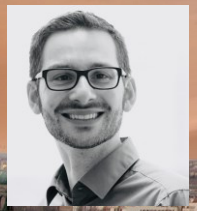
Deep Dive into Conditional Access



Thomas Naunheim

aMS Berlin 2022
19. Mai

Thomas Naunheim

Cloud Security Architect
@glueckkanja-gab AG

@Thomas_Live
www.cloud-architekt.net

glueckkanja-gab

Azure Meetup BONN

CLOUD IDENTITY SUMMIT '22

MVP Microsoft® Most Valuable Professional

Thanks to our SPONSORS

Vielen Dank an unsere Partner!

Organizing sponsor

CoreView

Granikos

DIAMOND sponsors

M365 Kaffeepause
Learning in the flow of work.

Mind Appeal

hub:raum
tech incubator of T

logitech

PLATINUM sponsor

MARTELLO

Organisatorischer Partner

Deep Dive into Conditional Access
Agenda

Overview of Azure AD Conditional Access

Extension of Conditions and Controls

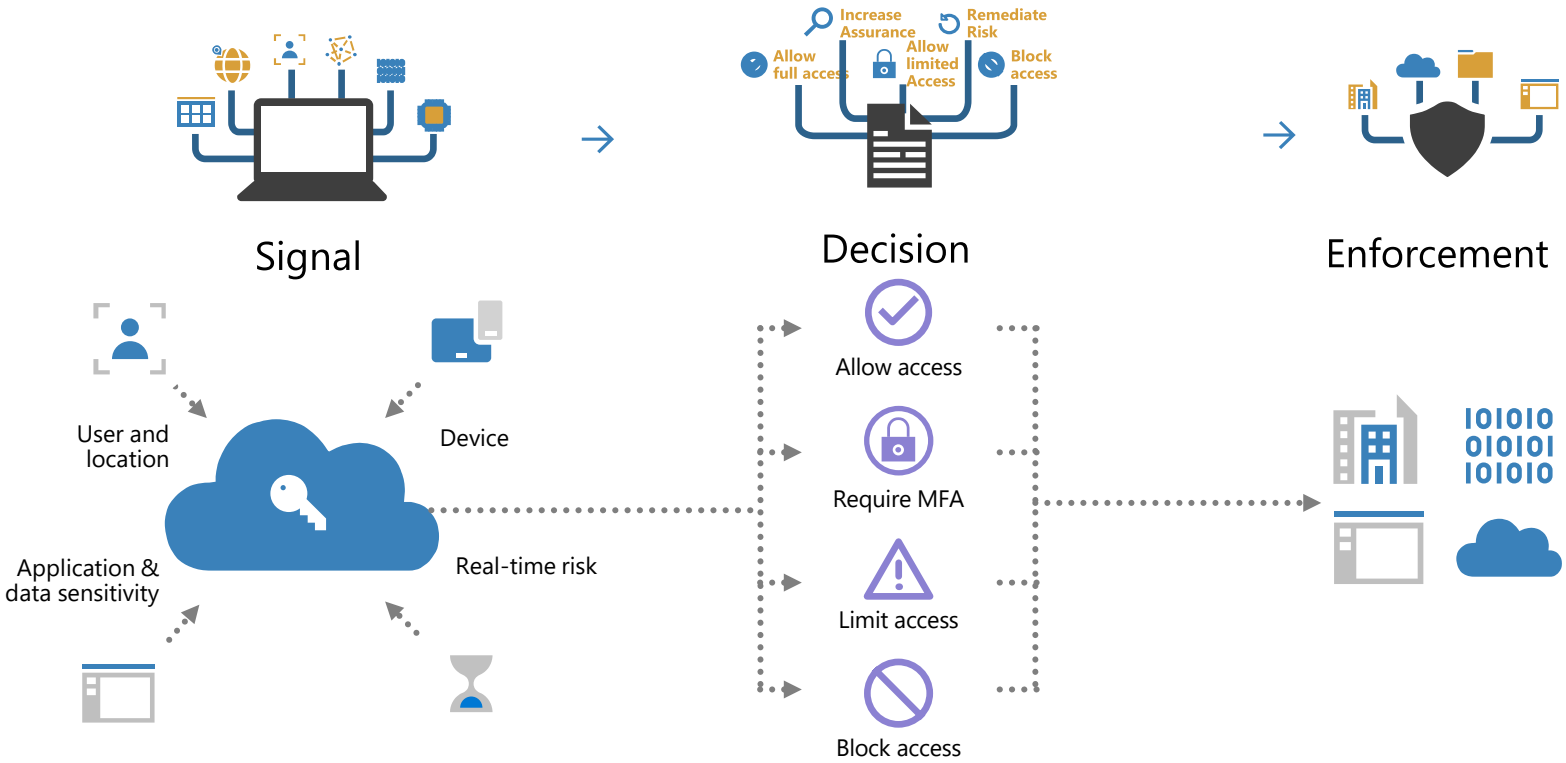
Design and Implementation of CA Policies

Monitoring and Reporting of "Zero Trust Policies"

Overview of Conditional Access

Principals of Signal, Decision and Enforcement

Conditional Access - Zero Trust Policy Engine



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

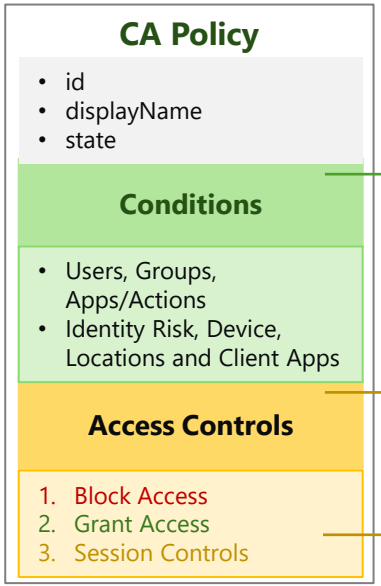
Conditional Access Policy

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.*



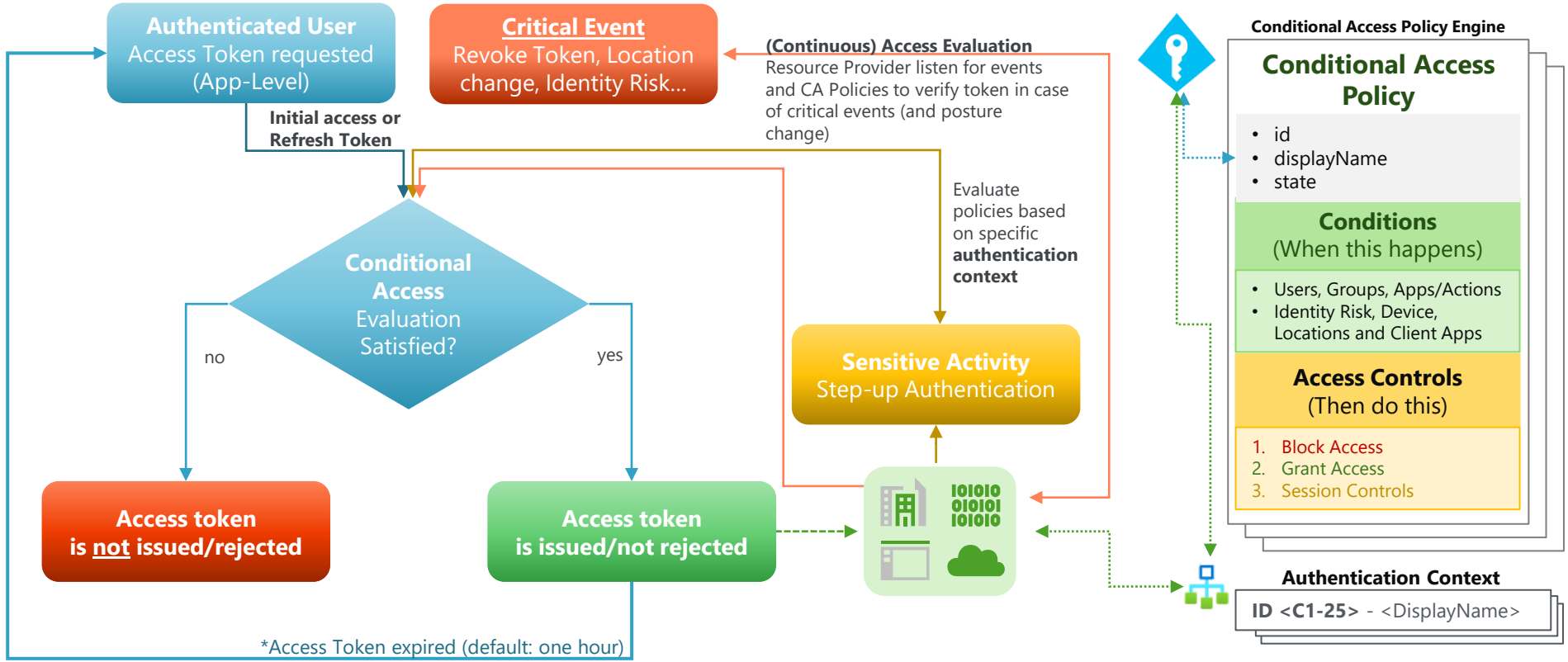
MS Graph: "/identity/conditionalAccess/policies"

```
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

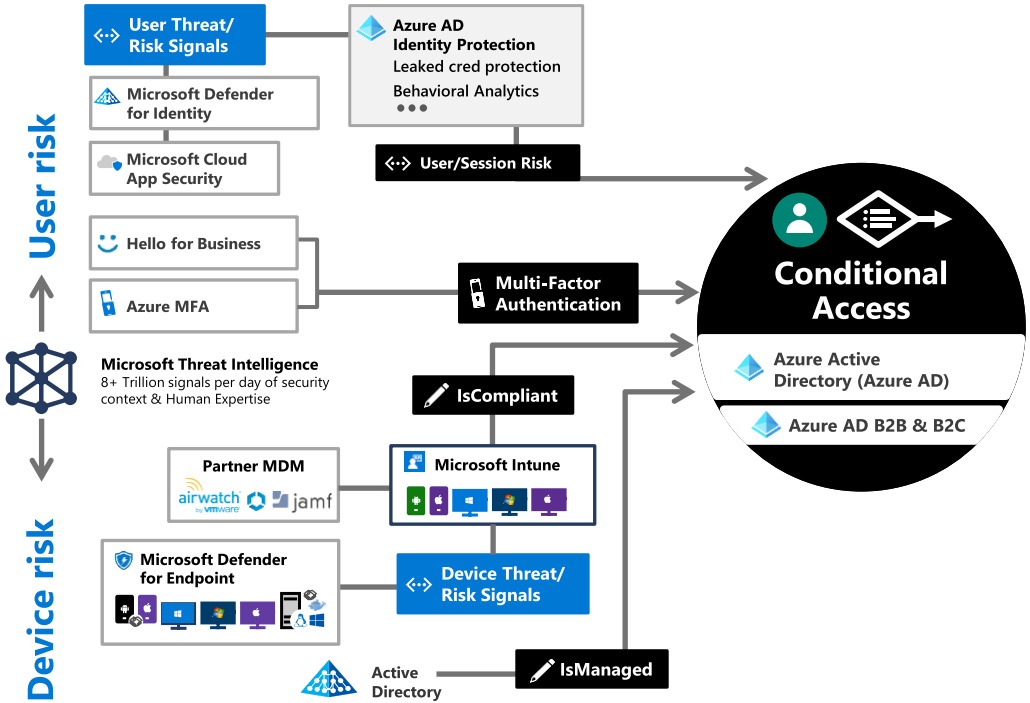


Extension of Conditions & Controls

Integration of Identity Protection and Defender for Cloud Apps

Conditional Access Integration Capabilities

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

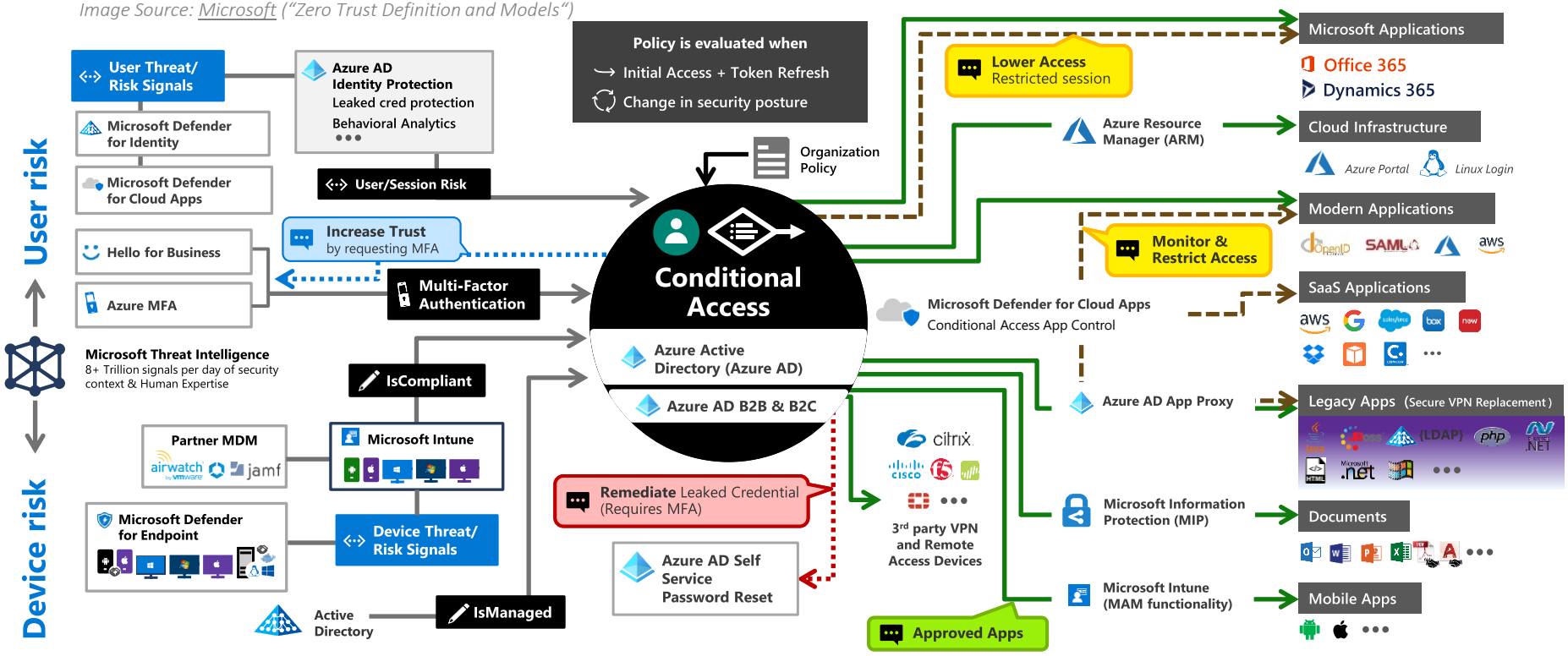


Signal
to make an informed decision

Decision
based on organizational policy

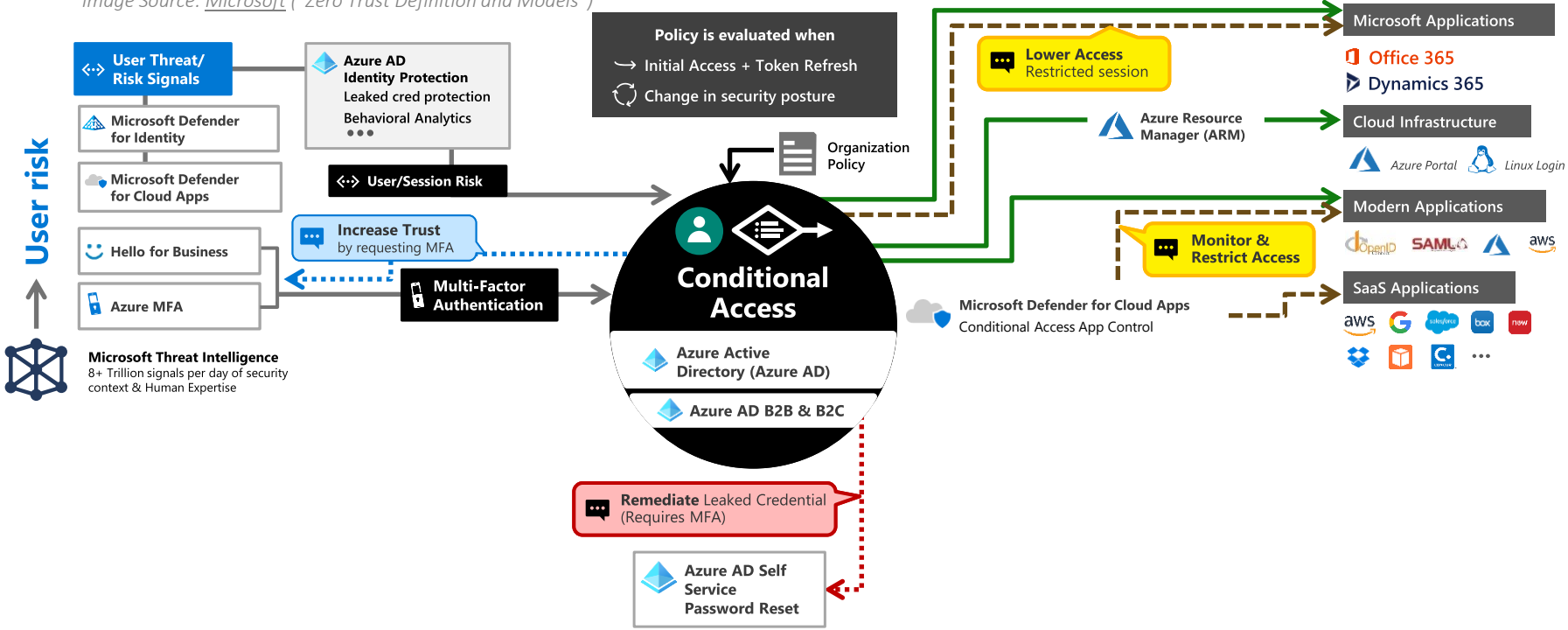
Conditional Access Integration Capabilities

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



Conditional Access Integration Capabilities

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



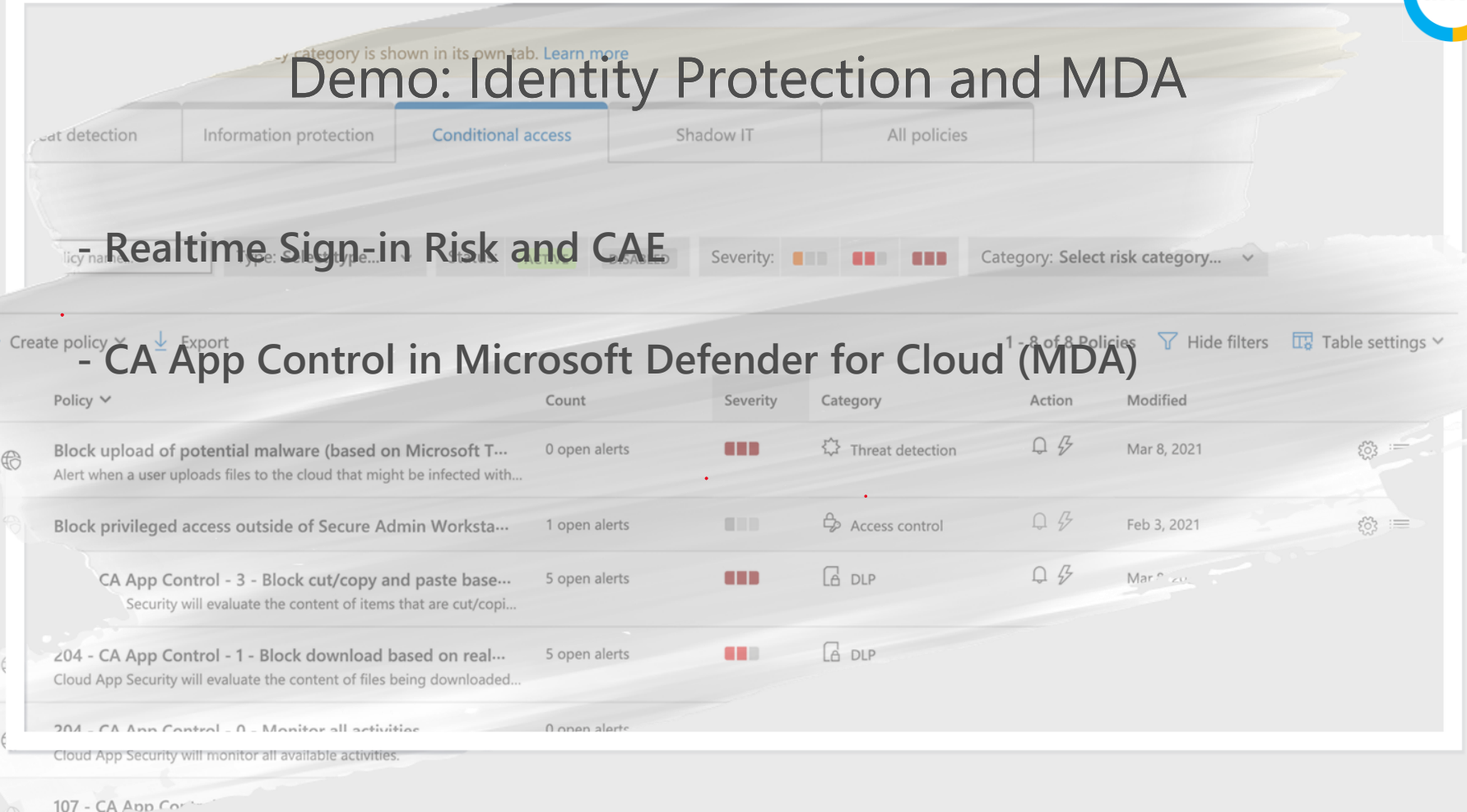
Signal
to make an informed decision

Decision
based on organizational policy

Enforcement
of policy across resources

Demo: Identity Protection and MDA

- Realtime Sign-in Risk and CAE
- CA App Control in Microsoft Defender for Cloud (MDA)



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!
Avoid inconsistent or duplicated policies by smart policy design!

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*

* 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

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

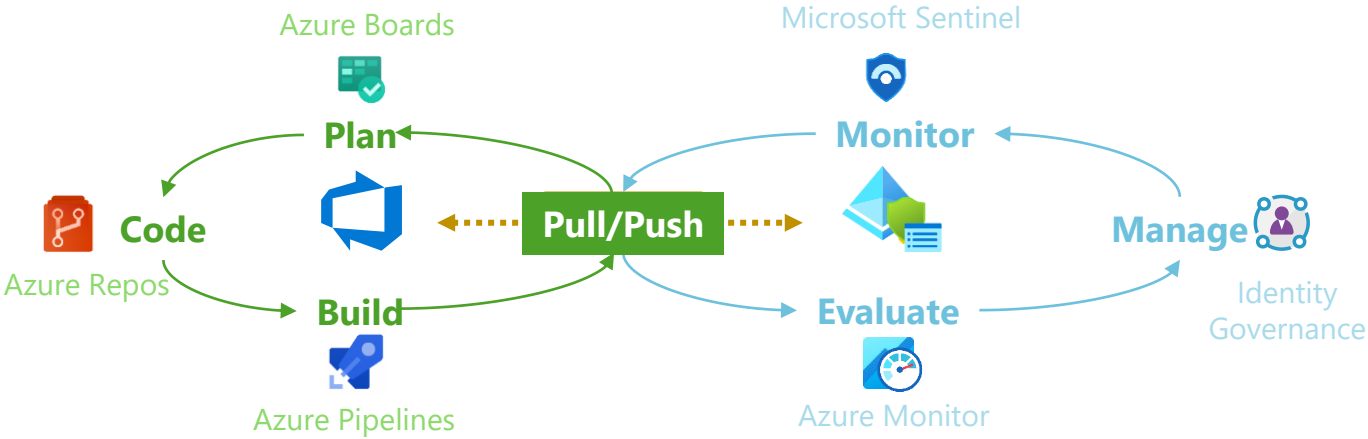
<SN>-	<Cloud app>:	<Response>	For	<Principal>	When	<Conditions>

- **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, AVD/VDI, BYOD?)

Demo: Analyze and implement CA baseline

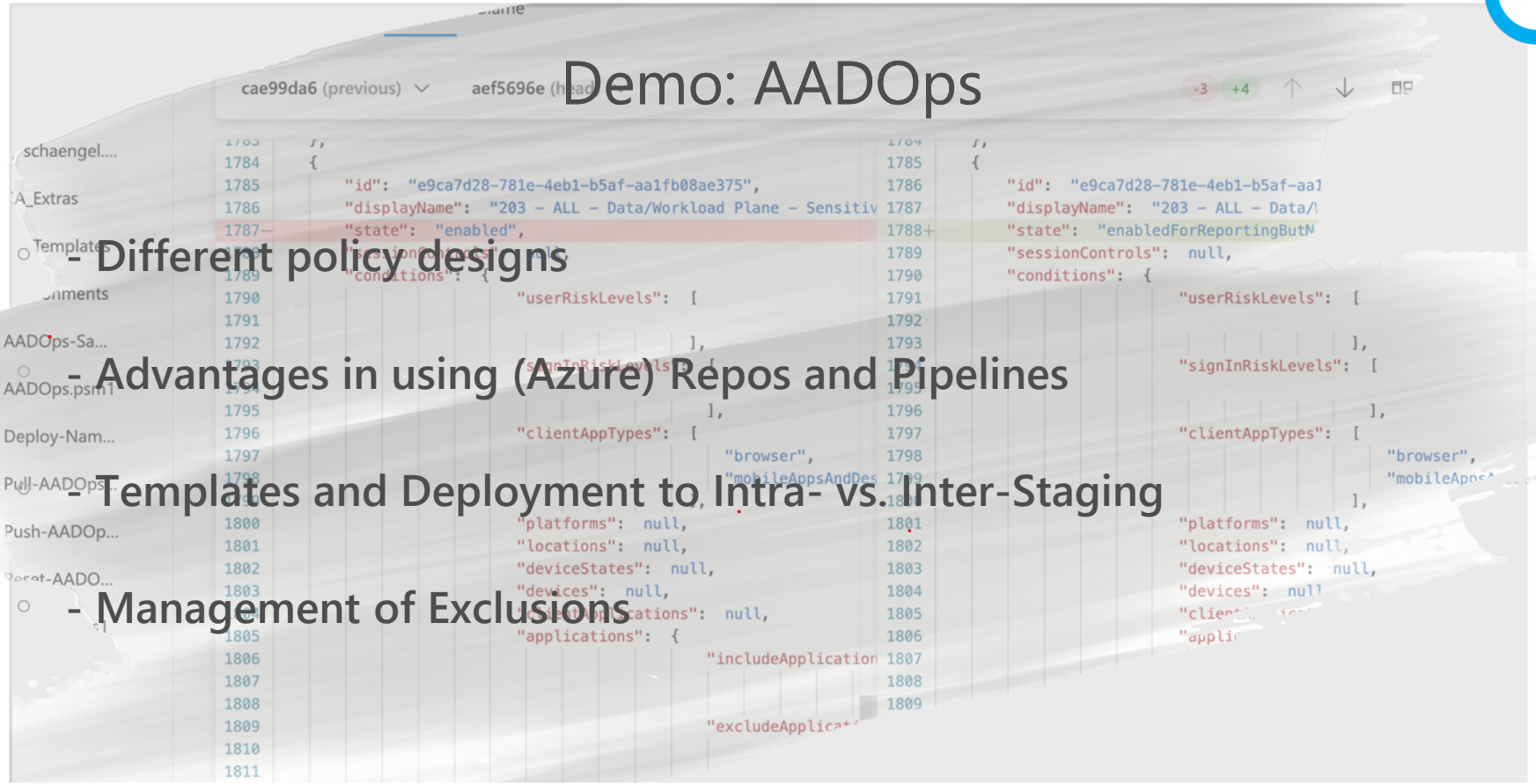
- - Integrated coverage analysis and recommendations
- - Usage & Insights of Authentication Methods / Auth. Prompts
- - Built-in Policy Templates

Policies As Code - Project “AADOps”



Demo: AADOps

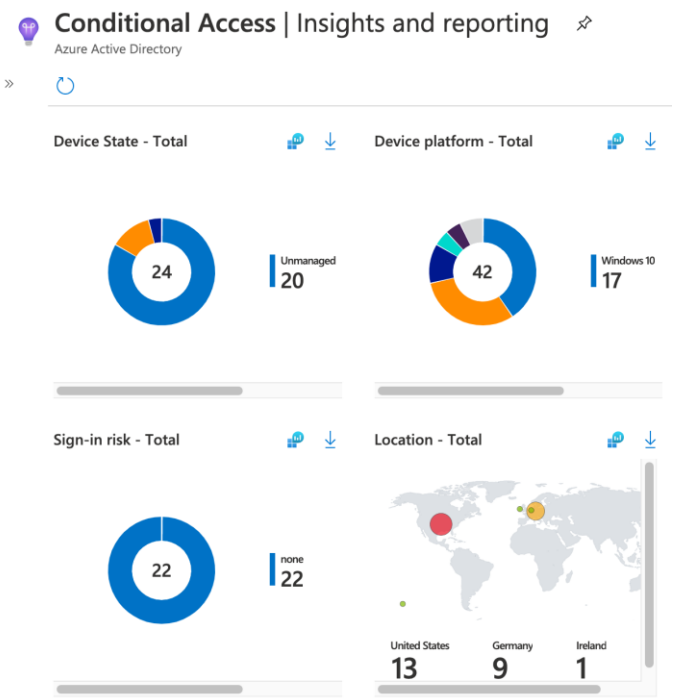
- Different policy designs
- Advantages in using (Azure) Repos and Pipelines
- Templates and Deployment to Intra- vs. Inter-Staging
- Management of Exclusions



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.

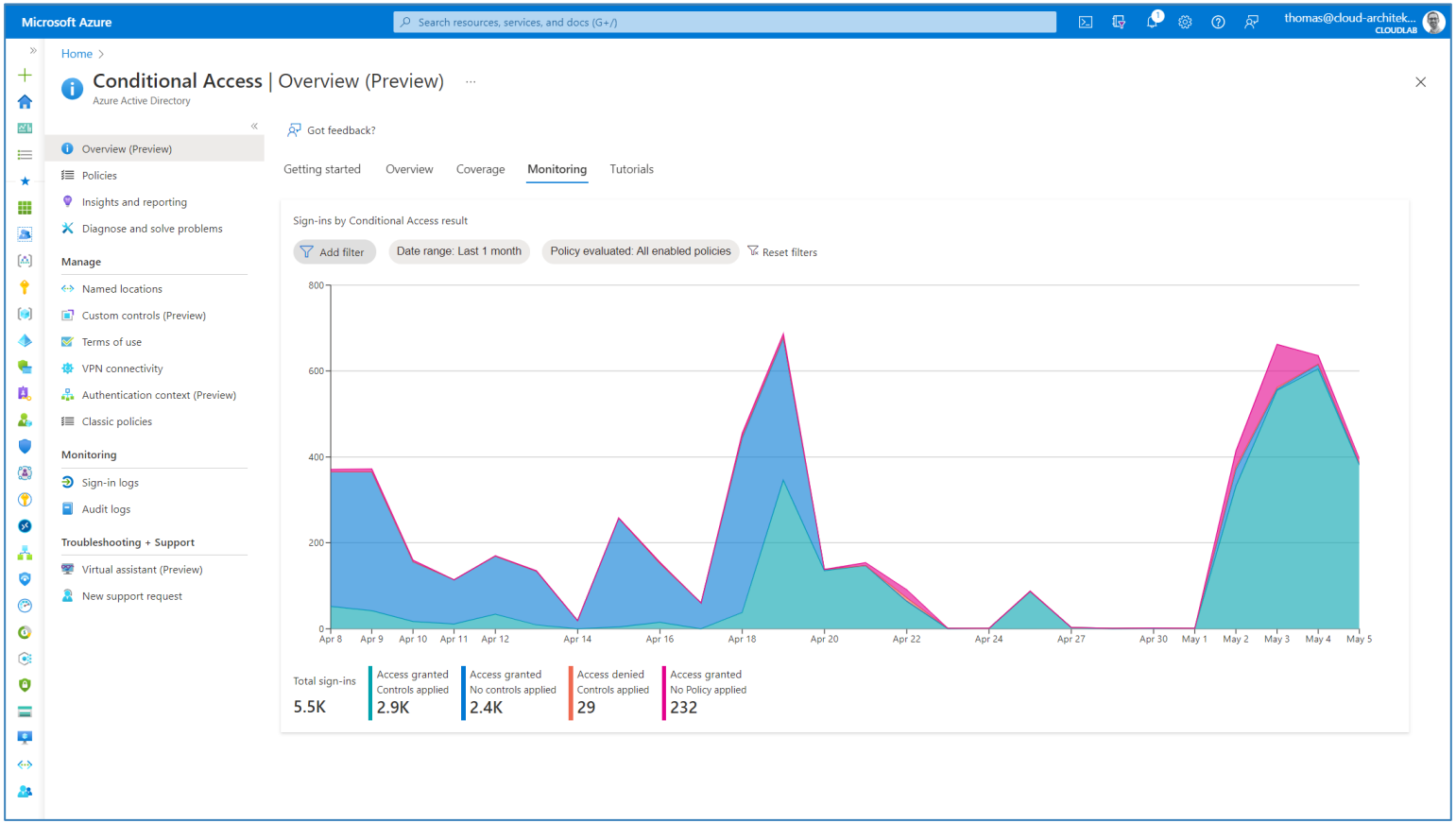
Audit of Management (Azure AD Audit Logs)

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

Security Monitoring (Microsoft Sentinel)

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

Conditional Access Monitoring in Azure AD Portal



Demo: Azure Workbooks and Azure Sentinel

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

aMS

Berlin 2022

Feedback form


THANK YOU!
Danke Schön!