Achieving Zero Trust Identity Management

→ David Guest

Solution Architect & Technology Evangelist

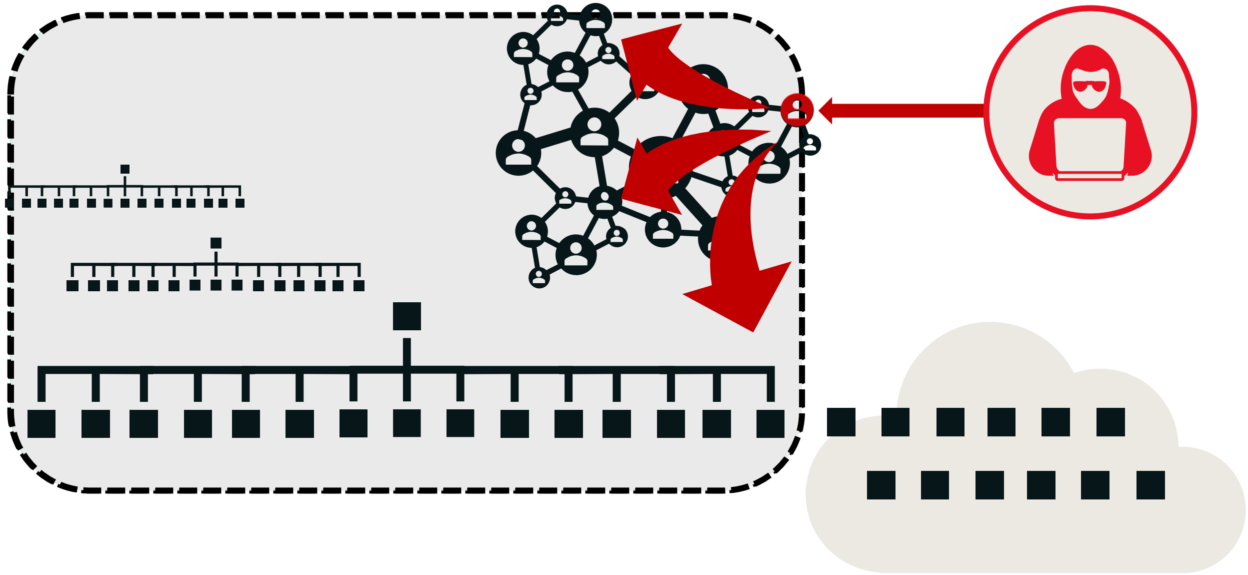
6 March 2024

Kocho

BECOME GREATER

Why are we having a Zero Trust conversation?

Access Control: Keep Assets away from **Attackers**



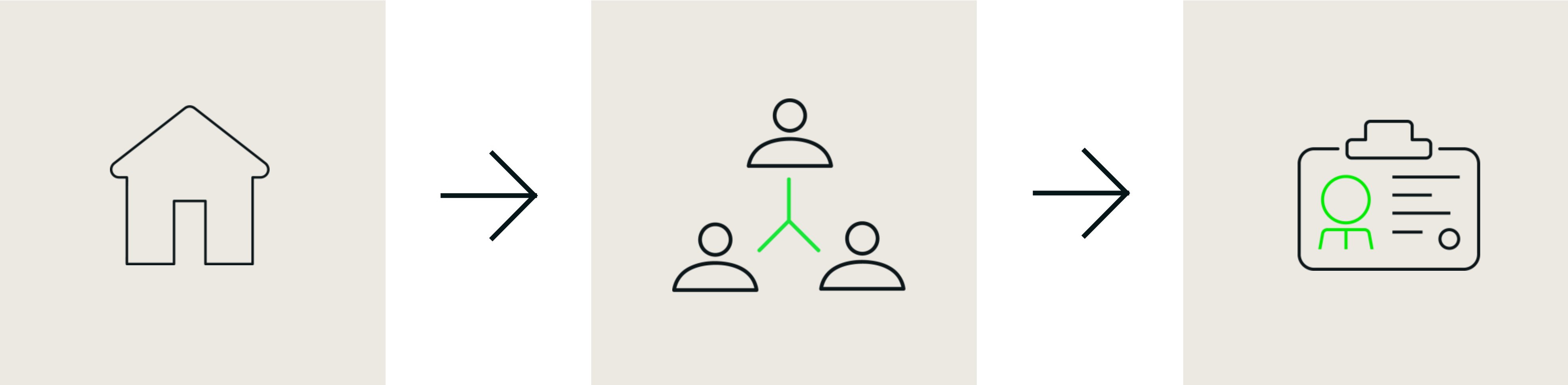
1. **IT Security is Complex**
   - Many Devices, Users, & Connections
2. **“Trusted network” security strategy**
   - Initial attacks were network based
   - *Seemingly* simple and economical
   - Accepted lower security within network
3. Assets increasingly leave network
   - BYOD, WFH, Mobile, and SaaS
4. Attackers shift to identity attacks
   - Phishing and credential theft
   - Security teams often overwhelmed

BECOME GREATER
KOCHO.CO.UK

Evolution of IT, threats, and Microsoft Identity security

MICROSOFT IDENTITY APPROACH	Windows NT Domains	+ Enterprise Active Directory + Smartcard Authentication	+ Azure Active Directory + Zero Trust Access Control (Conditional Access) + Password-less Authentication
	Widespread Password Weakness and Re-use	**Credential Theft Attacks Mass Password Compromises**	
IDENTITY AND ACCESS TRENDS	Local Identities	Enterprise Single Sign On + 2 factor authentication	Hybrid and Federated Cloud Identity
INFORMATION TECHNOLOGY	Mainframes + PCs	+ Datacenters + Mobile Devices	+ Cloud + Internet of Things (IoT)

Evolution of security perimeters



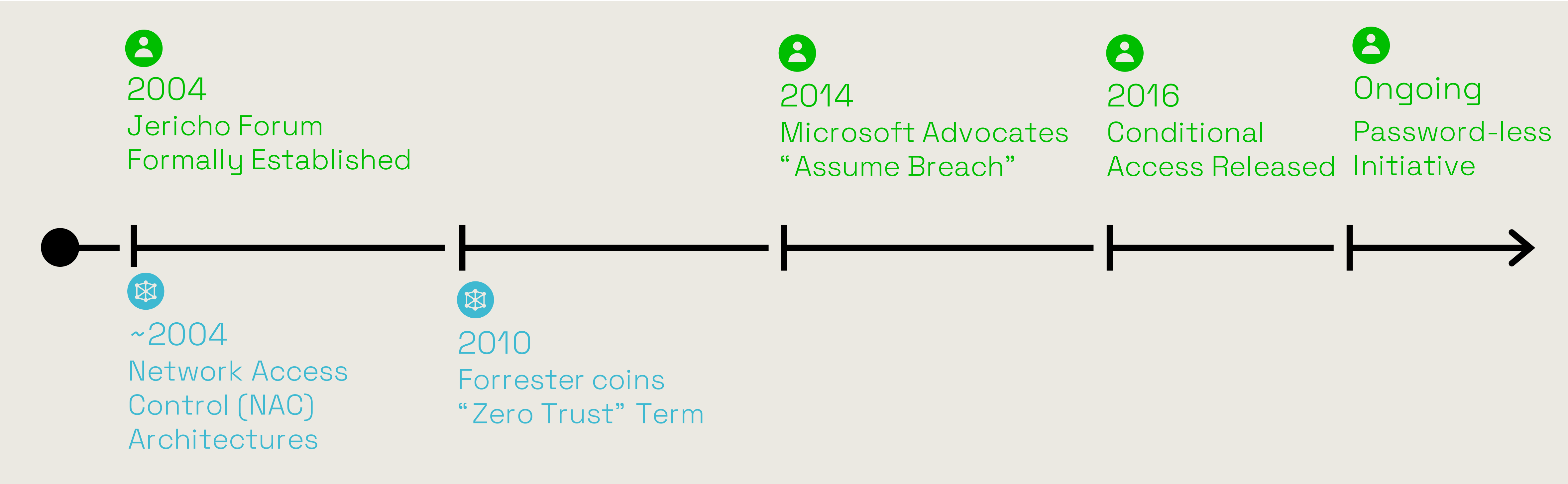
Physical

Network

Identity

A consistent set of controls between assets and threats

This “Zero Trust” is not new



2004
Jericho Forum
Formally Established

~2004
Network Access
Control (NAC)
Architectures

2010
Forrester coins
“Zero Trust” Term

2014
Microsoft Advocates
“Assume Breach”

2016
Conditional
Access Released

Ongoing
Password-less
Initiative

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

Trends and challenges

Attackers using identity to bypass network controls

- → Phishing allows attackers to impersonate valid user Identities
- → Credential theft allows attackers to expand access by impersonating identities

Passwords aren’t enough to protect identities

- → Single factor authentication (Passwords) without context isn’t enough assurance
- → Attacks on credentials circumvent software assurances (without hardware isolation)

Identities being used outside network

- → Cloud, Mobile, and IoT assets are frequently beyond reach of enterprise firewalls
- → Identity and Access controls are inconsistent on different cloud services and devices

Zero Trust Principles

Verify Explicitly

- Always authenticate and authorize based on all available data points, including user identity, location, device health, data classification, and anomalies.

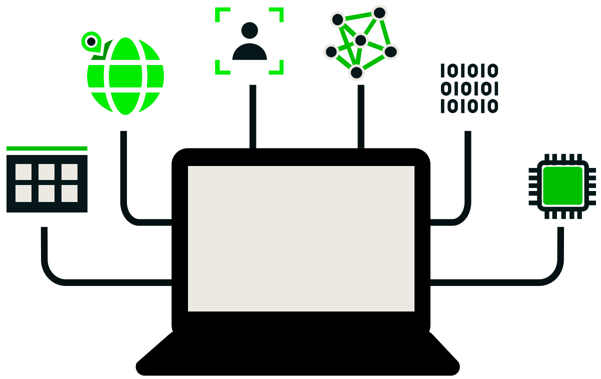
Least Privilege

- Minimize user access with Just-In-Time and Just-Enough Access (JIT/JEA), risk-based adaptive polices, and data protection which protects data and productivity.

Assume Breach

- Minimize scope of breach damage and prevent lateral movement by segmenting access via network, user, devices and applications.
- Verify all sessions are encrypted end to end.
- Use analytics to get visibility and drive threat detection.

Zero Trust Access Control Strategy



Signal

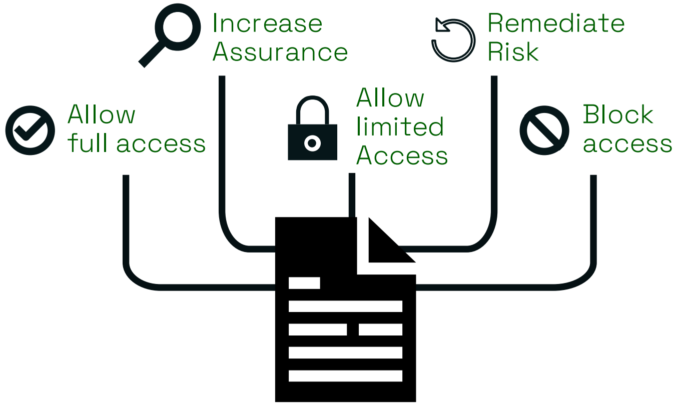
to make an informed choice

Device Risk

- → Device Management, Threat Detection and more...

User Risk

- → Multi-factor Authentication, Behaviour Analytics and more...



Increase Assurance

Remediate Risk

Allow full access

Allow limited Access

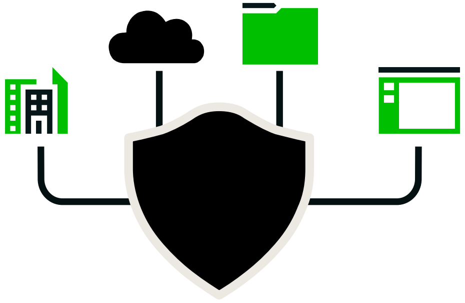
Block access

Decision

based on organization's policy

- → Apply to inbound requests
- → Re-evaluate during session

Never Trust. Always verify.



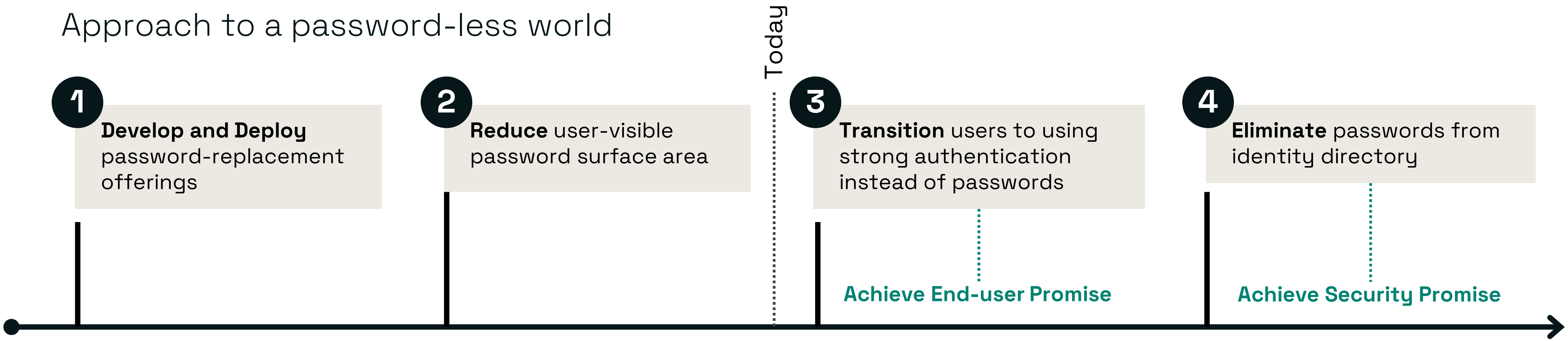
Enforcement

of policy across resource

- → Modern Applications
- → SaaS Applications
- → Legacy Applications
- → And more...

Eliminate passwords through strong multifactor authentication

Approach to a password-less world



1 **Develop and Deploy** password-replacement offerings

2 **Reduce** user-visible password surface area

Today

3 **Transition** users to using strong authentication instead of passwords

Achieve End-user Promise

4 **Eliminate** passwords from identity directory

Achieve Security Promise

Windows Hello for Business
Available on all Windows 10 Machines today

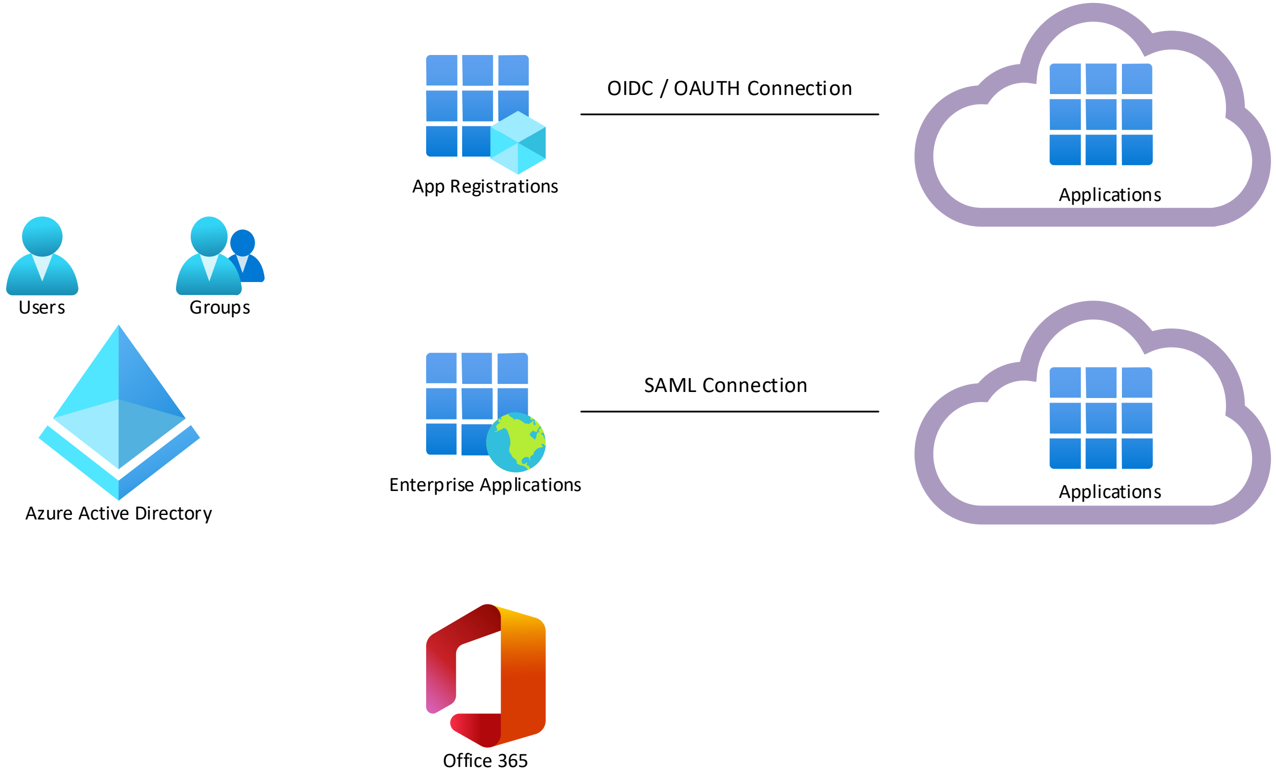
Microsoft Authenticator
Available today across all mobile platforms, integral in corporate bootstrapping of MFA

FIDO

Microsoft
+
Third Party

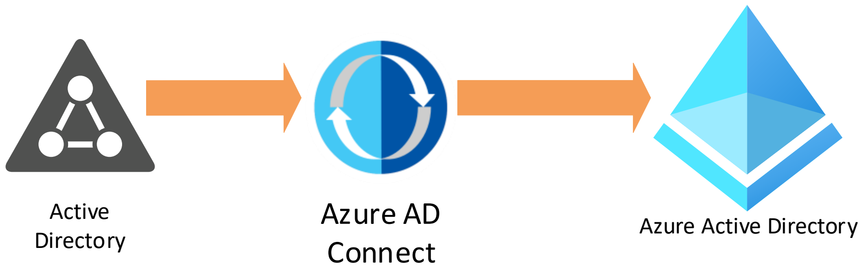
Connect users and Applications

- Use Azure AD as the Identity Provider
  - Provide cloud authentication to services
    - Office 365
    - SaaS

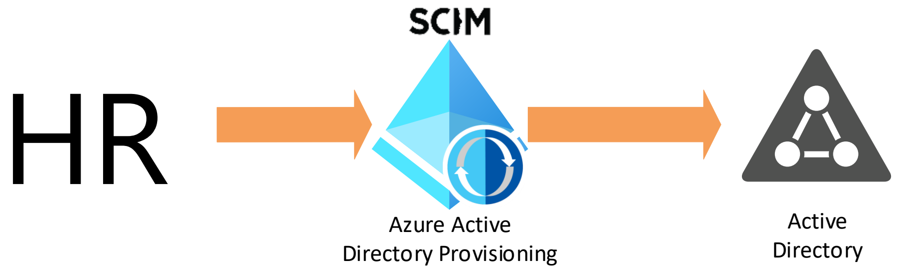


Provisioning into AAD

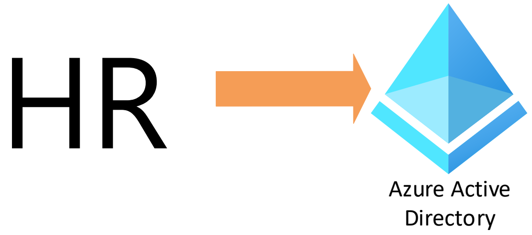
- Provisioning from AD



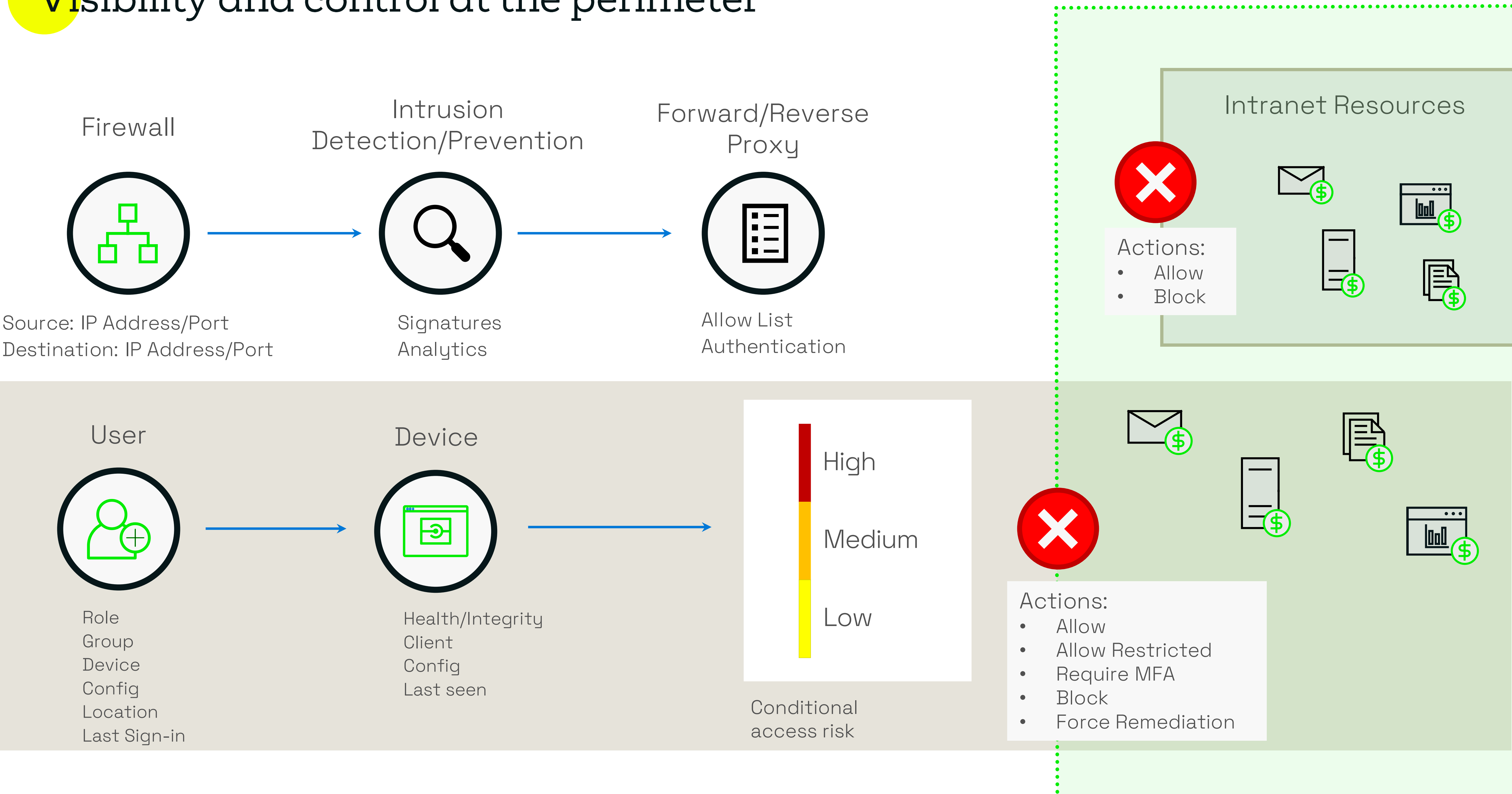
- Provisioning from HR to AD
  - Then onward to AAD as above



- Provisioning from HR directly to AAD



Visibility and control at the perimeter



Firewall

Source: IP Address/Port
Destination: IP Address/Port

Intrusion Detection/Prevention

Signatures
Analytics

Forward/Reverse Proxy

Allow List
Authentication

Intranet Resources

Actions:
- Allow
- Block

User

Role
Group
Device
Config
Location
Last Sign-in

Device

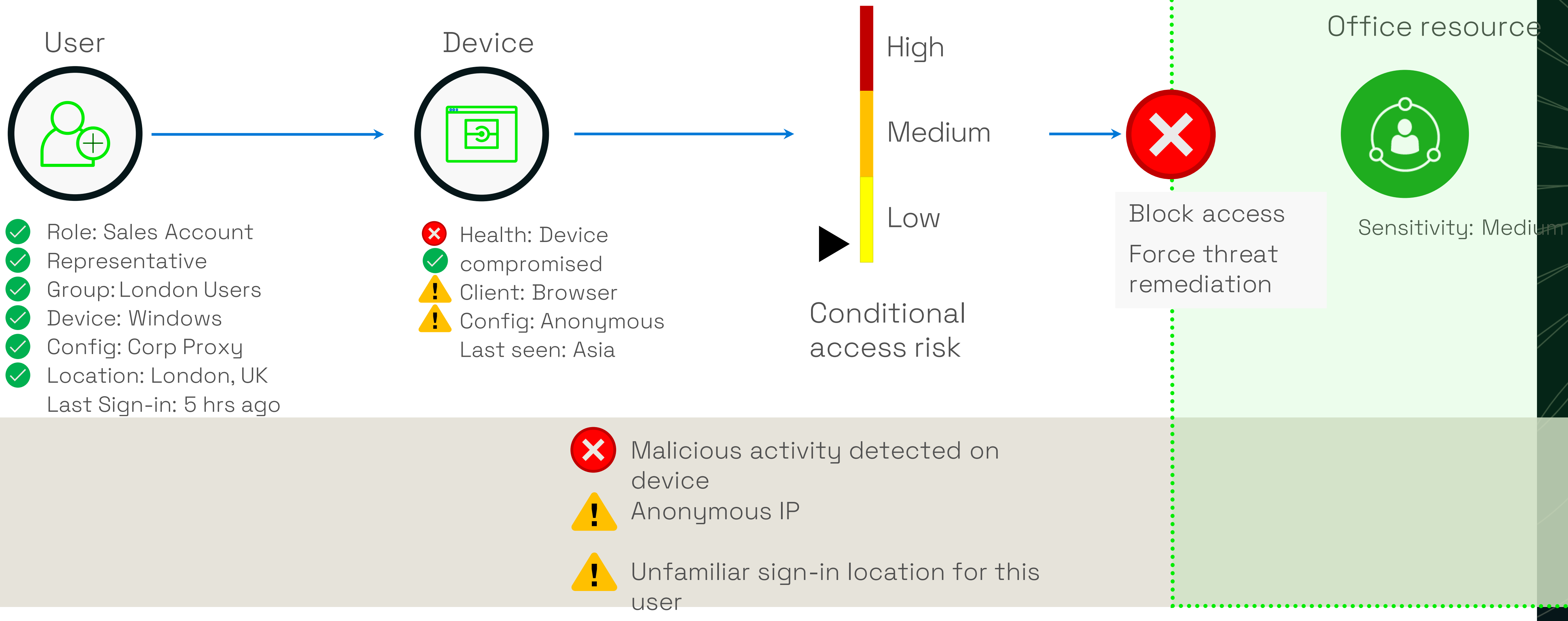
Health/Integrity
Client
Config
Last seen

High
Medium
Low

Conditional access risk

Actions:
- Allow
- Allow Restricted
- Require MFA
- Block
- Force Remediation

Conditional Access Example



User

- ✓ Role: Sales Account
- ✓ Representative
- ✓ Group: London Users
- ✓ Device: Windows
- ✓ Config: Corp Proxy
- ✓ Location: London, UK
- Last Sign-in: 5 hrs ago

Device

- ☒ Health: Device
- ✓ compromised
- ⚠ Client: Browser
- ⚠ Config: Anonymous
- Last seen: Asia

High

Medium

Low

Conditional access risk

Block access

Force threat remediation

Office resource

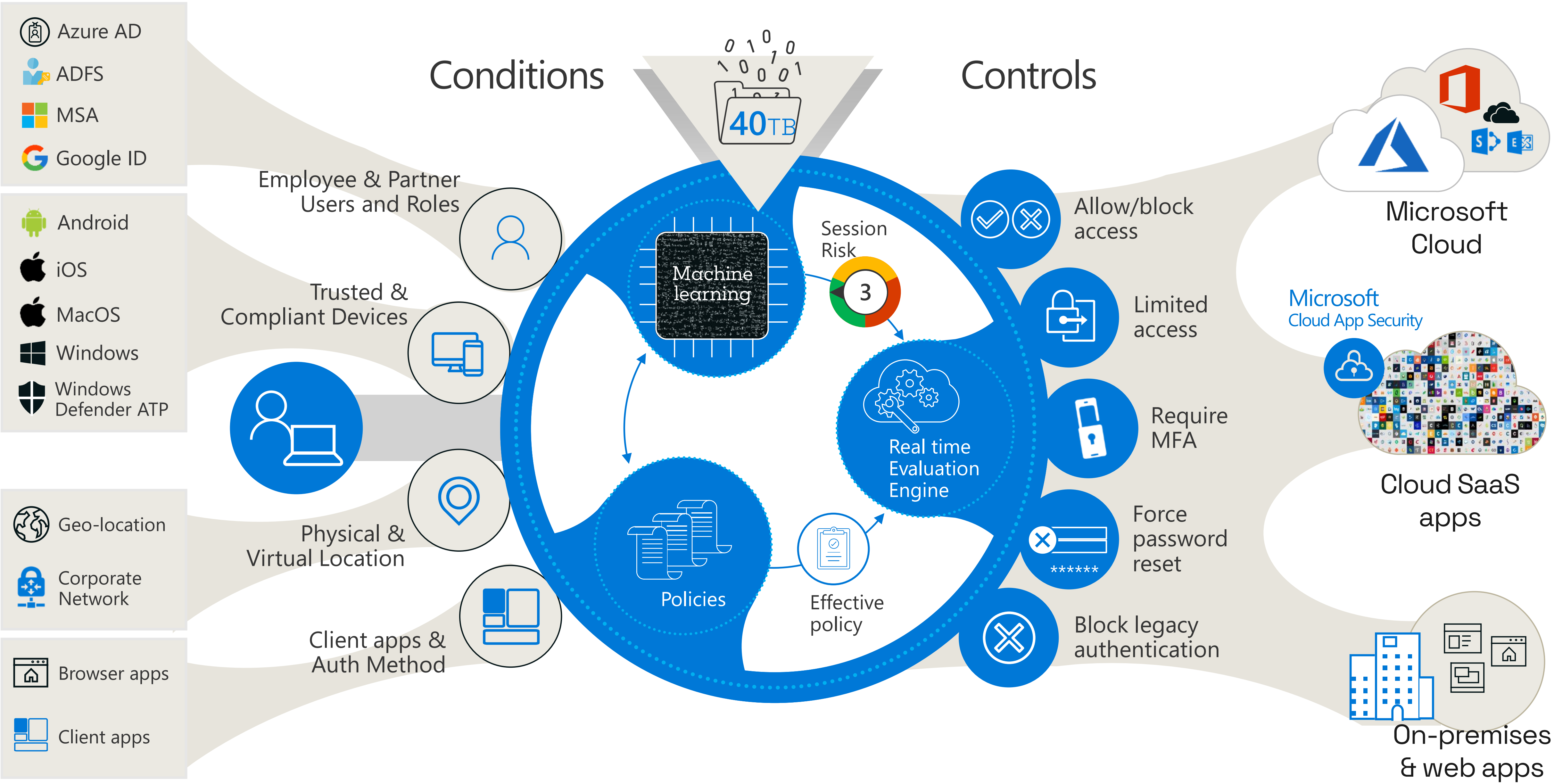
Sensitivity: Medium

- ☒ Malicious activity detected on device
- ⚠ Anonymous IP
- ⚠ Unfamiliar sign-in location for this user

BECOME GREATER

KOCHO.CO.UK

Azure AD conditional access (Zero Trust)



Azure AD
ADFS
MSA
Google ID

Android
iOS
MacOS
Windows
Windows Defender ATP

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

Real time Evaluation Engine

Policies

Effective policy

Controls

Allow/block access

Limited access

Require MFA

Force password reset

Block legacy authentication

Microsoft Cloud

Microsoft Cloud App Security

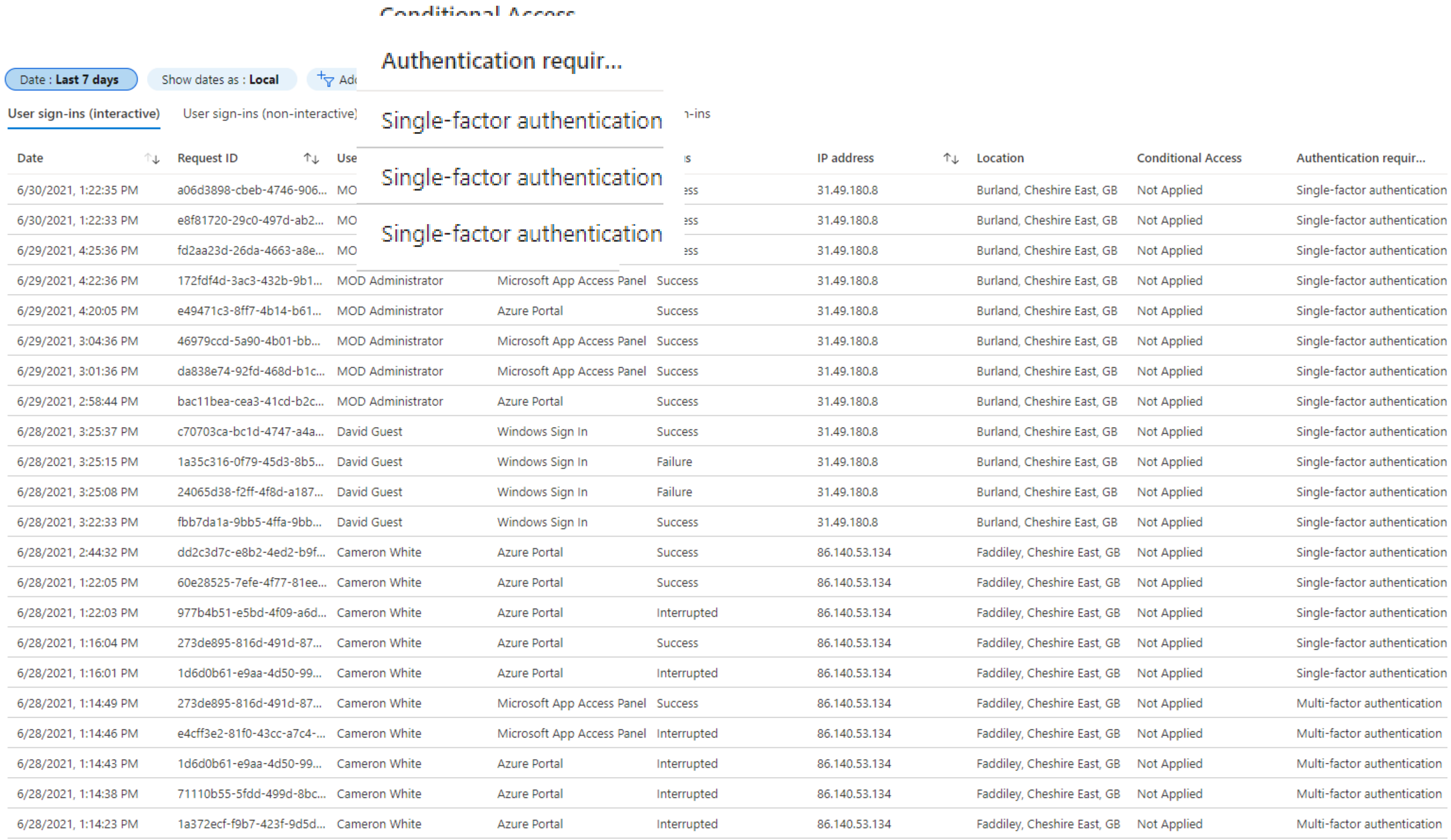
Cloud SaaS apps

On-premises & web apps

Who signed in – how – where - when

→ Azure Sign-In Logs

→ Watch out for -



Conditional Access

Authentication requir...

Single-factor authentication

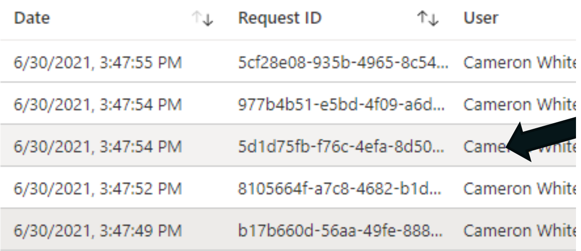
Single-factor authentication

Single-factor authentication

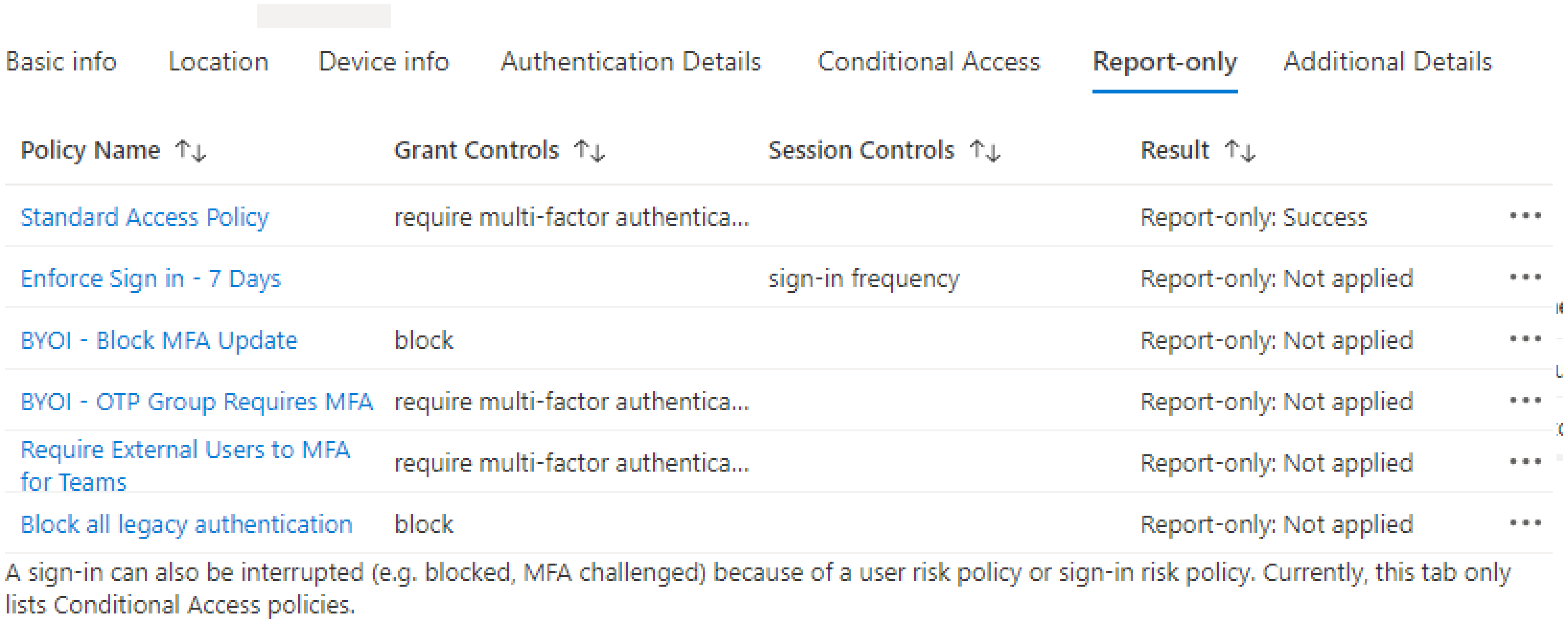
Date	Request ID	Use		s	IP address	Location	Conditional Access	Authentication requir...
6/30/2021, 1:22:35 PM	a06d3898-cbeb-4746-906...	MO		ess	31.49.180.8	Burland, Cheshire East, GB	Not Applied	Single-factor authentication
6/30/2021, 1:22:33 PM	e8f81720-29c0-497d-ab2...	MO		ess	31.49.180.8	Burland, Cheshire East, GB	Not Applied	Single-factor authentication
6/29/2021, 4:25:36 PM	fd2aa23d-26da-4663-a8e...	MO		ess	31.49.180.8	Burland, Cheshire East, GB	Not Applied	Single-factor authentication
6/29/2021, 4:22:36 PM	172fdf4d-3ac3-432b-9b1...	MOD Administrator	Microsoft App Access Panel	Success	31.49.180.8	Burland, Cheshire East, GB	Not Applied	Single-factor authentication
6/29/2021, 4:20:05 PM	e49471c3-8ff7-4b14-b61...	MOD Administrator	Azure Portal	Success	31.49.180.8	Burland, Cheshire East, GB	Not Applied	Single-factor authentication
6/29/2021, 3:04:36 PM	46979ccd-5a90-4b01-bb...	MOD Administrator	Microsoft App Access Panel	Success	31.49.180.8	Burland, Cheshire East, GB	Not Applied	Single-factor authentication
6/29/2021, 3:01:36 PM	da838e74-92fd-468d-b1c...	MOD Administrator	Microsoft App Access Panel	Success	31.49.180.8	Burland, Cheshire East, GB	Not Applied	Single-factor authentication
6/29/2021, 2:58:44 PM	bac11bea-cea3-41cd-b2c...	MOD Administrator	Azure Portal	Success	31.49.180.8	Burland, Cheshire East, GB	Not Applied	Single-factor authentication
6/28/2021, 3:25:37 PM	c70703ca-bc1d-4747-a4a...	David Guest	Windows Sign In	Success	31.49.180.8	Burland, Cheshire East, GB	Not Applied	Single-factor authentication
6/28/2021, 3:25:15 PM	1a35c316-0f79-45d3-8b5...	David Guest	Windows Sign In	Failure	31.49.180.8	Burland, Cheshire East, GB	Not Applied	Single-factor authentication
6/28/2021, 3:25:08 PM	24065d38-f2ff-4f8d-a187...	David Guest	Windows Sign In	Failure	31.49.180.8	Burland, Cheshire East, GB	Not Applied	Single-factor authentication
6/28/2021, 3:22:33 PM	fbb7da1a-9bb5-4ffa-9bb...	David Guest	Windows Sign In	Success	31.49.180.8	Burland, Cheshire East, GB	Not Applied	Single-factor authentication
6/28/2021, 2:44:32 PM	dd2c3d7c-e8b2-4ed2-b9f...	Cameron White	Azure Portal	Success	86.140.53.134	Faddiley, Cheshire East, GB	Not Applied	Single-factor authentication
6/28/2021, 1:22:05 PM	60e28525-7efe-4f77-81ee...	Cameron White	Azure Portal	Success	86.140.53.134	Faddiley, Cheshire East, GB	Not Applied	Single-factor authentication
6/28/2021, 1:22:03 PM	977b4b51-e5bd-4f09-a6d...	Cameron White	Azure Portal	Interrupted	86.140.53.134	Faddiley, Cheshire East, GB	Not Applied	Single-factor authentication
6/28/2021, 1:16:04 PM	273de895-816d-491d-87...	Cameron White	Azure Portal	Success	86.140.53.134	Faddiley, Cheshire East, GB	Not Applied	Single-factor authentication
6/28/2021, 1:16:01 PM	1d6d0b61-e9aa-4d50-99...	Cameron White	Azure Portal	Interrupted	86.140.53.134	Faddiley, Cheshire East, GB	Not Applied	Single-factor authentication
6/28/2021, 1:14:49 PM	273de895-816d-491d-87...	Cameron White	Microsoft App Access Panel	Success	86.140.53.134	Faddiley, Cheshire East, GB	Not Applied	Multi-factor authentication
6/28/2021, 1:14:46 PM	e4cff3e2-81f0-43cc-a7c4-...	Cameron White	Microsoft App Access Panel	Interrupted	86.140.53.134	Faddiley, Cheshire East, GB	Not Applied	Multi-factor authentication
6/28/2021, 1:14:43 PM	1d6d0b61-e9aa-4d50-99...	Cameron White	Azure Portal	Interrupted	86.140.53.134	Faddiley, Cheshire East, GB	Not Applied	Multi-factor authentication
6/28/2021, 1:14:38 PM	71110b55-5fdd-499d-8bc...	Cameron White	Azure Portal	Interrupted	86.140.53.134	Faddiley, Cheshire East, GB	Not Applied	Multi-factor authentication
6/28/2021, 1:14:23 PM	1a372ecf-f9b7-423f-9d5d...	Cameron White	Azure Portal	Interrupted	86.140.53.134	Faddiley, Cheshire East, GB	Not Applied	Multi-factor authentication

Details

→ Specific Sign-In deta

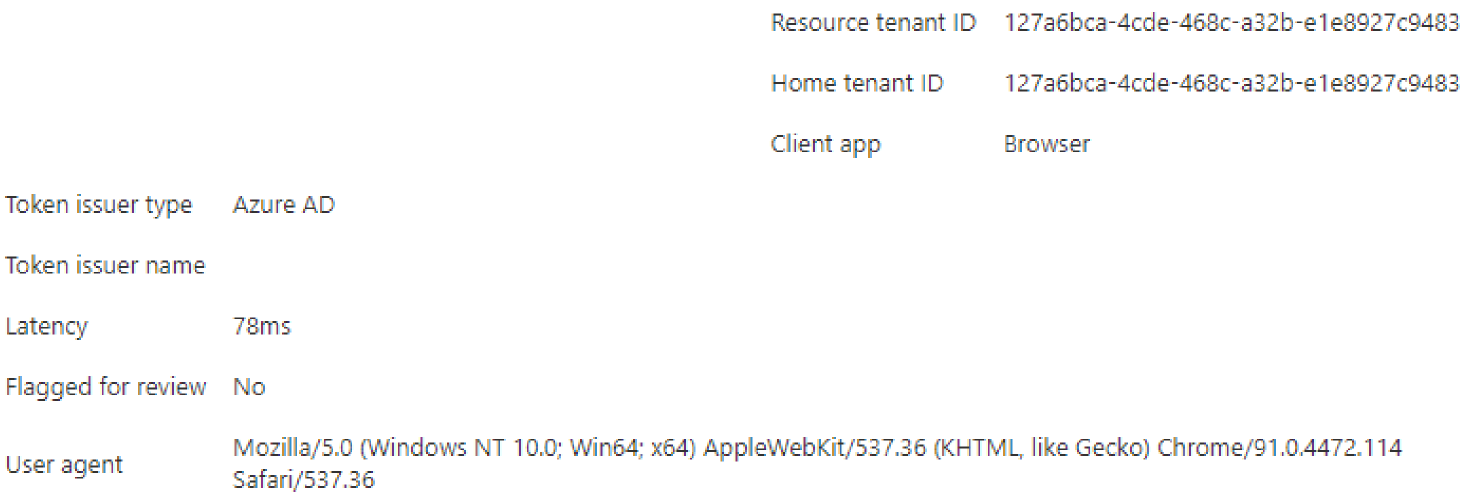


Date	Request ID	User
6/30/2021, 3:47:55 PM	5cf28e08-935b-4965-8c54...	Cameron White
6/30/2021, 3:47:54 PM	977b4b51-e5bd-4f09-a6d...	Cameron White
6/30/2021, 3:47:54 PM	5d1d75fb-f76c-4efa-8d50...	Cameron White
6/30/2021, 3:47:52 PM	8105664f-a7c8-4682-b1d...	Cameron White
6/30/2021, 3:47:49 PM	b17b660d-56aa-49fe-888...	Cameron White



Policy Name ↑↓	Grant Controls ↑↓	Session Controls ↑↓	Result ↑↓	
Standard Access Policy	require multi-factor authentica...		Report-only: Success	•••
Enforce Sign in - 7 Days		sign-in frequency	Report-only: Not applied	•••
BYOI - Block MFA Update	block		Report-only: Not applied	•••
BYOI - OTP Group Requires MFA	require multi-factor authentica...		Report-only: Not applied	•••
Require External Users to MFA for Teams	require multi-factor authentica...		Report-only: Not applied	•••
Block all legacy authentication	block		Report-only: Not applied	•••

A sign-in can also be interrupted (e.g. blocked, MFA challenged) because of a user risk policy or sign-in risk policy. Currently, this tab only lists Conditional Access policies.



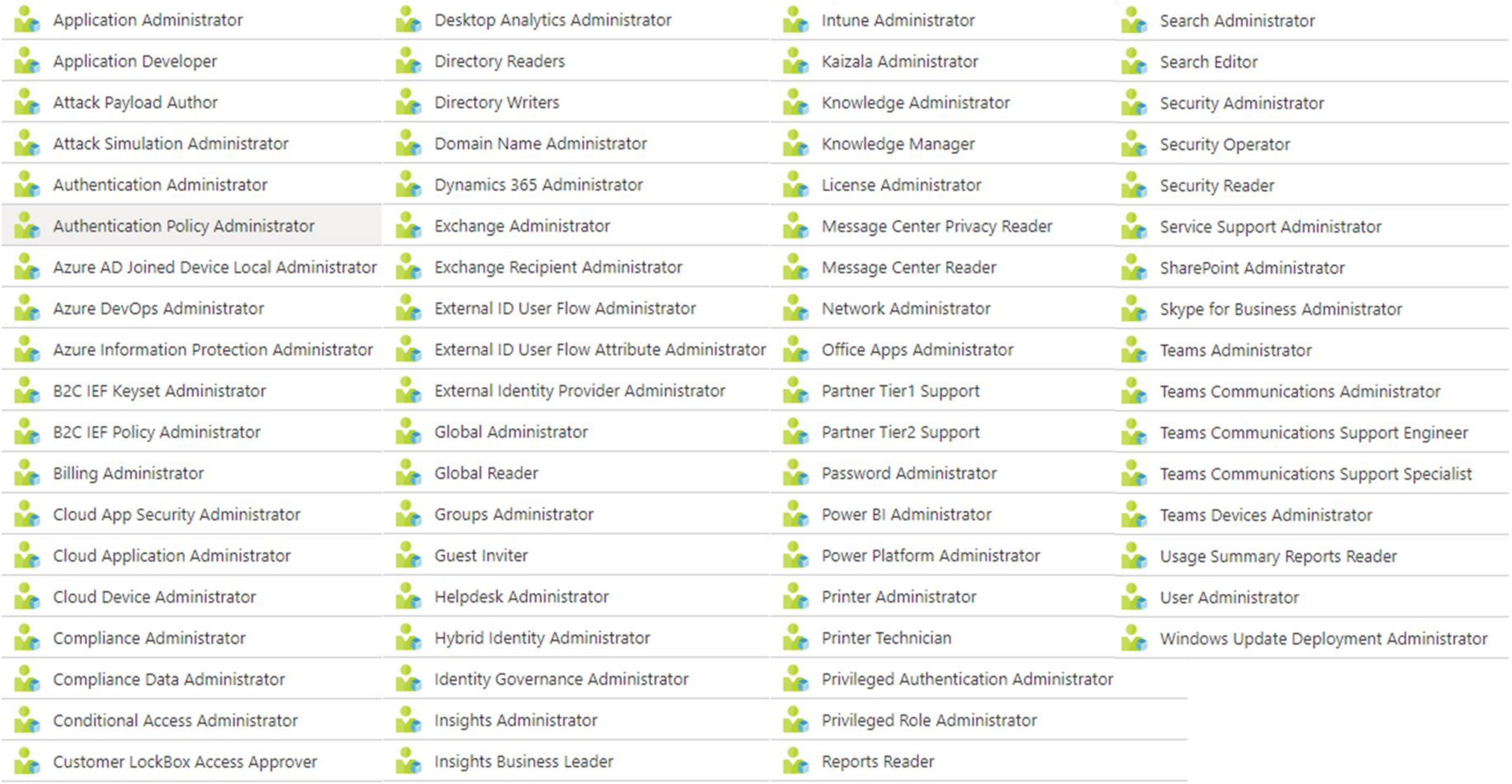
Resource tenant ID	127a6bca-4cde-468c-a32b-e1e8927c9483
Home tenant ID	127a6bca-4cde-468c-a32b-e1e8927c9483
Client app	Browser

Token issuer type	Azure AD
Token issuer name	
Latency	78ms
Flagged for review	No
User agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36

What about Privilege?

- → Privileged accounts should be used sparingly
- → Elevate privilege as required
  - → JIT – Just in time
- → Use the “least privilege”
  - → Just enough Privilege to perform
- → Using Azure Roles
  - → And linking to SaaS

Azure roles



- Application Administrator
- Application Developer
- Attack Payload Author
- Attack Simulation Administrator
- Authentication Administrator
- Authentication Policy Administrator
- Azure AD Joined Device Local Administrator
- Azure DevOps Administrator
- Azure Information Protection Administrator
- B2C IEF Keyset Administrator
- B2C IEF Policy Administrator
- Billing Administrator
- Cloud App Security Administrator
- Cloud Application Administrator
- Cloud Device Administrator
- Compliance Administrator
- Compliance Data Administrator
- Conditional Access Administrator
- Customer LockBox Access Approver
- Desktop Analytics Administrator
- Directory Readers
- Directory Writers
- Domain Name Administrator
- Dynamics 365 Administrator
- Exchange Administrator
- Exchange Recipient Administrator
- External ID User Flow Administrator
- External ID User Flow Attribute Administrator
- External Identity Provider Administrator
- Global Administrator
- Global Reader
- Groups Administrator
- Guest Inviter
- Helpdesk Administrator
- Hybrid Identity Administrator
- Identity Governance Administrator
- Insights Administrator
- Insights Business Leader
- Intune Administrator
- Kaizala Administrator
- Knowledge Administrator
- Knowledge Manager
- License Administrator
- Message Center Privacy Reader
- Message Center Reader
- Network Administrator
- Office Apps Administrator
- Partner Tier1 Support
- Partner Tier2 Support
- Password Administrator
- Power BI Administrator
- Power Platform Administrator
- Printer Administrator
- Printer Technician
- Privileged Authentication Administrator
- Privileged Role Administrator
- Reports Reader
- Search Administrator
- Search Editor
- Security Administrator
- Security Operator
- Security Reader
- Service Support Administrator
- SharePoint Administrator
- Skype for Business Administrator
- Teams Administrator
- Teams Communications Administrator
- Teams Communications Support Engineer
- Teams Communications Support Specialist
- Teams Devices Administrator
- Usage Summary Reports Reader
- User Administrator
- Windows Update Deployment Administrator

Implement PIM

- → Top down
- → Start with Highly privileged roles
  - → Global Admin
- → Work down to lesser roles
- → Assign through an access matrix

Access Matrix

AZURE AD ROLES	SERVICE DESK	INFRASTRUCTURE	WINTEL	SECURITY
Application administrator	🟥	🟨	🟨	🟩
Application developer	🟥	🟨	🟨	
Authentication administrator				🟩

🟩 Always active

🟨 Auto approved

🟥 Requires approval

BECOME GREATER
KOCHO.CO.UK

What do I need to do what

- → Which role can perform which activity

- → Delegate roles by admin task - Azure Active Directory | Microsoft Docs
  - → https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task