



Deep Dive into Conditional Access



aMS Germany

16.11.2021

Thomas Naunheim





Thomas Naunheim

Cloud Security Architect
@glueckkanja-gab AG

@Thomas_Live
www.cloud-architekt.net

glueckkanja■gab

Azure Meetup
BONN

 Microsoft®
Most Valuable
Professional

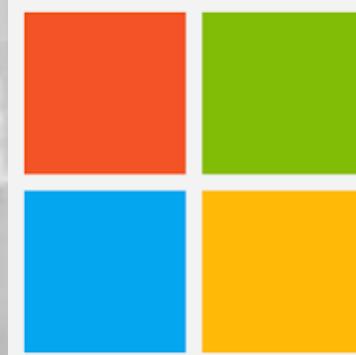
Thanks to our SPONSORS

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**



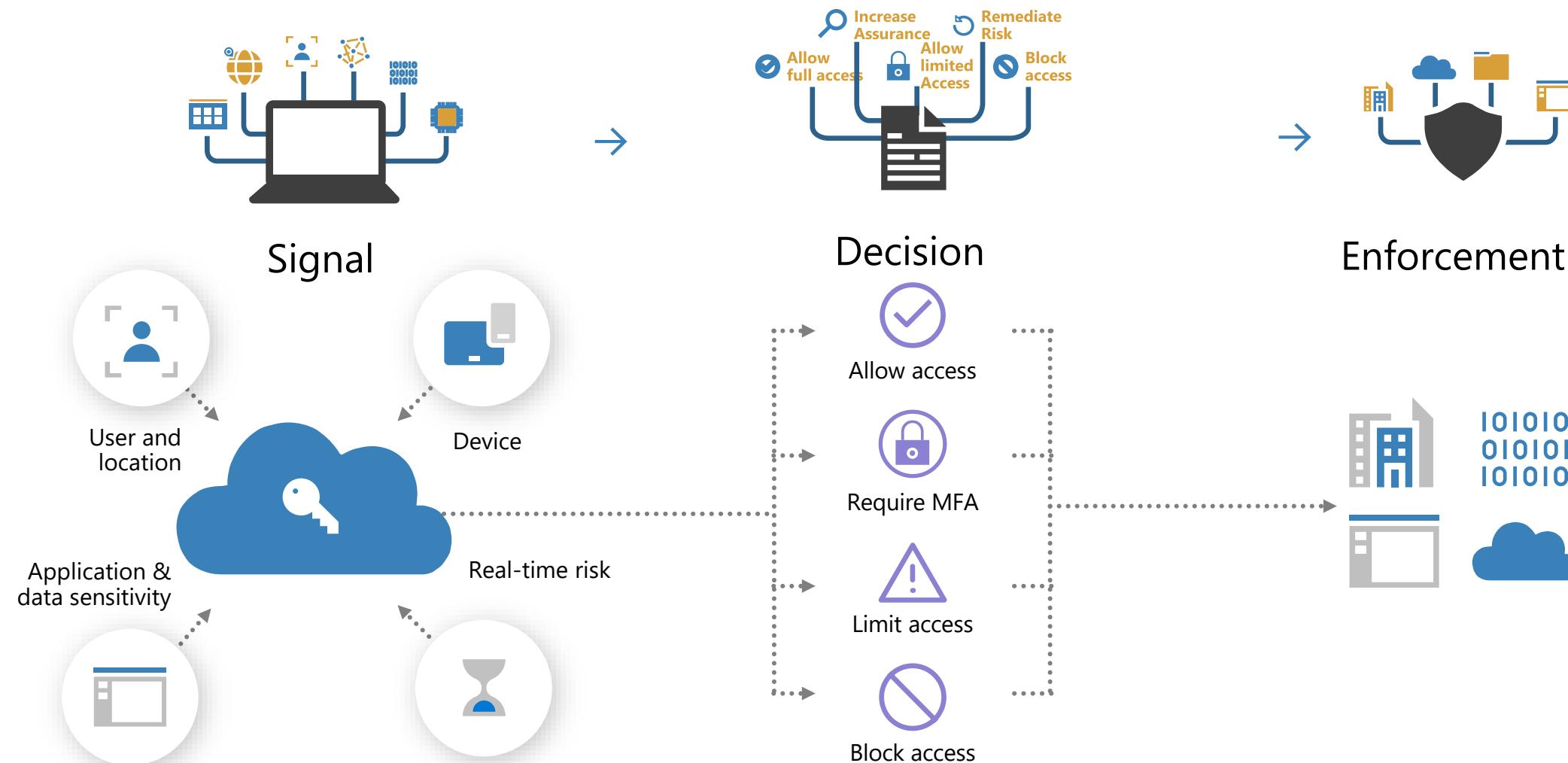
**Monitoring and
Reporting of
“Zero Trust Policies”**



Overview of Conditional Access

Principles of Signal, Decision and Enforcement

Overview of Conditional Access



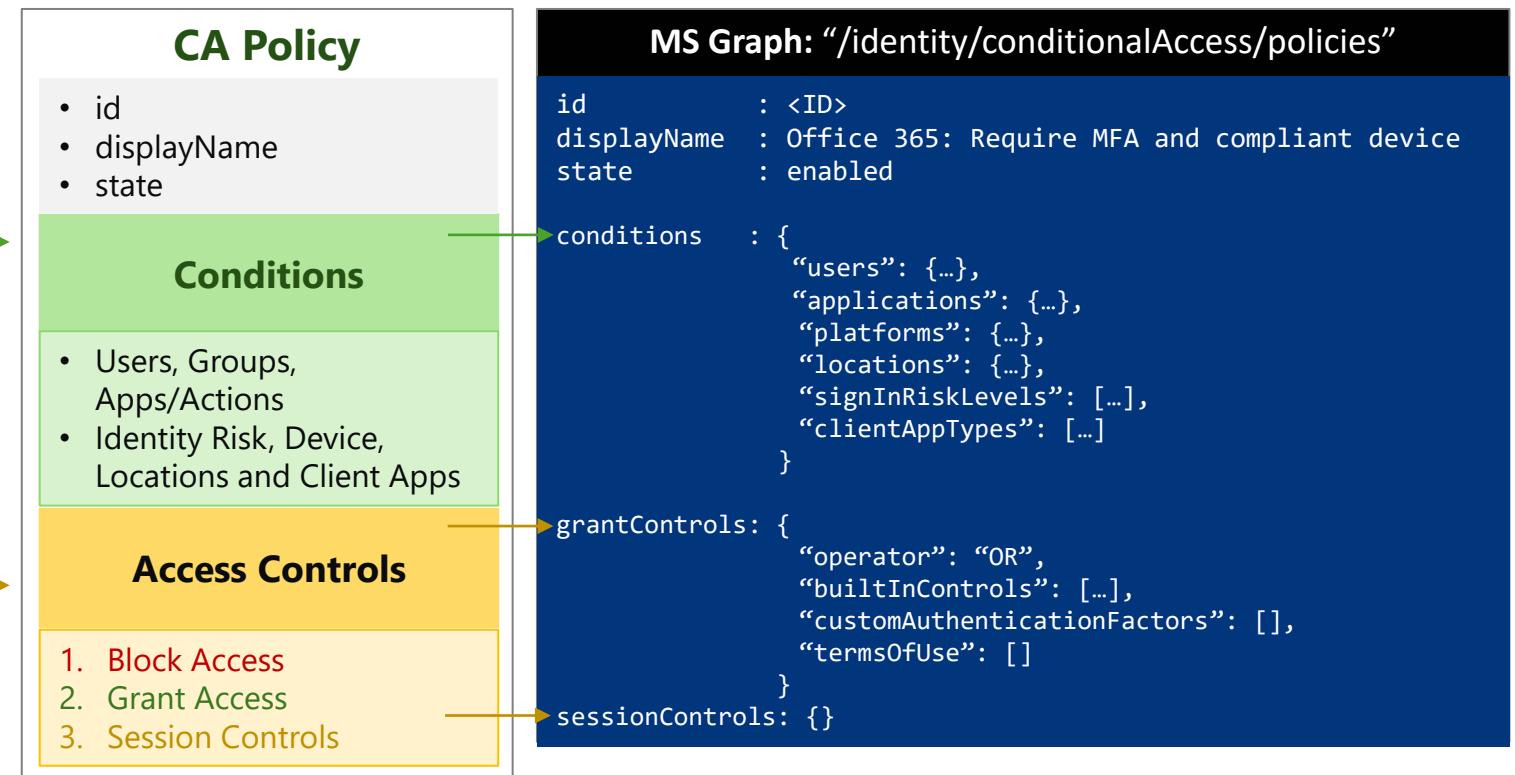
Overview of Conditional Access

When this happens...

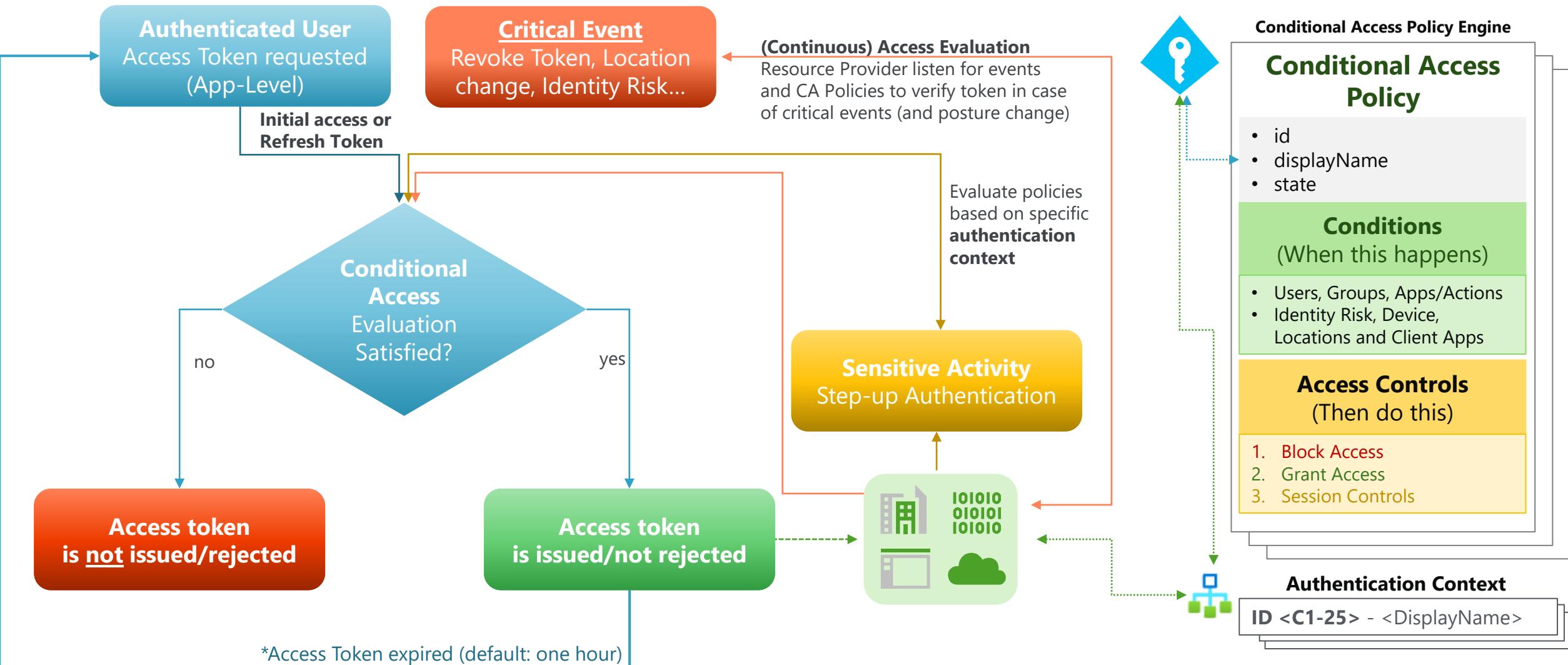
A user from (group) “**Marketing employees**” is accessing “**Office 365**” from a browser on a **Windows** device from **any location** and **no sign-in risk** was detected.

...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.



Trigger of Conditional Access Evaluation



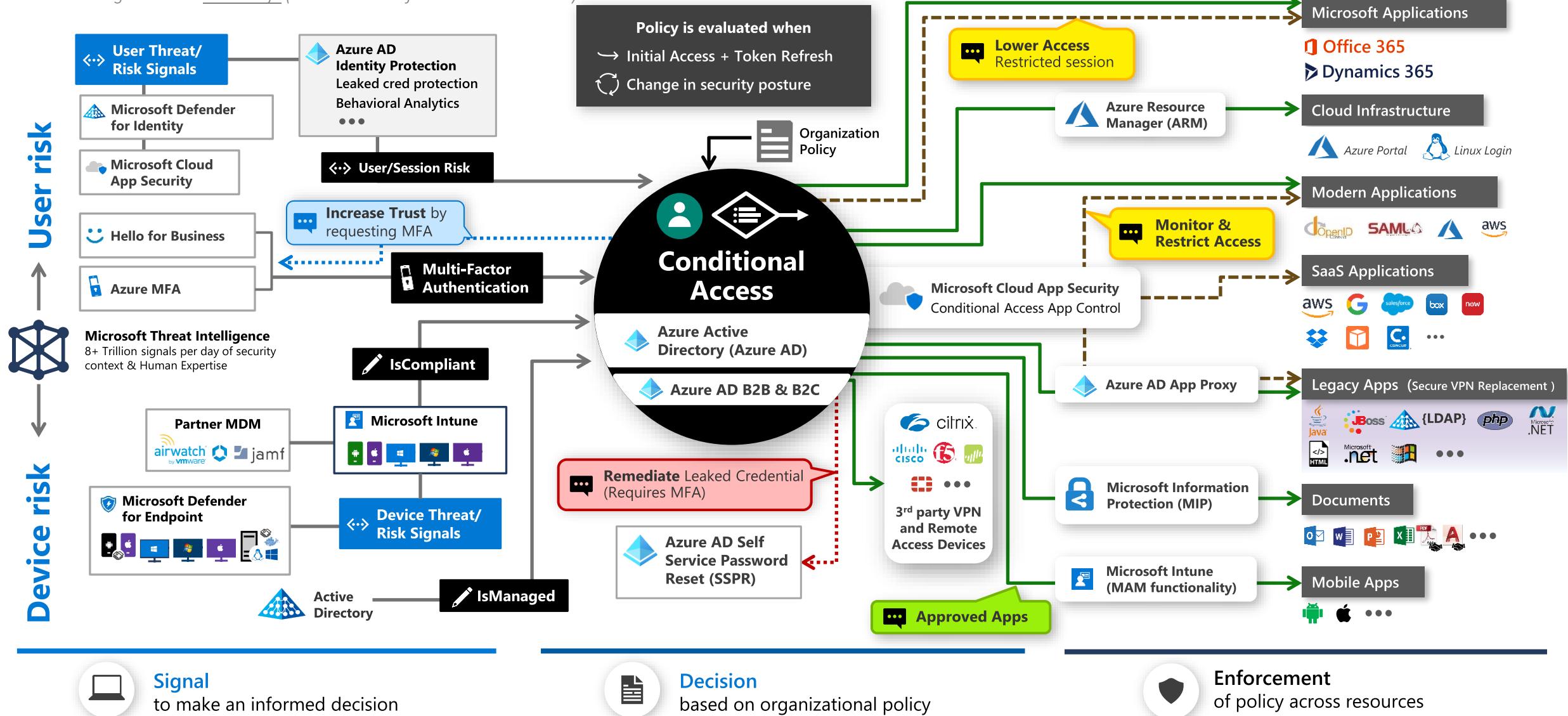
Extension of Conditions & Controls

Integration of Identity Protection and Defender for Cloud Apps

Conditional Access Integration Capabilities



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





category is shown in its own tab. [Learn more](#)

Demo: Identity Protection and MCAS

Wat detection

Information protection

Conditional access

Shadow IT

All policies

Policy name...

Type: Select type... ▾

Status:

ACTIVE

DISABLED

Severity:



Category: Select risk category... ▾

- Realtime Sign-in Risk and CAE

+ Create policy ▾ Export

1 - 8 of 8 Policies

Hide filters

Table settings ▾

Policy

- MCAS Governance actions



Block upload of potential malware (based on Microsoft T...

Count

0 open alerts

Severity

Category

Action

Modified



Mar 8, 2021



Alert when a user uploads files to the cloud that might be infected with...

- MCAS CA App Control



CA App Control - 3 - Block cut/copy and paste base...

1 open alerts

5 open alerts



Access control



Feb 3, 2021



Security will evaluate the content of items that are cut/copi...

204 - CA App Control - 1 - Block download based on real...

5 open alerts



DLP



Mar 8, 2021



Cloud App Security will evaluate the content of files being downloaded...

204 - CA App Control - 0 - Monitor all activities

0 open alerts

Cloud App Security will monitor all available activities.

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)

Block Legacy Authentication
(IMAP, SMTP...)

Require MFA for Admins
(Directory Roles)

Require MFA for Azure Management
(Targeted App)

Require MFA for all users
(on conditions?)

Require Azure AD MFA registration*

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

* Azure AD P2 License required

** Intune License required



Ignite H2/2021: Improvements for CA Adoption

- Summary of Conditional Access Configuration and coverage incl. recommendations



Policy Recommendations

Severity	Description	Recommendations
High	4.2K sign-ins using legacy authentication in the last 7 days. Learn more	Create policy to block legacy authentication for all users
High	100% of sign-ins lack MFA requirement in the last 7 days. Learn more	Create policy to require multi-factor authentication for all users

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

The screenshot shows a web interface for selecting a Conditional Access policy template. At the top, there are three navigation links: 'Optimize your build', 'Select template' (which is underlined, indicating it's the active tab), and 'Review + create'. Below this, a heading says 'Recommend the following templates based on your response'. There are six policy templates listed in two columns of three.

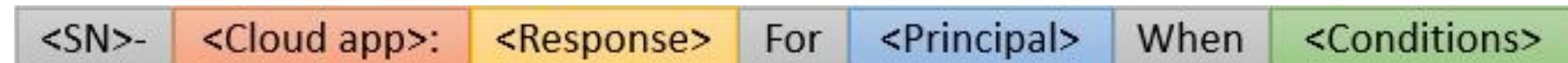
Template Description	Template Description	Template Description	Template Description		
Require multi-factor authentication for admins	Securing security info registration	Block legacy authentication	Require multi-factor authentication for all users	Require multi-factor authentication for guest access	Require multi-factor authentication for Azure management
Require multi-factor authentication for privileged administrative accounts to reduce risk of compromise. This policy will target the same roles as Security Default.	Secure when and how users register for Azure AD Multi-Factor Authentication and self-service password.	Block legacy authentication endpoints that can be used to bypass multi-factor authentication.	Require multi-factor authentication for all user accounts to reduce risk of compromise.	Require guest users perform multi-factor authentication when accessing your company resources.	Require multi-factor authentication to protect privileged access to Azure resources. (Requires an Azure AD Premium 2 License)
View policy summary	View policy summary	View policy summary	View policy summary	View policy summary	View policy summary

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 following 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

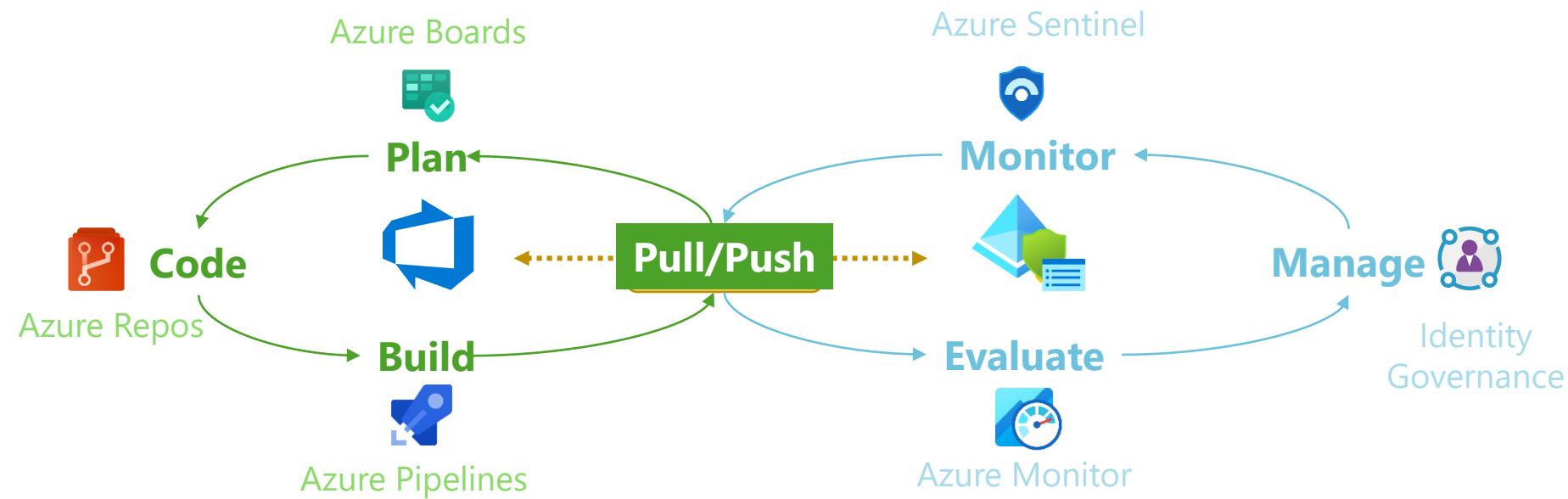
Automation solution

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

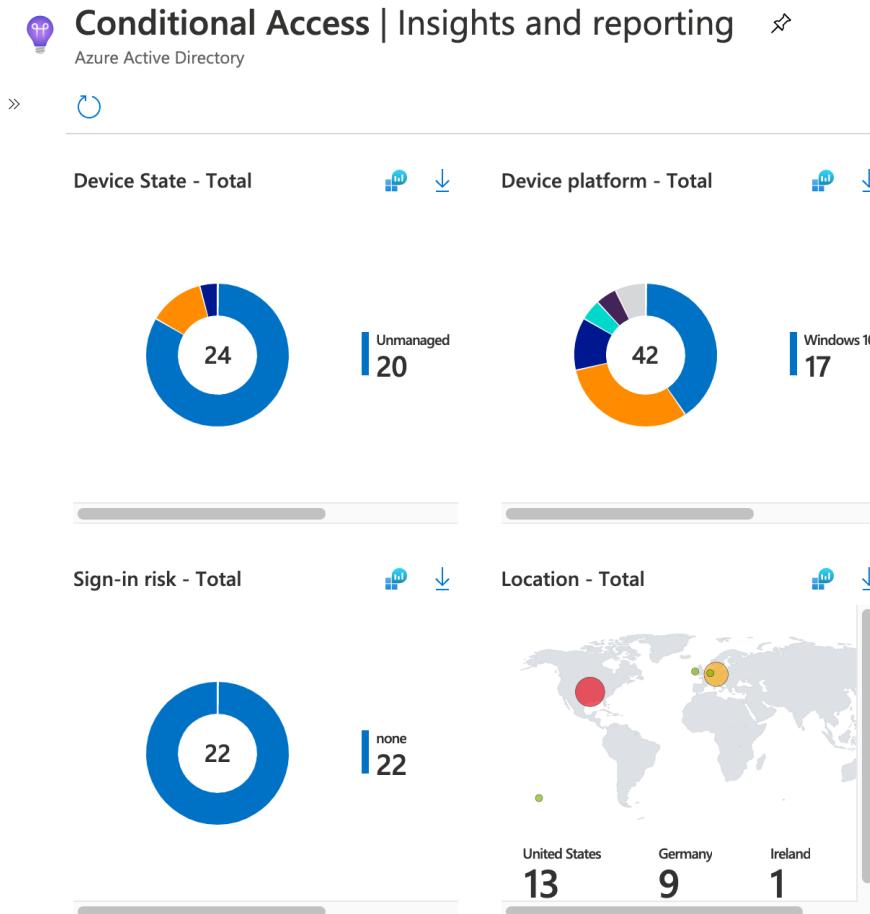
- Management of Exclusions



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

Conditional Access policy: All enabled policies

Time range: Last 24 hours

User: All users

App: All apps

Data view: users

Impact Summary

Click on a tile to filter by the policy result below

- Workbooks in Azure AD and Azure Sentinel



- Audit Logs in Azure AD and M365 Defender

- Analytic Rules in Azure Sentinel

Breakdown per condition and sign-in status

Download results to Excel or open query in Log Analytics by clicking the icons in the upper right corner of each query.

Device state - Total



Device platform - Total



THANK YOU!
MERCI!

