Deep Dive into Conditional Access

Thomas Naunheim

aMS Germany
16.11.2021

Thomas Naunheim

Cloud Security Architect
@glueckkanja-gab AG

@Thomas_Live
www.cloud-architekt.net

glueckkanja-gab

Azure Meetup BONN

Microsoft® Most Valuable Professional

Thanks to our SPONSORs

Vielen Dank an unsere Partner!

Sponsors

yubico

CRESTRON

Jabra GN

Organizing sponsor

BECHTLE

Organisatorischer Partner

Deep Dive into Conditional Access
Agenda

Overview of Azure AD Conditional Access

Extension of Conditions and Controls

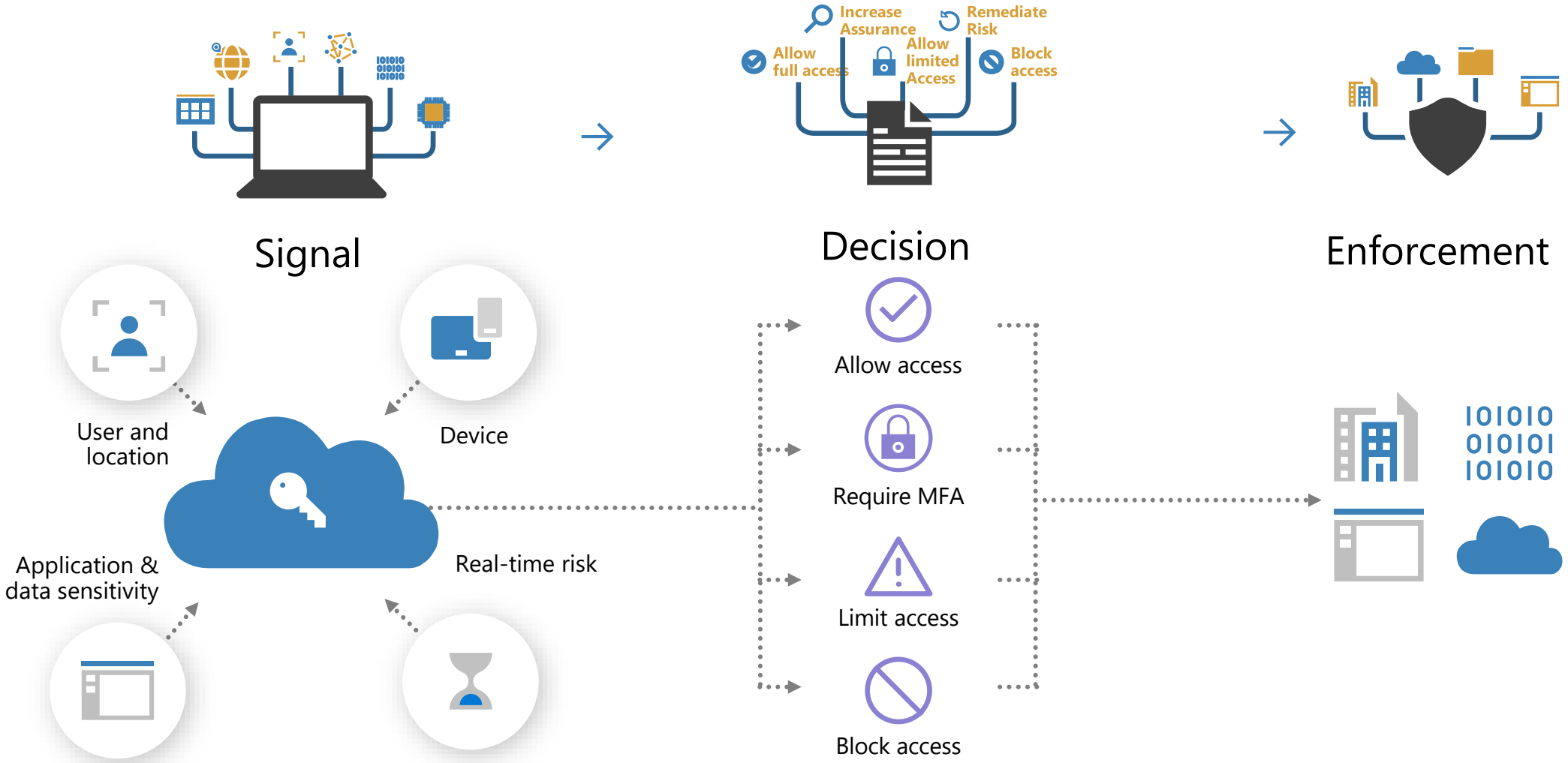
Design and Implementation of CA Policies

Monitoring and Reporting of "Zero Trust Policies"

Overview of Conditional Access

Principals of Signal, Decision and Enforcement

Overview of Conditional Access



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

Overview of Conditional Access

When this happens…

*A **user** from **(group) "Marketing employees"** is accessing **"Office 365"** from **a browser** on a **Windows** device from **any location** and **no sign-in risk** was detected.*

…then do this!

*Require a user with strong **(multi-factor) authentication** and **device to be marked as compliant.** No session control (device) or password change (user) is required.*

CA Policy

- id
- displayName
- state

Conditions

- Users, Groups, Apps/Actions
- Identity Risk, Device, Locations and Client Apps

Access Controls

1. Block Access
2. Grant Access
3. Session Controls

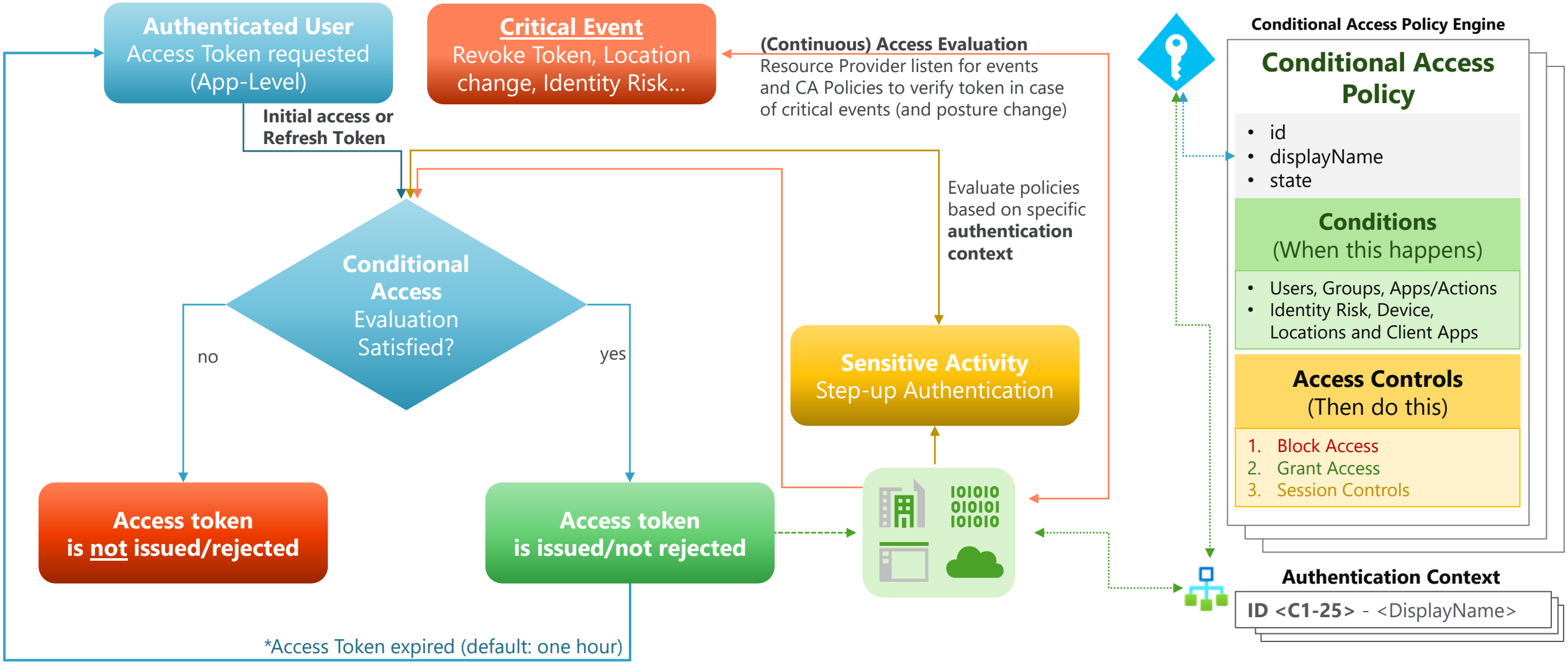
MS Graph: "/identity/conditionalAccess/policies"

```
id             : <ID>
displayName    : Office 365: Require MFA and compliant device
state          : enabled

conditions     : {
                  "users": {…},
                  "applications": {…},
                  "platforms": {…},
                  "locations": {…},
                  "signInRiskLevels": […],
                  "clientAppTypes": […]
                 }

grantControls: {
                  "operator": "OR",
                  "builtInControls": […],
                  "customAuthenticationFactors": [],
                  "termsOfUse": []
                 }
sessionControls: {}
```

Trigger of Conditional Access Evaluation

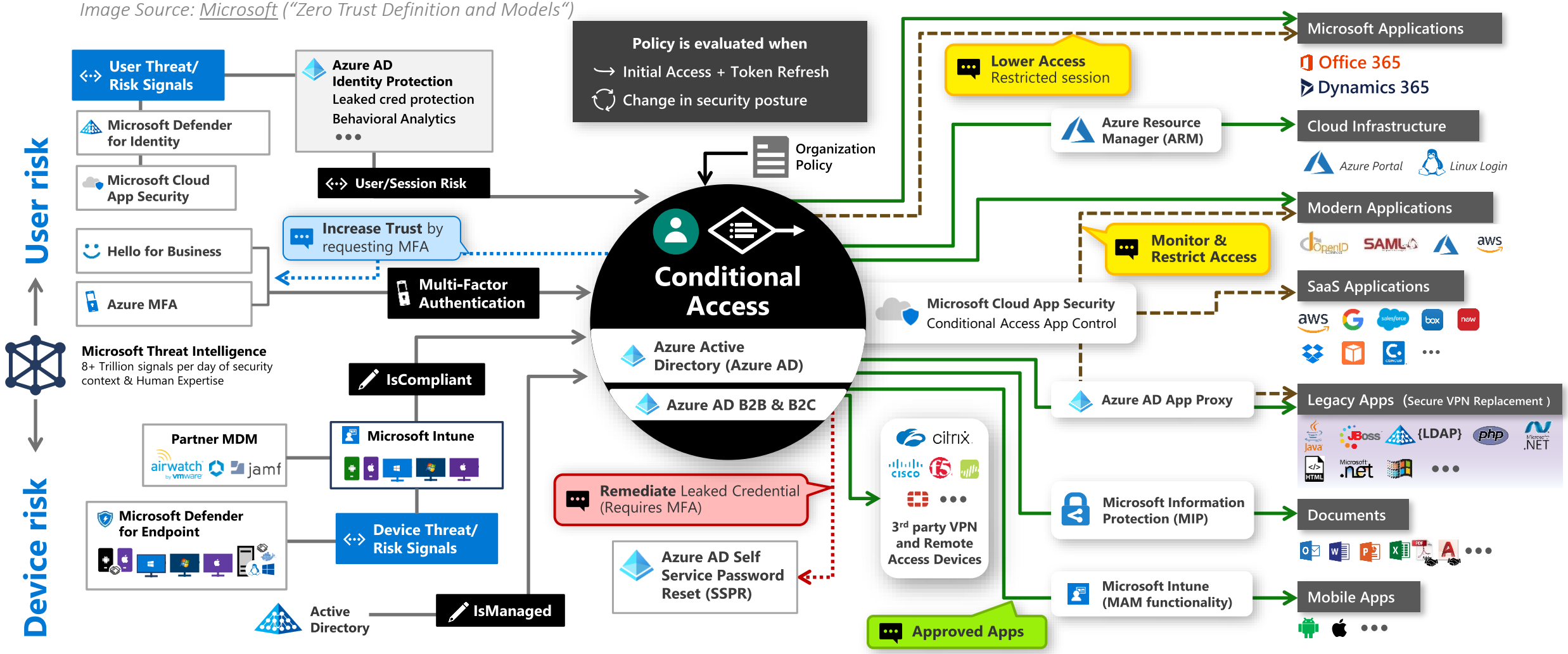


Extension of Conditions & Controls

Integration of Identity Protection and Defender for Cloud Apps

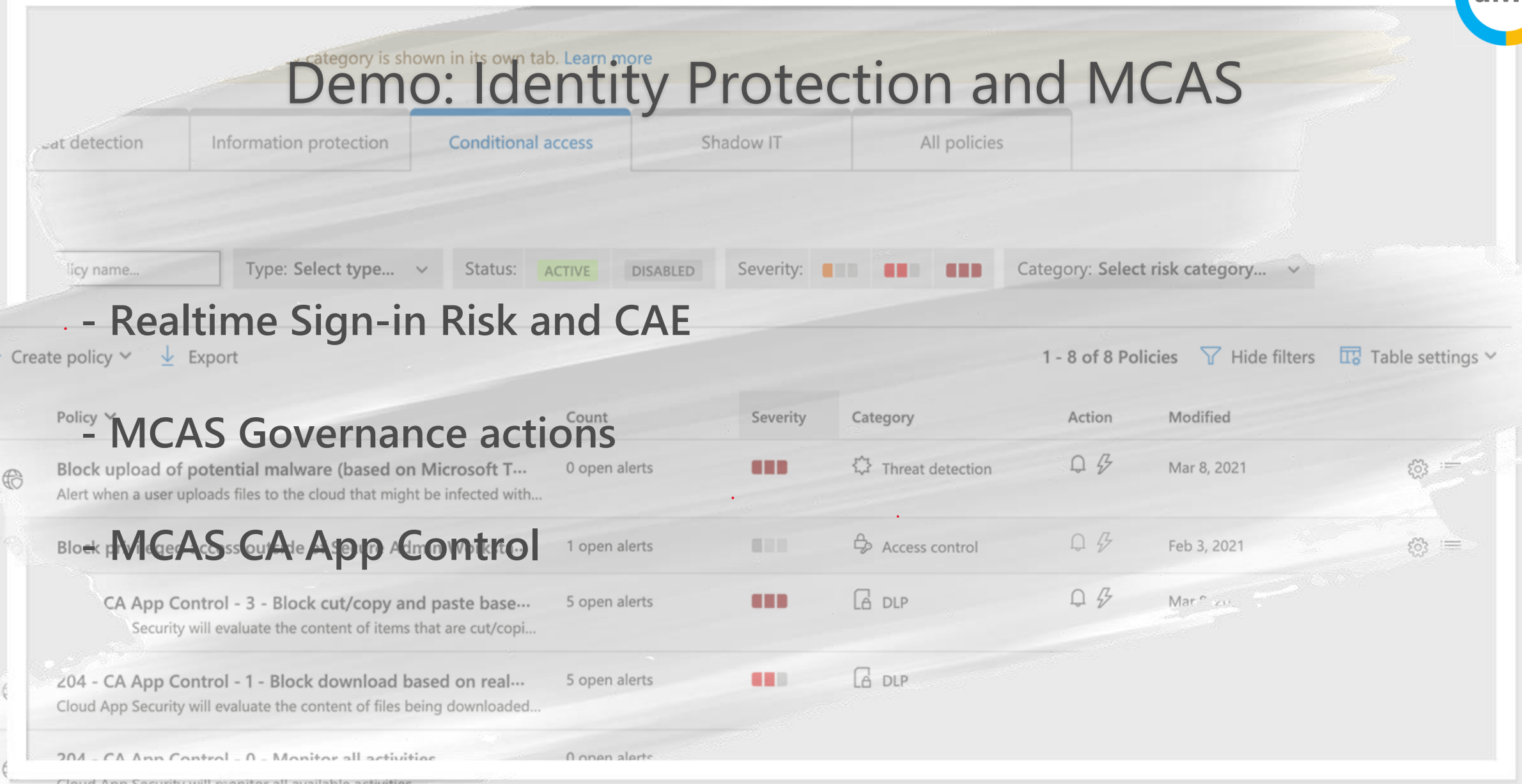
Conditional Access Integration Capabilities

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



Demo: Identity Protection and MCAS

- Realtime Sign-in Risk and CAE
- MCAS Governance actions
- MCAS CA App Control



Design and Implementation of CA Policies

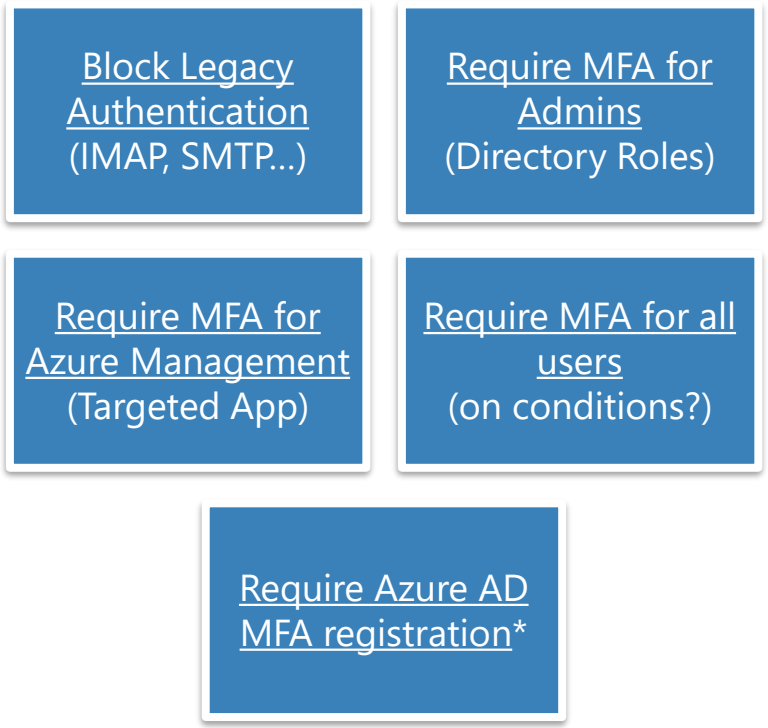
Best Practices and Common Policies

Design of CA Baseline

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

Common Policies by Microsoft

Equivalent policies (enabled by security defaults)



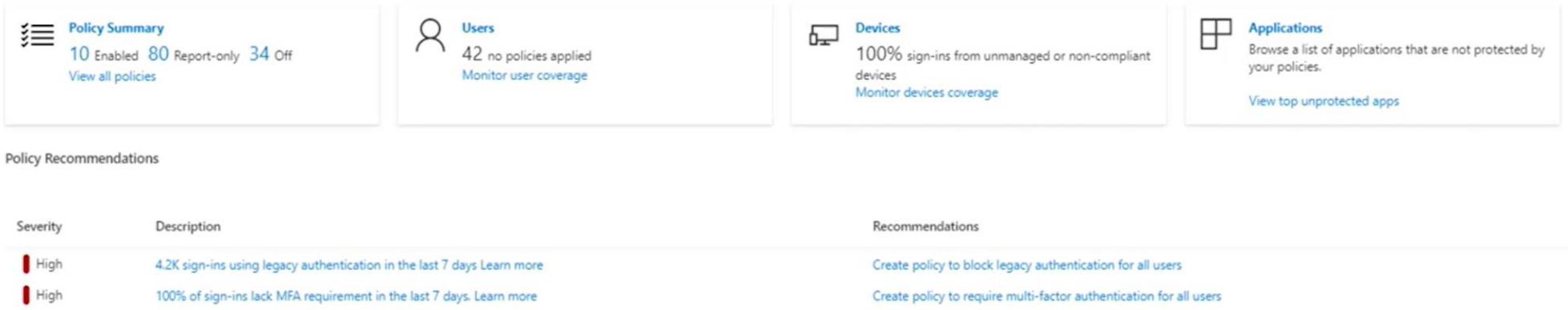
* Azure AD P2 License required
** Intune License required

Additional Policies (Common policies)

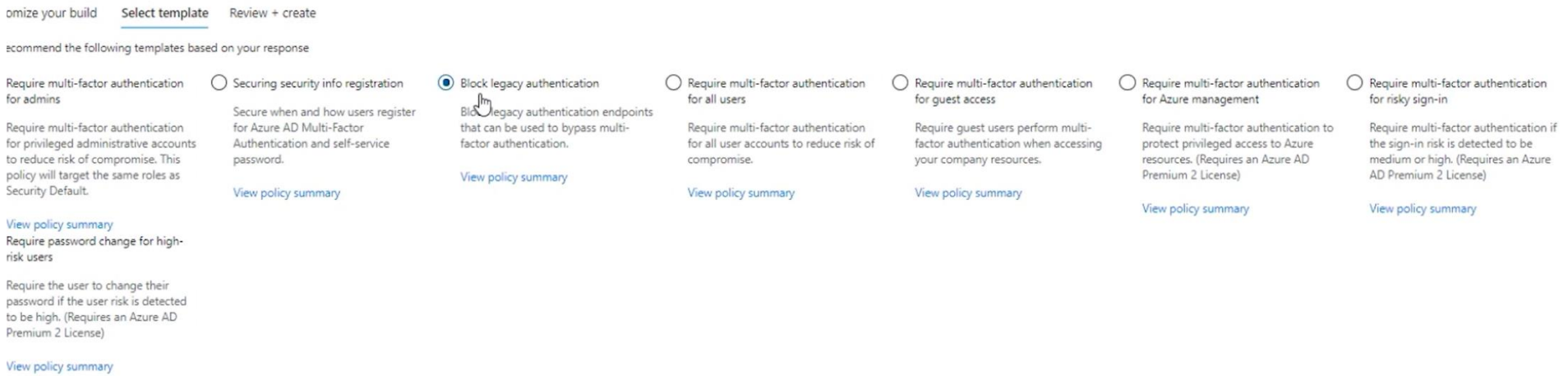
- Sign-in risk-based Conditional Access*
- User risk-based Conditional Access*
- Require compliant device**
- Securing security info registration
- Apply app data protection policies**
- Require approved apps and app protection**
- Block access except specific apps
- Block access by location

Ignite H2/2021: Improvements for CA Adoption

- Summary of Conditional Access Configuration and coverage incl. recommendations



- Create built-in policy templates for common use cases (right from recommendations/overview)



Source: Ignite Session (BRK242) "Strengthen resilience with identity innovations in Azure Active Directory"

Policy Fundamentals in Design

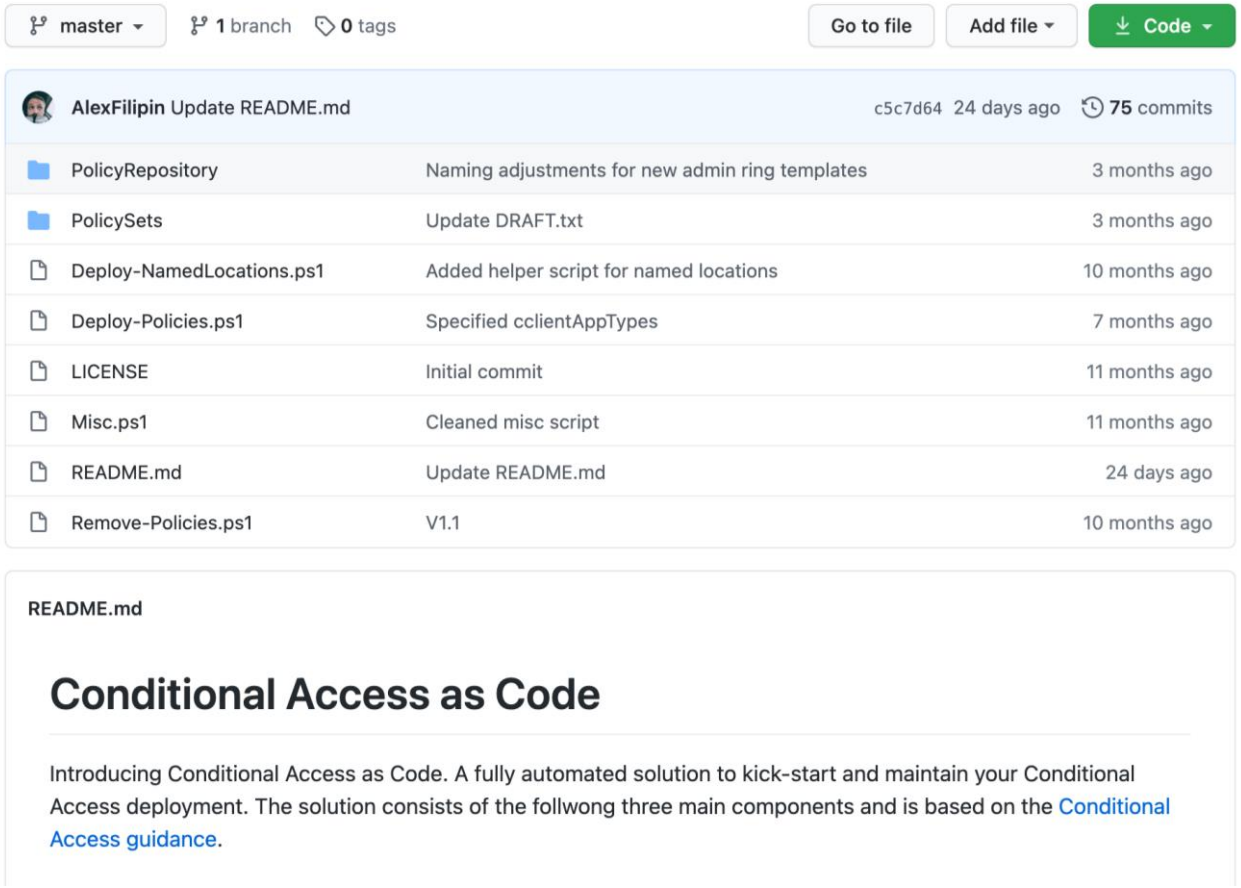
- **Build strong baselines for users** (hybrid, privileged and guests) **and apps/APIs**
- Define a **consistent naming** convention for policies (that fits to your policy set and env.)

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

- **Consider your environment** (types of apps, devices and authentication methods)!
  - Rollout of **Strong (User) Authentication and Passwordless Journey** (MFA, WHfB)
  - Security level on personas (Guest, Trusted Partners, CXO, Privileged Users)
  - **Protection level and access paths of „Apps & Data“** (incl. Privileged Interfaces)
  - **Integration level and signals from Endpoints** (AAD-joined + MDM, VDI, BYOD?)

Conditional Access As Code (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

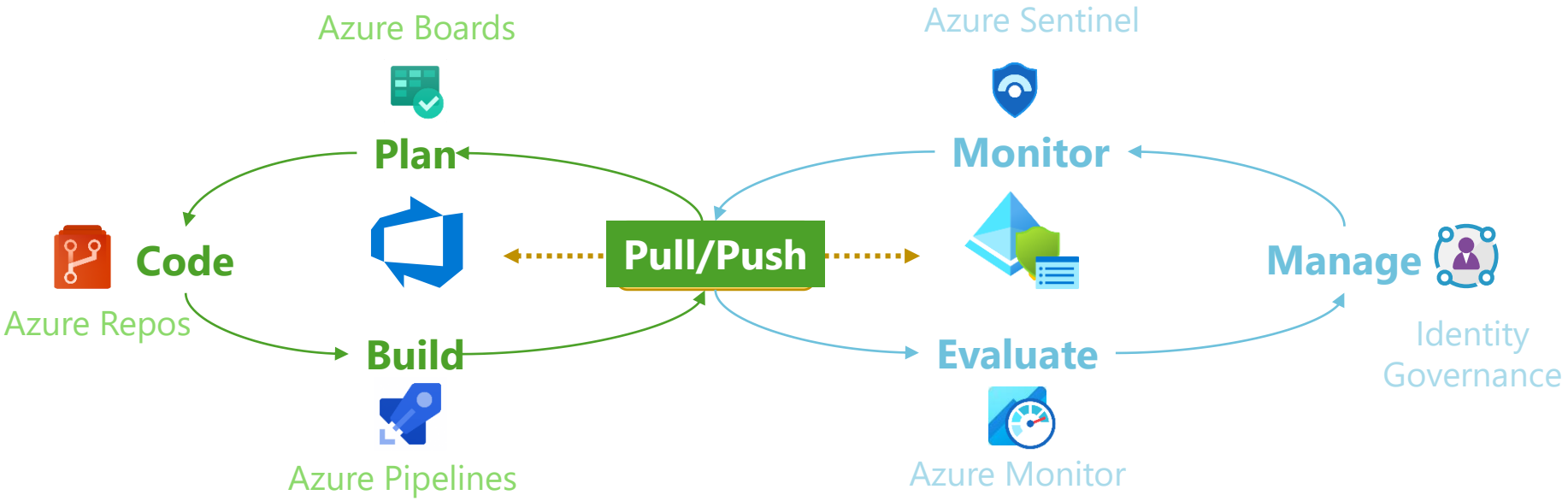
Automation solution

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.

- Repository: „AlexFilipin/ConditionalAccess“ (GitHub)
- 425show episode with talk about the policy templates

Policies As Code - Project “AADOps”



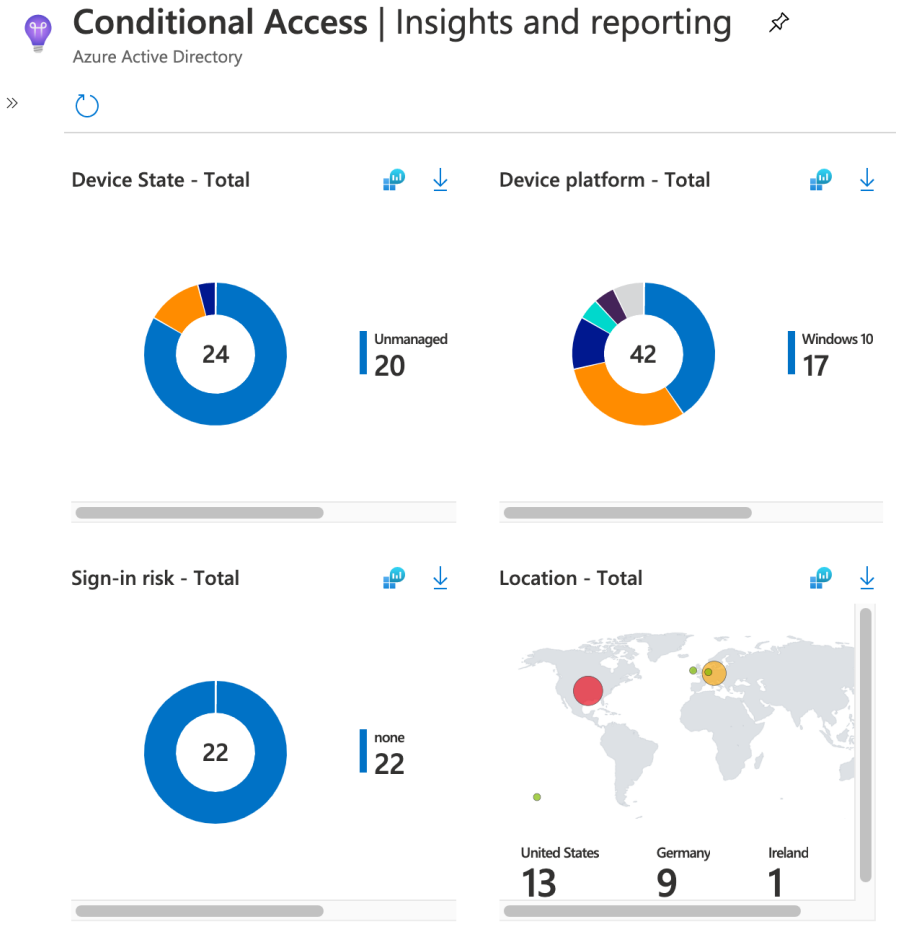
Demo: AADOps

- Different policy designs
- Advantages in using (Azure) Repos and Pipelines
- Templates and Deployment to Intra- vs. Inter-Staging
- Management of Exclusions

Monitoring and Reporting of "Zero Trust Policies"

Insights (Workbooks) and Azure Sentinel for SecOps

Overview of Capabilities and Use Cases



Identity Operations (Azure AD Workbooks)
Analyses and Visualizations to understand impact of Conditional Access Policies and gaps in your environment.

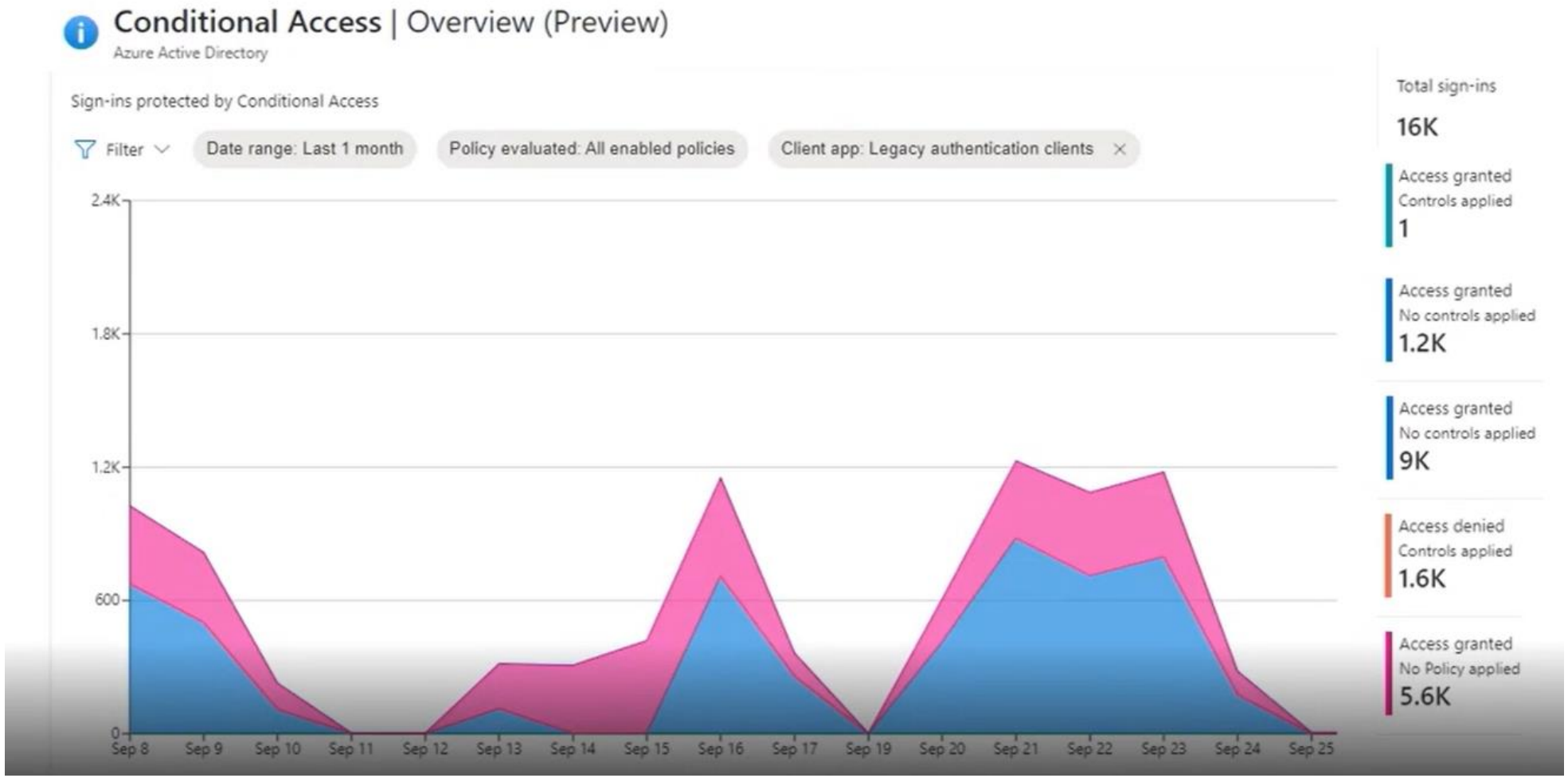
Audit of Management (Azure AD Audit Logs)

- CA Policies (changes outside of automated process)
- Exclusion Groups (changes outside of Identity Governance)
- State change (Deactivated, Report-only, Activated)

Security Monitoring (Azure Sentinel)

- Attempt to bypass conditional access rule in Azure AD
- Anomalous sign-in detections from CA excluded accounts

Ignite H2/2021: Improvement of CA Dashboard with Gap-Analyzer and Recommendations



Source: Ignite Session (BRK242) "Strengthen resilience with identity innovations in Azure Active Directory"

Demo: Azure Workbooks and Azure Sentinel

- Workbooks in Azure AD and Azure Sentinel
- Audit Logs in Azure AD and M365 Defender
- Analytic Rules in Azure Sentinel


THANK YOU!
MERCI !