SECURING YOUR APPS & IDENTITIES

WITH AZURE AD CONDITIONAL ACCESS

Thomas Naunheim
Koblenz, March 2021

THOMAS NAUNHEIM

Cloud Solutions Architect
Koblenz, Germany

@Thomas_Live

www.cloud-architekt.net

Azure Meetup BONN

MVP Microsoft® Most Valuable Professional

Microsoft Certified Azure Solutions Architect Expert

Most Valuable Mentor

AZURE AD MONTHLY ACTIVE USERS

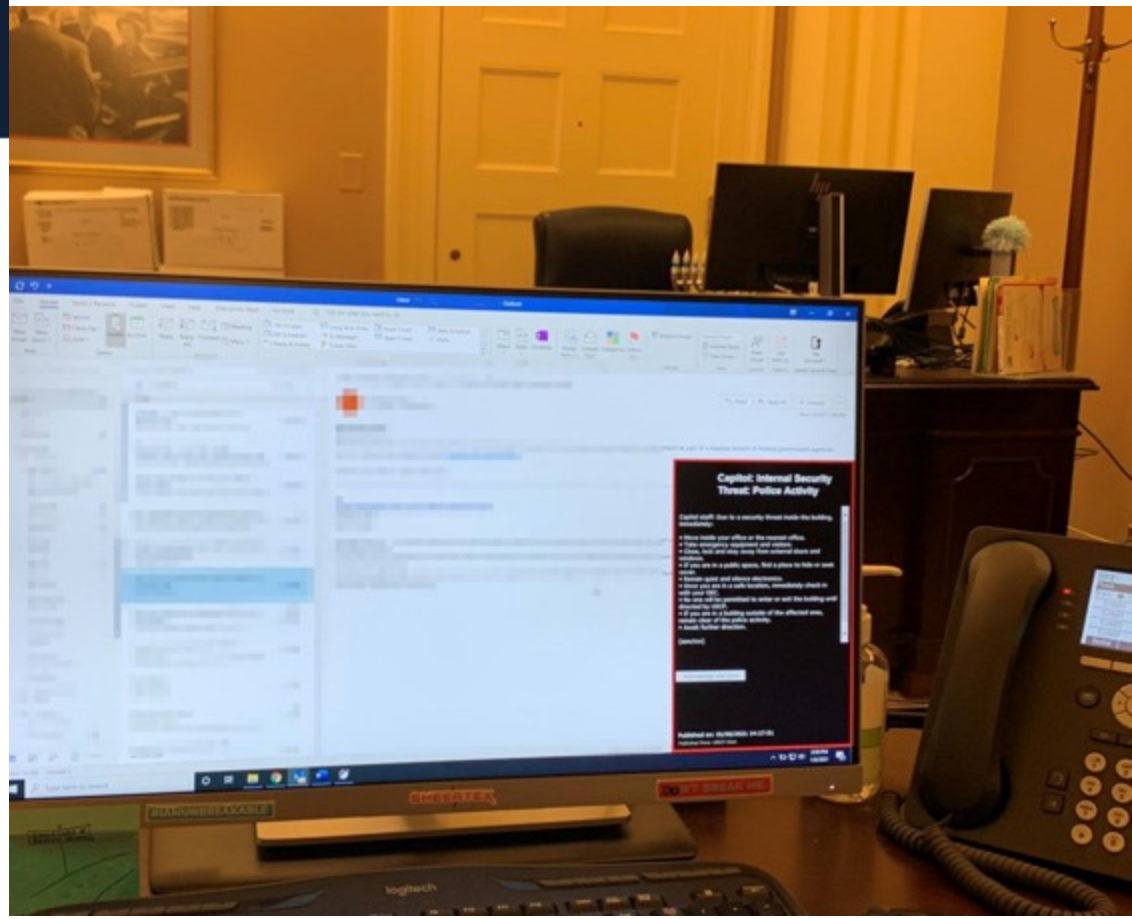
SHIFT TO CLOUD AUTHENTICATION

Source: "Azure Active Directory: our vision and roadmap to help you secure remote access and boost employee productivity"

Law enforcement officials across the U.S. shocked by police failure to stop Capitol invasion

Ex-Seattle Police Chief Carmen Best said police shouldn't have been surprised by the actions of pro-Trump protesters given the heated rhetoric of 2020.

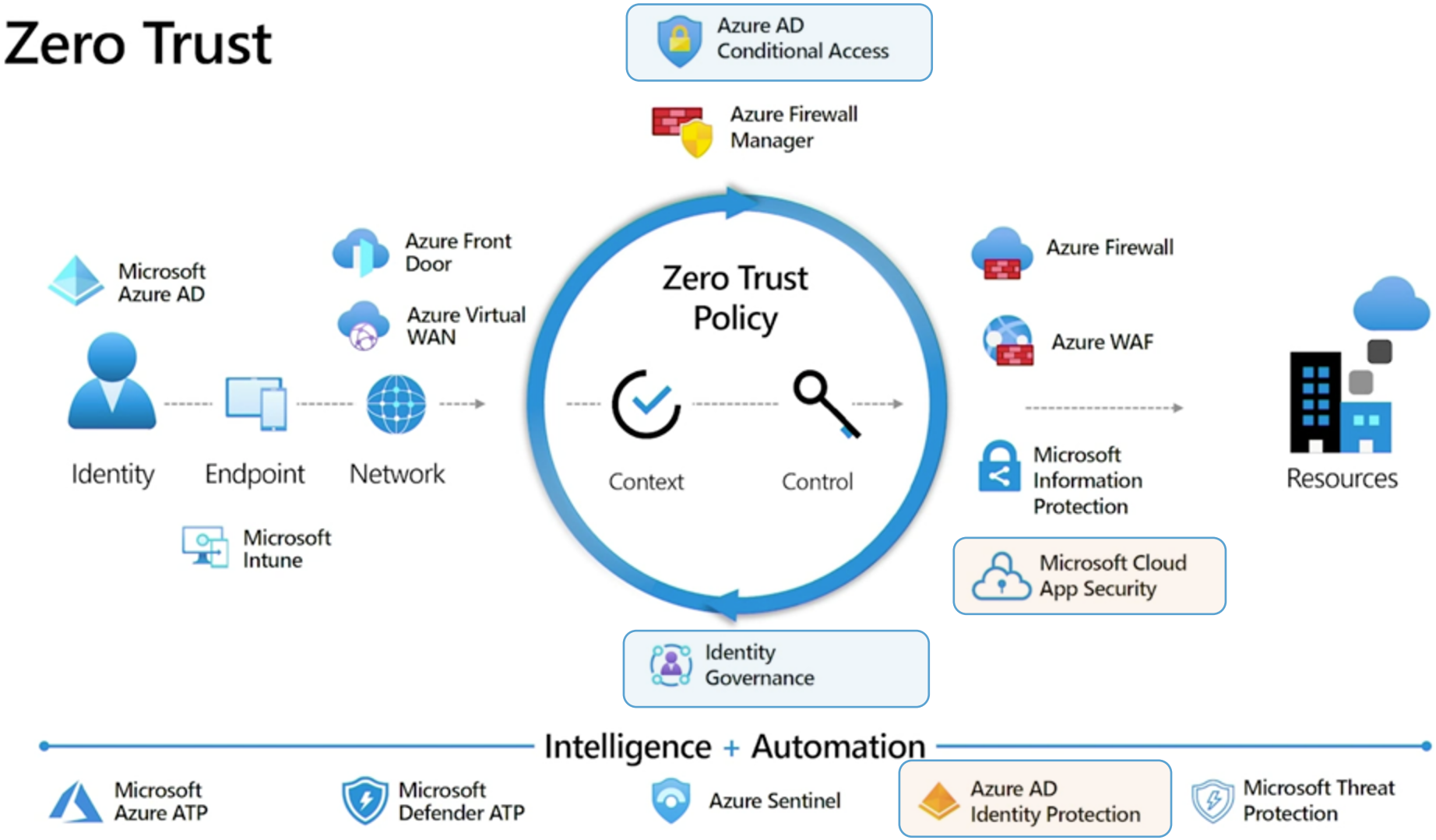
U.S. CAPITOL BREACH & SECURITY PERIMETER



Source: NBC News

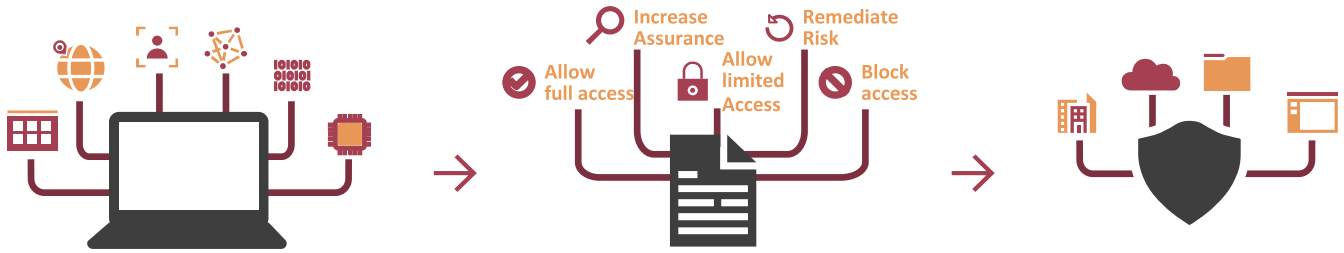

ZERO TRUST
EVERYWHERE!
LIGHTYEAR

NEVER TRUST, ALWAYS VERIFY

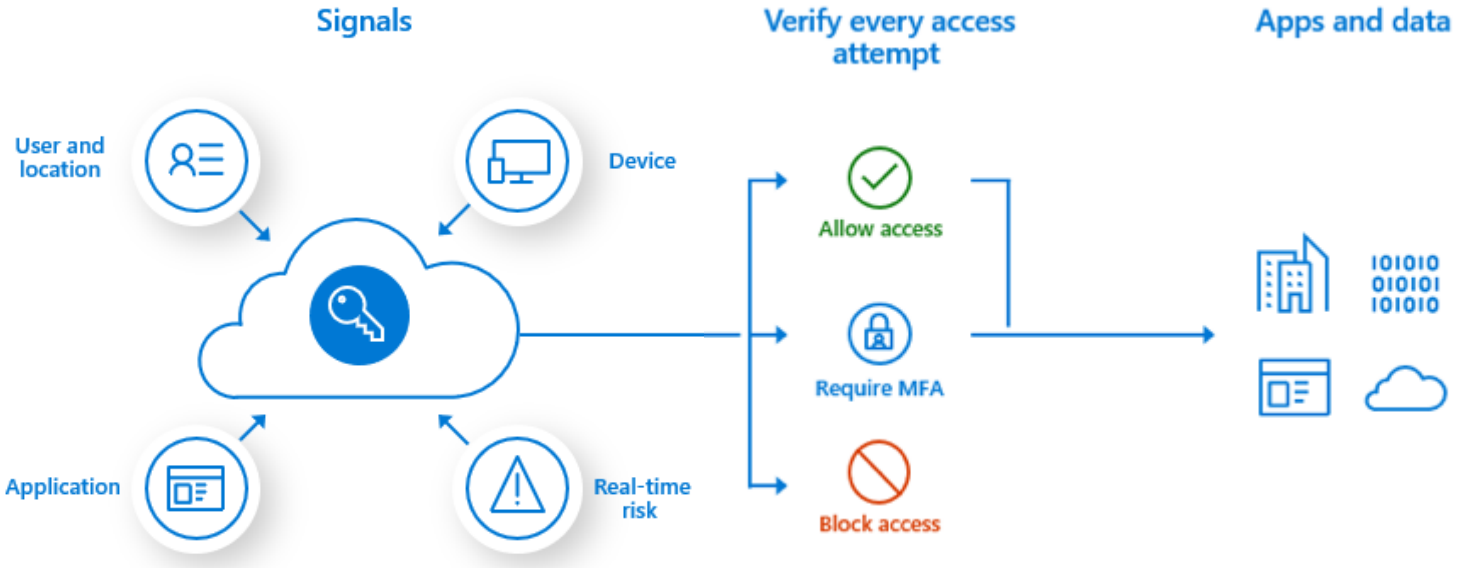


Details: Zero Trust deployment guide for Identity (https://aka.ms/ZTIdentity)

ZERO TRUST MODEL AND POLICY ENGINE

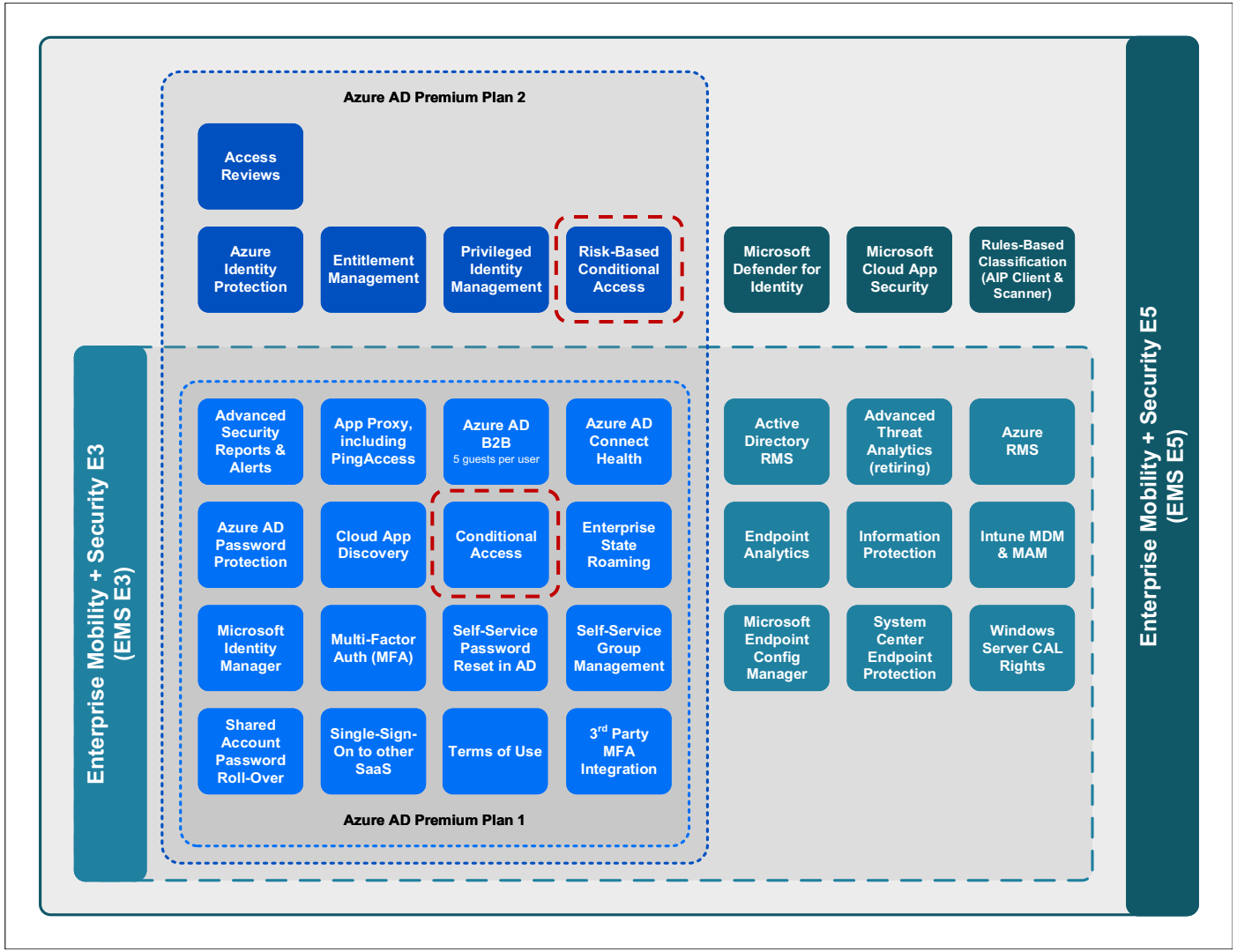


Signal Decision Enforcement



Source: Microsoft ("Zero Trust Definition and Models")

(CLOUD) SECURITY COSTS MONEY?



Source: Licensing Repository by Aaron Dinnage

AGENDA

Design and Implementation

A

Management and Monitoring

B

Identity Protection & MCAS:

Advanced Integration

C

Use Case:

Access from External Identities

D

Use Case:

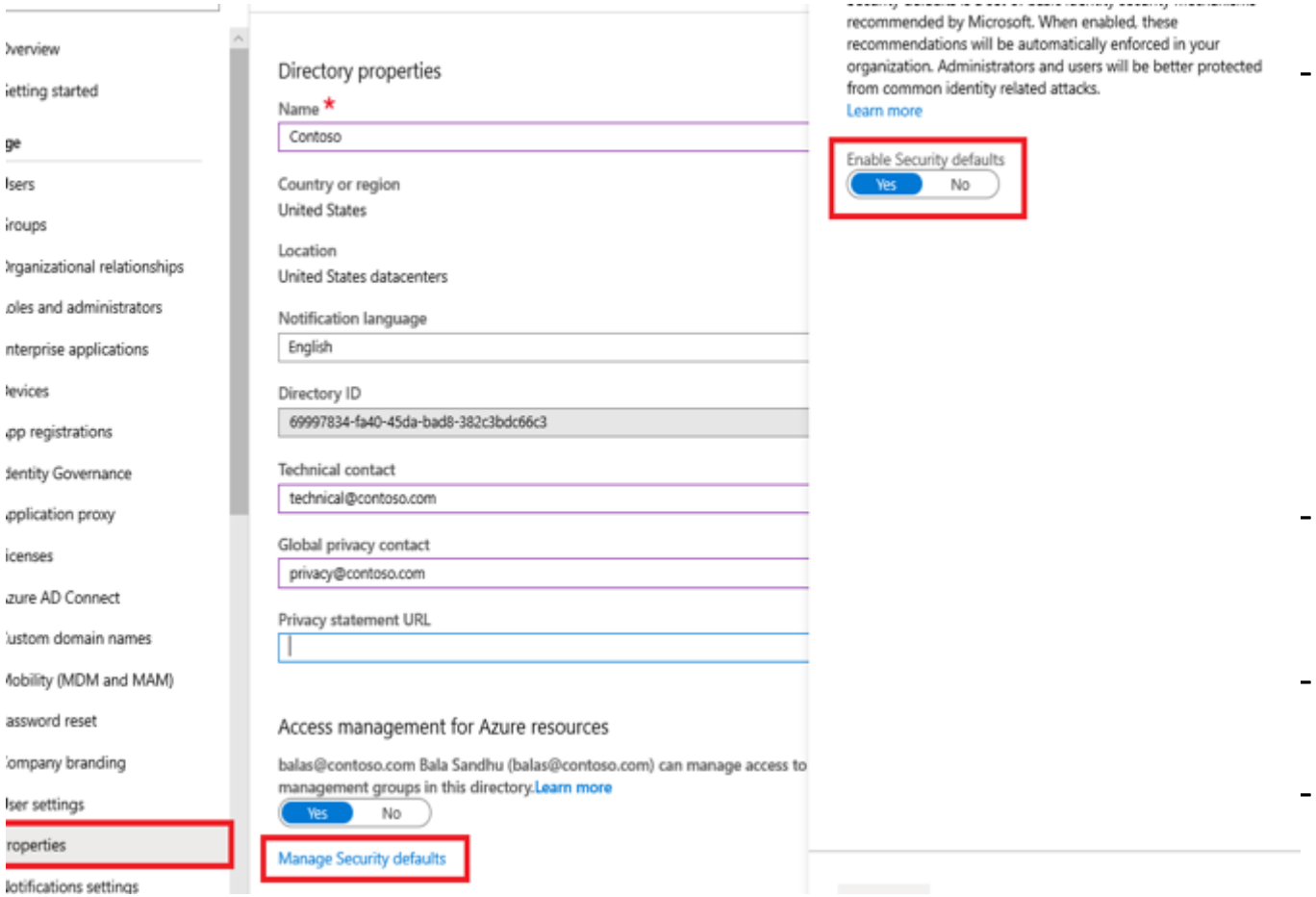
Securing Privileged Access

E

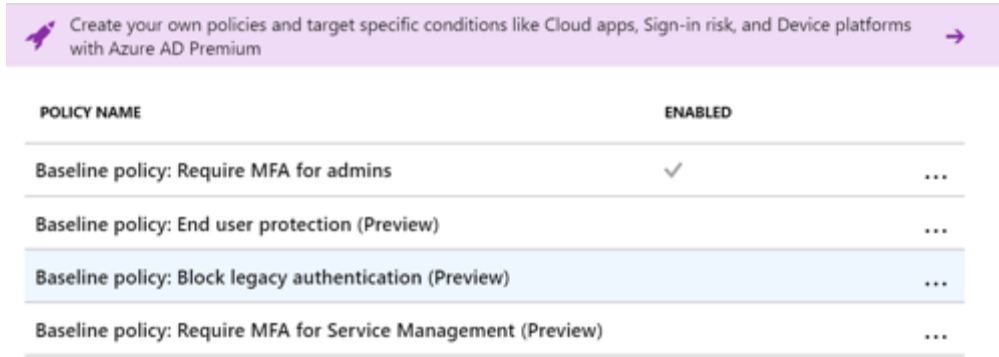
DESIGN AND IMPLEMENTATION OF CA POLICIES

PRACTICES AND CONSIDERATIONS

SECURITY (BY) DEFAULTS?

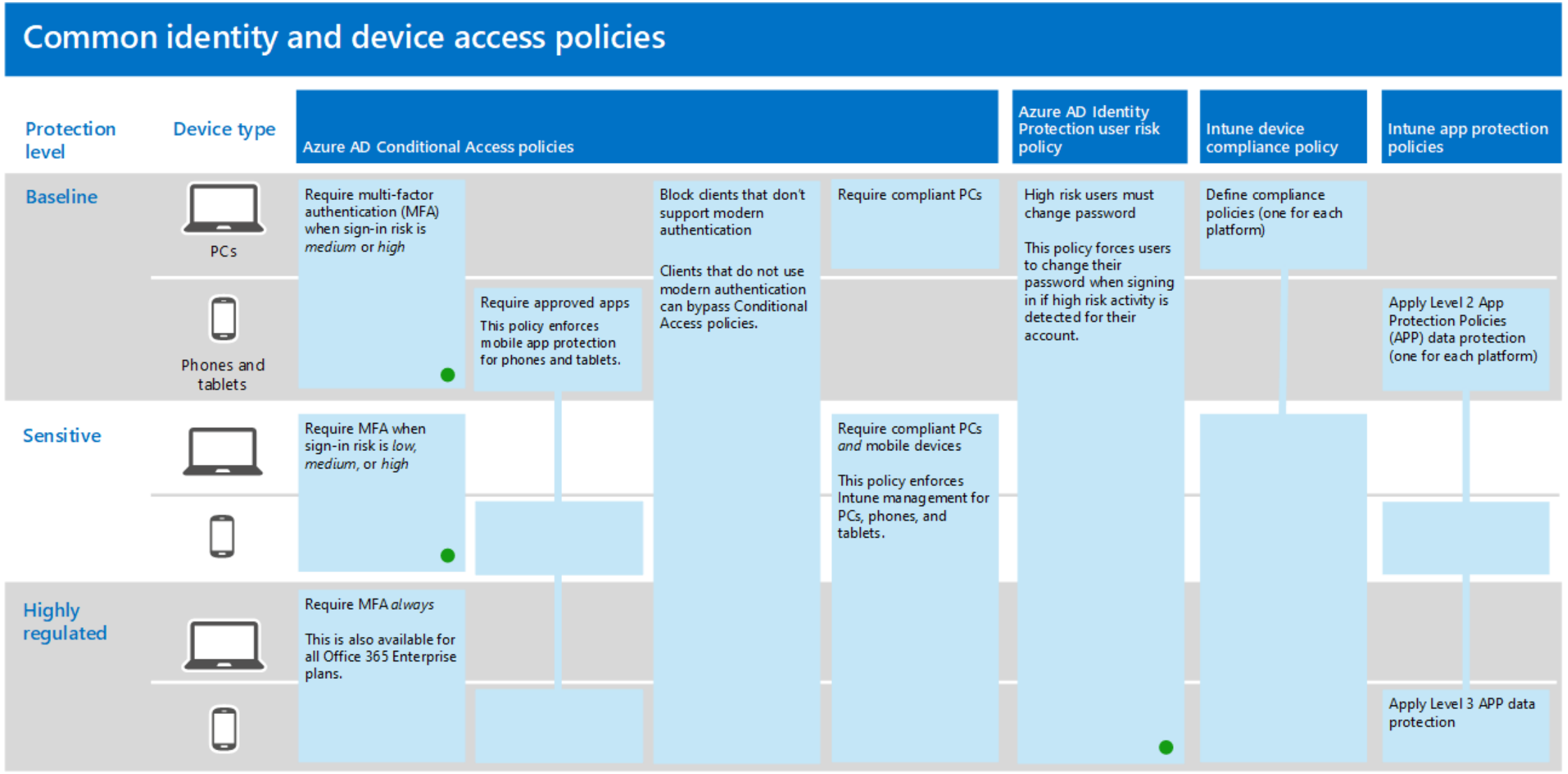


- Replacement of “Baseline”-Policies



- No extra costs or AAD license required (available for all tenant, enabled by default)
- Minimal security baseline by enforced policies
- *“Security defaults provide secure default settings that (Microsoft) manages on behalf of organizations to keep customers safe **until they are ready to manage their own identity security story.**”*
  Quote from Alex Weinert’s Blog post

M365 "GOLDEN CONFIG"



Source: Microsoft („Common identity and device access policies")

DESIGN YOUR CA POLICY BASELINE

Ensure to protect every user and every app by minimal but strong baseline!

DESIGN YOUR CA POLICY BASELINE

- **Build strong baselines for users** (hybrid, privileged and guests) **and apps/APIs**
- Define a standard **naming** convention for policies

CA01 - Dynamics CRP: Require MFA for marketing When on external networks

<SN>-	<Cloud app>:	<Response>	For	<Principal>	When	<Conditions>

- **Draft policies** (when this happens → do this)

When this happens	Then do this

- **Microsoft Deployment Plan** for Conditional Access
- **Consider your environment** (types of apps, devices and authentication methods)!

Source: Microsoft Docs („How To: Plan your Conditional Access deployment in Azure Active Directory“)

DRAFT, DESIGN AND CONFIGURATION

1. Assignment of required licenses to all users?
2. All devices are under control of the company? BYOD Strategy?
3. External Collaboration Strategy? B2B/Guest users?
4. Trust on Network or Identity-Driven Perimeter (+ Modern Client Management)?
    1. Strong authentication (methods) for everyone (WHfB, Passwordless, MFA Enrollment)?
    2. Integration-Level of Endpoints (Hybrid Joined Devices, Compliance Status)?
5. Security Level on Personas? (Admins, CXO, R&D Engineers, Frontline Workers)?
6. Protection Level of Applications/Data or Enterprise Access Model?

DRAFT, DESIGN AND CONFIGURATION

1. Draft: Scenarios of user access with expected result (= Test plan)

When this happens	Then do this
An access attempt is made: • **To all cloud apps** • **By synchronized users (= hybrid identities)**	Require Hybrid Azure AD Joined Device

Result is a statement: *Every synchronized users in my organization needs to be authenticated from a hybrid Azure AD joined device.*

Evaluation & Testing: *What is the definition of hybrid AAD joined device (to pass this policy?)*

2. Design the policy in your Dev/QA environment (Inter- vs. Intra-Tenant-Staging)
3. Evaluate a simulated sign-in with „What if“-tool, Test CA Policy (Report-only)
4. Staged deployment in „Rings“ and/or QA Tenant → Verification → Next Stage → …

SAMPLE OF CA POLICY BASELINE

Conditions

- **User Attributes** (Group Member)
- **Location** (IP Range)
- **Platform Type** (Windows, iOS,..)
- **Type of client** (Web, Mobile,…)

All Users & Apps

Policy and Controls: Risk-based & Conditional Access Policy

High **risk user** must change passwords

Password Change

Block clients with legacy authentication

Block unsupported (e.g. ChromeOS) and forbidden platform types

Block

Require **Hybrid Joined /compliant device** or approved apps (MAM)

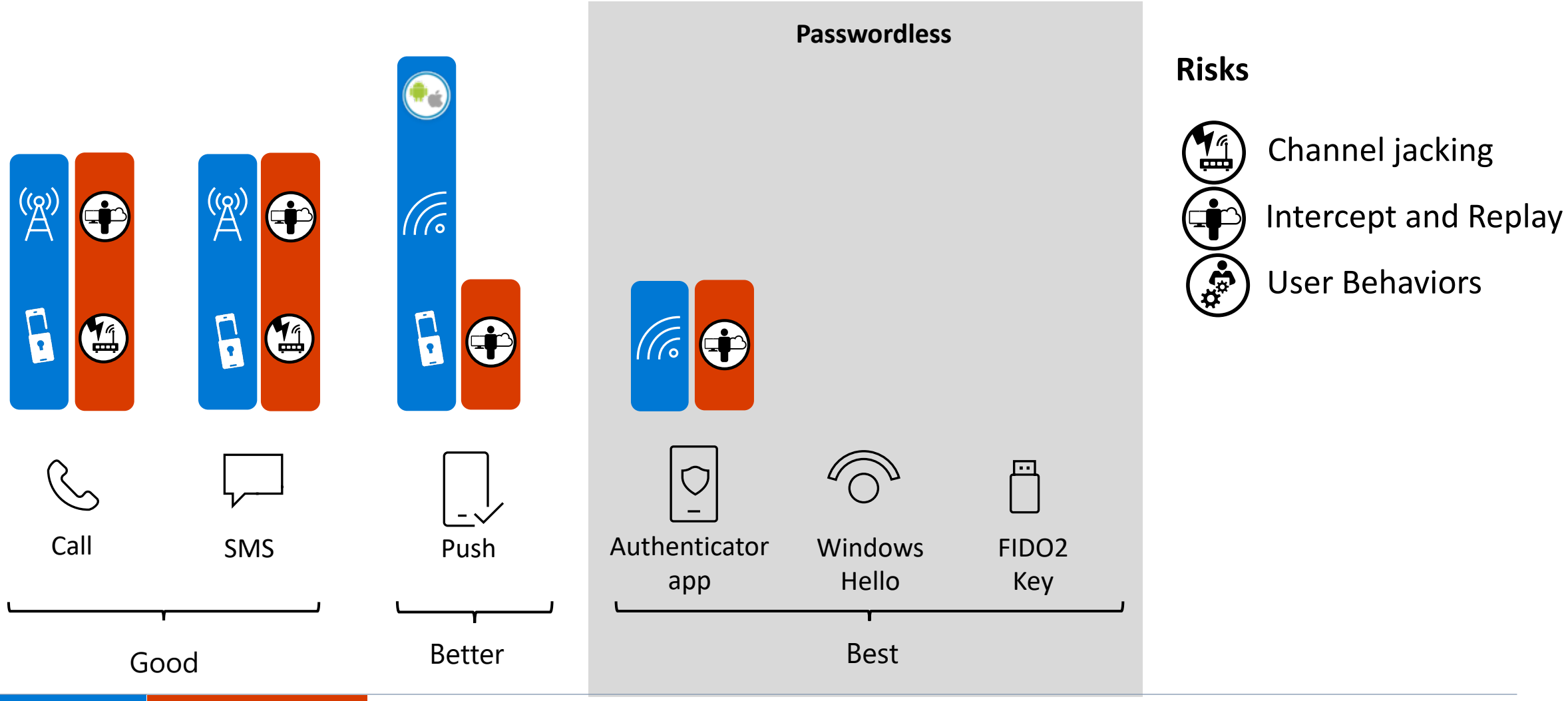
Require MFA when sign-in risk is medium or high

Allow

Design and Implementation of CA Policies
Attack Reduction and Base Protection

LIVE DEMO

DEPENDENCIES & RISK OF AUTH. METHODS



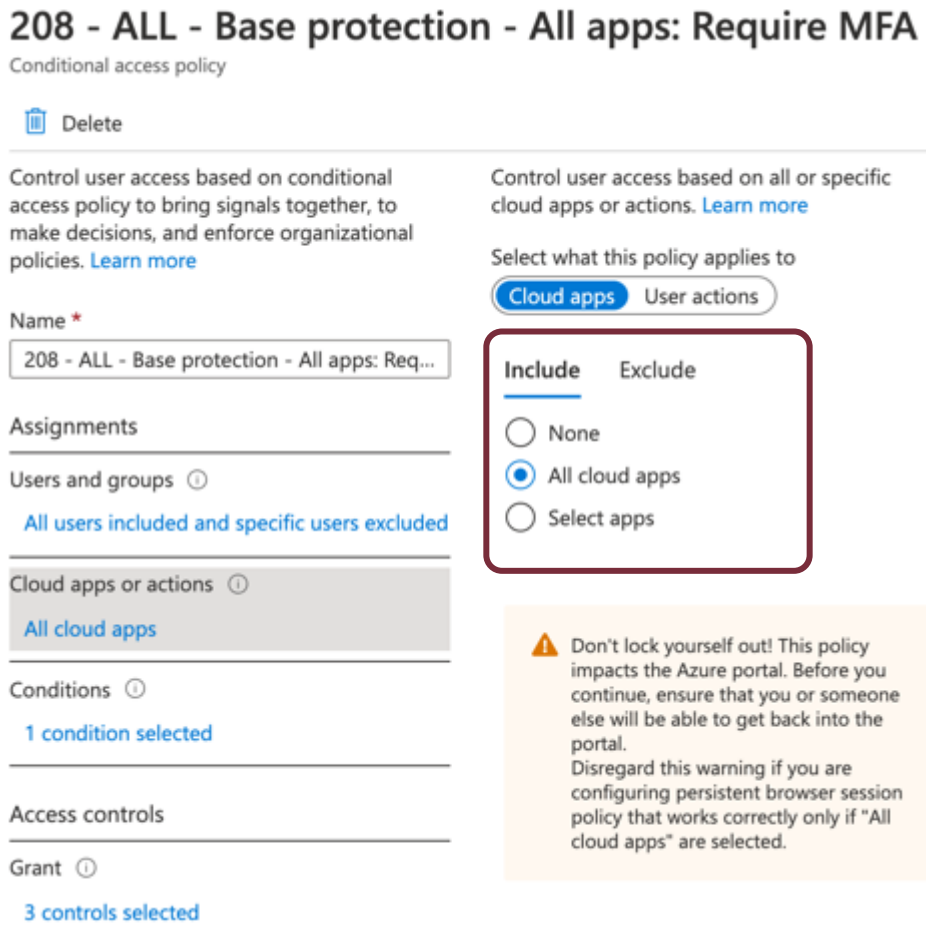
Source: „Identity and access management best practices from around the world“

EMERGENCY OPTIONS (DISRUPTION)

- **Important part of your resilient access control management strategy**
- Microsoft‘s Sample of **contingency policy**
  - EMnnn - ENABLE IN EMERGENCY: [Disruption][i/n] - [Apps] - [Controls] [Conditions]

    Example A - Contingency Conditional Access policy to restore Access to mission-critical Collaboration Apps
  - Sample: Trusted Device Status replaces Grant Control of Strong Authentication (in case of Azure MFA outtage)
- Real-world example: Status of BitLocker isn‘t detected for Intune Device Compliance
  - What could be a contigency policy for this case?

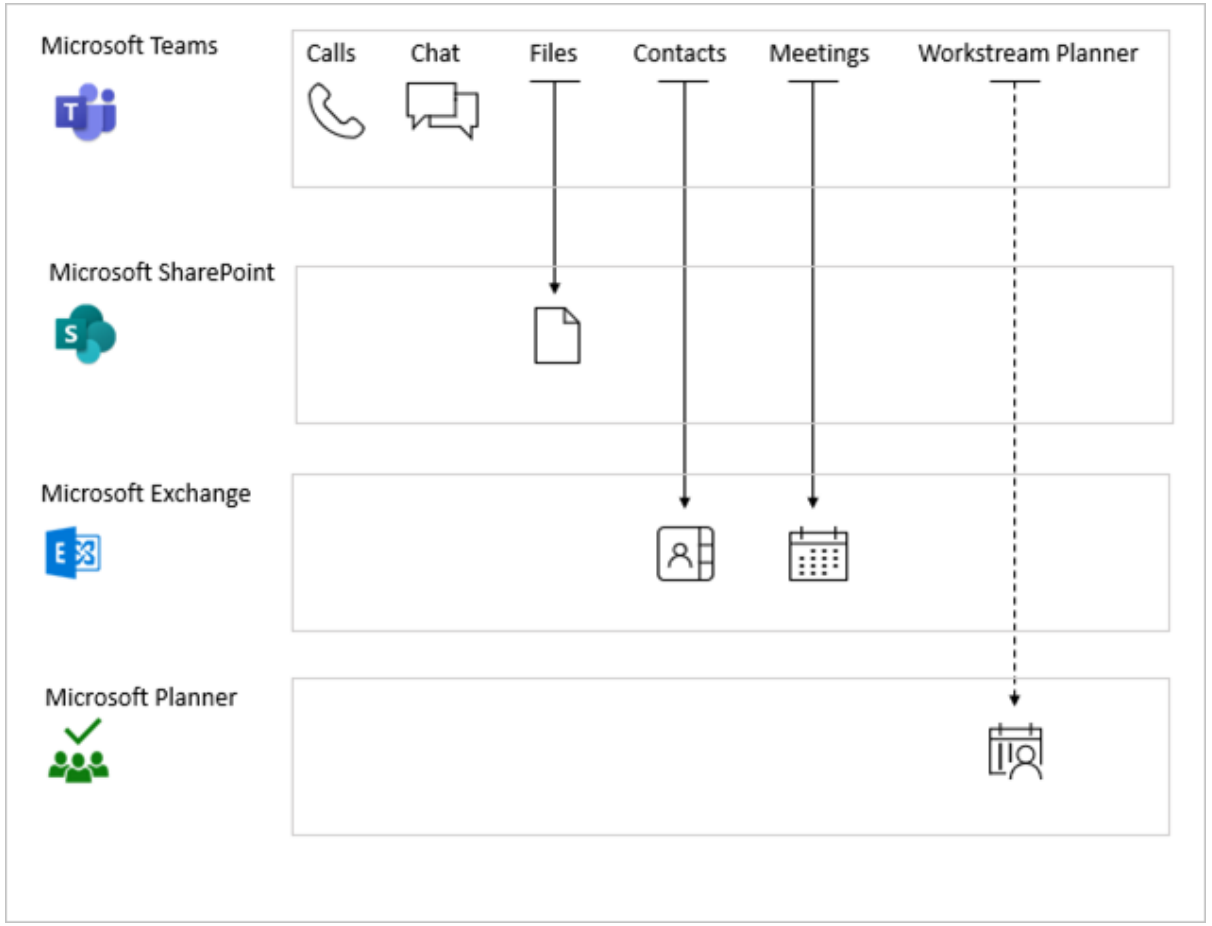
APP TARGETING: CLOSED ARCHITECTURE



- **Covered all (new) cloud apps automatically (approach of „Deny“ ZTN design)**
- **Covered all non-supported CA app (e.g. MyApps or EA Portal)**
- **Potential issues with „Device-based“ Authentication Flows**
- **…**

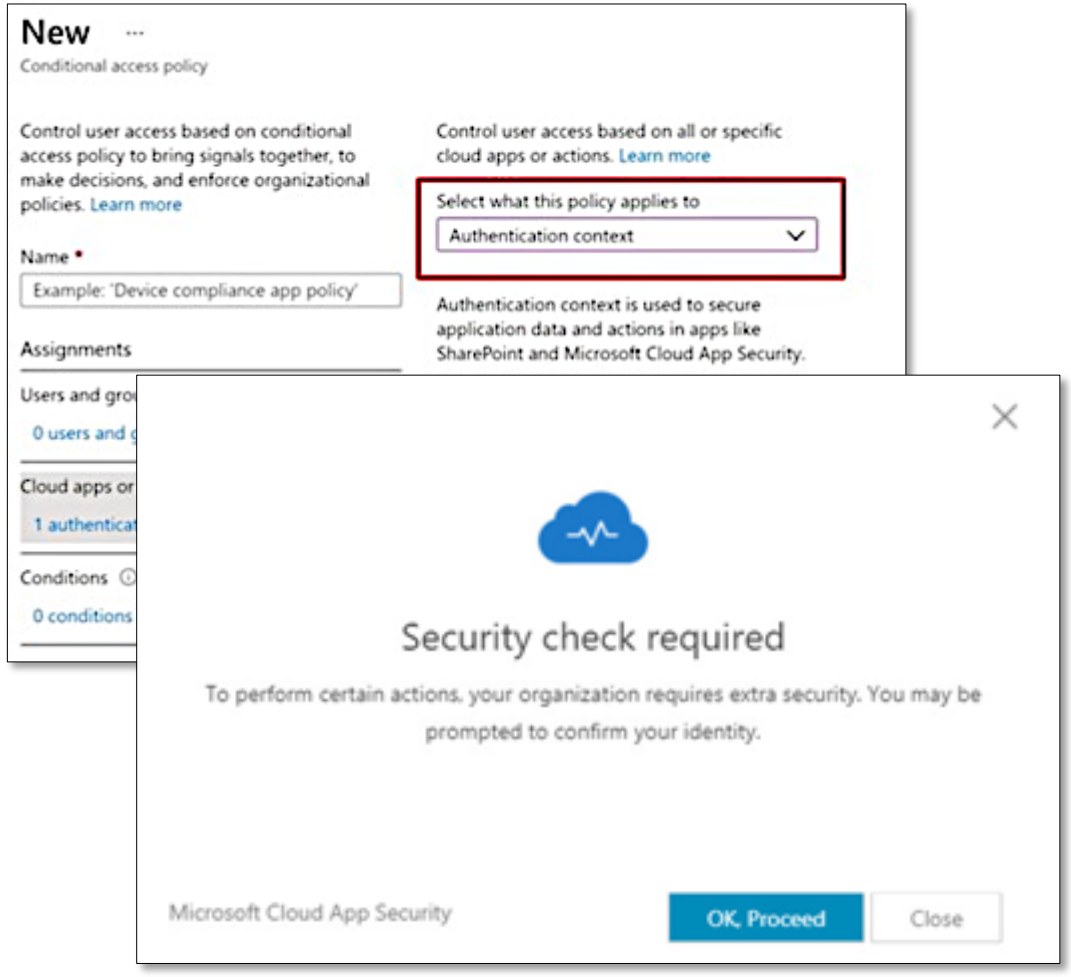
SERVICE DEPENDENCIES

Policy enforcement:



Source: Microsoft (What are service dependencies in Azure Active Directory Conditional Access?)

TARGETING ON AUTHENTICATION CONTEXT



- Granular policies based on user actions or the data they are trying to access
- Step up authentication based on what the user is trying to do within the app or data

Source: Microsoft (Winning Azure Active Directory strategies for identity, security, and governance

MANAGEMENT & MONITORING

LIFECYCLE & OPERATIONS AT SCALE

USER (GROUP) TARGETING

- Exclude Group for each CA Policy
- Azure AD access reviews to **manage exclusions** from policies
- **Access Package to request (temporary) exclusions** for specific CA Policies
- Who can manage CA Exclusions?
  All Delegated Roles with (Security) Group Management Permissions!

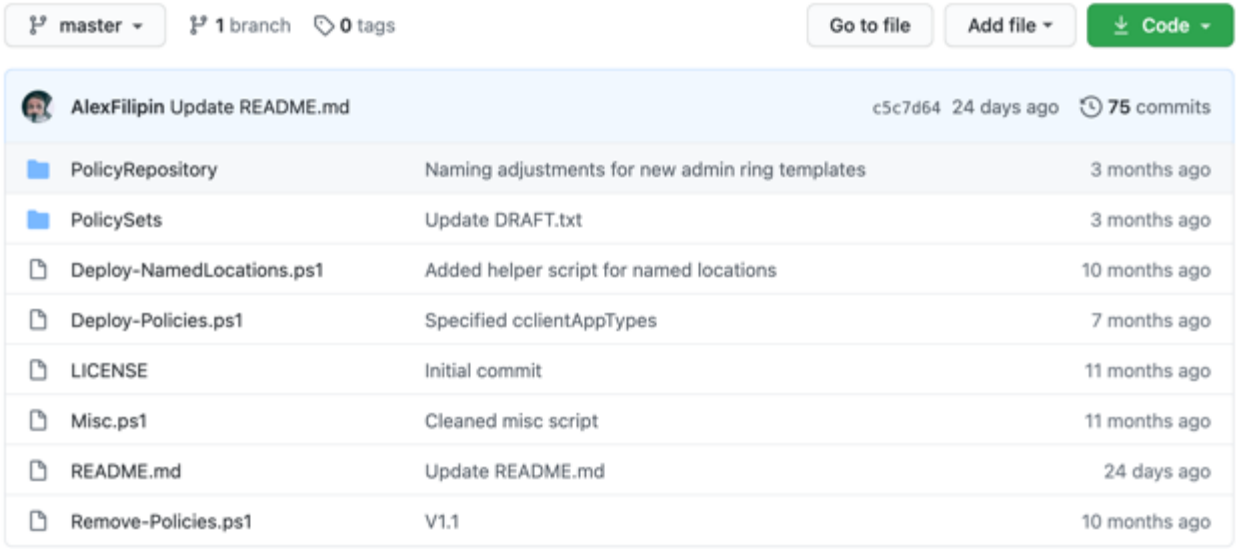
Automation & Lifecycle

Management of Permanent or Temporary Exclusions

LIVE DEMO

DEPLOYMENT OF TEMPLATES

- “Conditional Access As Code” GitHub Project by Alex Filipin



master · 1 branch · 0 tags · Go to file · Add file · Code

AlexFilipin Update README.md — c5c7d64 24 days ago — 75 commits

PolicyRepository	Naming adjustments for new admin ring templates	3 months ago
PolicySets	Update DRAFT.txt	3 months ago
Deploy-NamedLocations.ps1	Added helper script for named locations	10 months ago
Deploy-Policies.ps1	Specified cclientAppTypes	7 months ago
LICENSE	Initial commit	11 months ago
Misc.ps1	Cleaned misc script	11 months ago
README.md	Update README.md	24 days ago
Remove-Policies.ps1	V1.1	10 months ago

README.md

Conditional Access as Code

Introducing Conditional Access as Code. A fully automated solution to kick-start and maintain your Conditional Access deployment. The solution consists of the follwong three main components and is based on the Conditional Access guidance.

Policy repository

A collection of conditional access policies in JSON format which are divided into the following categories:

- Admin protection
- Application protection
- Attack surface reduction
- Base protection
- Compliance
- Data protection

Policy sets

Policy sets are based on the policies in the repository and form complete policy sets depending on company maturity and licensing:

- Bare minimum
- Device trust with AADP1
- Device trust with AADP1 and AADP2
- Device trust with AADP2
- Network trust with AADP1
- Network trust with AADP1 and AADP2
- Network trust with AADP2
- Your custom policy set

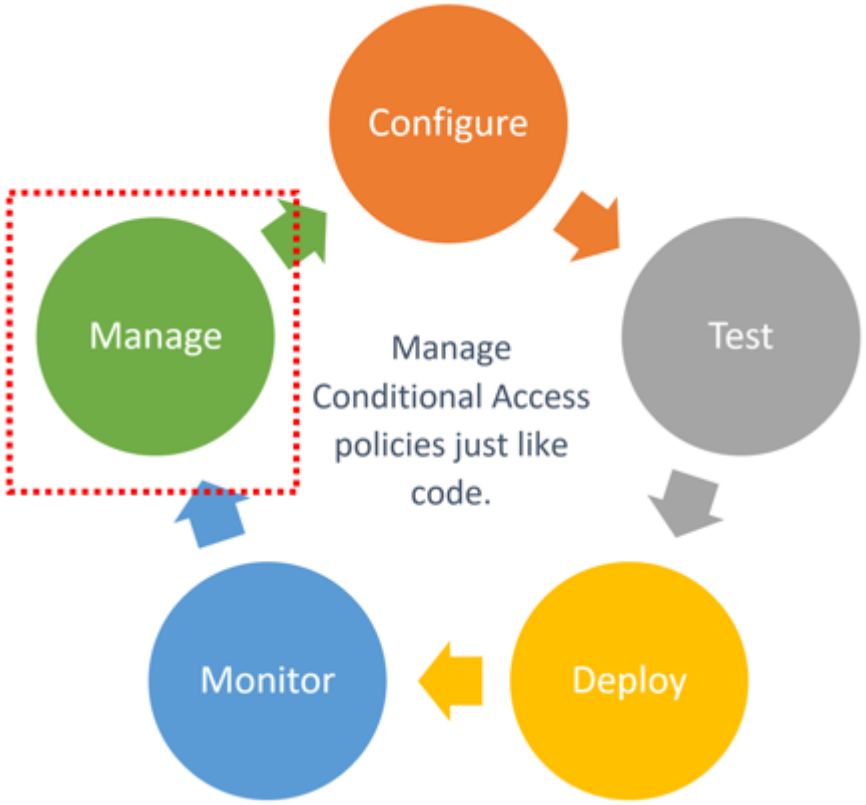
Automation solution

A script based automation solution to deploy and update policy sets in environments.

Together, these three components enable an extremely fast deployment of conditional access concepts and their long-term maintenance, e.g. in the form of source control.

Source: „AlexFilipin/ConditionalAccess“ (GitHub)

AUTOMATION VIA MS GRAPH + LOGIC APP



- Samples for "Conditional Access as Code" by Microsoft:
  - GitHub Repo includes Samples
  - Microsoft Docs: “Management of Lifecycle via API”

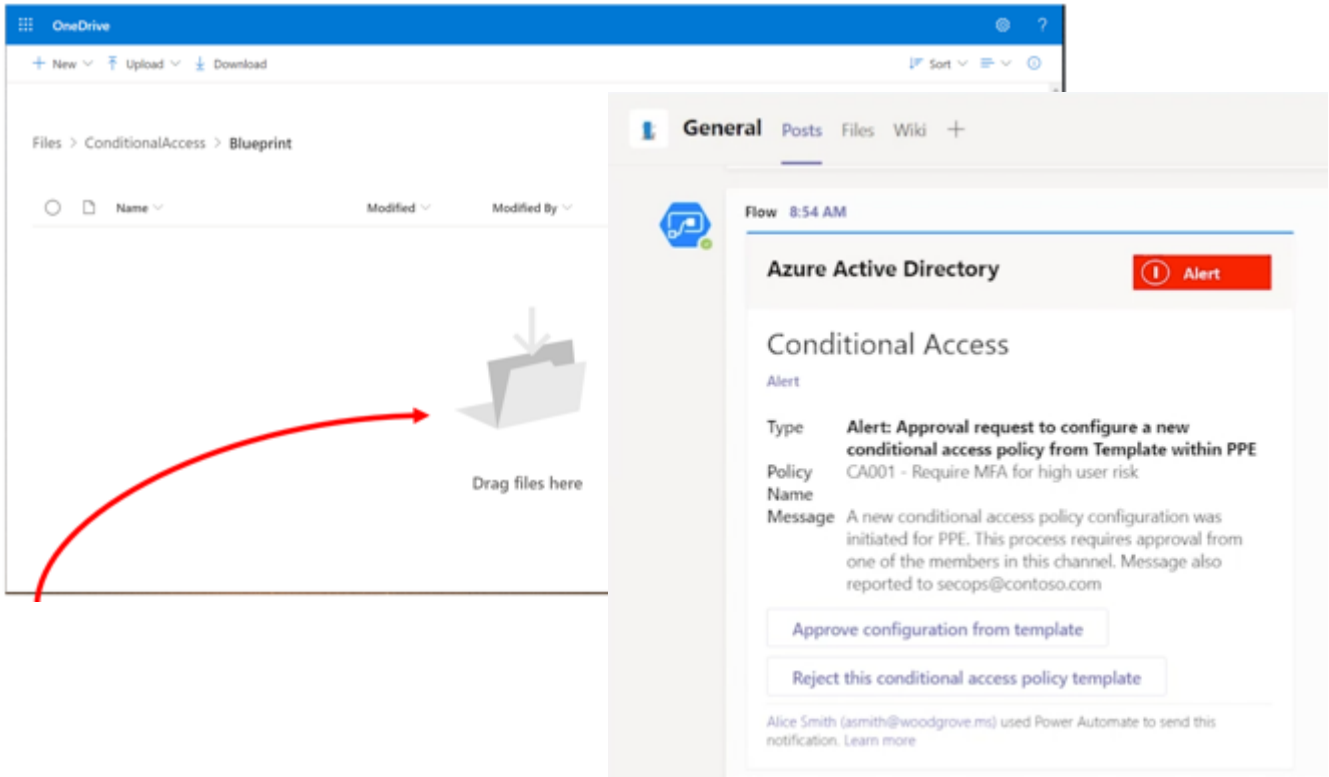


Image Source: “Azure Active Directory: our vision and roadmap to help you secure remote access and boost employee productivity”

Automation & Lifecycle

Microsoft Graph & Conditional Access “As Code”

LIVE DEMO

AUTOMATED DOCUMENTATION

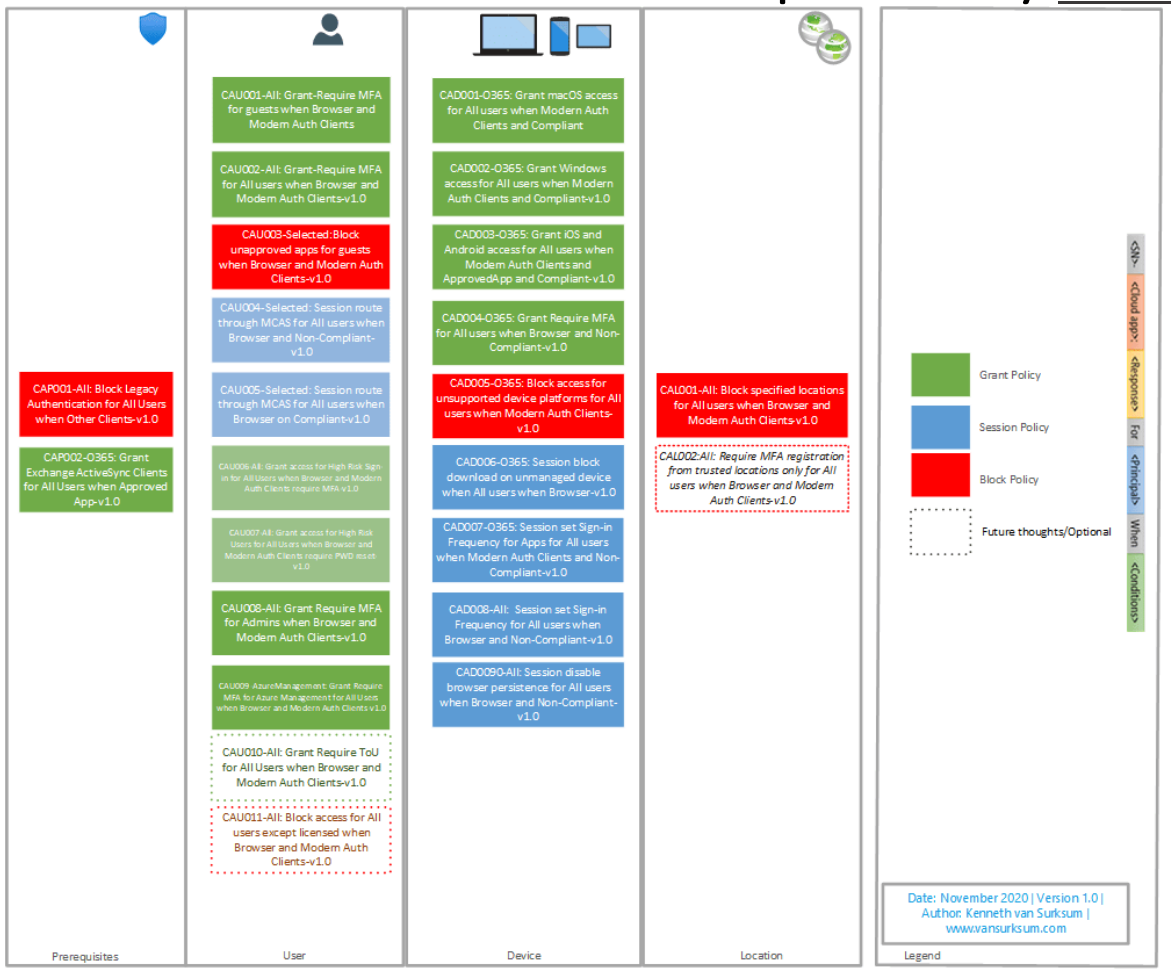
- Azure AD Conditional Access Policy Design Baseline by Daniel Chronlund ("DCToolbox")

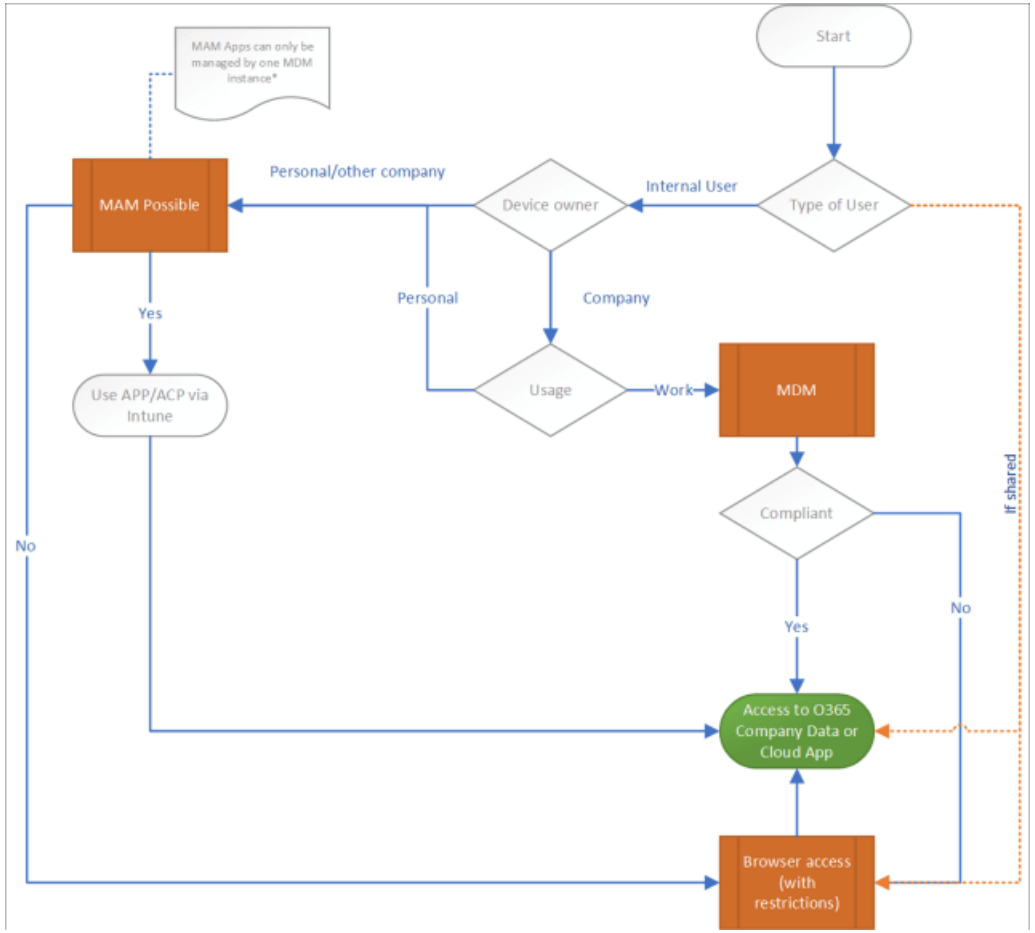
displayName	state	includeUsers	excludeUsers	includeGroups	excludeGroups	includeRoles	excludeRoles	includeApplications	excludeApplic
BLOCK - Legacy Authentication	enabled	All			Excluded from CA			All	
BLOCK - Unsupported Device Platforms	enabled	All			Excluded from CA			All	
BLOCK - High-Risk Sign-Ins	enabled	All			Excluded from CA			All	
BLOCK - Countries not Allowed	enabled	All			Excluded from CA			All	
BLOCK - Service Accounts (Trusted Locations Excluded)	enabled			Service Accounts	Excluded from CA			All	
BLOCK - Explicitly Blocked Cloud Apps	enabled	All			Excluded from CA			None	
BLOCK - Guest Access (Allowed Apps Excluded)	enabled	GuestsOrExternalUsers			Excluded from CA			All	Office365
GRANT - Terms of Use	enabled	All			Excluded from CA Service Accounts			All	
GRANT - MFA for All Users	enabled	All			Excluded from CA Service Accounts			All	Microsoft Intu Microsoft Intu
GRANT - Mobile Apps and Desktop Clients	enabled	All			Excluded from CA Service Accounts			All	
GRANT - Mobile Device Access Requirements	enabled	All			Excluded from CA Service Accounts			All	Microsoft Intu Microsoft Intu
SESSION - Block Unmanaged File Downloads	enabled	All			Excluded from CA			Office 365 Exchange Online Office 365 SharePoint Online	

Source: „Azure AD Conditional Access Policy Design Baseline with Automatic Deployment Support"

VISUALIZATION AND DOCUMENTATION

- Recommended default set of policies by Kenneth van Surksum





Source: Conditional Access demystified: My recommended default set of policies

Automation & Lifecycle

Azure Sentinel and Azure AD Workbooks

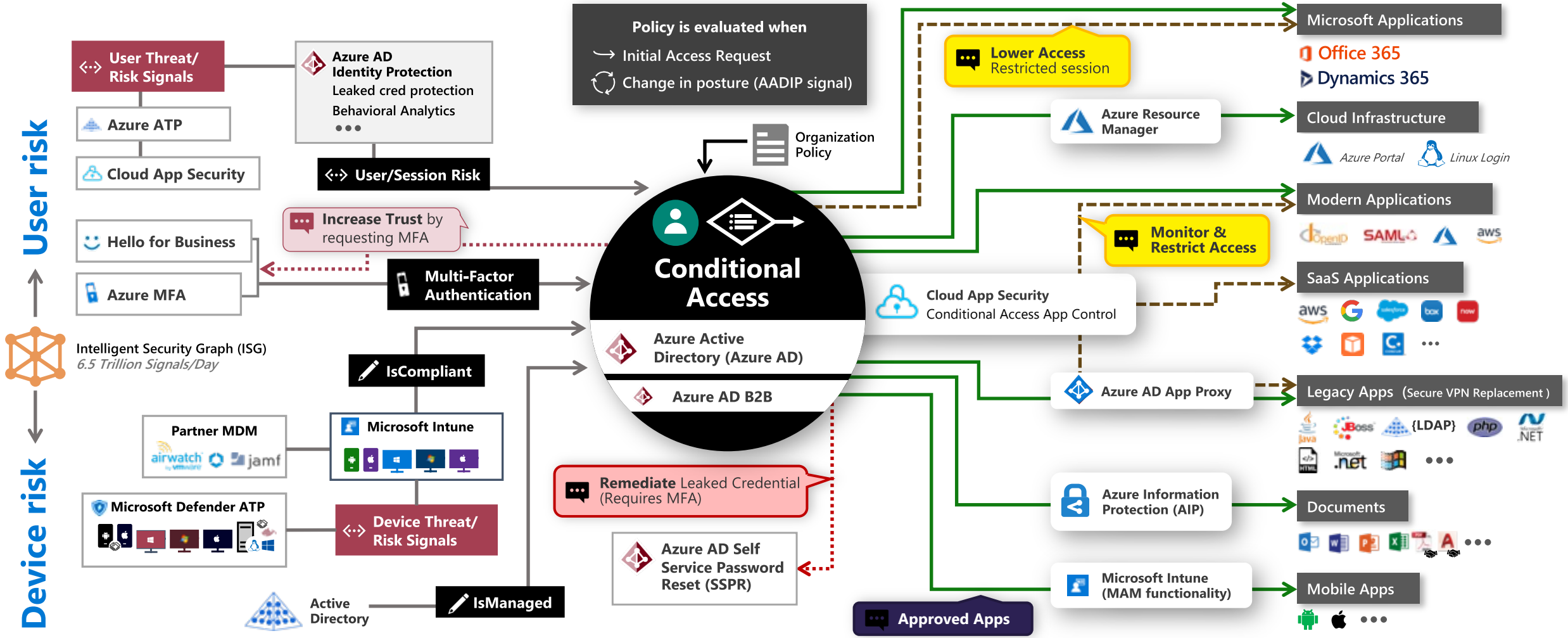
LIVE DEMO

ADVANCED INTEGRATION

IDENTITY PROTECTION & MCAS

ZERO TRUST POLICY ENGINE

Image Source: Microsoft ("Zero Trust Definition and Models")

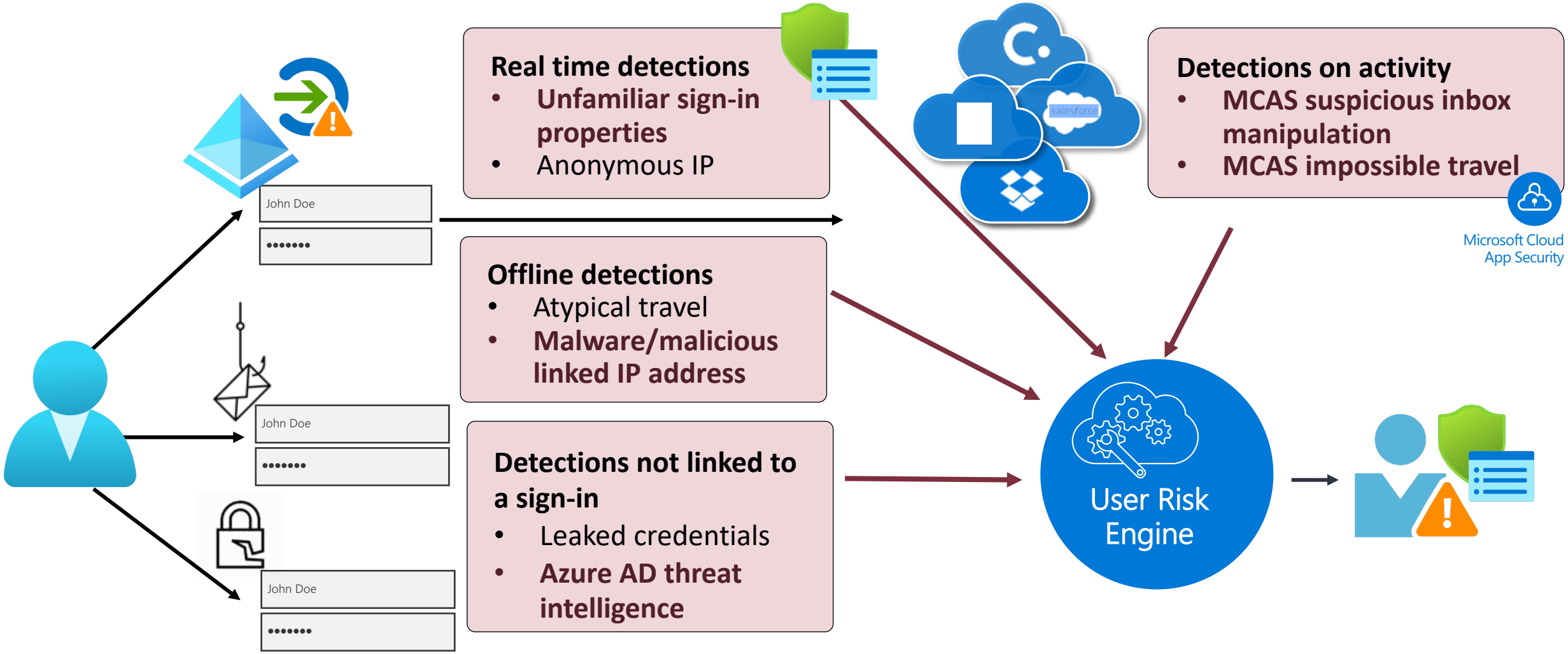


Signal
to make an informed decision

Decision
based on organizational policy

Enforcement
of policy across resources

IDENTITY PROTECTION



Source: Microsoft Ignite Session ("The science behind Azure Active Directory Identity Protection")

Advanced Scenarios

“Real-Time Detection of Sign-in Risk”

LIVE DEMO

CONTINUOUS ACCESS EVALUATION (CAE)

Reduce the lag between condition changes and policy (re)enforcement:

- Critical Event Evaluation (Examples):
  - Revocation all refresh tokens for a user (by Admin)
  - Client IP Address changes (outside of "Trusted Network")
  - …
- Current scenarios in public preview (resource provider support)
  - Exchange Online, SharePoint

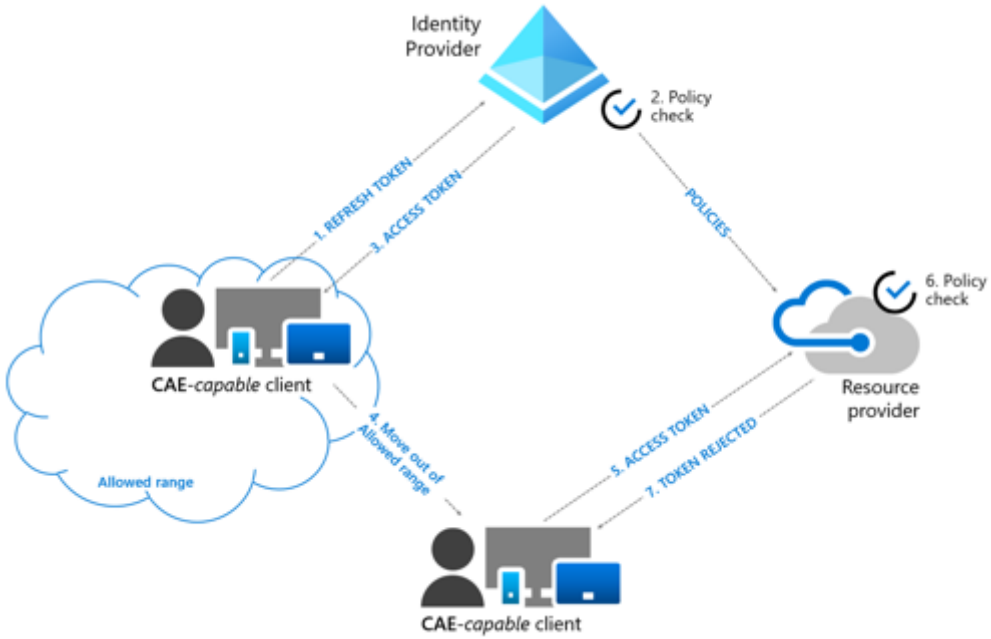


Image Source: "Azure Active Directory: our vision and roadmap to help you secure remote access and boost employee productivity"

CONDITIONAL ACCESS EVALUATION (CAE)

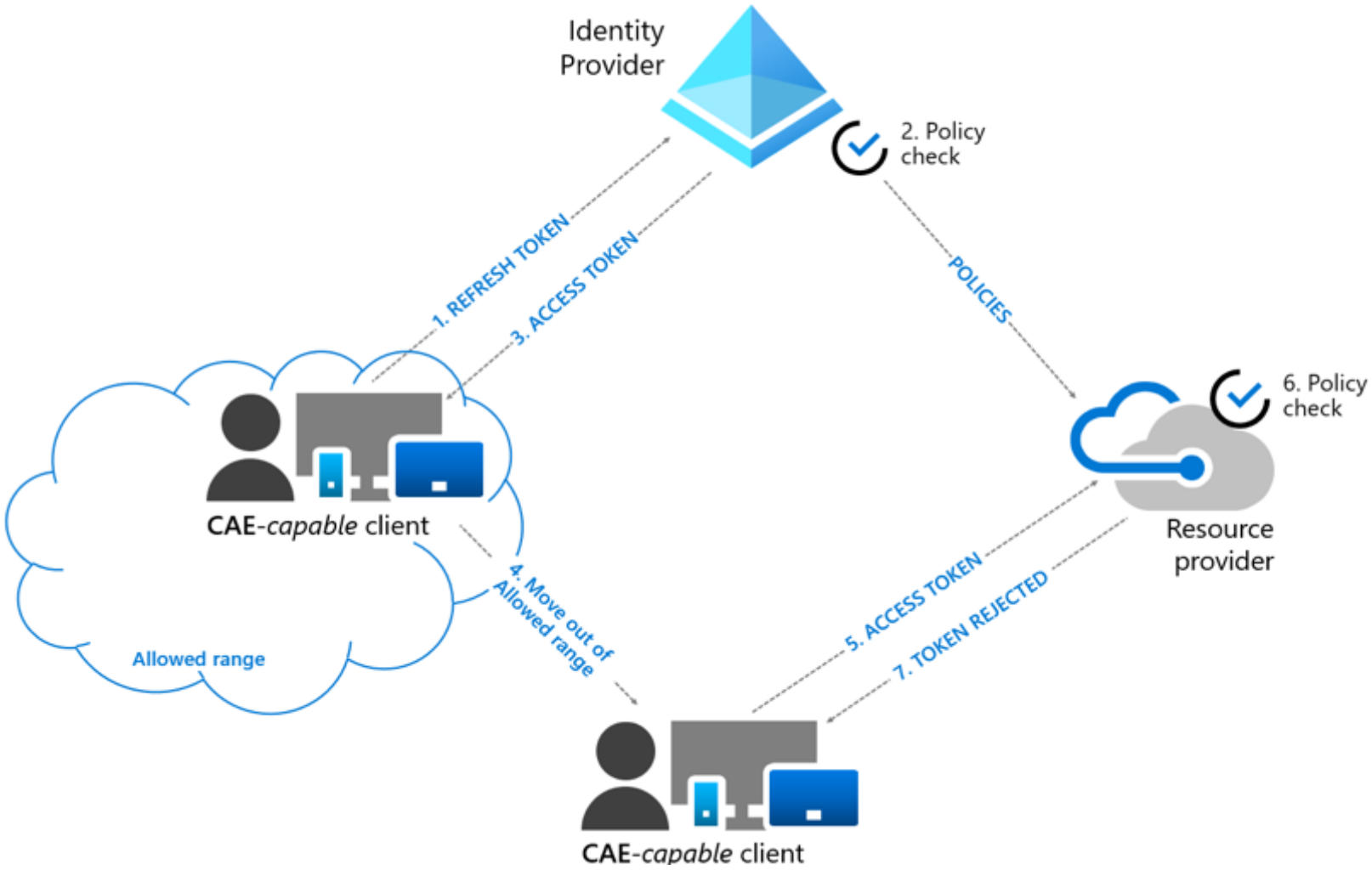


Image Source: "Continuous access evaluation (Microsoft Docs)"

RESILIENCY CONSIDERATIONS

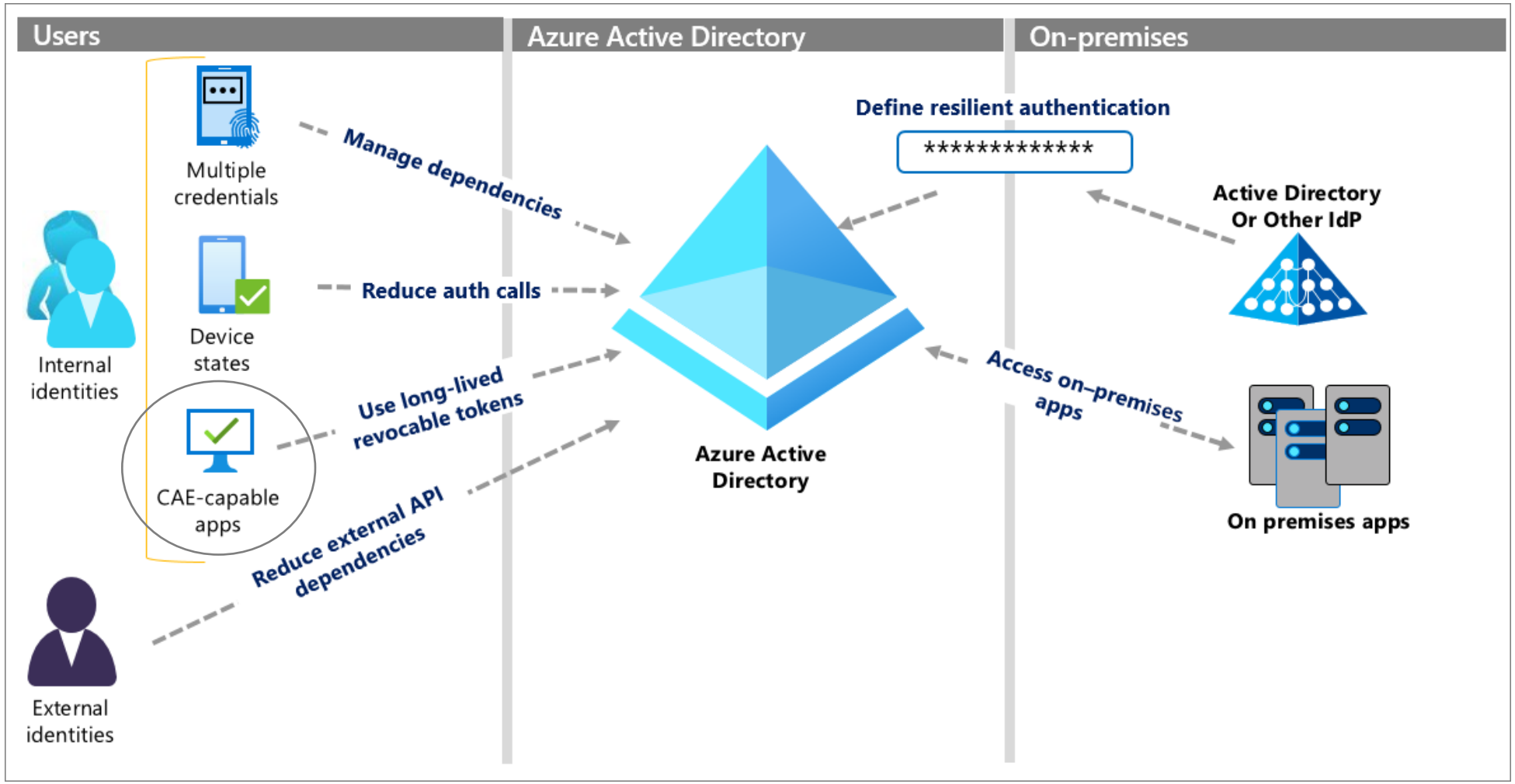


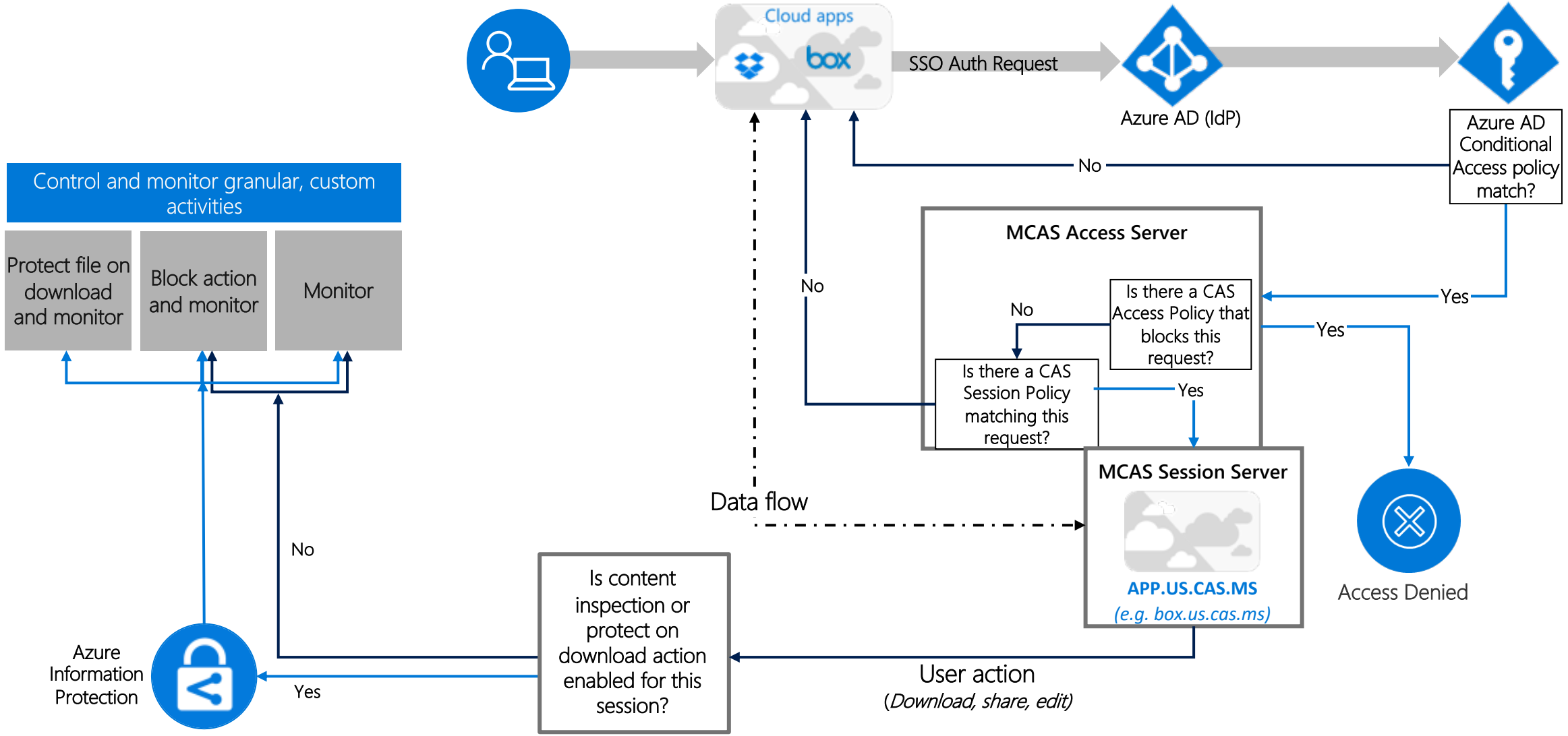
Image Source: "Build resilience by using Continuous Access Evaluation (Microsoft Docs)"

USE CASE:

ACCESS FROM EXTERNAL IDENTITIES

CONDITIONAL ACCESS & MCAS

CLOUD APP SECURITY



Source: Microsoft Cloud App Security (MCAS) Ninja Training

Advanced Scenarios and Controls

„Conditional Access App Control“

LIVE DEMO

CONSIDERATIONS FOR B2B USERS

- Device-based Policies (Require Compliant or Hybrid Azure AD joined)
  → can only satisfy compliance if the resource tenant can manage their device

- User Risk-based Policies
  → cannot be resolved in the resource tenant

- MFA “Double Authentication” vs. “Bypass”
  → Management of B2B MFA reset, Require MFA always for guests

- Recommended Policies: External access with CA policies

USE CASE:

SECURING PRIVILEGED IDENTITY & ACCESS

DEVICE COMPLIANCE OF SAW

CA POLICIES FOR PRIVILEGED IDENTITIES

Conditions and Controls

User

- ❑ Group: Privileged Identities
- ❑ Authentication: Strong
- ❑ **Location: "managed network"**

Device

- ❑ Platform: Windows
- ❑ Client: Browser
- ❑ **(Group: Specific Device)**

All Apps

Risk-based policies and Session management

Identity Protection

- ❑ **Sign-in Risk: No risk**
- ❑ ***User-Risk: No risk***

Device Compliance

- ❑ **Health: Compliant**
- ❑ **Device Risk: Low Score**

Session Controls

- ➢ Browser Session: Non-persistent
- ➢ Sign-in Frequency: Limited duration
- ➢ App Controls (MCAS): Blocked or monitored

Block access, Force threat remediation

Grant access

Restricted and monitored via MCAS

DEVICE COMPLIANCE PROFILES

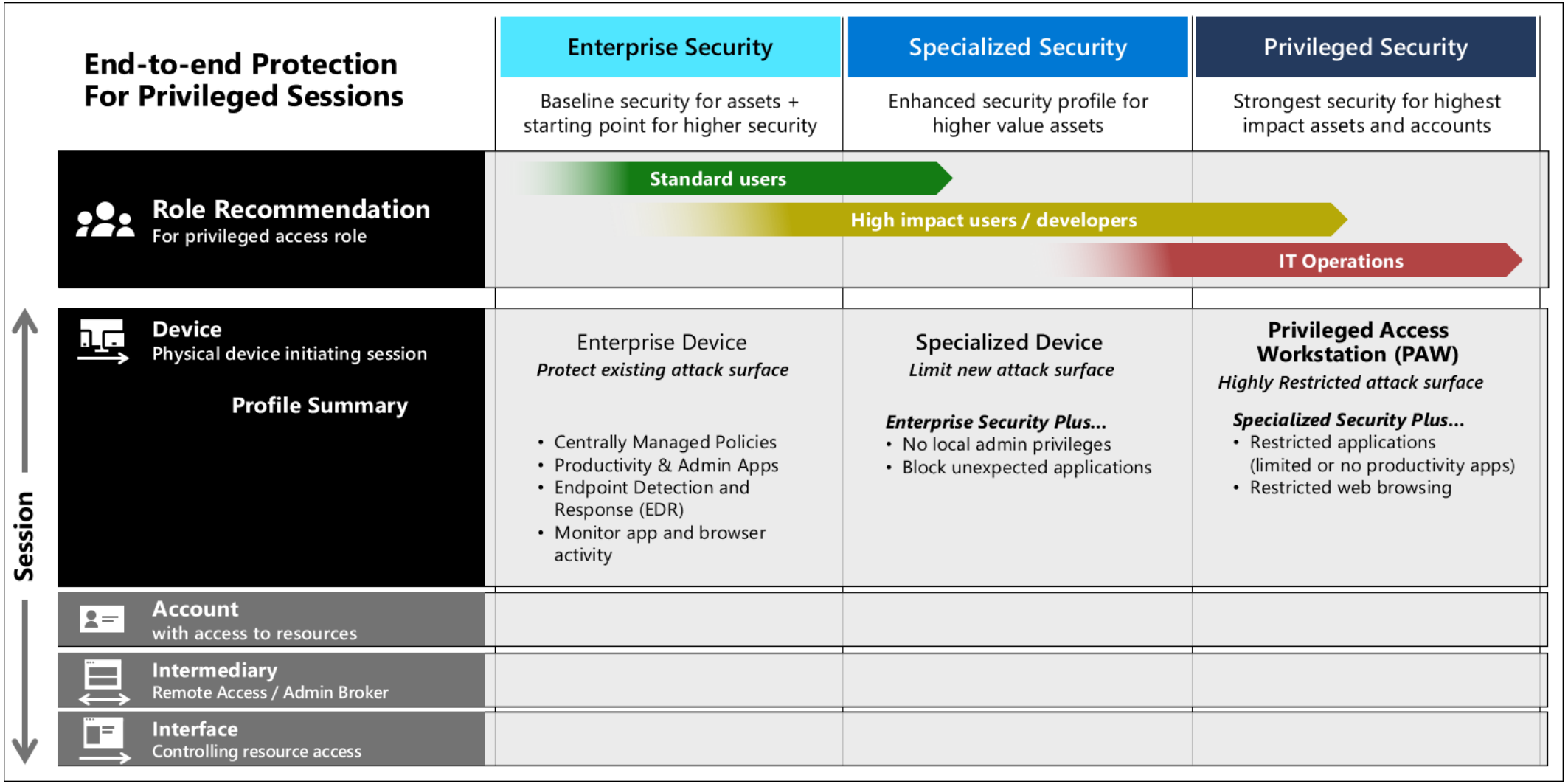


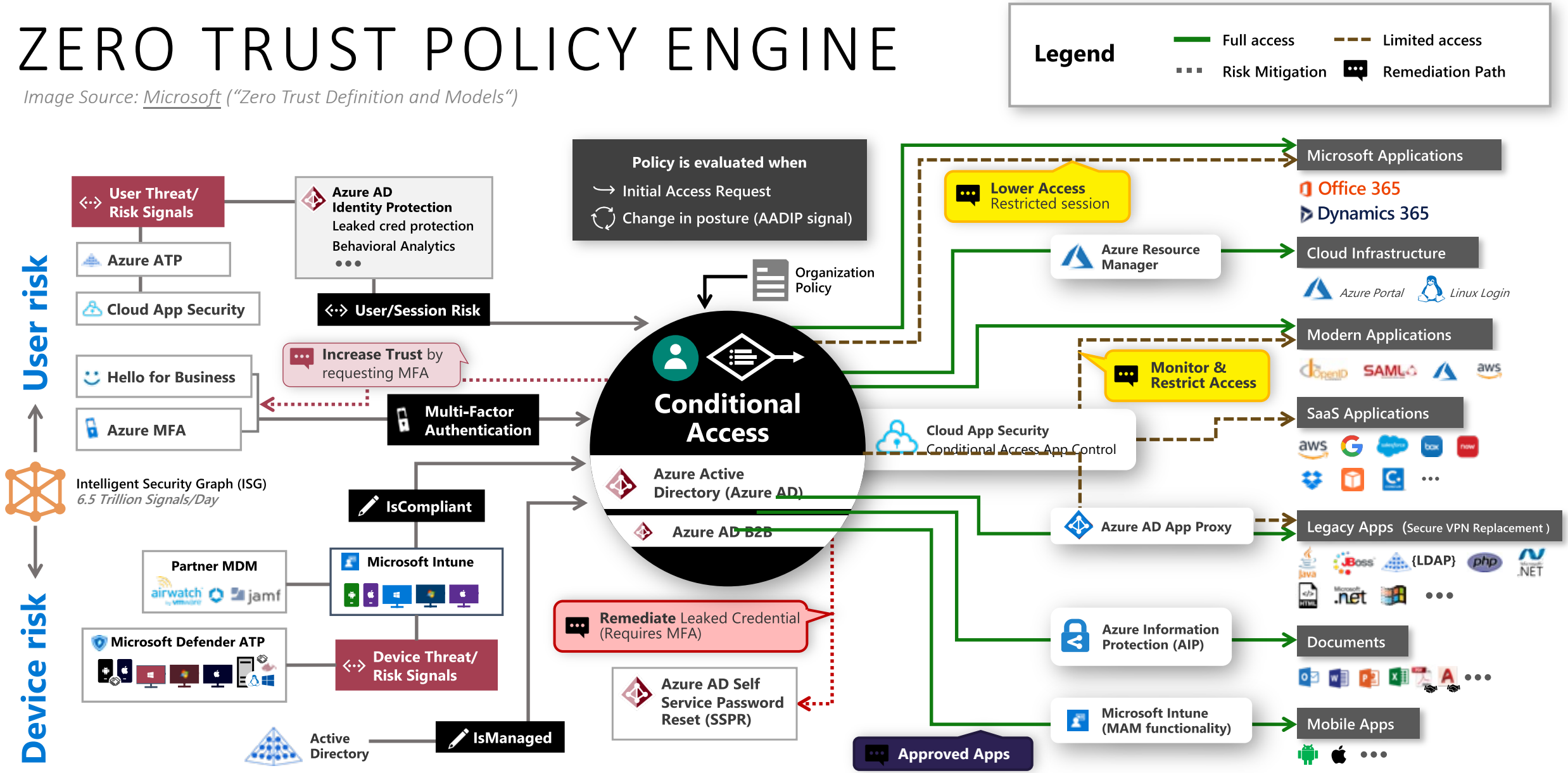
Image Source: Microsoft ("Securing devices as part of the privileged access story")

Advanced Scenarios:
Privileged Access and CA Policies

LIVE DEMO

ZERO TRUST POLICY ENGINE

Image Source: Microsoft ("Zero Trust Definition and Models")

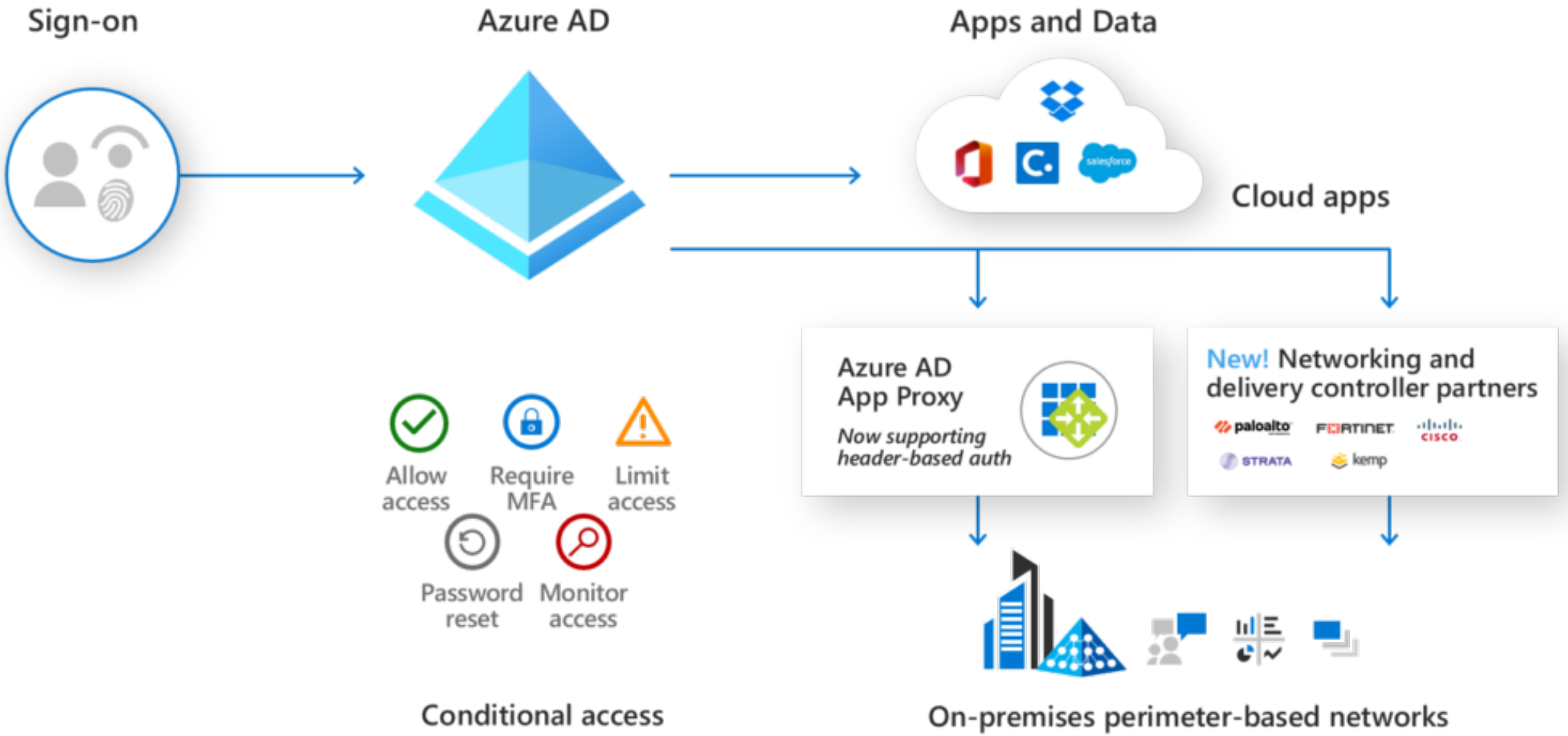


Signal
to make an informed decision

Decision
based on organizational policy

Enforcement
of policy across resources

SECURE HYBRID ACCESS



Source: Identity at Microsoft Ignite: Rising to the challenges of secure remote access and employee productivity

SECURE HYBRID ACCESS

SILVERFORT

Discover applications on:

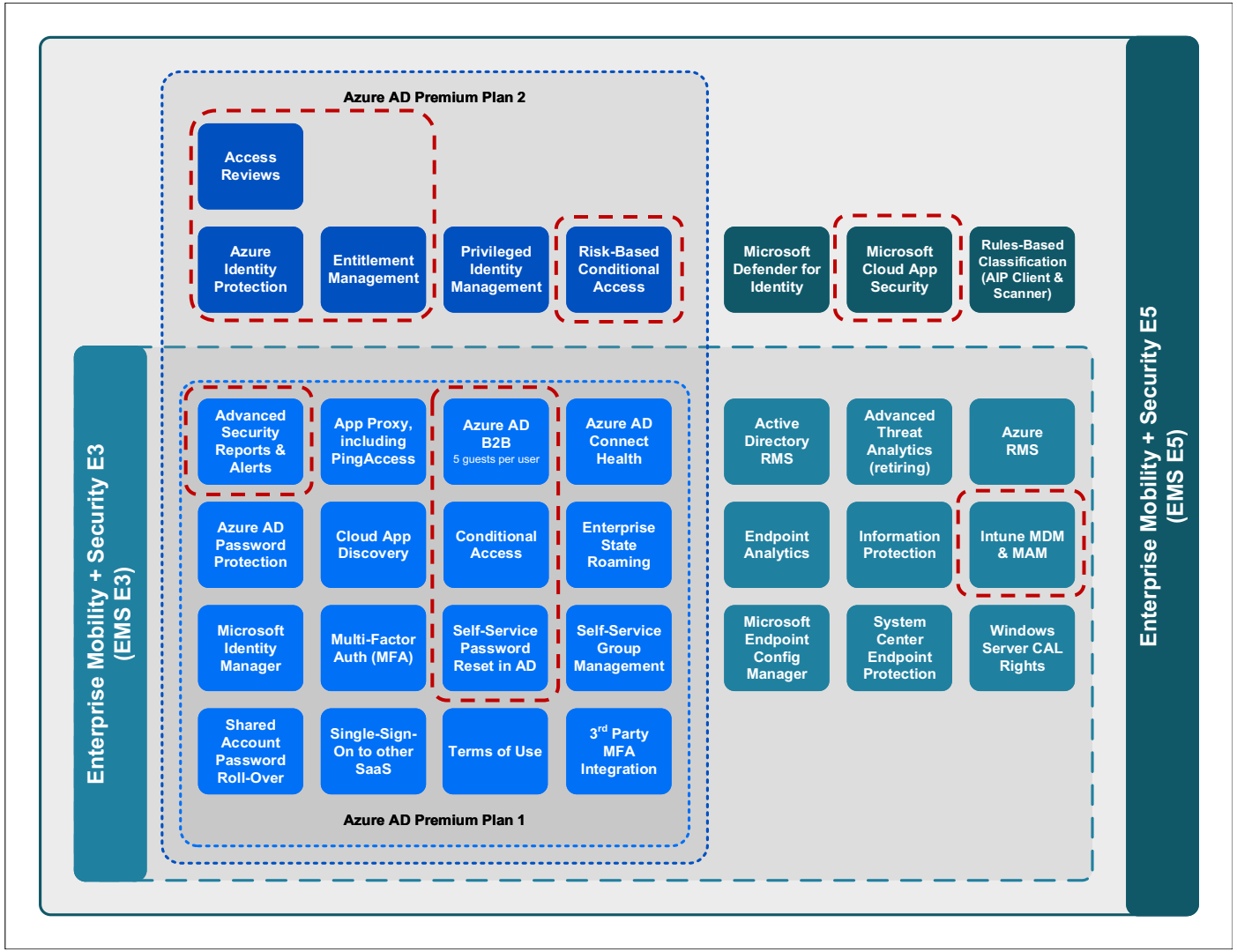
- AD FS
- Active Directory
- 3rd party identity providers
- LDAP directories

Protect legacy resources such as:

- Homegrown / legacy apps
- Remote administration (SSH, PowerShell)
- Windows RDP
- File shares and databases
- Domain Controllers
- Hypervisors

Source: "Top 7 Microsoft Identity partnership announcements at Ignite 2020" & Prevent attacks by protecting your applications with Azure Active Directory

(CLOUD) SECURITY COSTS MONEY!



Source: Licensing Repository by Aaron Dinnage

THANK YOU

@Thomas_Live

Thomas@Naunheim.net

www.cloud-architekt.net