The Experts Conference

Sponsored by Quest®

Jeff Bley

Adwoa Boateng-Kwakye

Five steps to embark on your Zero Trust journey with M365

#TEC2023

TEC | The Experts Conference
Sponsored by Quest®

Jeff Bley

Senior Product Manager – Microsoft Identity CXE

He/Him

TEC | The Experts Conference
Sponsored by Quest®

Adwoa Boateng-Kwakye

Founder, *BreachProtect Consulting LLC*

Former Senior Product Manager, *Microsoft Identity and Network Access*

Agenda

- Introduction to Zero Trust
- Zero Trust Principles and Architecture
- 5 Zero Trust Steps
- Go-Dos

Disclaimer – Recent Brand Change

- Azure AD = Entra ID
- Hybrid Azure AD Join = Hybrid Entra ID Join
- Etc.

Forgive us if we use the wrong term ☺

Better than blurry pictures

You can find a PDF of this deck at aka.ms/5stepsZT (on GitHub)

Agenda

- Introduction to Zero Trust
- Zero Trust Principles and Architecture
- 5 Zero Trust Steps
- Go-Dos

NotPetya Attack

- NotPetya attack: Maersk – June 2017
- Cost Maersk $200- $300 million and disrupted operations for two weeks

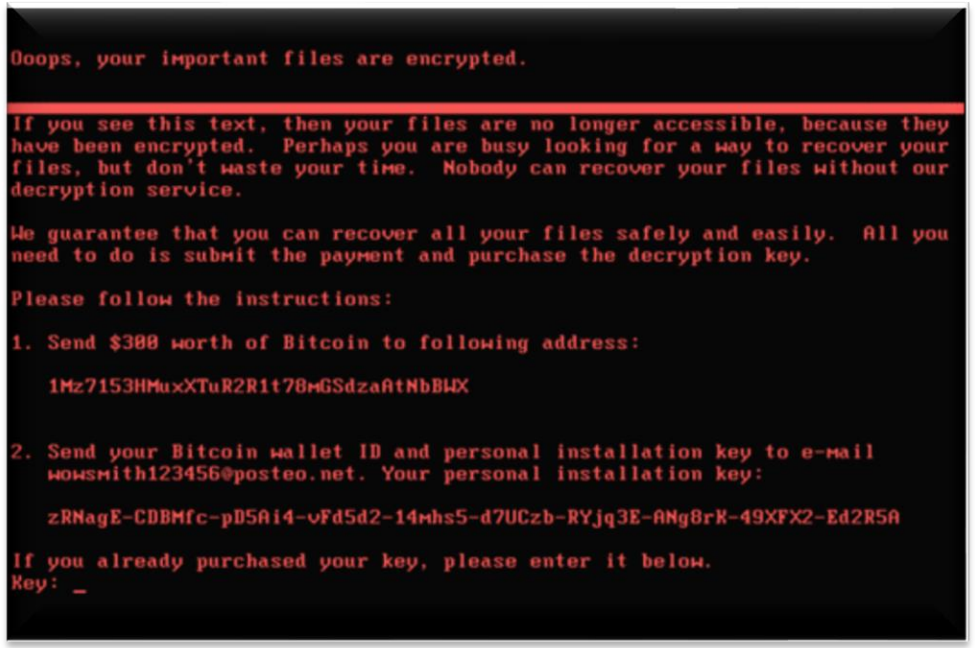
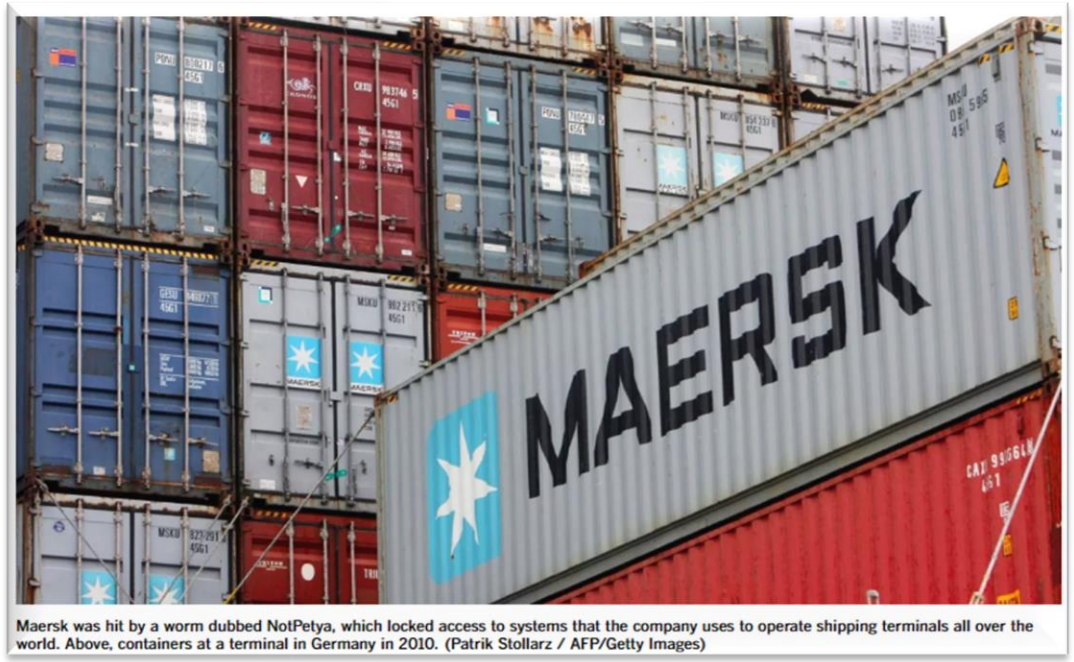


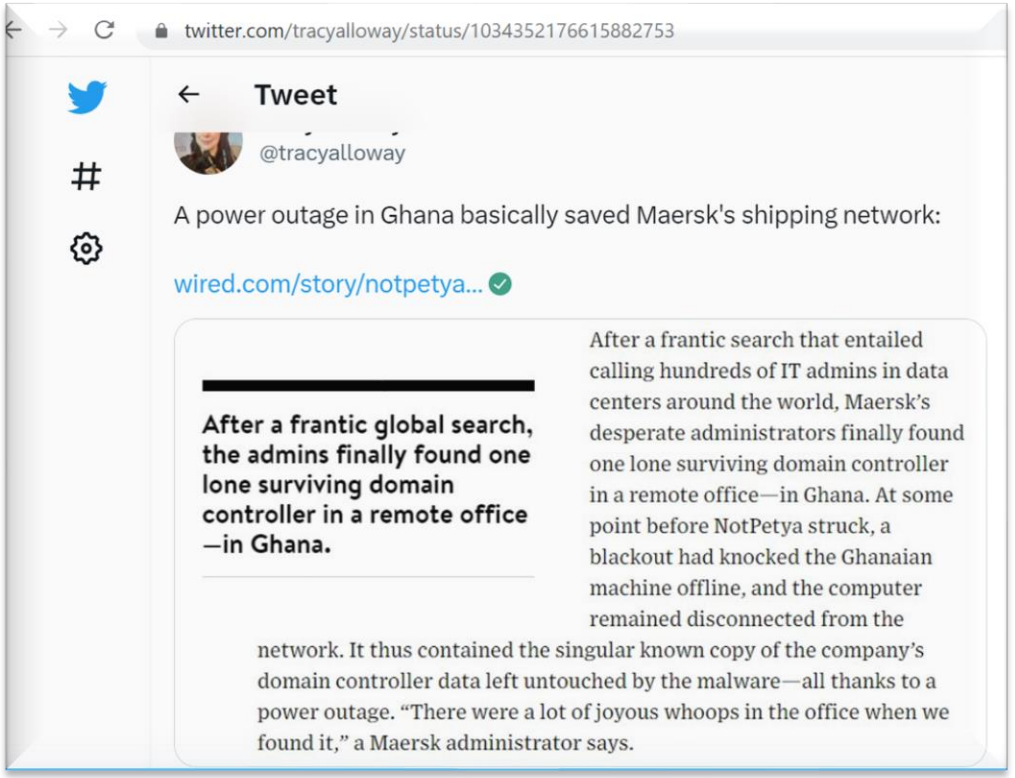
Photo credit: CrowdStrike



Maersk was hit by a worm dubbed NotPetya, which locked access to systems that the company uses to operate shipping terminals all over the world. Above, containers at a terminal in Germany in 2010. (Patrik Stollarz / AFP/Getty Images)

Maersk: Impact & Recovery

Trucks loaded with containers are lined up outside a terminal at the Jawaharlal Nehru Port Trust in Mumbai, India, Thursday, June 29, 2017. Operations at a terminal at India's busiest container port have been stalled by the malicious software that suddenly burst across the world's computer screens Tuesday, another example of the disruption that continues to be felt globally. (AP Photo/Rajanish Kakade)



- https://www.hypr.com/security-encyclopedia/notpetya
- https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Zero Trust Isn't

- LITERAL - You can't build a practical strategy around absolutes
- AN ADJECTIVE – You aren't going to "be" zero trust
- FOR SALE – There's no such thing as "Zero Trust" tech
- INSTANT– You can't boil the ocean
- A REVOLUTION – Build on what you've got

Zero Trust is a mindset

- Zero Trust requires 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

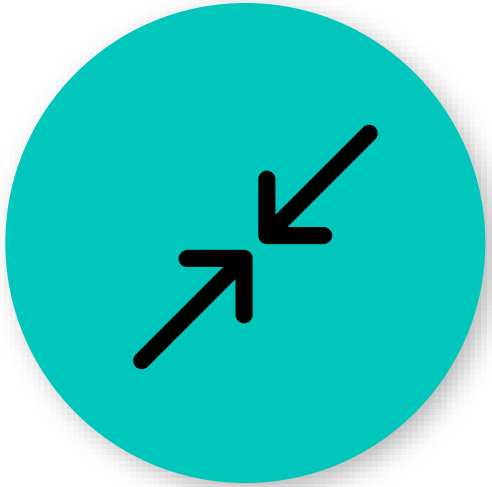
Agenda

- Introduction to Zero Trust
- Zero Trust Principles and Architecture
- 5 Zero Trust Steps
- Go-Dos

Core Principles of Zero Trust

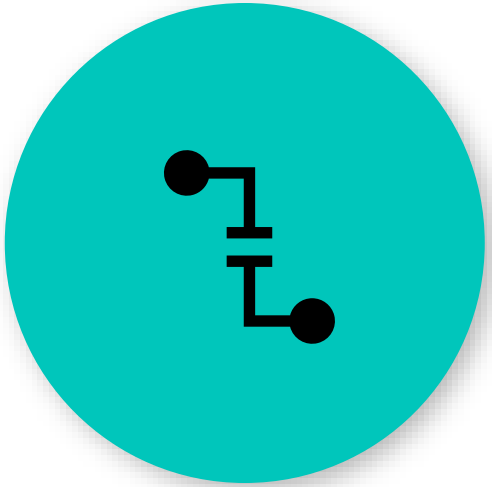
Verify Explicitly

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 application awareness. Verify all sessions are encrypted end to end.

Pillars of Zero Trust

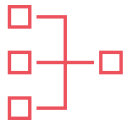
Identities

Devices/
Endpoints

Applications

Data

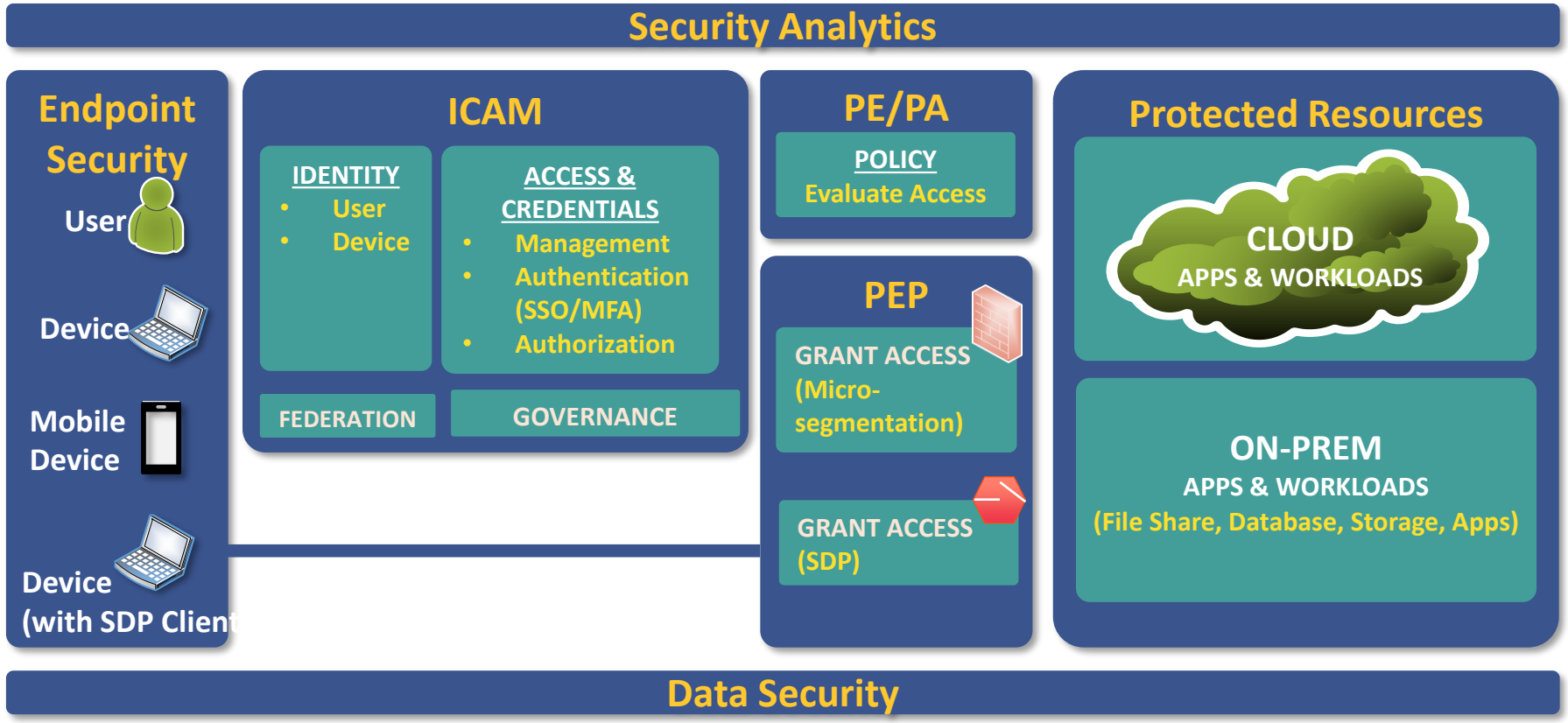
Infrastructure



Network

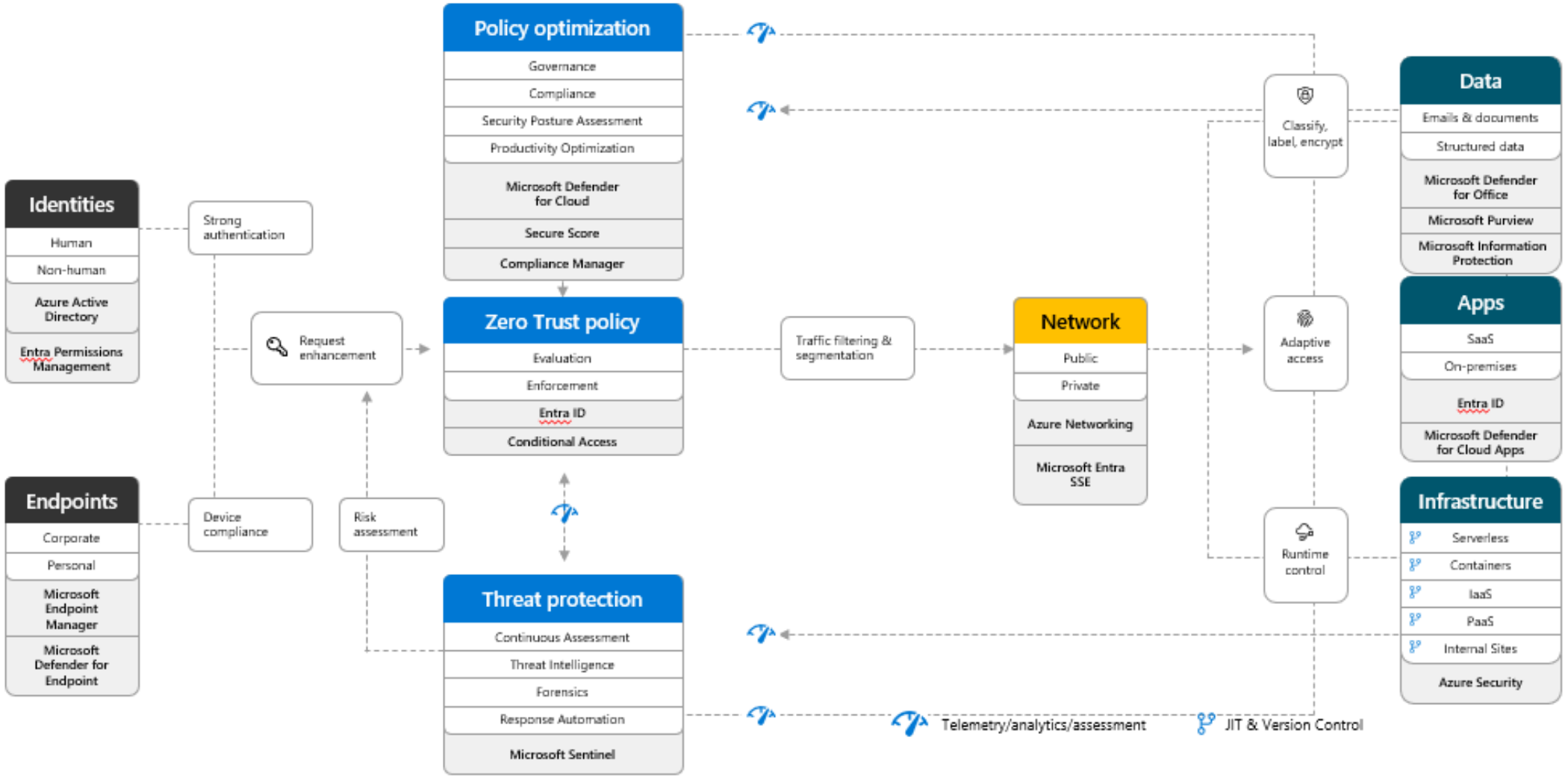
aka.ms/ztmodel

National Zero Trust Architecture - NIST

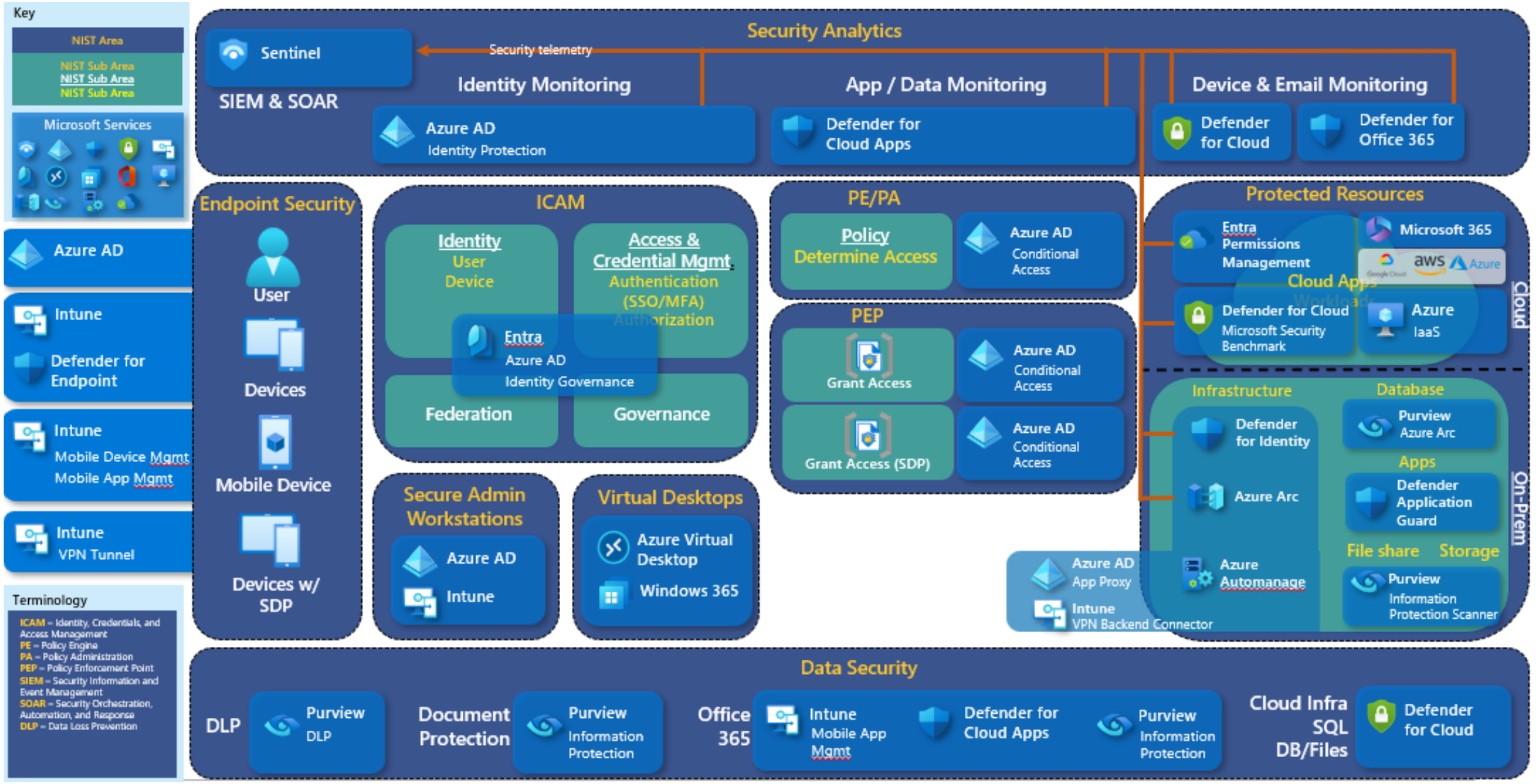


ICAM	*Identity, Credential and Access Management*
PA	*Policy Administrator*
PE	*Policy Engine*
PEP	*Policy Enforcement Point*
SDP	*Software Defined Perimeter*

Microsoft Zero Trust Architecture



Introduction to ZT | ZT Principles + Architecture | 5 Zero Trust Steps | Go-Dos


Key
NIST Area
NIST Sub Area
NIST Sub Area
NIST Sub Area
Microsoft Services
Azure AD
Intune
Defender for Endpoint
Intune
Mobile Device Mgmt
Mobile App Mgmt
Intune
VPN Tunnel
Terminology
ICAM = Identity, Credentials, and Access Management
PE = Policy Engine
PA = Policy Administration
PEP = Policy Enforcement Point
SIEM = Security Information and Event Management
SOAR = Security Orchestration, Automation, and Response
DLP = Data Loss Prevention
Security Analytics
Sentinel
SIEM & SOAR
Security telemetry
Identity Monitoring
Azure AD
Identity Protection
App / Data Monitoring
Defender for Cloud Apps
Device & Email Monitoring
Defender for Cloud
Defender for Office 365
Endpoint Security
User
Devices
Mobile Device
Devices w/ SDP
ICAM
Identity
User
Device
Access & Credential Mgmt.
Authentication
(SSO/MFA)
Authorization
Entra
Azure AD
Identity Governance
Federation
Governance
PE/PA
Policy
Determine Access
Azure AD
Conditional Access
PEP
Grant Access
Azure AD
Conditional Access
Grant Access (SDP)
Azure AD
Conditional Access
Protected Resources
Entra
Permissions Management
Microsoft 365
aws
Azure
Cloud Apps
Workloads
Defender for Cloud
Microsoft Security Benchmark
Azure
IaaS
Cloud
Infrastructure
Defender for Identity
Azure Arc
Azure Automanage
Database
Purview
Azure Arc
Apps
Defender Application Guard
File share
Storage
Purview
Information Protection Scanner
On-Prem
Azure AD
App Proxy
Intune
VPN Backend Connector
Secure Admin Workstations
Azure AD
Intune
Virtual Desktops
Azure Virtual Desktop
Windows 365
Data Security
DLP
Purview
DLP
Document Protection
Purview
Information Protection
Office 365
Intune
Mobile App Mgmt
Defender for Cloud Apps
Purview
Information Protection
Cloud Infra
SQL
DB/Files
Defender for Cloud

Agenda

- Introduction to Zero Trust
- Zero Trust Principles and Architecture
- 5 Zero Trust Steps
- Go-Dos

1. Strengthen Identities

Deploy strong authentication methods

Protect identities using Microsoft Conditional Access and Identity Protection

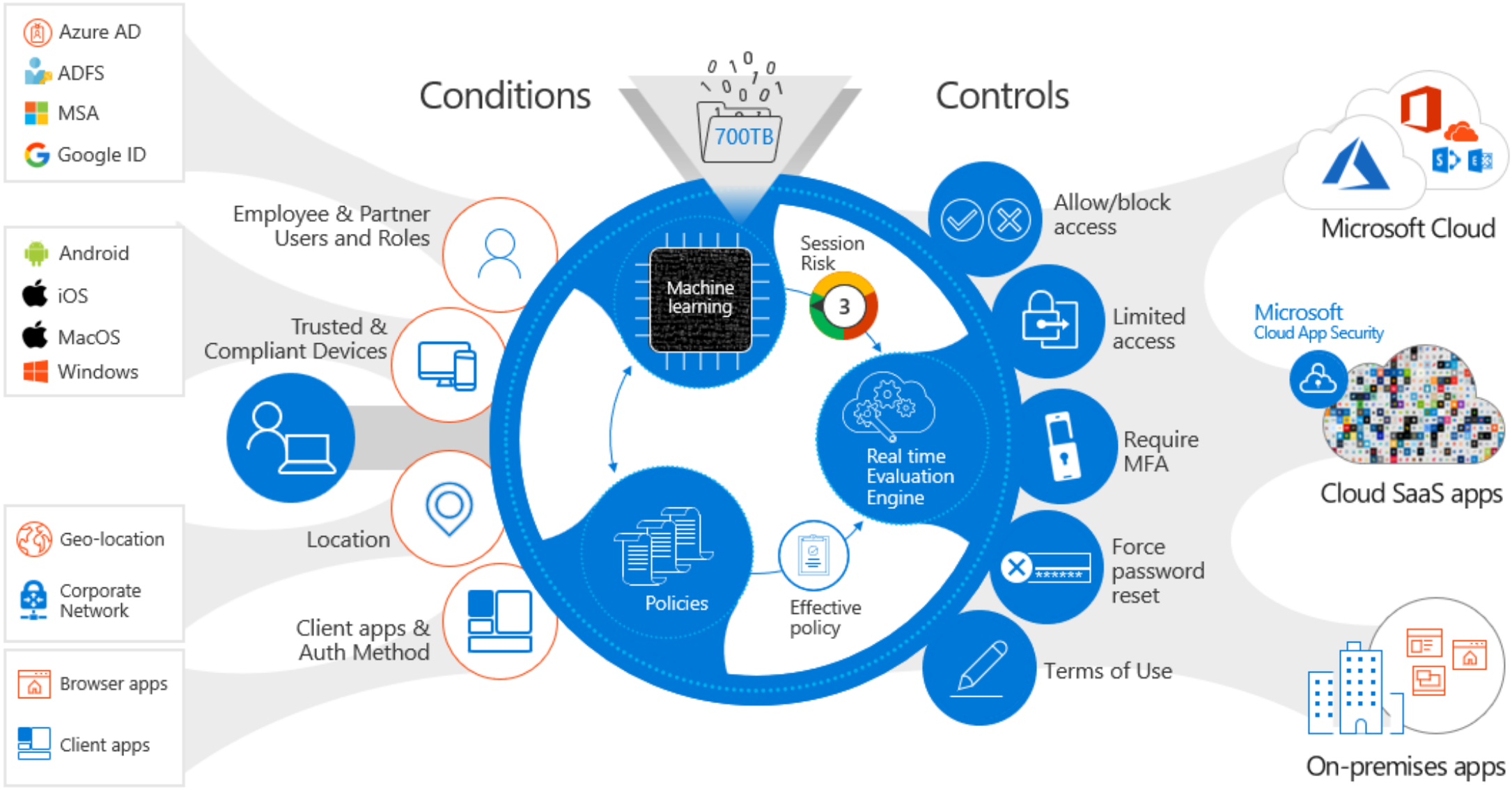
Modernize Conditional Access policies

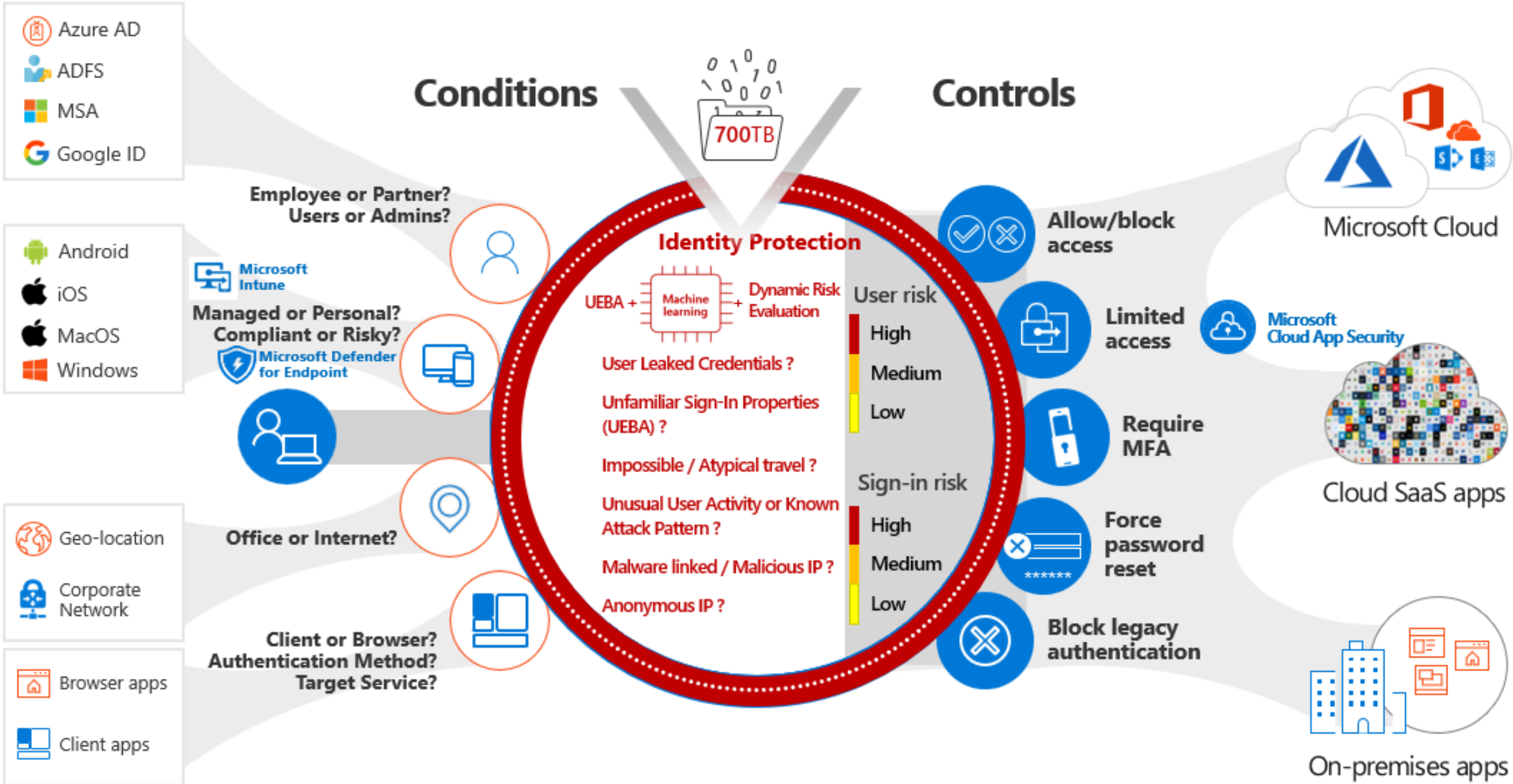
Authentication Methods

Bad: Password	**Good:** Password and...	**Better:** Password and...	**Best:** Passwordless
123456	SMS	Authenticator (Push Notifications)	Authenticator (Phone Sign-in)
qwerty	Voice	Software Tokens OTP	Window Hello
password		Hardware Tokens OTP (Preview)	FIDO2 security key
iloveyou			Certificates
Password1			

Introduction to ZT | ZT Principles + Architecture | 5 Zero Trust Steps | Go-Dos

Microsoft Conditional Access




Azure AD
ADFS
MSA
Google ID
Android
iOS
MacOS
Windows
Geo-location
Corporate Network
Browser apps
Client apps
Conditions
700TB
Employee or Partner?
Users or Admins?
Microsoft Intune
Managed or Personal?
Compliant or Risky?
Microsoft Defender for Endpoint
Office or Internet?
Client or Browser?
Authentication Method?
Target Service?
Identity Protection
UEBA +
Machine learning
+ Dynamic Risk Evaluation
User Leaked Credentials ?
Unfamiliar Sign-In Properties (UEBA) ?
Impossible / Atypical travel ?
Unusual User Activity or Known Attack Pattern ?
Malware linked / Malicious IP ?
Anonymous IP ?
User risk
High
Medium
Low
Sign-in risk
High
Medium
Low
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 apps

Modernize Conditional Access Policies

- Design an audience matrix with an established baseline
- Establish a naming convention

Policy Naming Prefix	Meaning
L	Lockdown
P	Privileged
A	All Accounts
G	Guests

Modernize Conditional Access Policies

- **Avoid** "**Block All Applications**" policy
- Classify applications – ensure every application is subject to at least one Conditional Access policy

Example 1

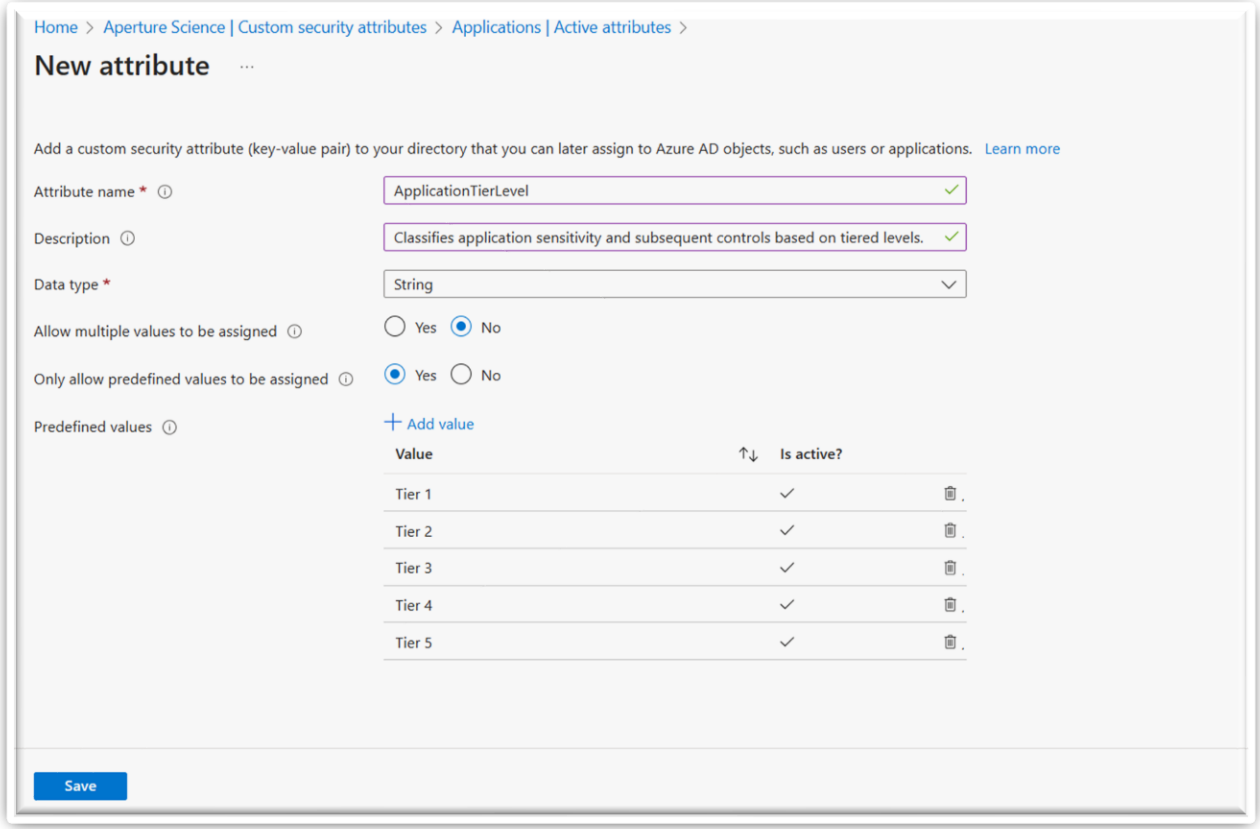
High Business Impact (HBI)
Medium Business Impact (MBI)
Low Business Impact (LBI)

Example 2

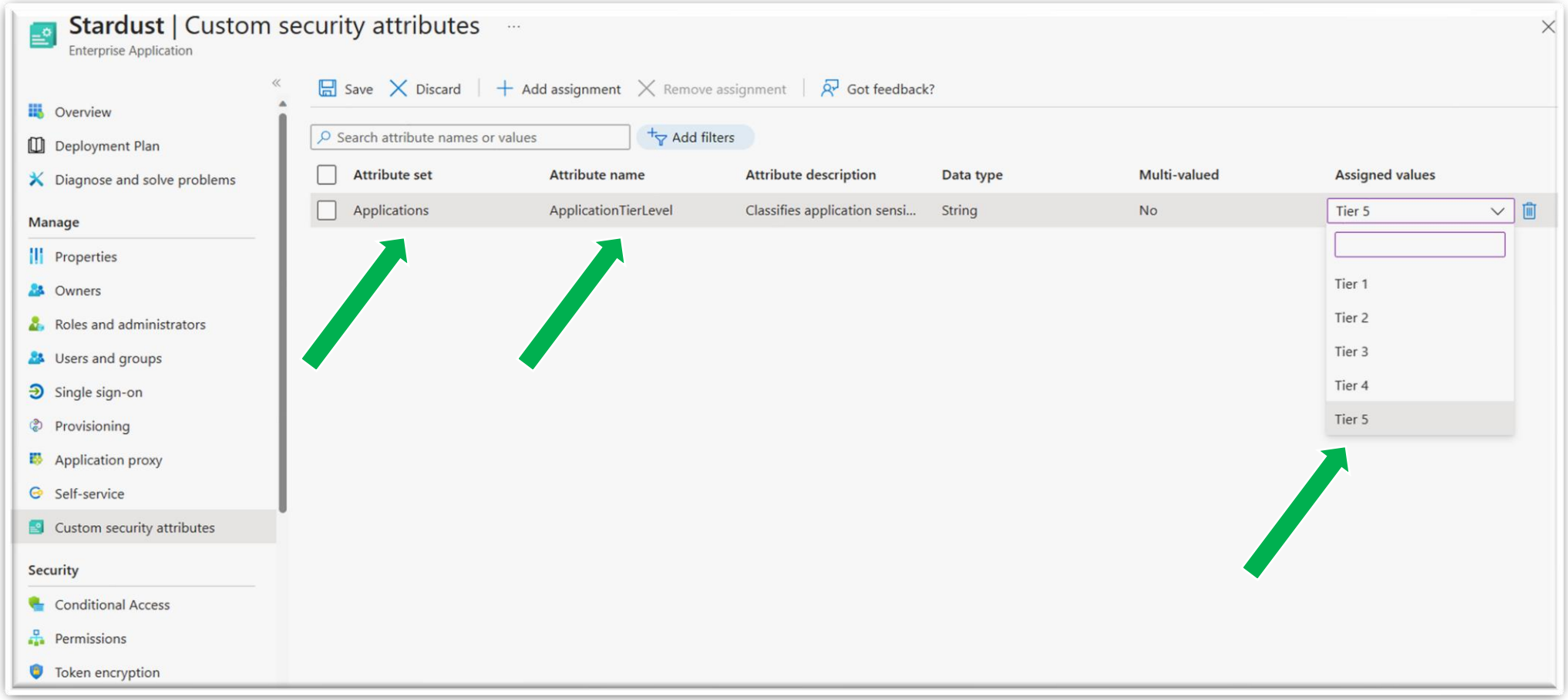
Tier 1
Tier 2
Tier 3
Tier 4
Tier 5

Dynamic App targeting in Conditional Access

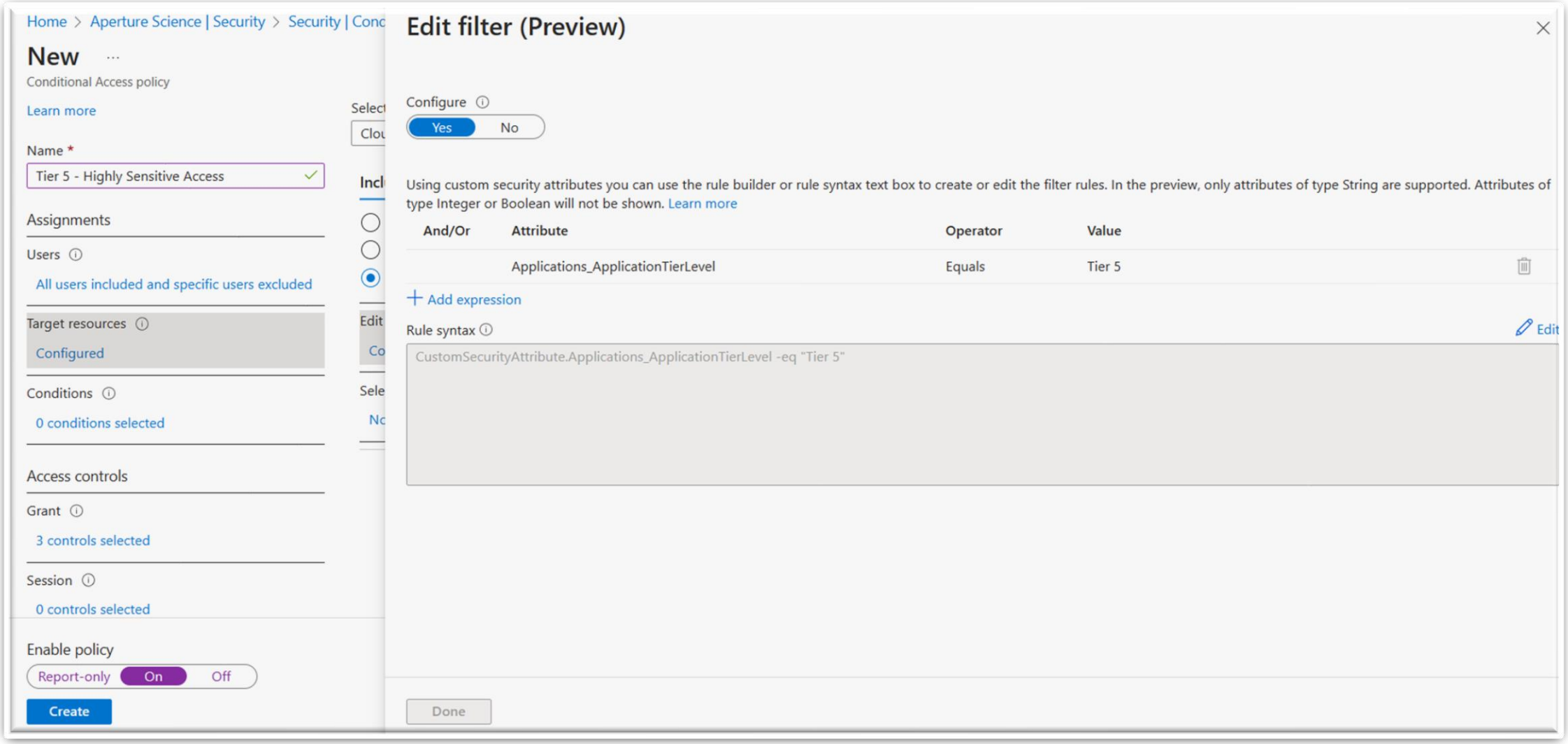
- Custom Security Attributes to dynamically target applications in Conditional Access



Dynamic App targeting in Conditional Access

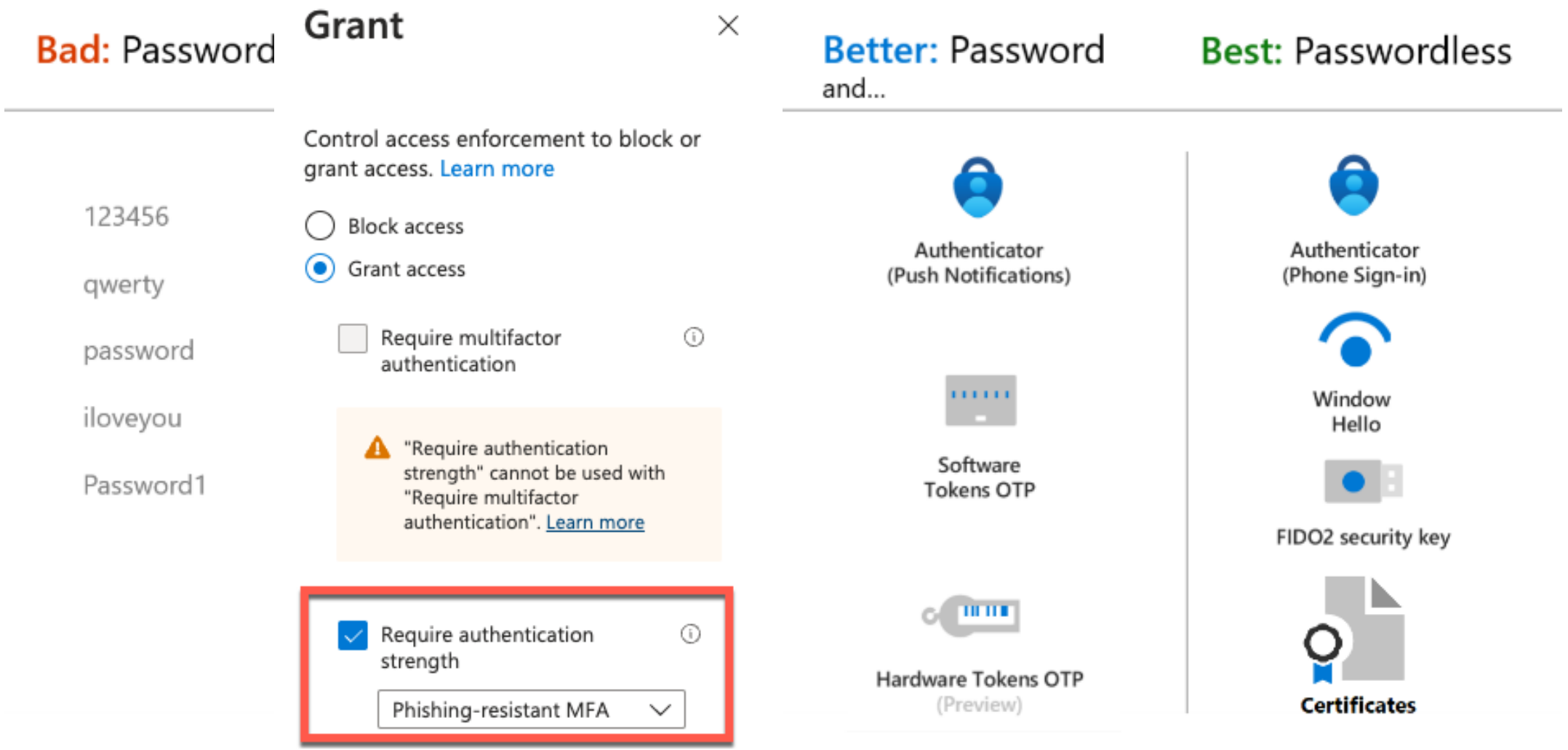


Dynamic App targeting in Conditional Access

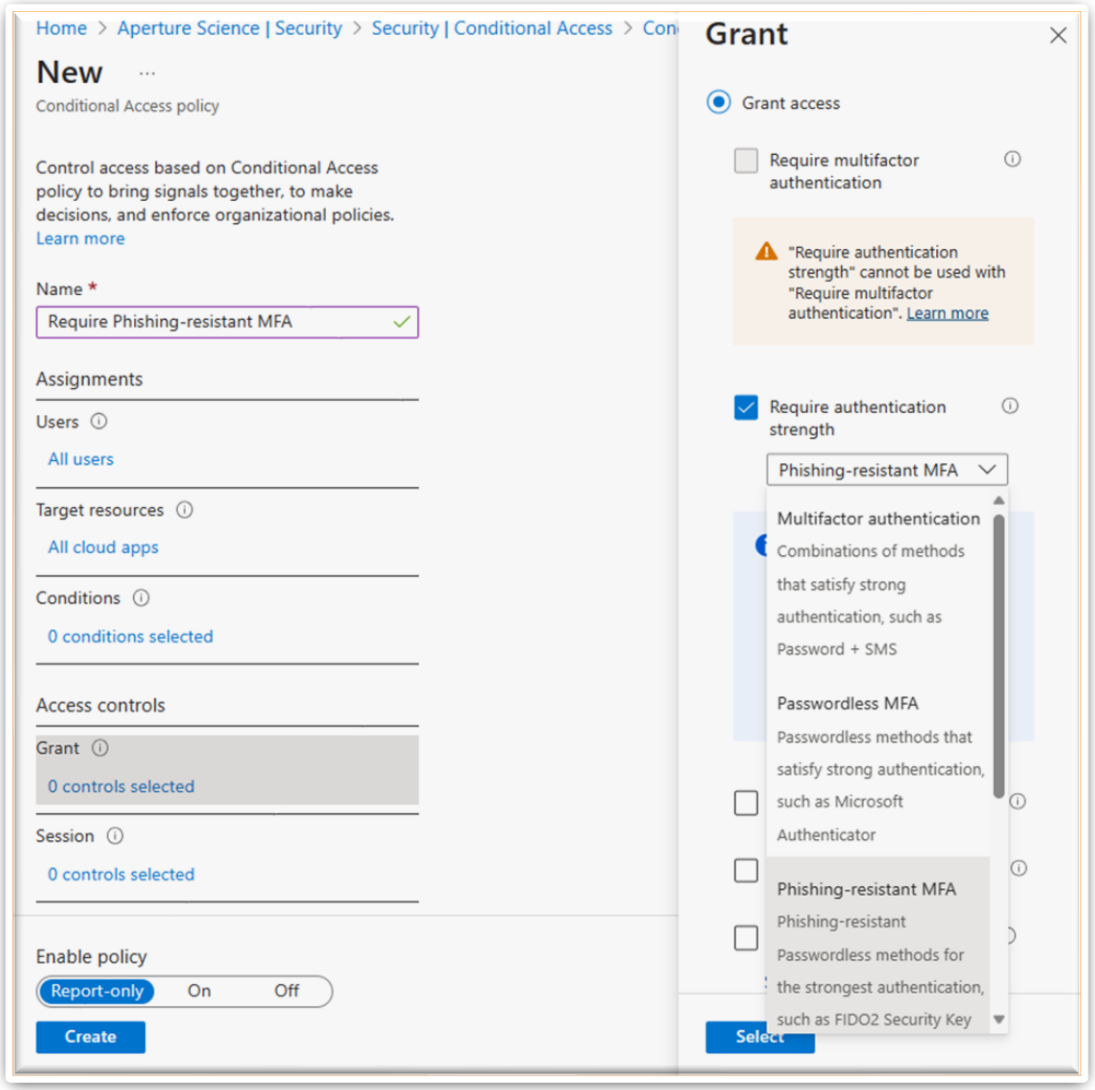


Introduction to ZT | ZT Principles + Architecture | 5 Zero Trust Steps | Go-Dos

Use Authentication Strengths



Use Authentication Strengths



Authentication method combination	MFA strength	Passwordless MFA strength	Phishing-resistant MFA strength
FIDO2 security key	✓	✓	✓
Windows Hello for Business	✓	✓	✓
Certificate-based authentication (Multi-Factor)	✓	✓	✓
Microsoft Authenticator (Phone Sign-in)	✓	✓	
Temporary Access Pass (One-time use AND Multi-use)	✓		
Password + something you have[1]	✓		
Federated single-factor + something you have[1]	✓		
Federated Multi-Factor	✓		
Certificate-based authentication (single-factor)			
SMS sign-in			
Password			
Federated single-factor			

Example Policy Set – Core Tier Policies

Policy	App Tier	Targeted Scenario	Controls Enforced
A001 – Tier1 Require ToU	1	Any type of access to Tier 1 applications	Must accept Terms of Use
A002 – Tier2 Require MFA	2	Any type of access to Tier 2 applications	Require any type of MFA
A003 – Tier3 Zero Trust Passwordless	3 (Default)	Any type of access to Tier 3 applications	Require Stronger Auth Strength (no SMS or Voice MFA)
A004 – Tier3 Zero Trust Device State	3 (Default)	Any type of access to Tier 3 applications	Require compliant device or require Hybrid Azure AD Joined device
A005 – Tier4 Zero Trust Compliant + Phish Resistant	4	Any type of access to Tier 4 applications	Require compliant device and *phishing-resistant* Auth Strength
A006 – Tier5 Zero Trust Compliant + Phish Resistant	5	Any type of access to Tier 5 applications	Require compliant device and *phishing-resistant* Auth Strength
A007 – Tier5 PAW	5	Any type of access to Tier 5 applications	Block access unless the user is on a Privileged Access Workstation
A008 – Tier5 Trusted Network	5	Any type of access to Tier 5 applications	Block access unless the user is on a trusted network

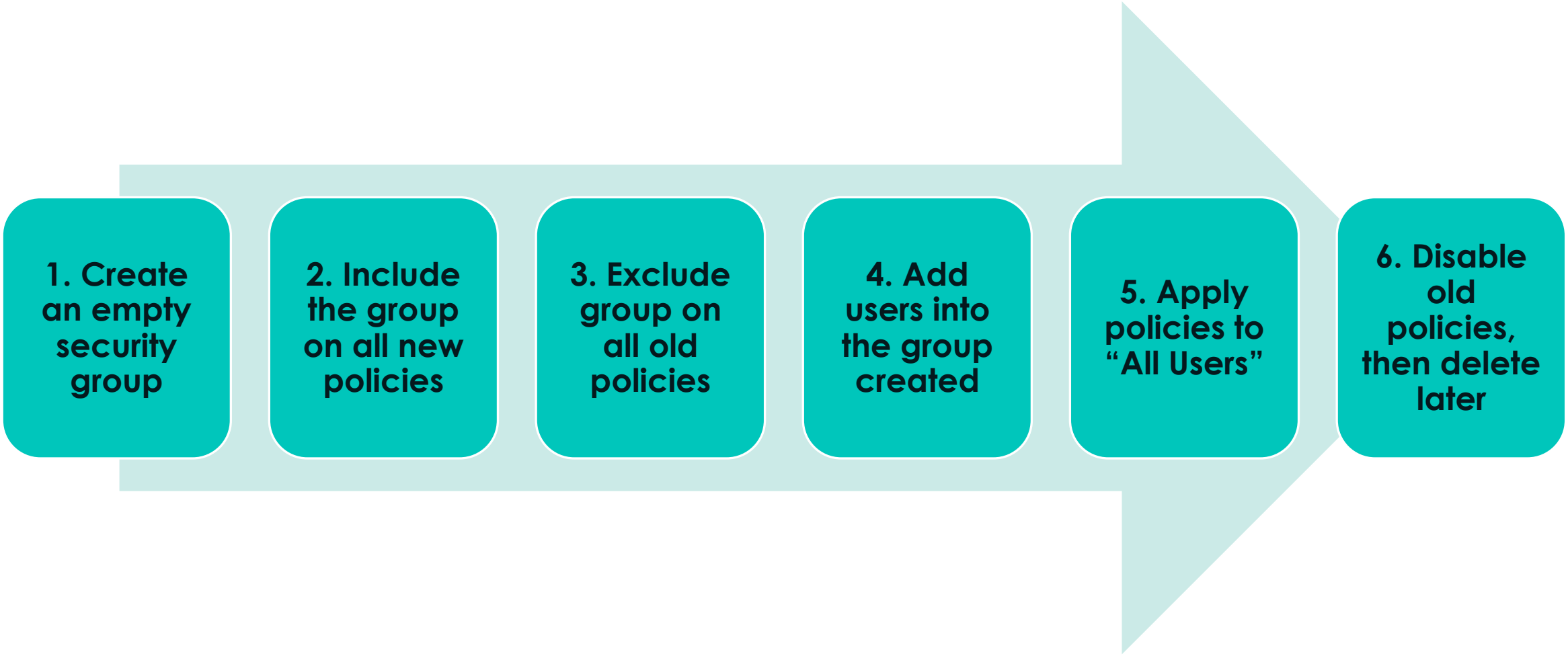
Example Policy Set – Specialty Policies

Policy	App Tier	Targeted Scenario	Controls Enforced
A009 – Interactive MFA for Intune Enrollment	n/a – Intune Enrollment app only	Require user-interactive MFA to enroll a device in Intune	MFA, Sign-In Frequency require interactive authentication
A010 – MFA to Register/Join Device	n/a	Require MFA to AAD Register or AAD Join a device to Azure AD	MFA
A011 – Tier2/3/4/5 App Access SIF on Unmanaged Devices	2, 3, 4, 5	Any type of access from an unmanaged device to Tier 2-5 apps	Sign-In Frequency maximum session lifetime of 12 hours
A013 – Tier4/5 Block Guests	4, 5	Any access to Tier 4 or 5 apps by a guest user	Block
G001 – Guests Require MFA	All	Any access to any app by a guest user	MFA
L001 – Block Untrusted Locations	All	Any access from countries you do not do ANY business in, such as sanctioned countries	Block
L002 – Block Legacy Authentication	All	Any access using legacy authentication	Block
W001 – Block Medium and High Risk Workload Identities	All	Any access by a workload identity identified as Medium or High Risk	Block

Example Policy Set – Admin and Risk Policies

Policy	App Tier	Targeted Scenario	Controls Enforced
P001 – Admins Compliant + Phish Resistant	n/a	Any access by an Azure AD administrator role holder	Require compliant device and *phishing-resistant* MFA
P002 – Admins Compliant + Phish Resistant for Admin Actions	n/a	Any sensitive operation carried out by an administrator	Require compliant device and *phishing-resistant* MFA
R001 – MFA Sign In Risk	All	Any sign in categorized by Identity Protection as Low, Medium, or High Risk	MFA, Sign-In Frequency require interactive authentication
R002 – PWD Change High User Risk	All	Any access by a High Risk user	Require secure password change, Sign-In Frequency require interactive authentication

Conditional Access Migration Strategy



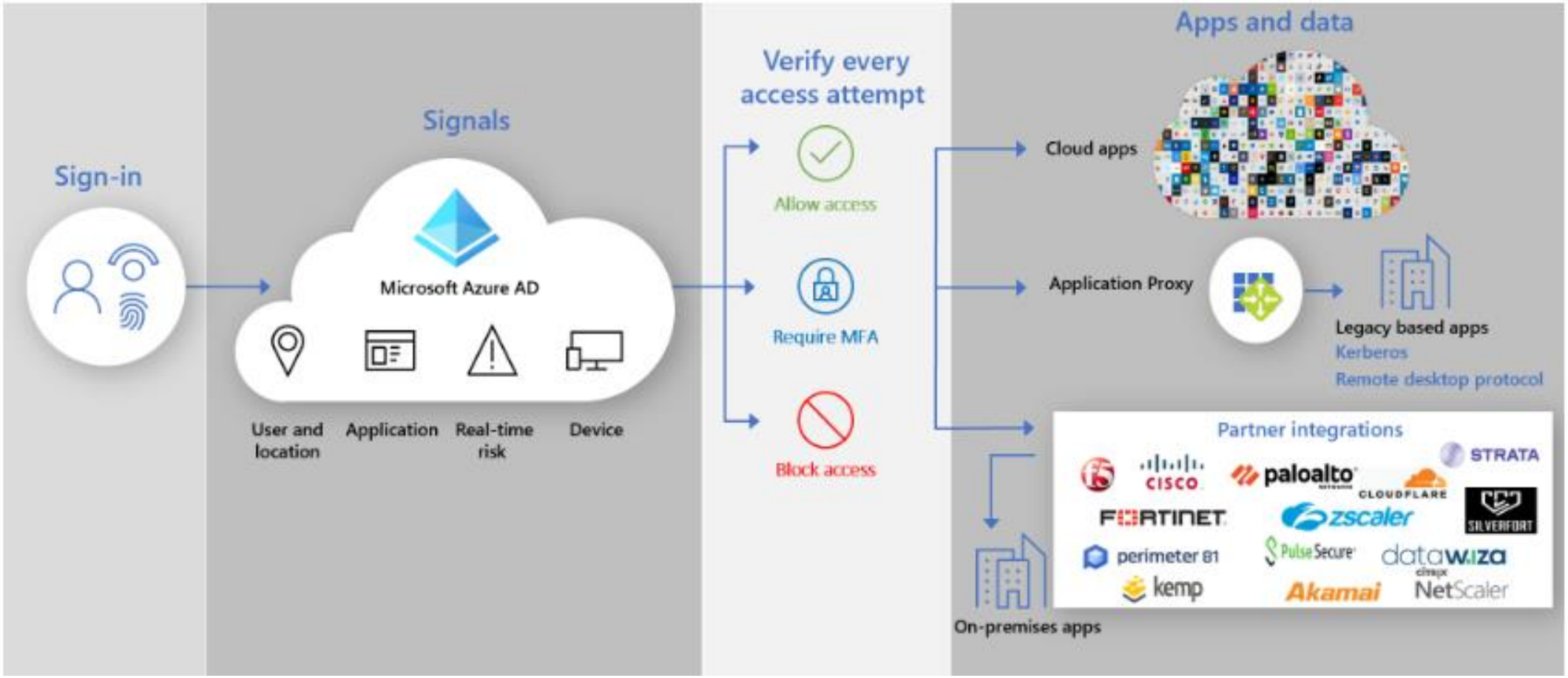
2. Integrate Applications

Integrate SaaS + On-prem applications with Entra ID

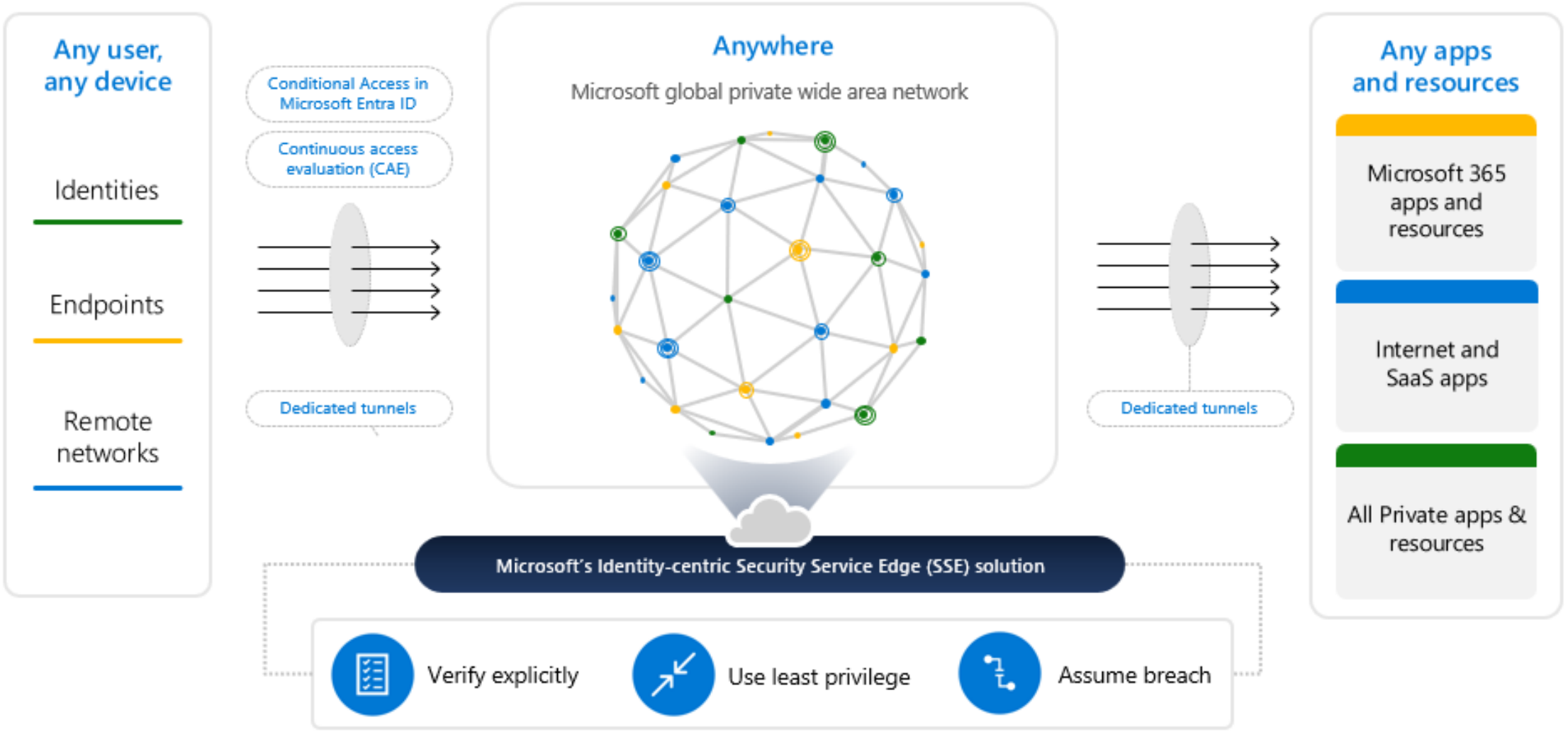
Protect applications with Microsoft Defender for Cloud Apps

Protect application data with Microsoft Purview

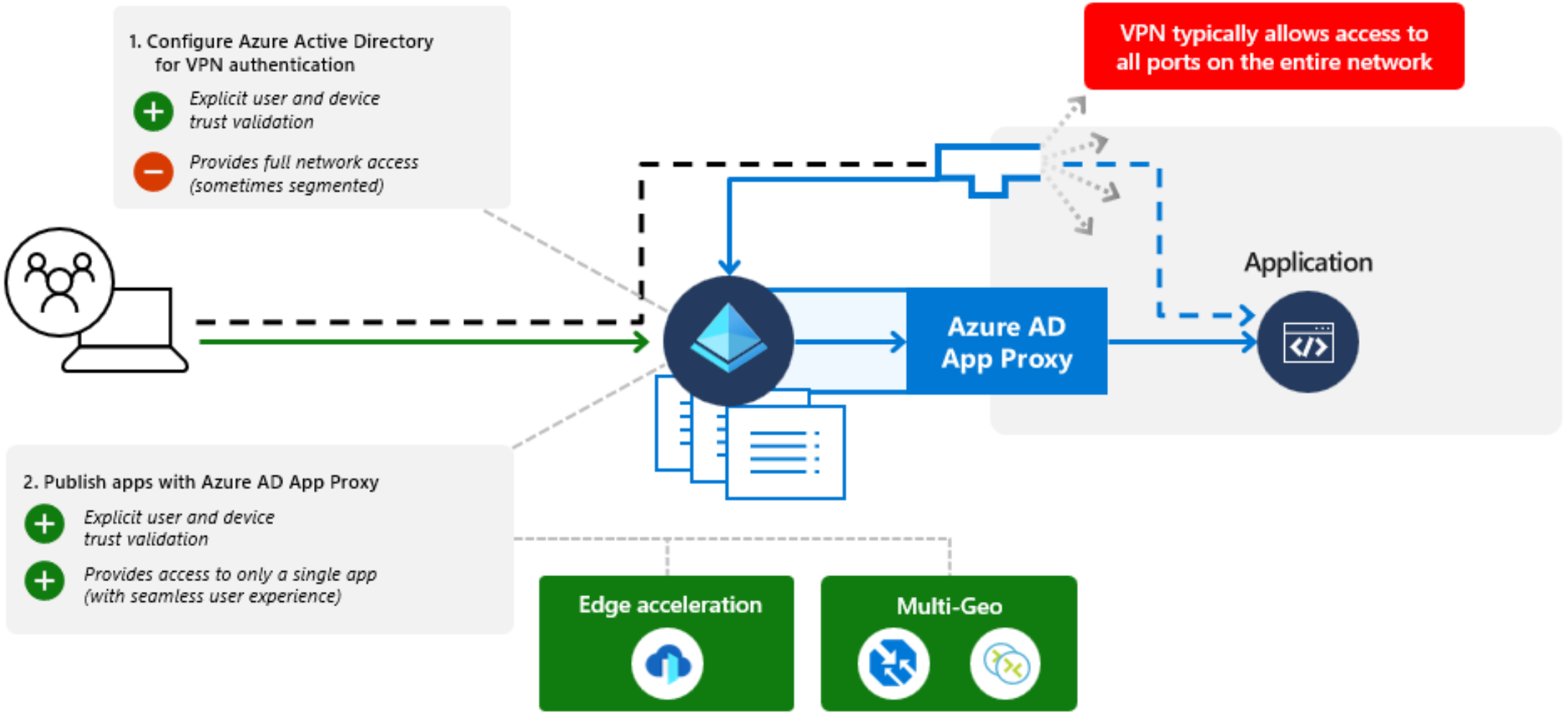
Integrate SaaS and On-prem Applications



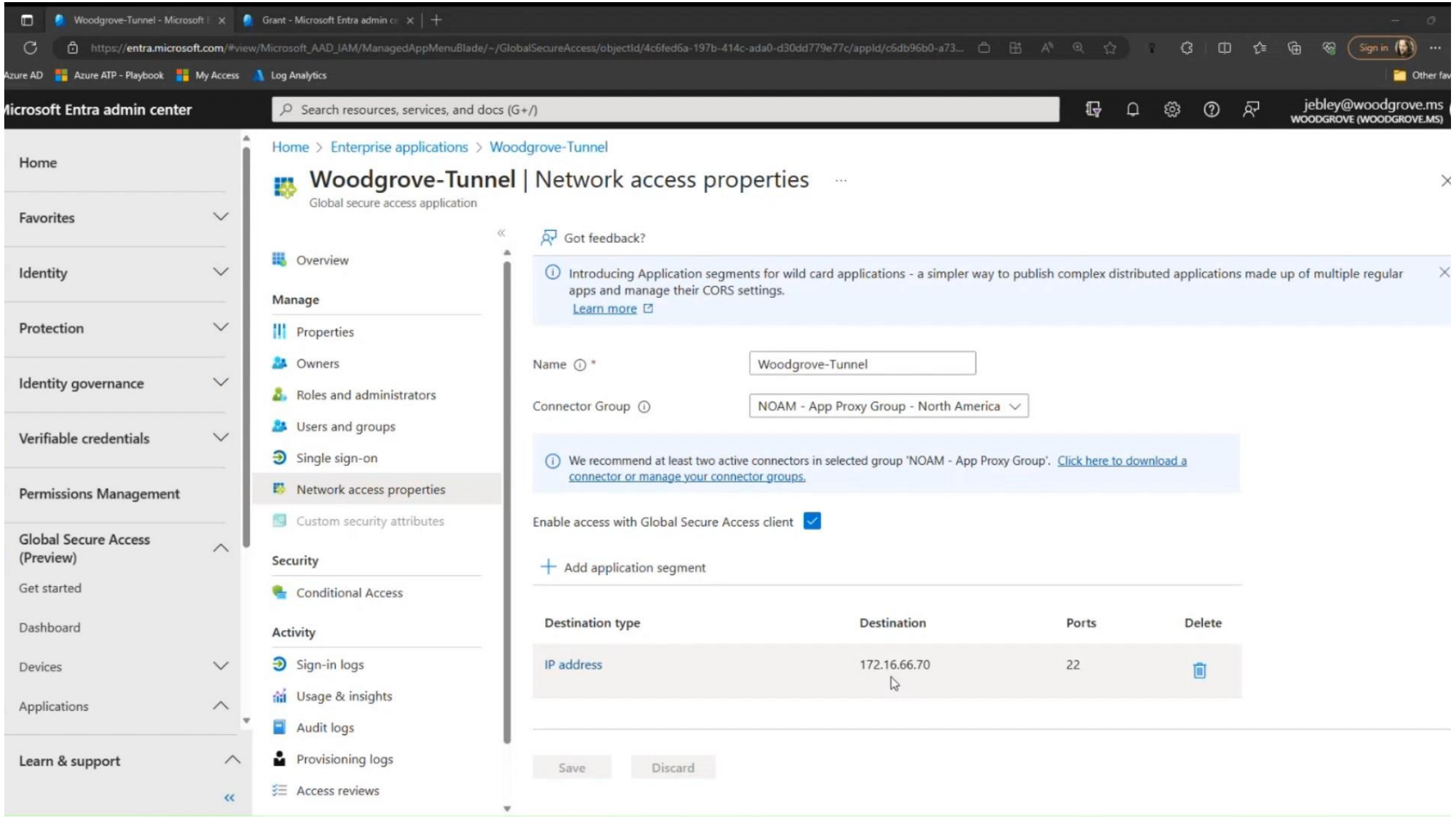
Microsoft's Identity-centric SSE solution



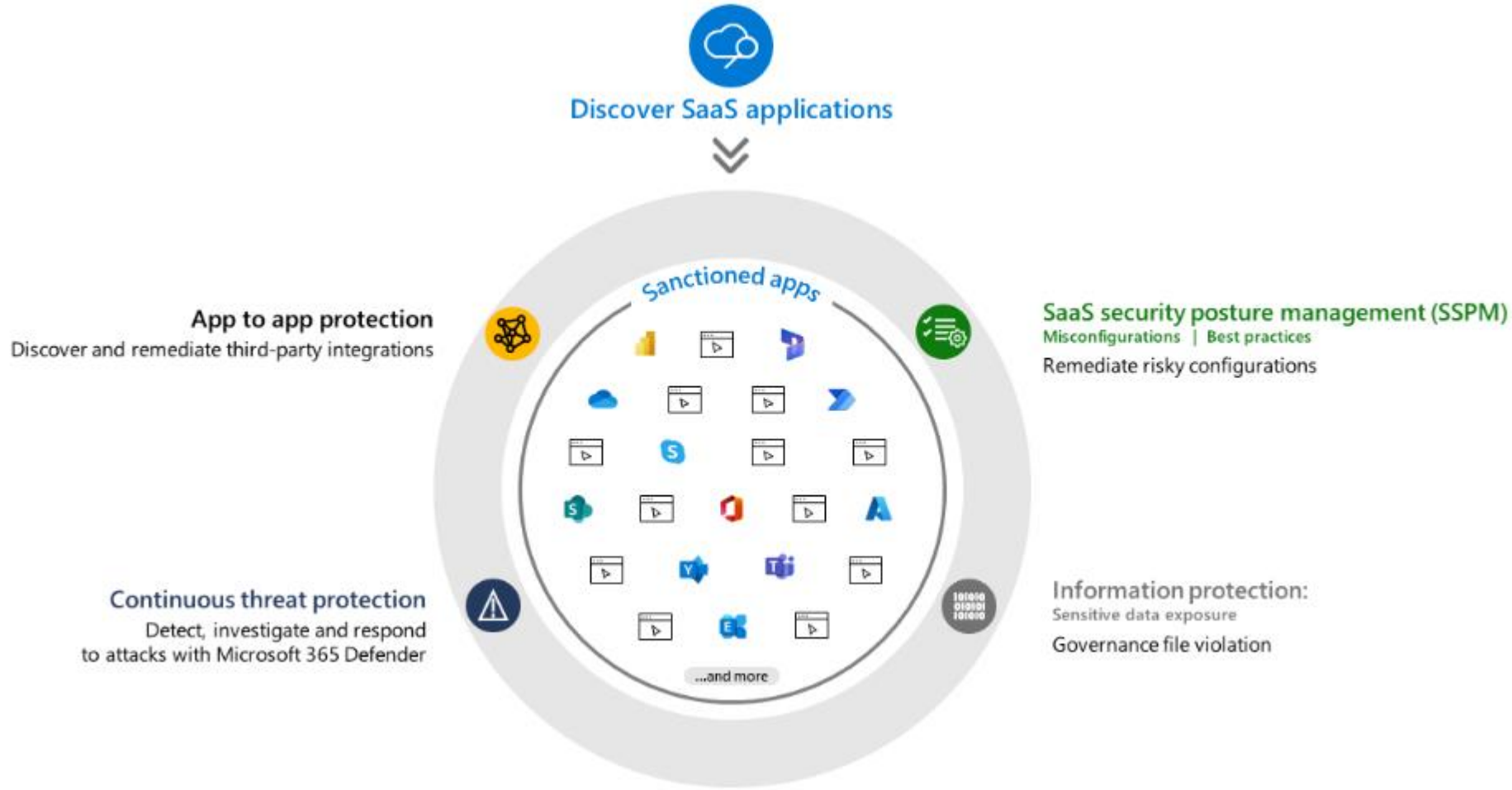
Microsoft's Identity-centric SSE solution



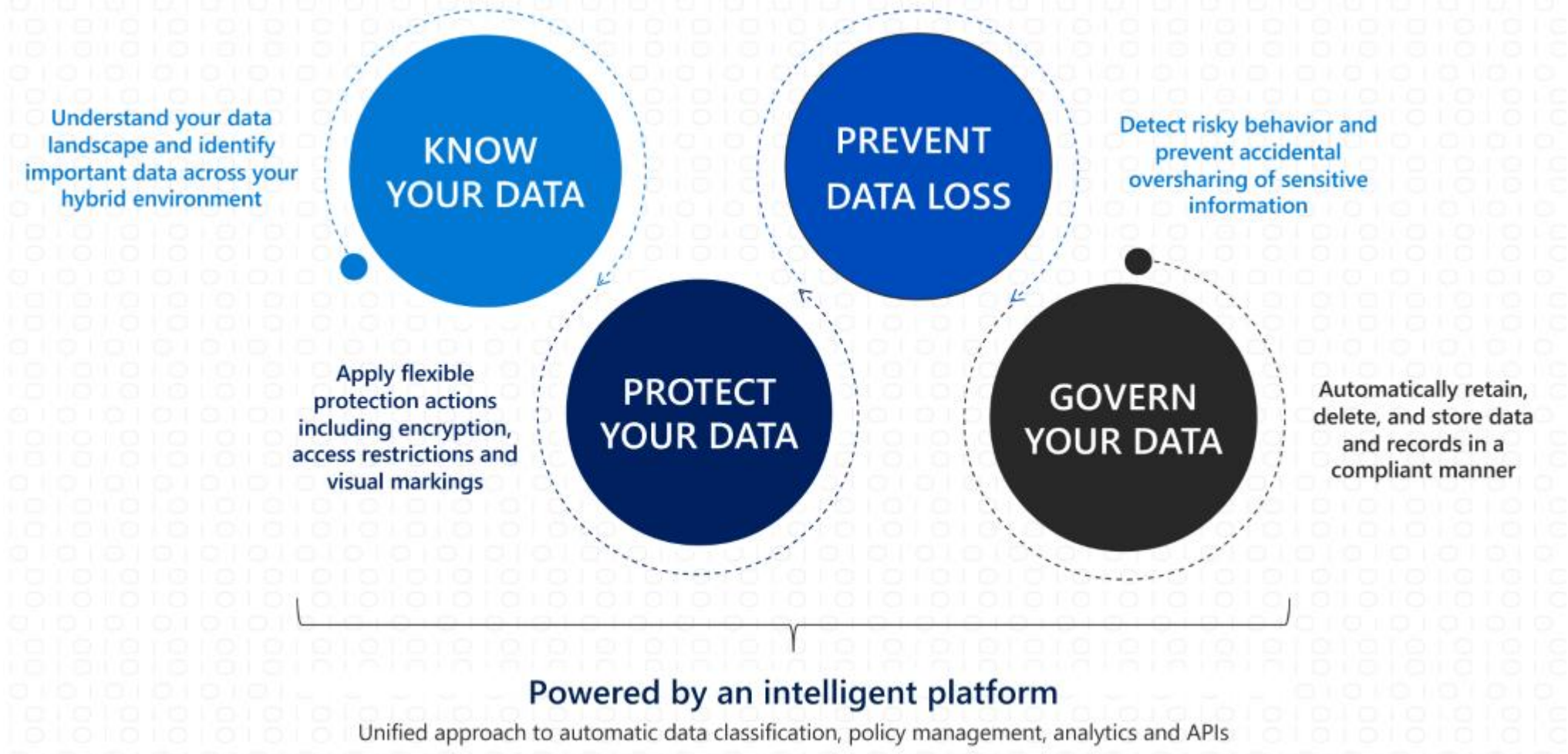
Microsoft Entra Private Access Demo



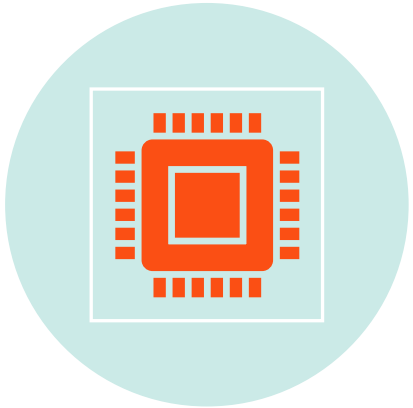
Microsoft Defender for Cloud Apps



Microsoft Purview



3. Adopt Least Privilege



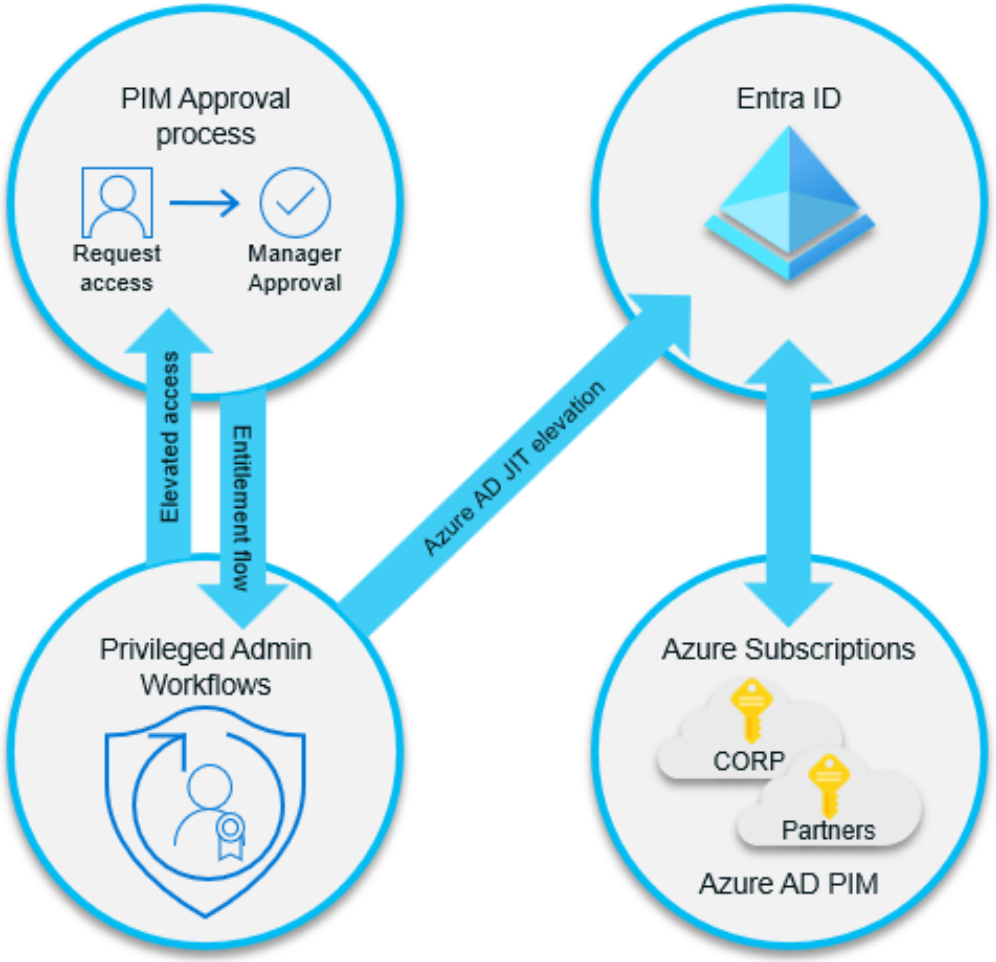
Minimize user access with Just-In-Time and Just-Enough Access (JIT/JEA)

Leverage Privileged Identity Management

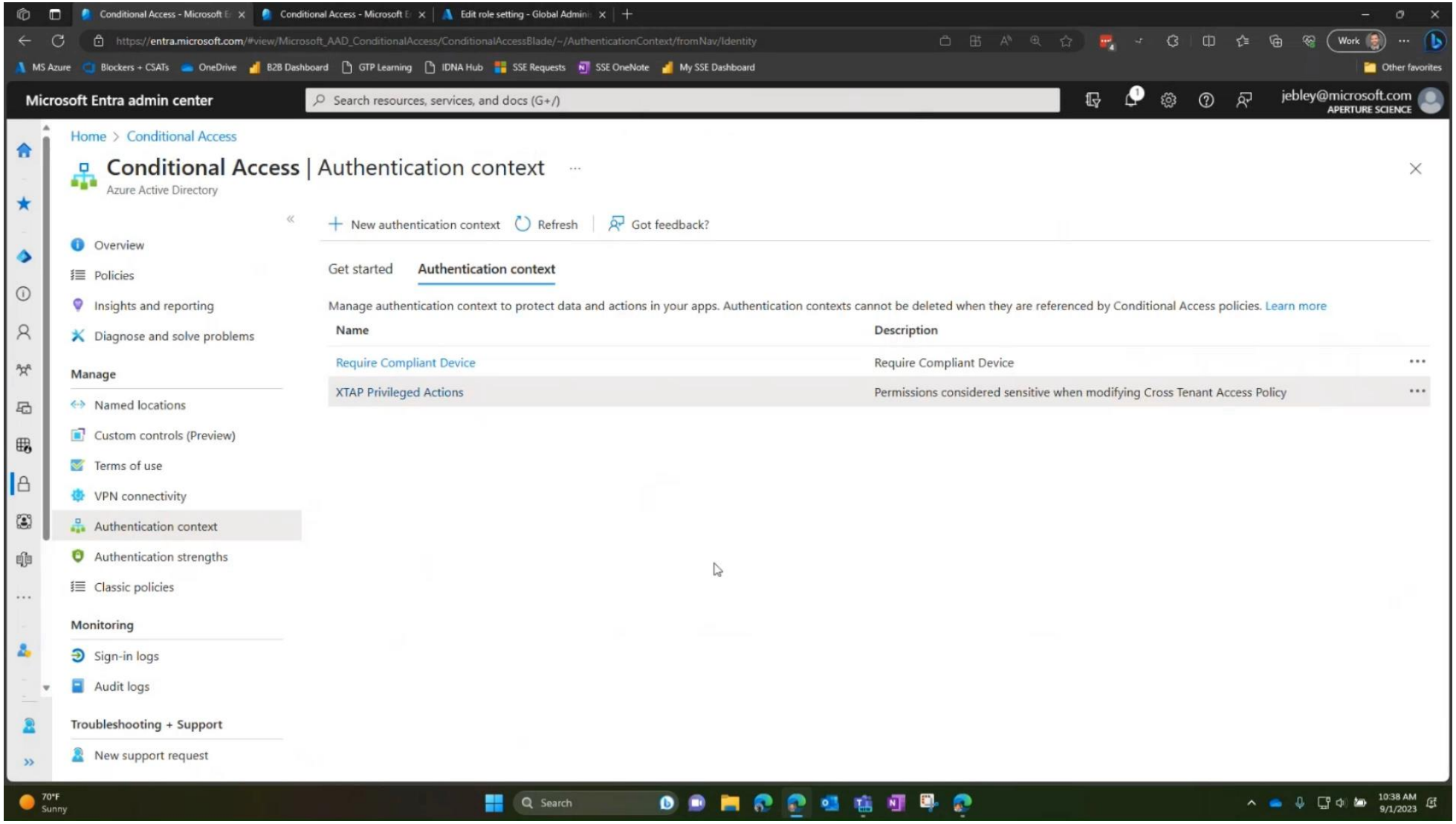
Leverage Entra Permissions Management

Privileged Identity Management (PIM)

- Privilege Management at Scale
  - Leverage JIT/JEA controls for Tier 0 roles, expand to other roles as well
- No Persistent Elevated Access
  - Do not allow persistent elevated access on-premises or in the cloud
- Reduce Surface Area
  - Significantly lower blast radius if identity is compromised



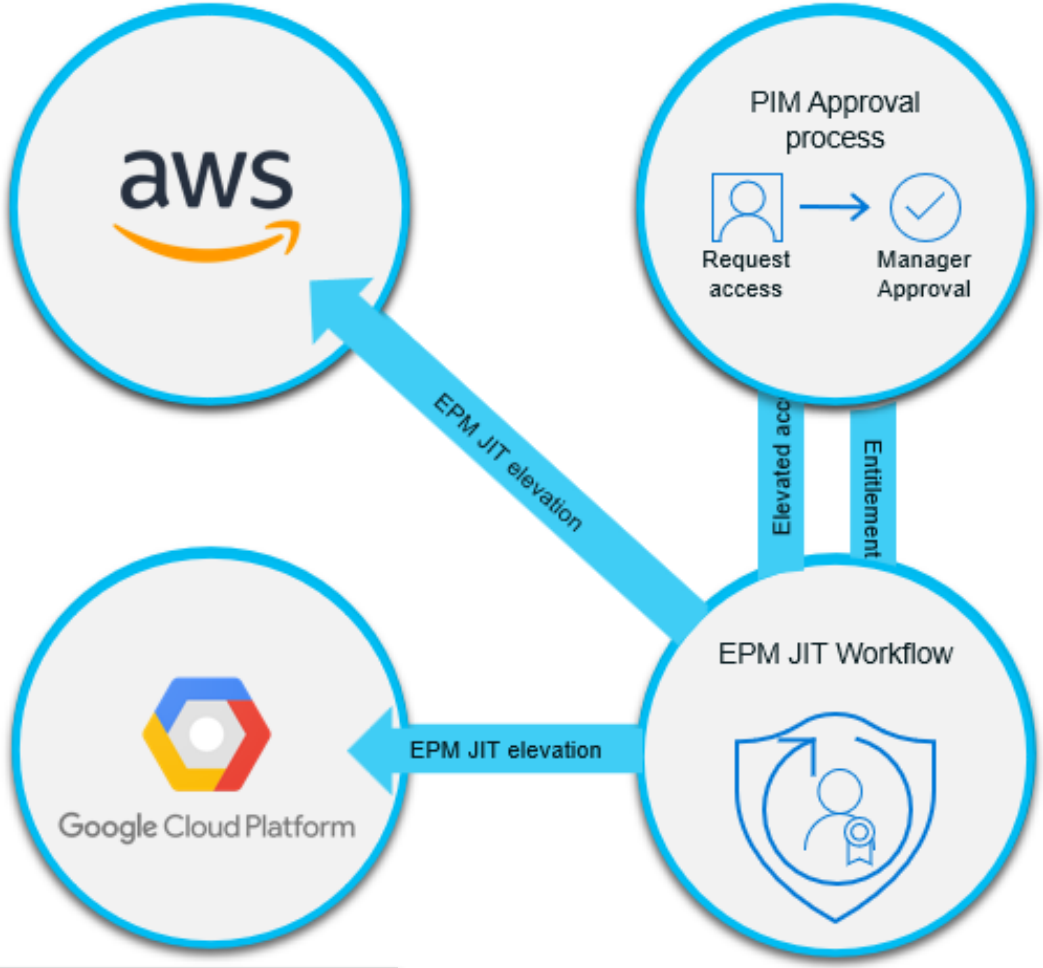
PIM + Conditional Access Demo



Entra Permissions Management (EPM)

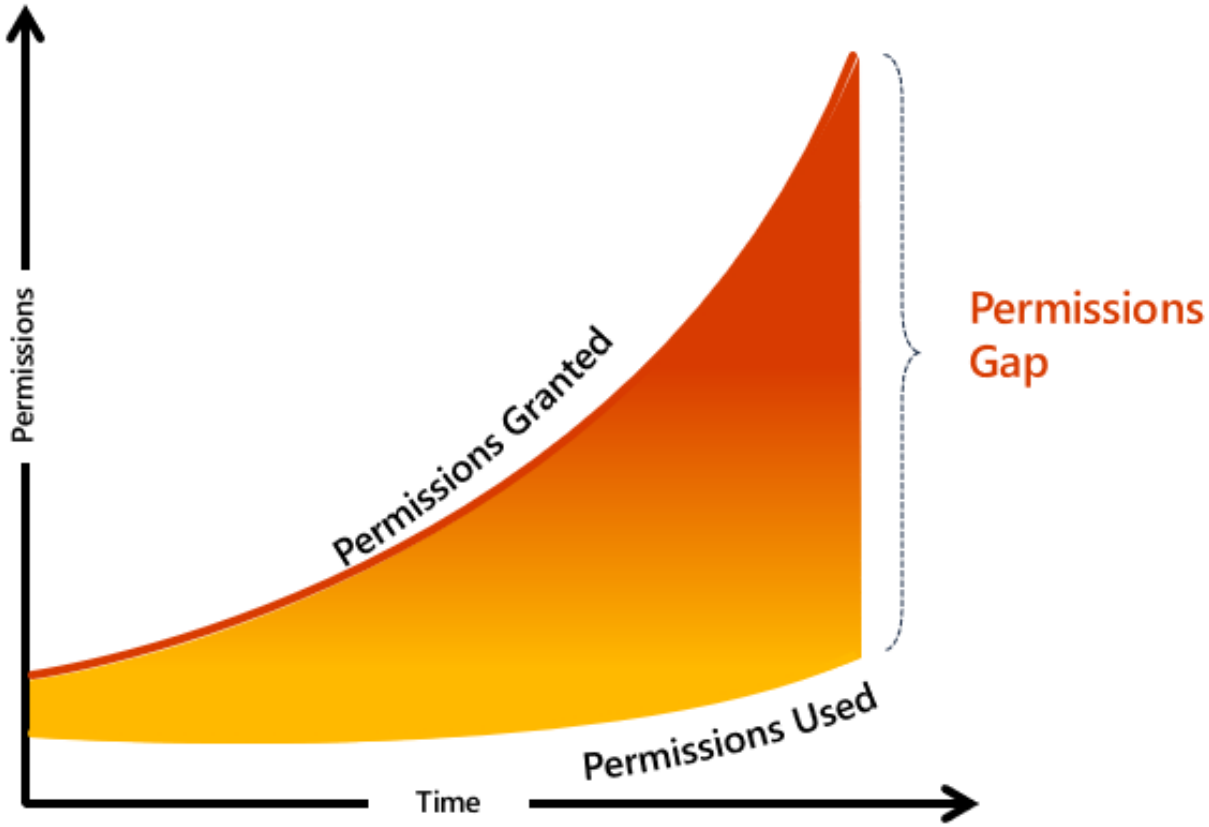
Managing permissions across multi-cloud environments requires *a new, dynamic approach*

- Grant permissions based on historical usage and activity
- Allow temporary access to high-risk permissions on-demand
- Continuously monitor and right-size identities to prevent privilege creep



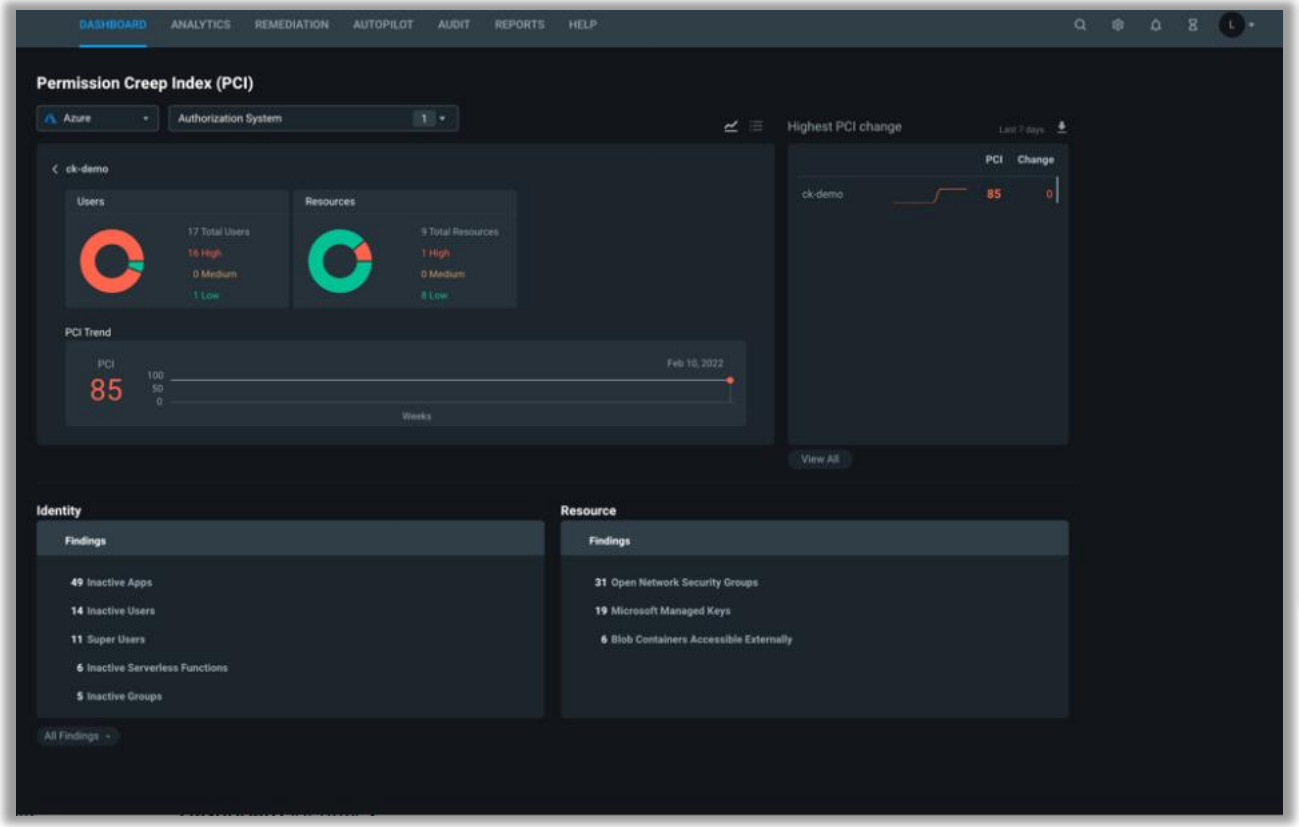
Introduction to ZT | ZT Principles + Architecture | 5 Zero Trust Steps | Go-Dos

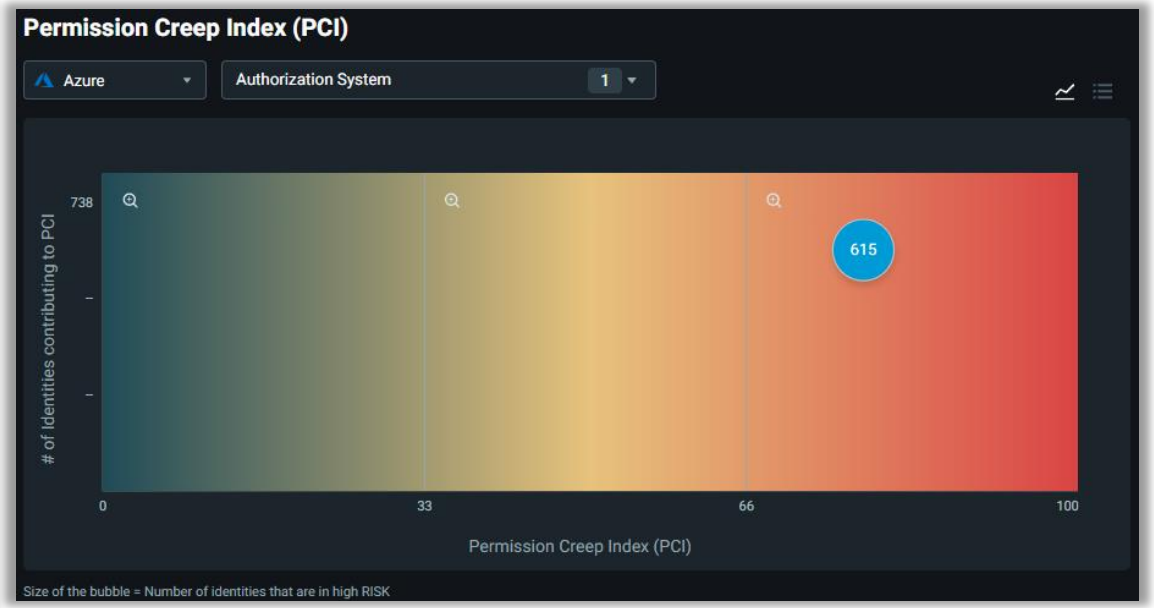
Permissions creep



- Lack of comprehensive visibility into identities, permissions and resources
- Increased complexity for IAM and security teams to manage permissions across multicloud environments
- Increased risk of breach from accidental or malicious permission mis-use

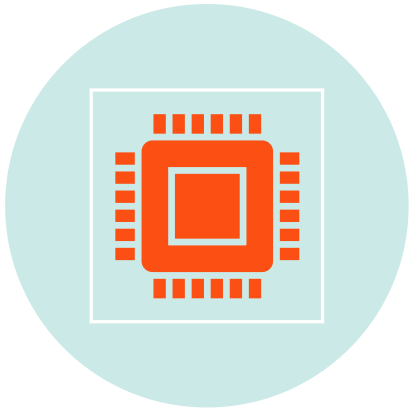
Entra Permissions Management (EPM) Portal





Introduction to ZT | ZT Principles + Architecture | 5 Zero Trust Steps | Go Do's

4. Strengthen Endpoints

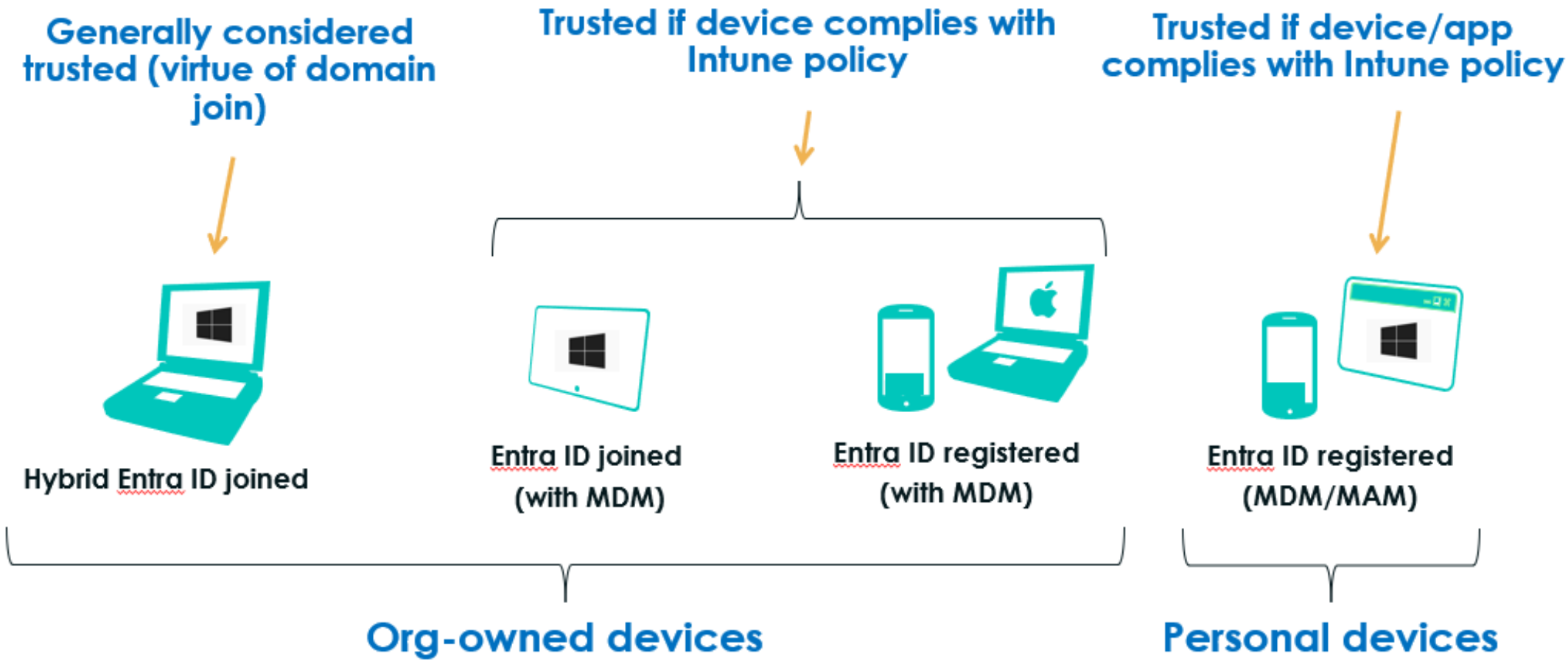


Migrate to Entra ID joined devices

Manage devices with an MDM

Enhance device security with Microsoft Defender for Endpoint

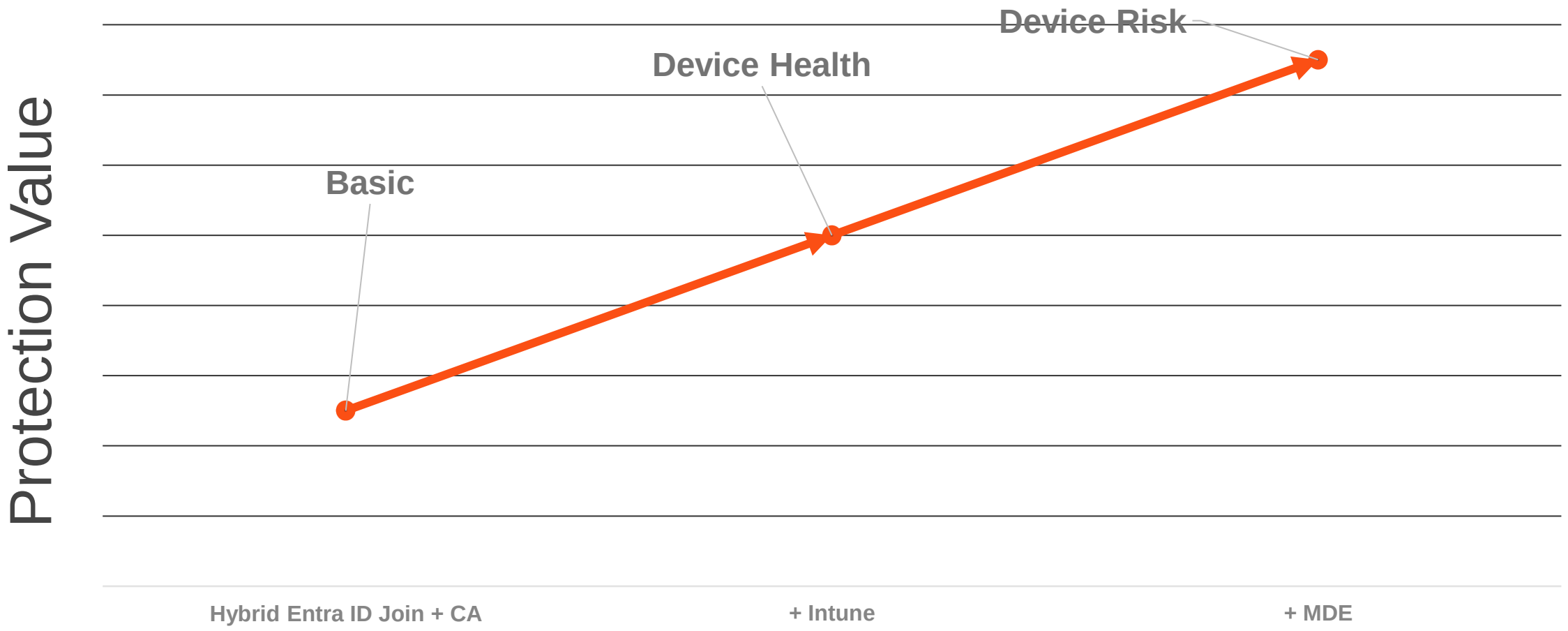
Device States in Entra ID



Migrate from HEIDJ to EIDJ devices

- Decouple device management requirements from needing line-of-sight to Domain Controllers
  - E.g. Password changed in Entra ID, but I need the local cached password to update
- Simplify modern device deployment (aka Autopilot)
  - Out-of-the-box enroll in MDM and setup Windows Hello for Business
- Better security posture
  - EIDJ + MDM > HEIDJ

Stages of Device-based Conditional Access



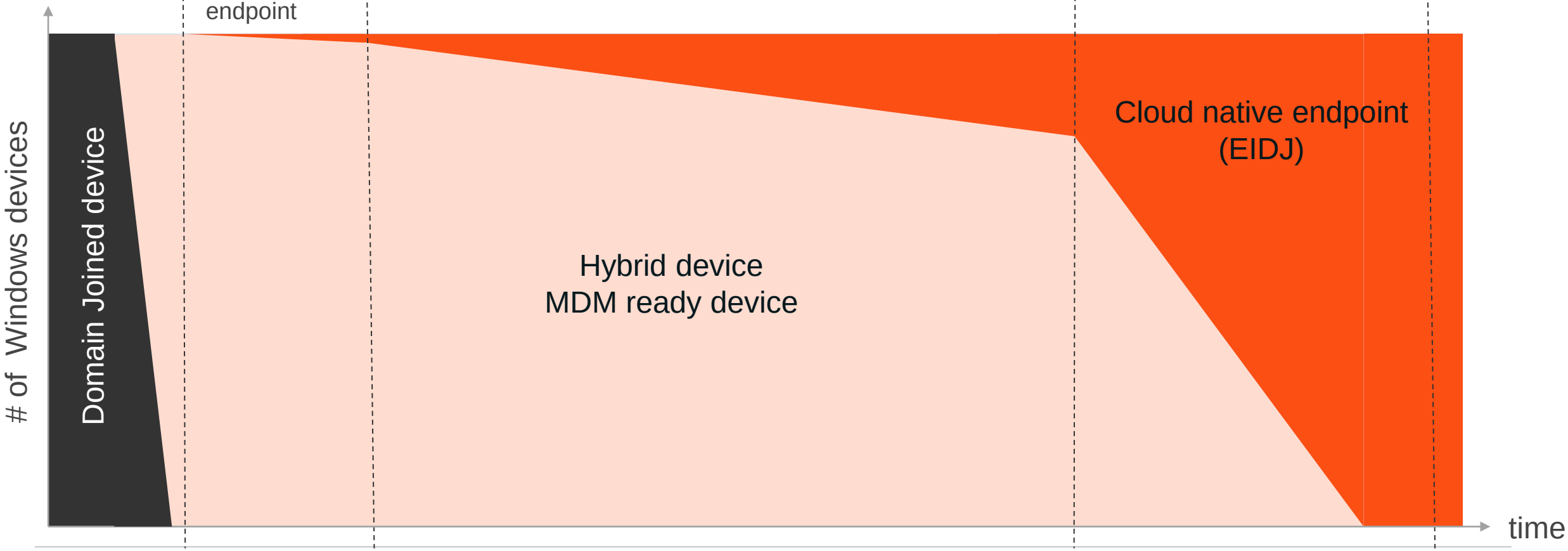
Device States in Entra ID

Ph0: Prep
Prep pilot, HEIDJ existing devices

Ph1: Pilot
Small group starts using cloud native endpoint

Ph2: Scale deployment
New device for all users gets EIDJ (aka no more Domain Join)

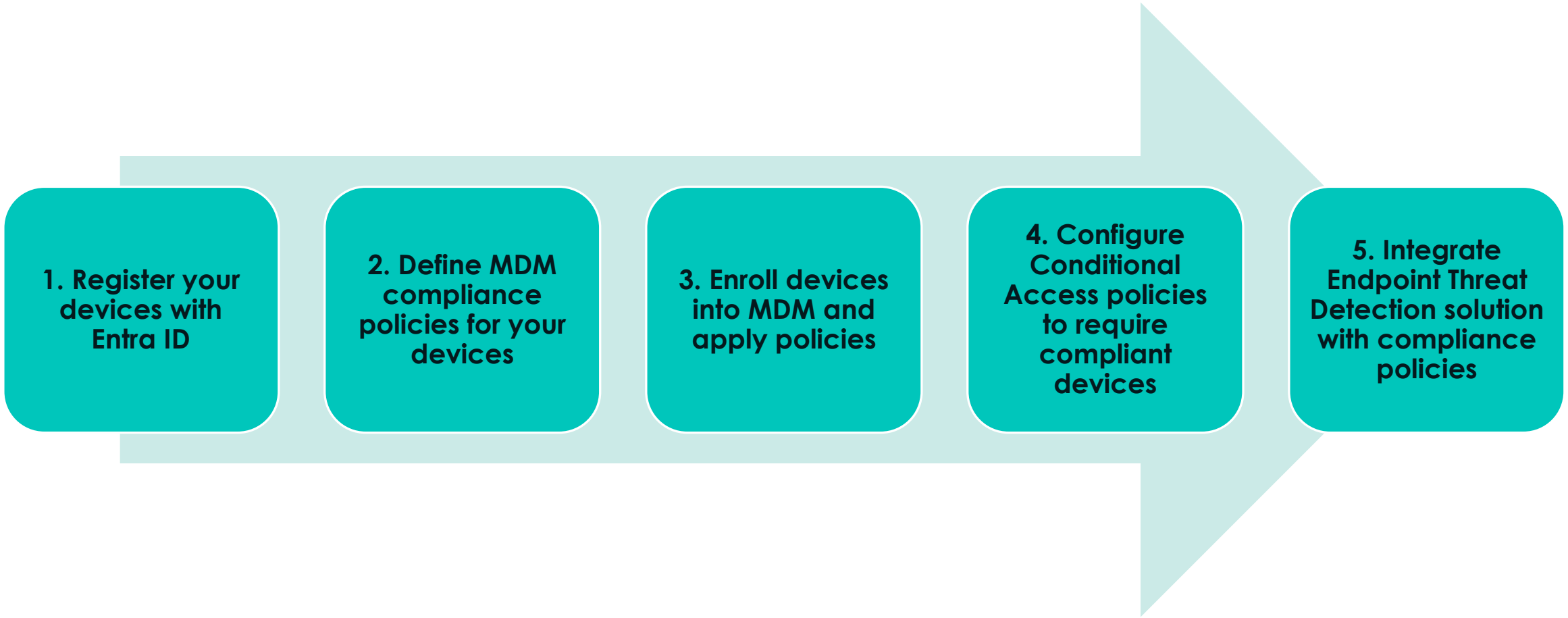
Ph3: (optional) Velocity migration
Convert existing DJ/HEIDJ devices to EIDJ via reset



Common Migration “Gotchas”

- GPO transition – one of the more challenging aspects of the migration
  - Need to move all policy and management to the MDM, leverage Intune Group Policy analytics
- “My users can’t SSO to on-premises resources, like printers and file shares”
  - Common perception, but its not true!
  - SSO to on-premises works for both password and Windows Hello for Business
  - Learn how it works at https://aka.ms/EIDJonpremSSO

Strengthen Devices Strategy



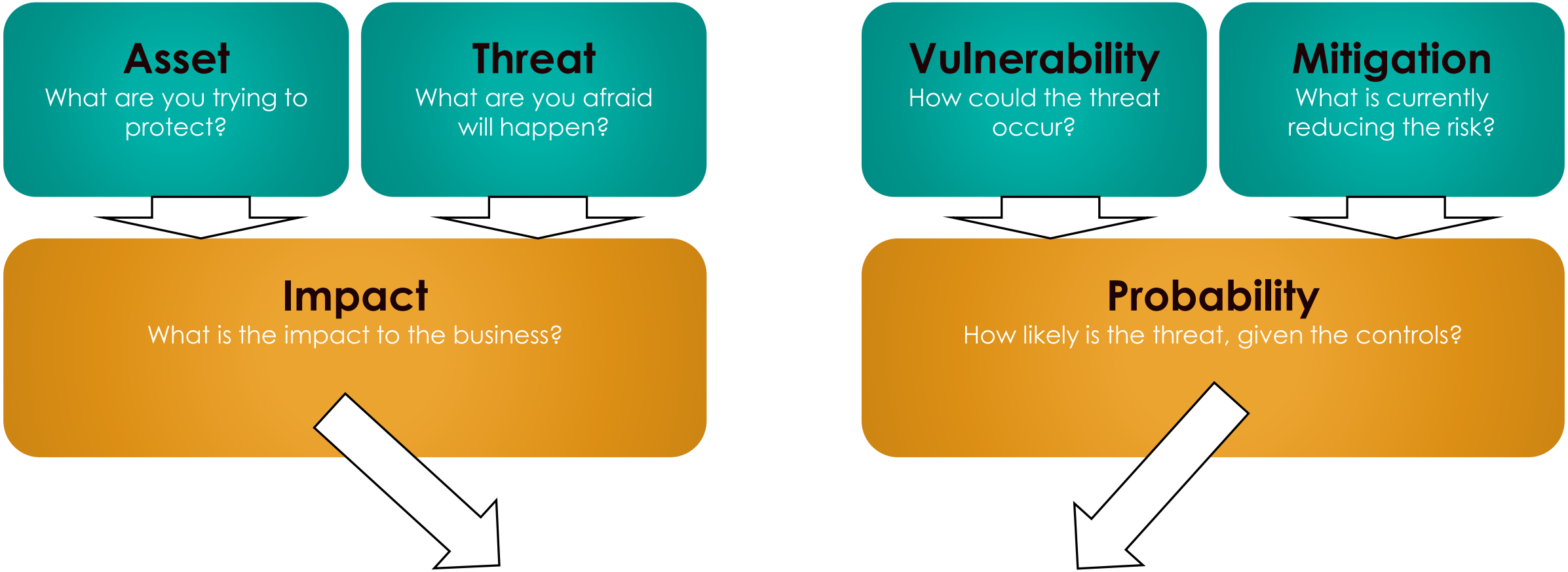
5. Use your Log Data

Establish a baseline of normal behavior in your environment

Leverage Microsoft Sentinel

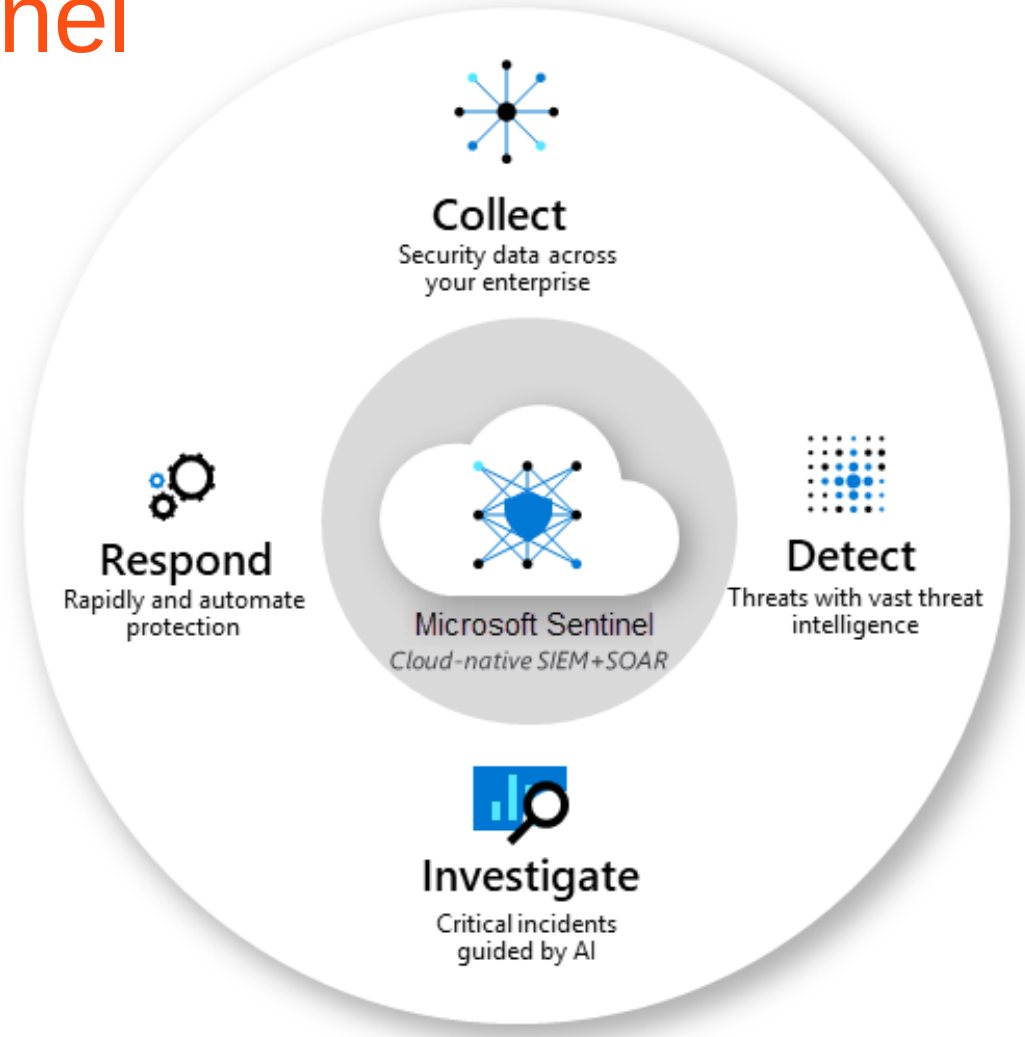
Read our SecOps Guide: aka.ms/aadsecopsguide

Prioritize based on risk

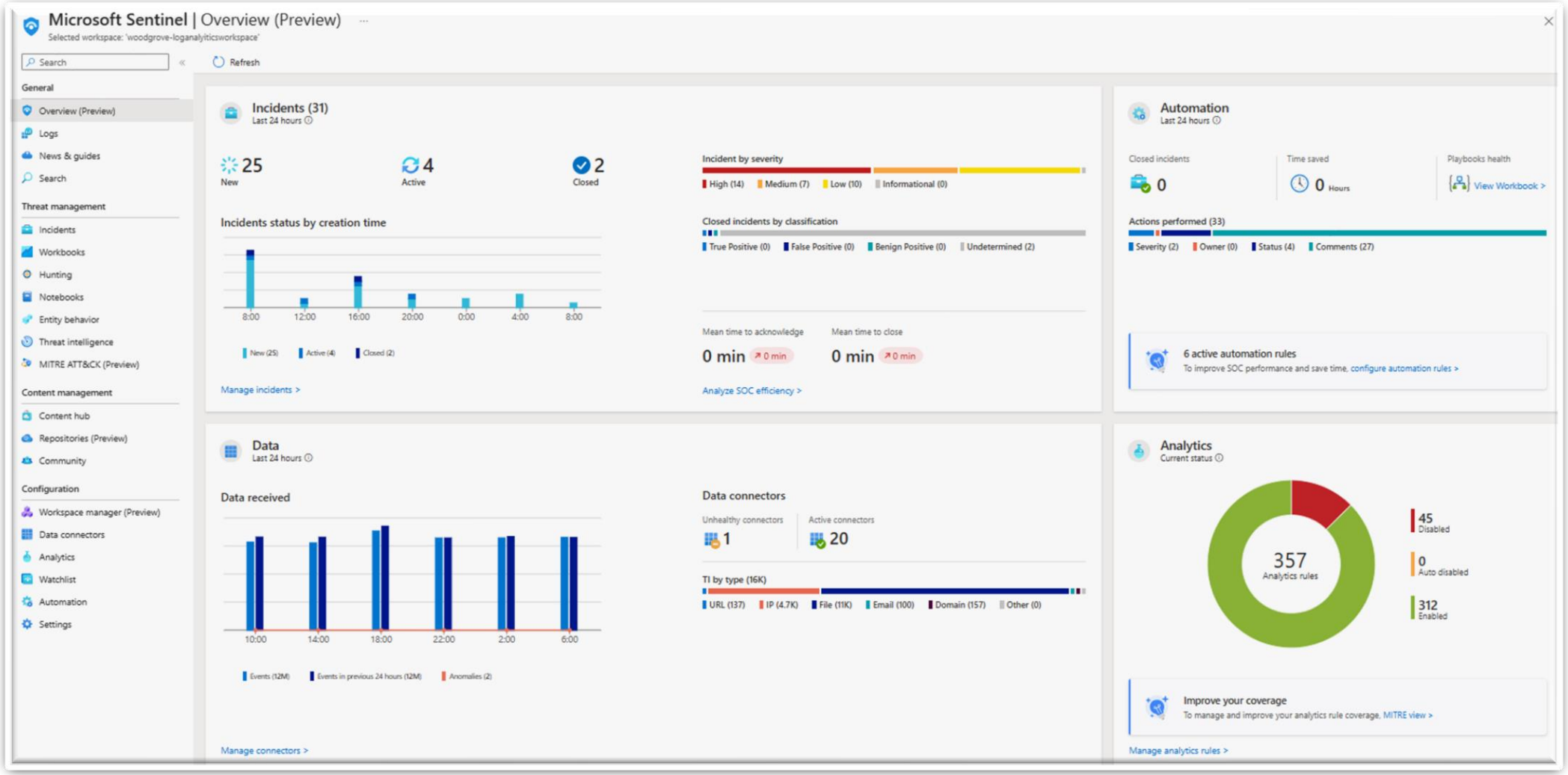


Risk Exposure = Impact x Probability

Microsoft Sentinel



Microsoft Sentinel portal

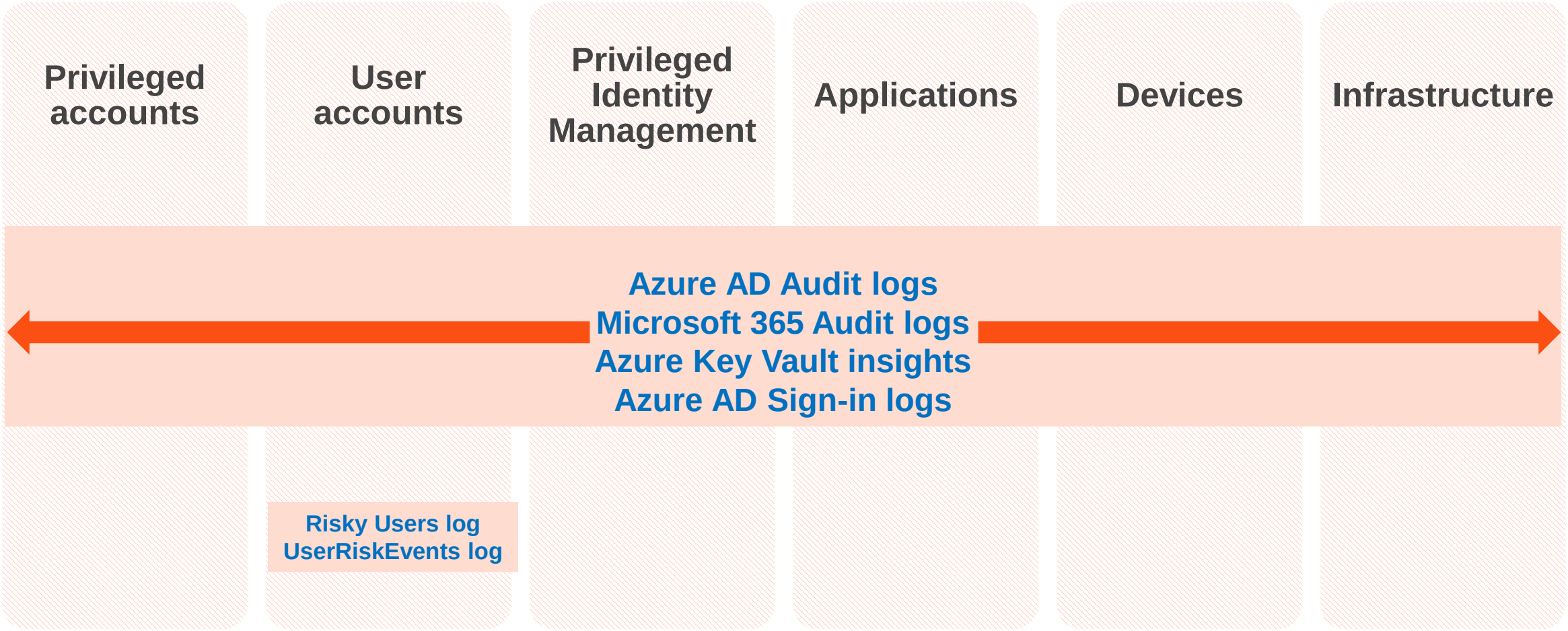


SecOps guide scope

- Password audit and strategy recommendations
- Overview of the tools available for hybrid and cloud Azure environments
- SIEM configuration guidance
- Monitoring and alerting strategies for:-
  - User accounts
  - Privileged accounts
  - Privileged Identity Management
  - Applications
  - Devices
  - Infrastructure

aka.ms/aadsecopsguide

Log files to monitor



Go-Dos

Strengthen Identities

- Deploy strong authentication methods
- Leverage **Conditional Access** and **Identity Protection**

Integrate Applications

- Integrate applications with Entra ID, Entra SSE
- Protect Applications with **Defender for Cloud Apps** and **Purview**

Adopt Least Privilege

- Minimize user access with Just-In-time and Just-Enough Access (JIT/JEA)
- Leverage **PIM** and **Entra Permissions Management**

Strengthen Endpoints

- Migrate to EIDJ devices
- Leverage **Microsoft Intune** and **Microsoft Defender for Endpoint**

Use your log data

- Establish a baseline of normal behavior
- Leverage **Microsoft Sentinel**
- Read the SecOps guide: **aka.ms/aadsecopsguide**

References

- aka.ms/NISTZeroTrust
- aka.ms/ztmodel
- aka.ms/EIDJonpremSSO
- aka.ms/aadSecOpsGuide
- https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-strengths
- https://learn.microsoft.com/en-us/azure/global-secure-access/overview-what-is-global-secure-access
- https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings
- https://www.hypr.com/security-encyclopedia/notpetya
- https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Questions?

Slides found at aka.ms/5stepsZT

Thank you!

Slides found at aka.ms/5stepsZT