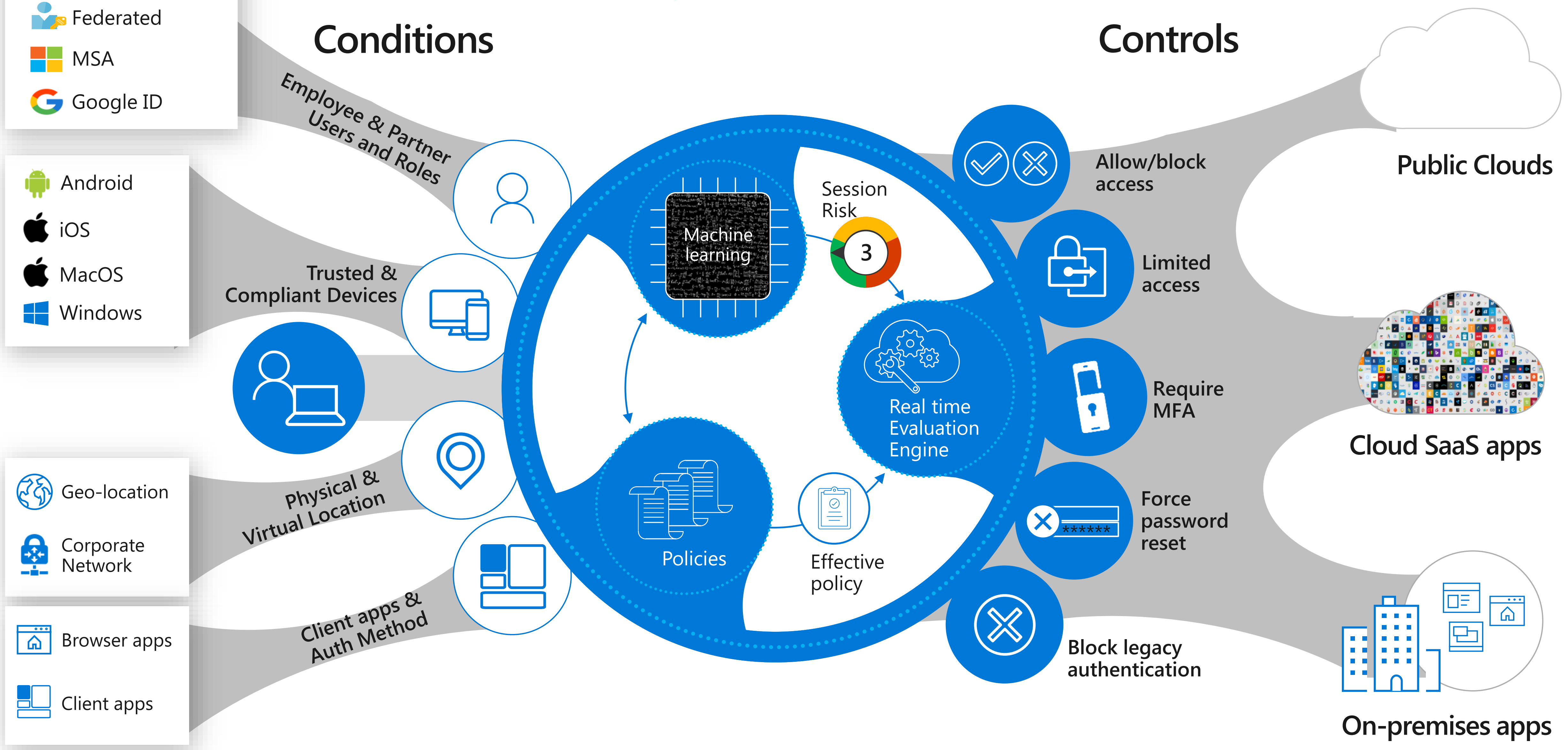
Block legacy authentication

Public Clouds

Cloud SaaS apps

On-premises apps

Zero Trust based on conditional access controls



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.
- Identity is everything, make it the control plane.
- Consider an *"if-this-then-that"* automated approach to Zero Trust.
- Zero Trust *can* enable new business outcomes that were not possible before.

Thank You!

Reference:
http://aka.ms/ZeroTrustDemos
Matt Soseman – Presentation
Security Architect
Microsoft