OPERATIONALIZATION OF AZURE AD CONDITIONAL ACCESS

PROJECT “AADOPS”

Melbourne Azure Nights

Thomas Naunheim

12th October 2020

THOMAS NAUNHEIM

Cloud Security Architect
@glueckkanja-gab AG

Koblenz, Germany

@Thomas_Live

cloud-architekt.net

AGENDA

- CONDITIONAL ACCESS AND MICROSOFT GRAPH
- INTRODUCTION OF "AADOPS" PROJECT
- CODING AND CI/CD OF CONDITIONAL ACCESS TEMPLATES
- MANAGEMENT OF DEPLOYED CONDITIONAL ACCESS POLICIES

WHAT IS YOUR FAVORITE TOPIC?

1. GRAPH API & AUTOMATION?

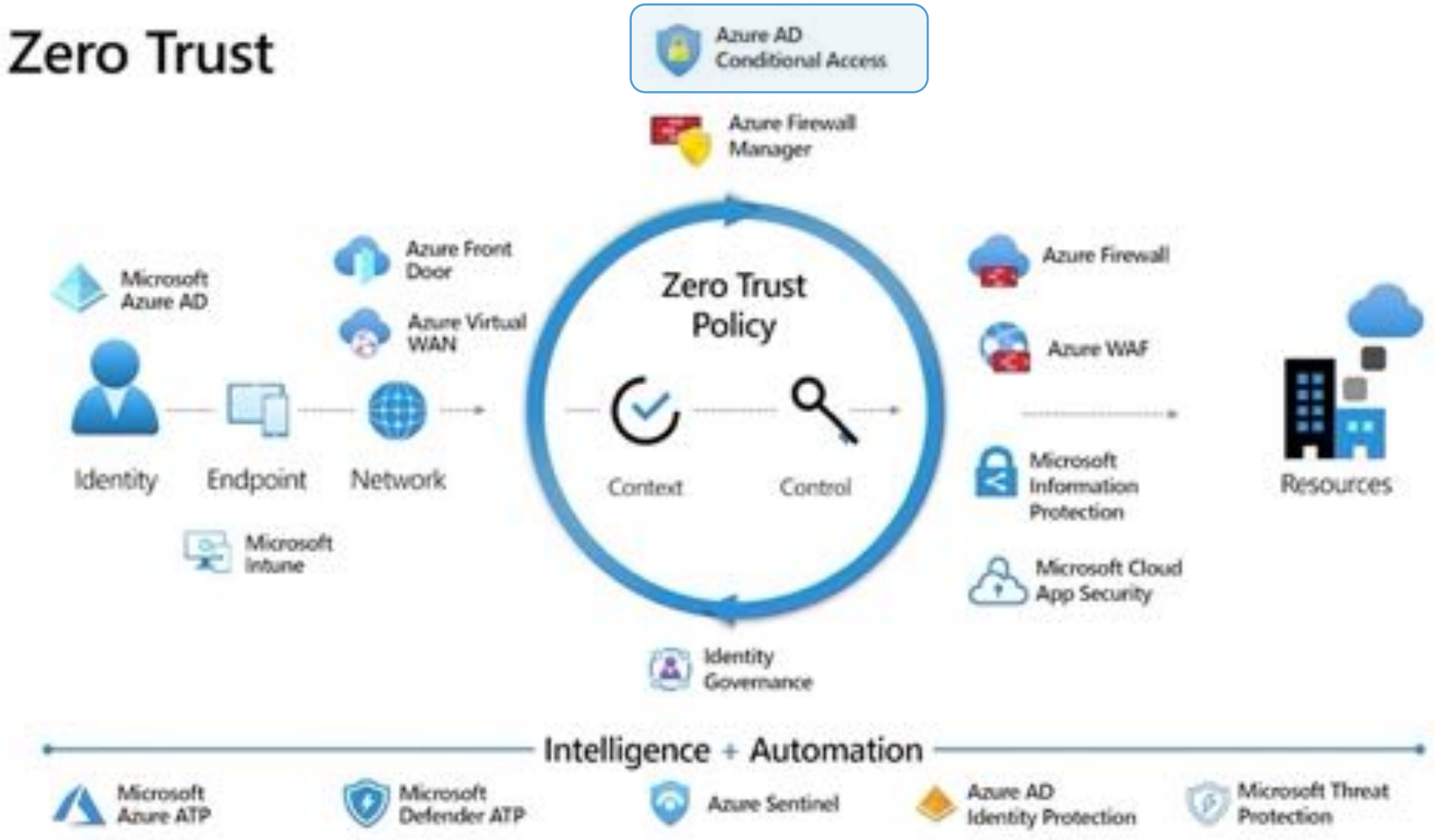
2. SECURITY IN AZURE AD AUTOMATION?

3. REPOS & PIPELINES FOR “CONFIG AS CODE”?

4. MANAGEMENT OF DEPLOYED CA POLICIES

CONDITIONAL ACCESS & MICROSOFT GRAPH

Conditional Access as “Zero Trust” Policy



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

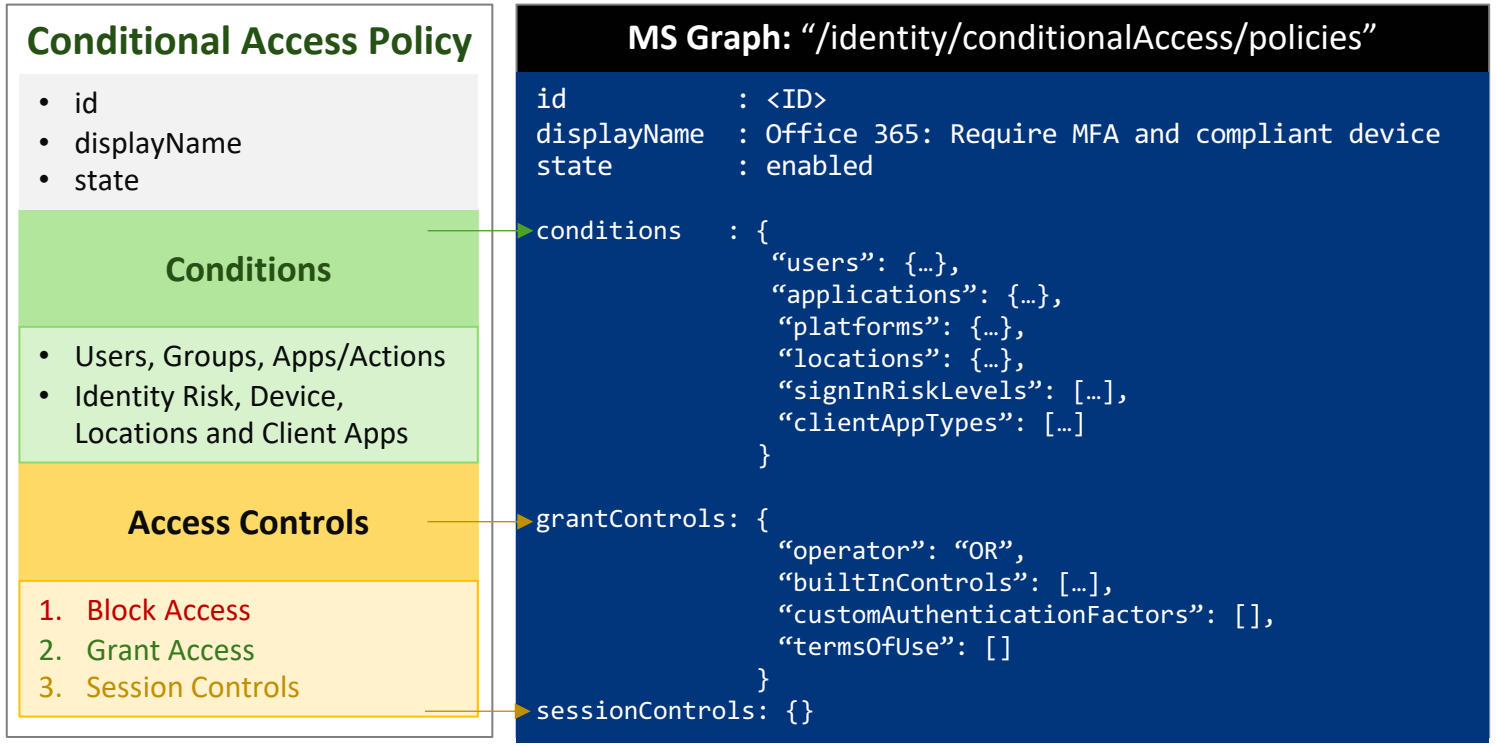
Overview of Conditional Access Policies

When this happens…

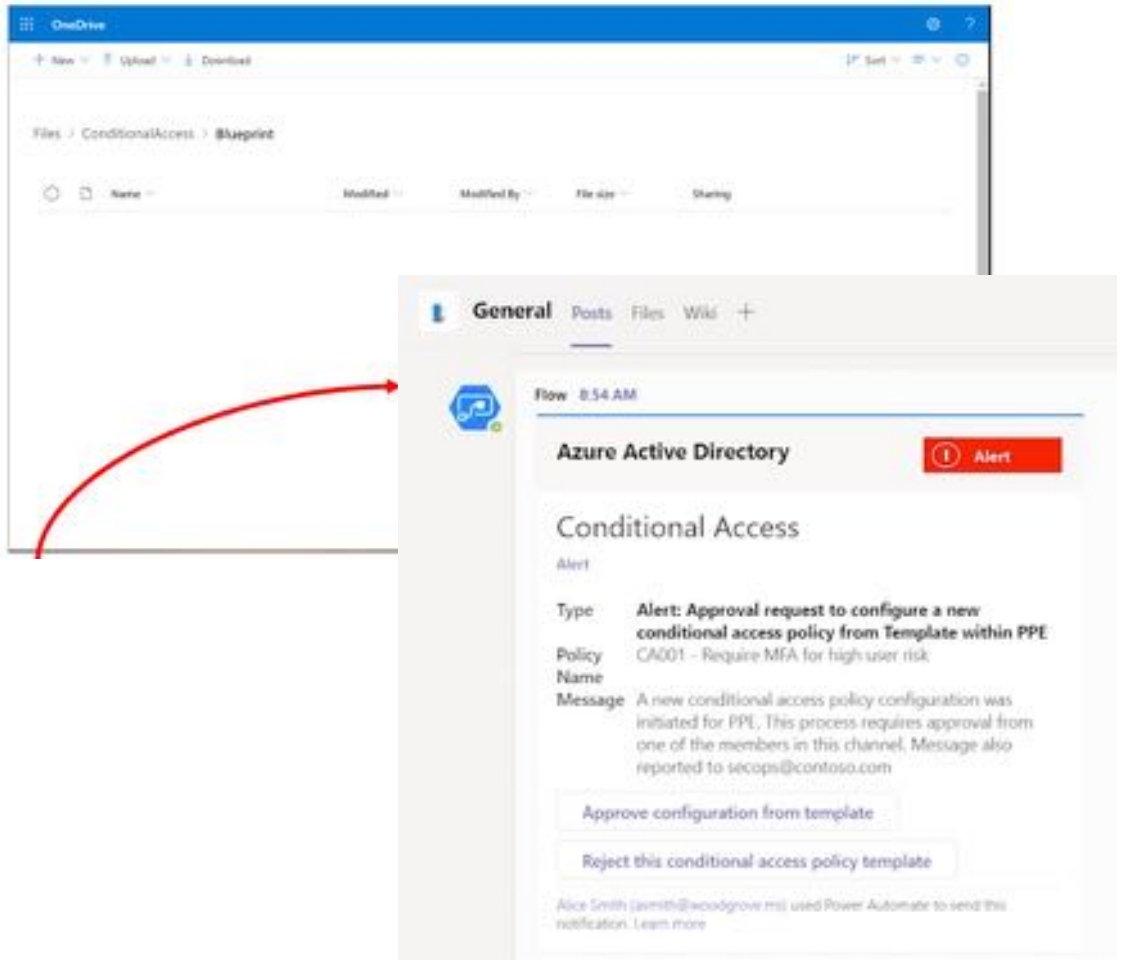
*A **user** from **(group) "Marketing employees"** is accessing **"Office 365"** from **a browser** on a **Windows** device from **any location** and **no sign-in risk** was detected.*

…then do this!

*Require a user with strong **(multi-factor) authentication** and **device to be marked as compliant.** No session control (by MCAS CA App Control policies or limited sign-in frequency).*



“CA policies like code” sample



Sample from the Microsoft Ignite 2020

Using OneDrive, Logic Apps (+ Azure KeyVault), Teams

GitHub Repo includes Samples

- Ignite Session: “Ninja skills: Manage your Conditional Access policies at scale”
- Docs: “Management of Lifecycle via API”

PowerShell Modules

microsoftgraph/**msgraph-sdk-powershell**

Powershell SDK for Microsoft Graph

Replacement of the AzureAD PowerShell Module

includes Cross-Platform Support and access to MS Graph

- "Identity.SignIns" contains CA cmdlets
- App-only Authentication by using certificates
- Mapping Azure AD and MSGraph cmdlets

DanielChronlund/**DCToolbox**

Tools for Microsoft cloud fans

Developed by Daniel Chronlund

includes Export/Import policies, templates and reporting

- Blog post and detailed instruction
- Assignment Report (part of the module)
- GitHub repository

Configuration-as-Code solutions

Microsoft365DSC

Configuration-as-Code for the Cloud

OS Initiative - lead by Microsoft & community-driven

Configuration and Monitoring of M365 via PowerShell DSC

- Project page incl. getting started guide and videos
- Guideline to use it for CA Automation with Azure DevOps and Certificate by Claus Jespersen

hashicorp/**terraform-provider-azuread**

Terraform provider for Azure Active Directory

Released in September 2021 (Version 2.2.0)

Almost all conditions and controls are supported (except Device Filters)

- Terraform Registry “azuread”
- GitHub Repo “terraform-provider-azuread”

“CA As Code” GitHub Repository

AlexFilipin/
ConditionalAccess

Automated solution and policy (template repository)

Using Microsoft.Graph SDK for automation,

creation of exclusion groups and ring-based deployment

- GitHub Repo includes scripts and templates

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

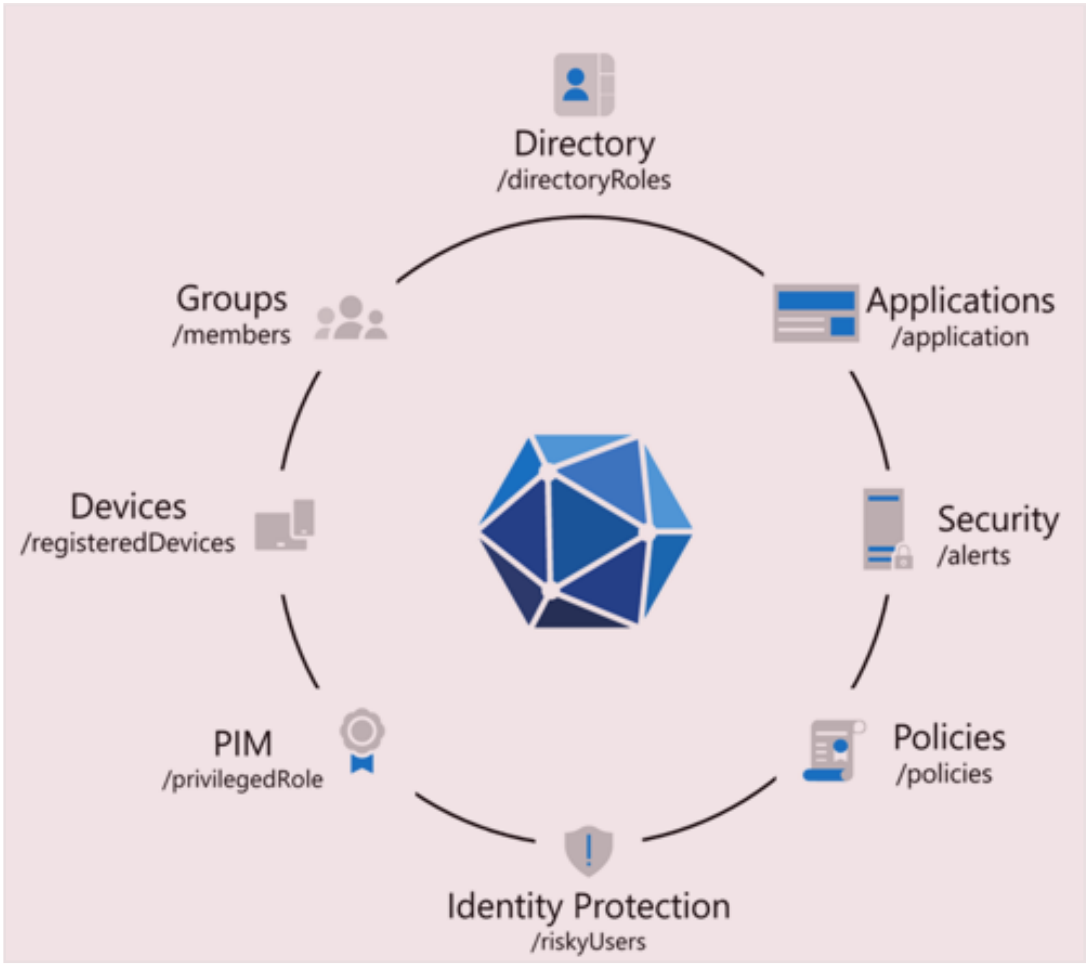
Introducing Conditional Access as Code. A fully automated solution to kick-start and maintain your Conditional Access deployment. The solution consists of the follwong three main components and is based on the Conditional Access guidance.

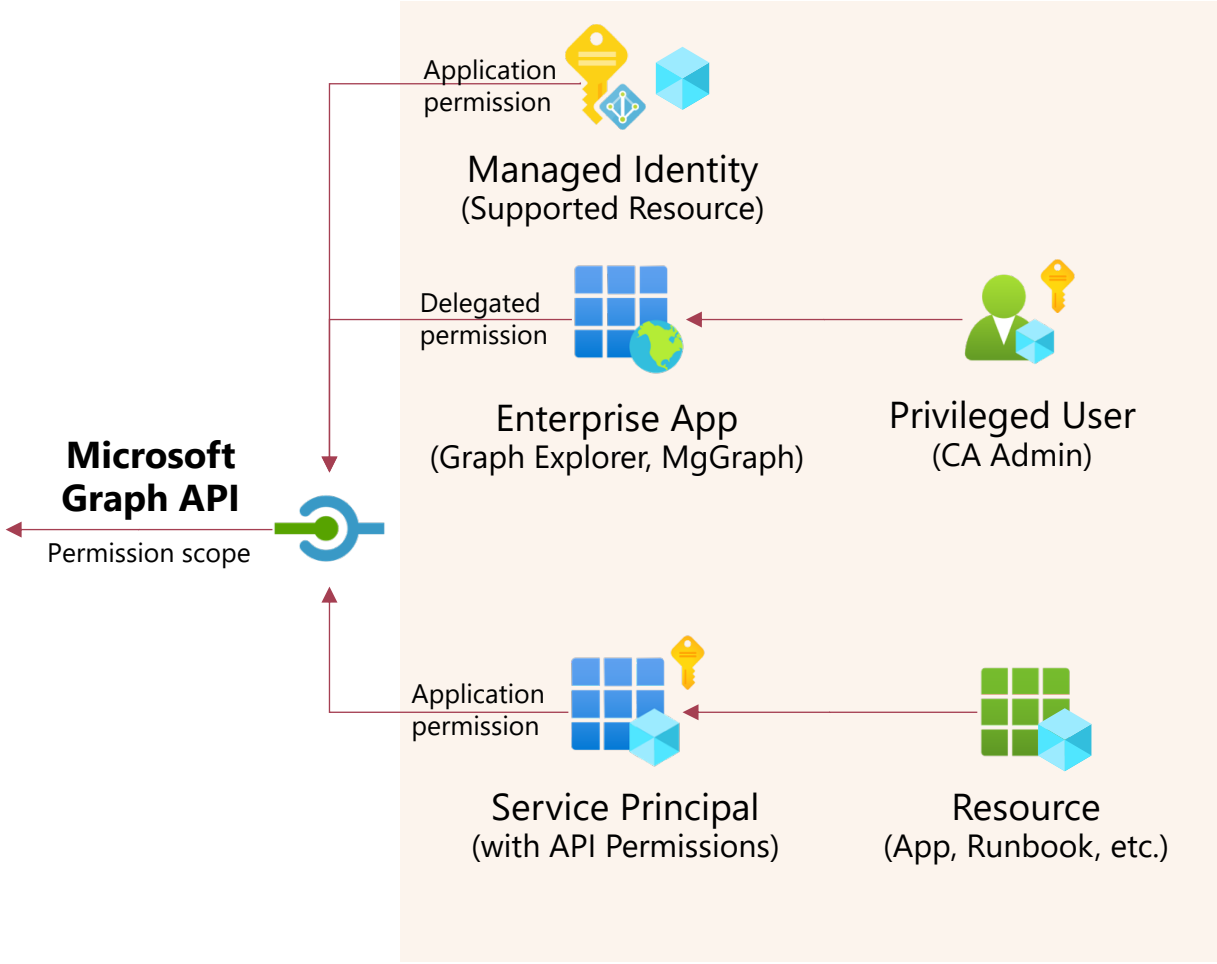
Policy repository

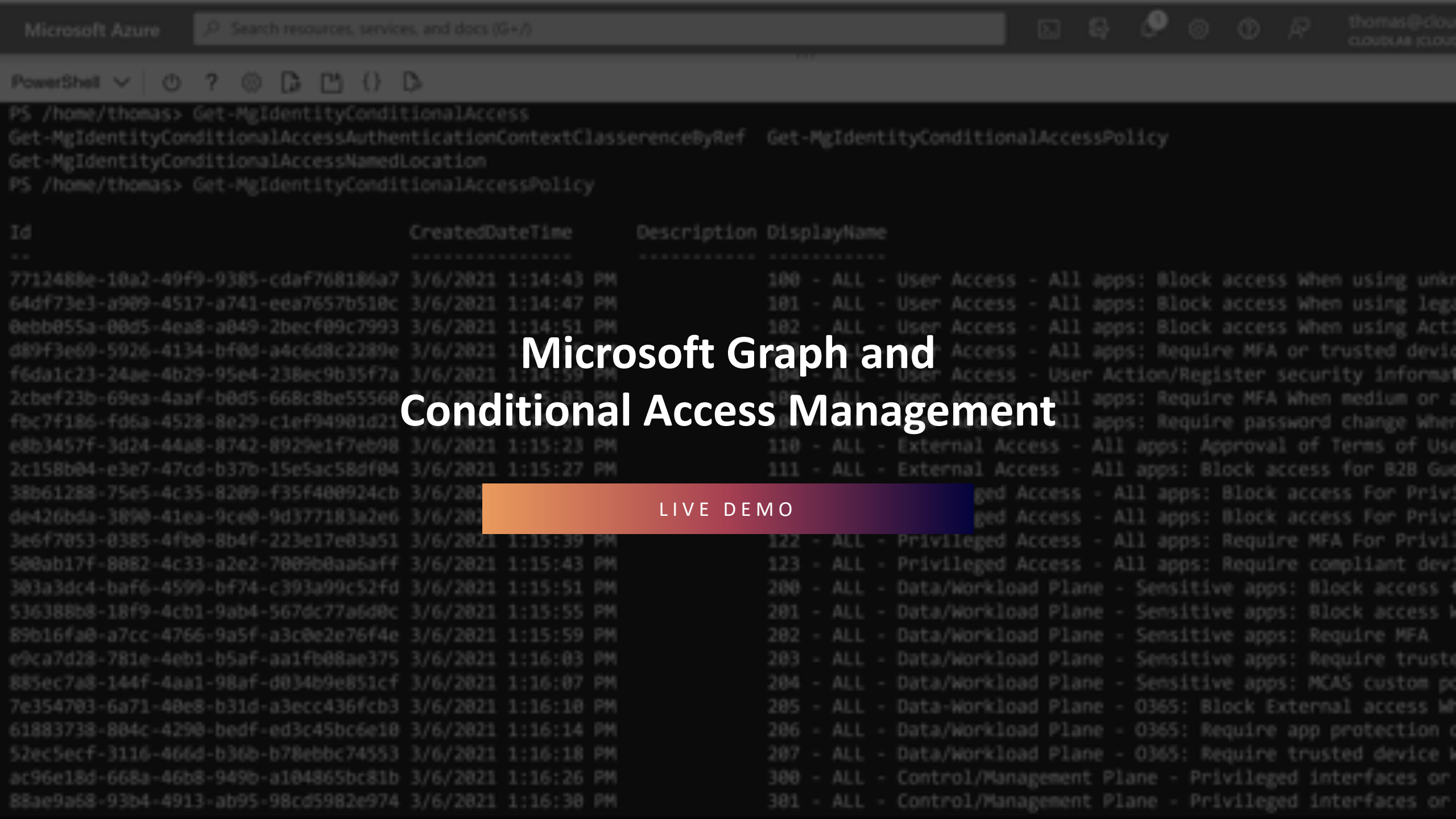
A collection of conditional access policies in JSON format which are divided into the following categories:

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

Access to Microsoft Graph





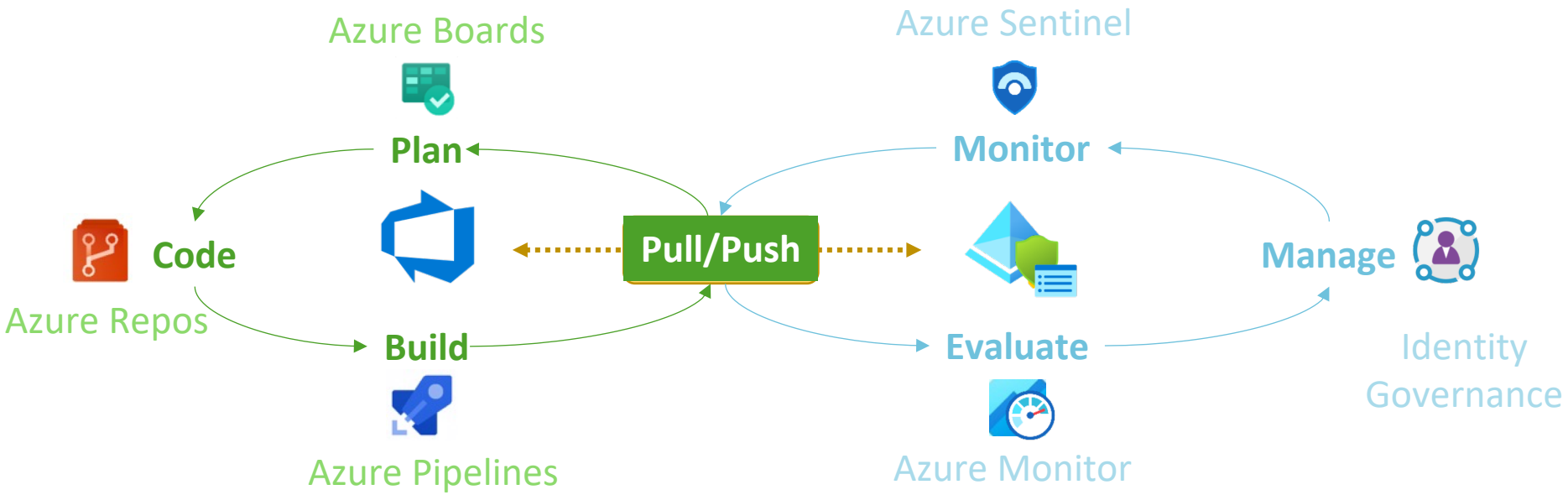


Microsoft Graph and Conditional Access Management

LIVE DEMO

INTRODUCTION OF "AADOPS" PROJECT

DevOps Lifecycle for Azure AD Conditional Access

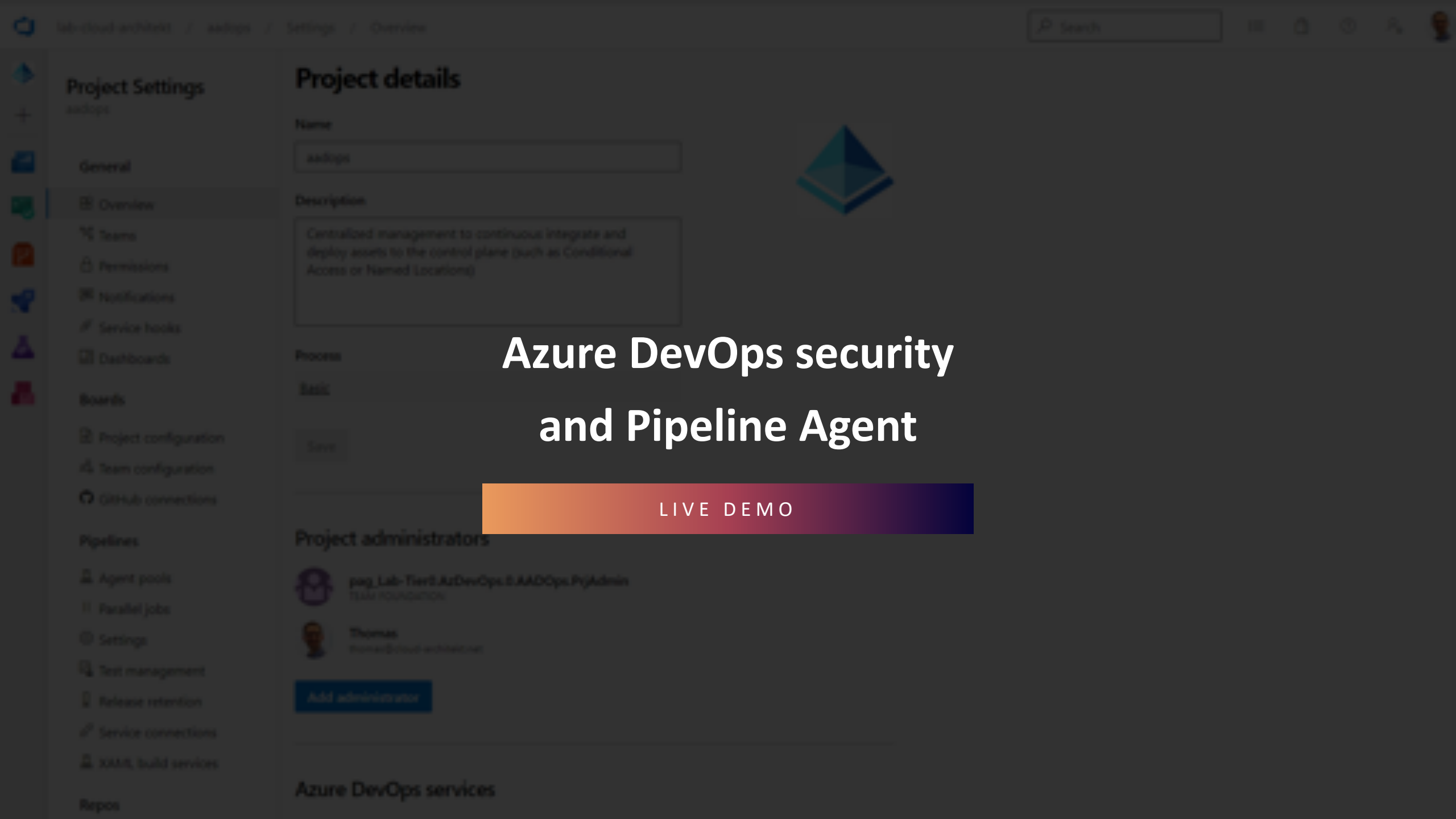


Why using DevOps approach for CA?

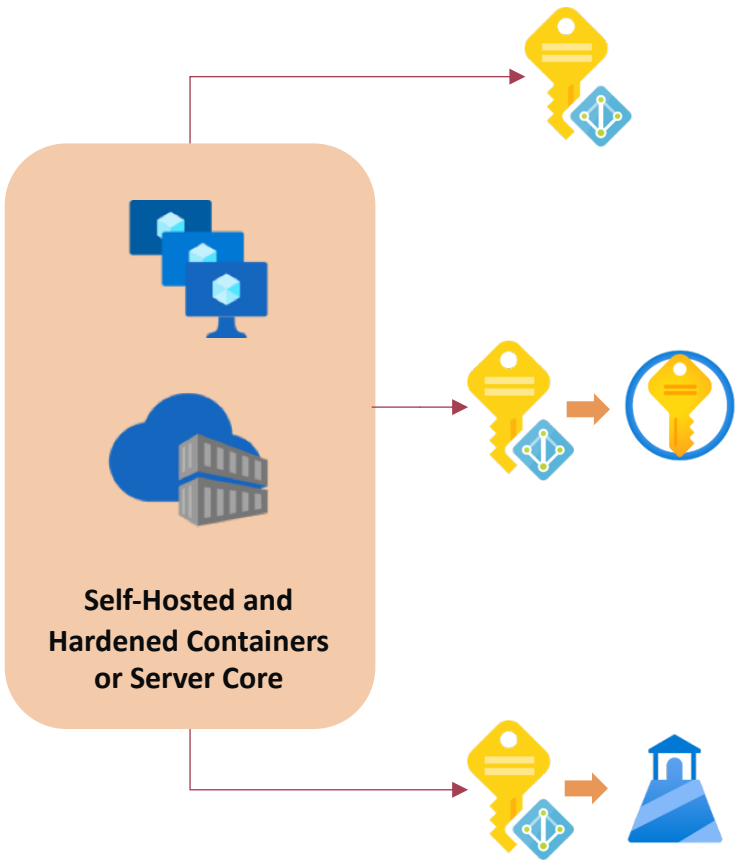
Change Management for Zero Trust Policies
- Documentation of requirements and implementation status
- Planning, versioning (incl. backup/restore) and tracking policy changes
- Integration of “Quality Gates” and “Approval Workflows”

Integrated ring-based and “multi-tenant” staging
- Deploy policy configuration across various target groups or tenants
- Using templates to standardized policy sets
- Balance of reduced deployment risks and high management overhead

Policy-As-Code and Pipeline
- Limit numbers of delegated “Conditional Access Administrator” roles
- Comparison and “full visibility” of deployed policies (and changes)
- Roll-out of resilient access controls
  (e.g. in case of MFA disruption or emergency access)


Azure DevOps security
and Pipeline Agent
LIVE DEMO

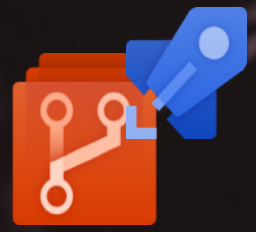
Service Connections and Agent Pools



Managed Identity (Single Instance / Single Tenant)
One ADO project manages one tenant
Agent pool uses Managed Identity for one tenant

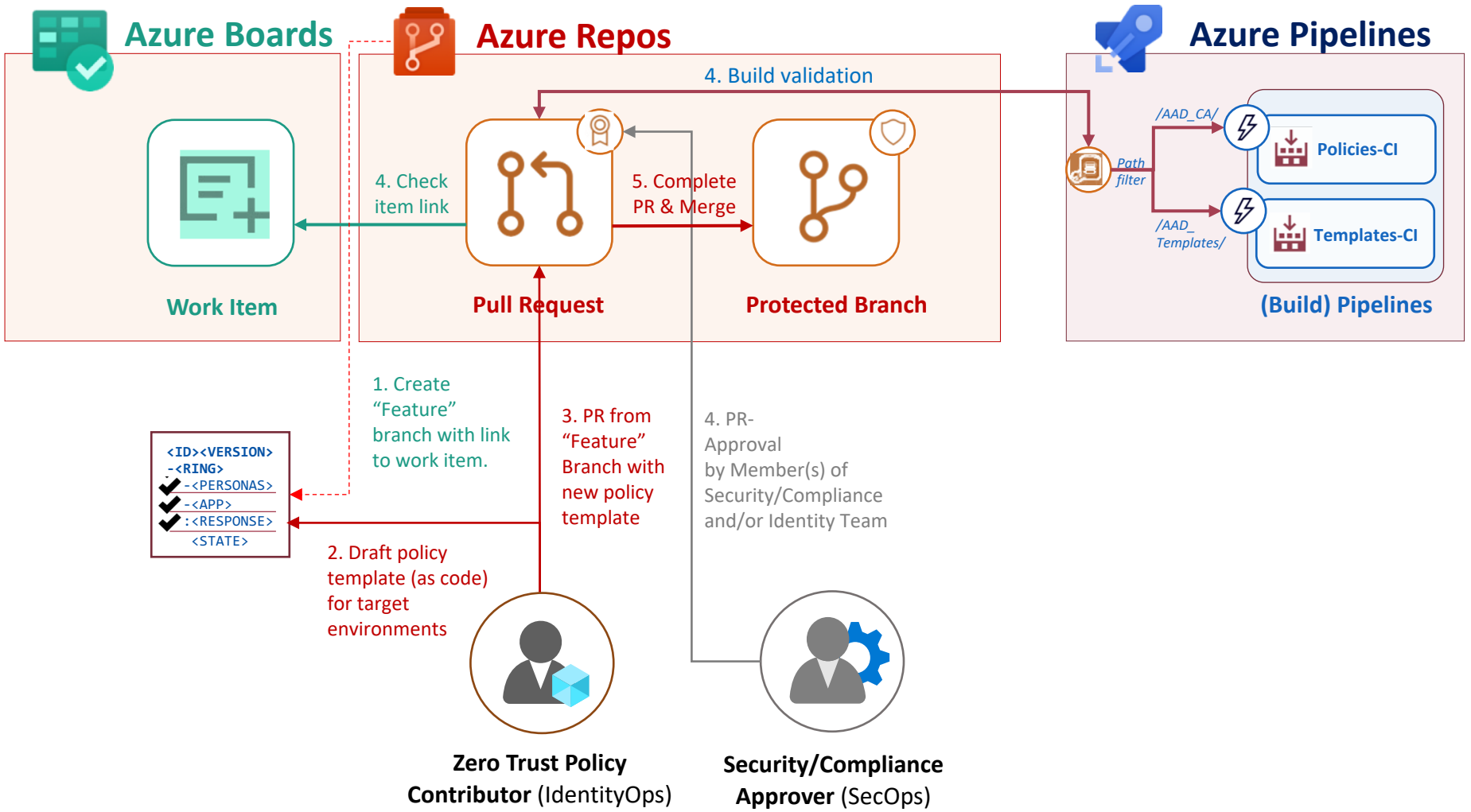
Managed Identity + KeyVault (Single Instance / Multi-Tenant)
One ADO project manages multiple tenants
Agent pool uses Managed Identity for KeyVault access
KeyVault stores credentials/certificates of service principal

Managed Identity + Lighthouse (Managing/Managed Tenant)
One ADO instance manages multiple tenants
Agent pool uses Managed Identity for multiple tenants
Lighthouse delegation required to delegate access to MSI

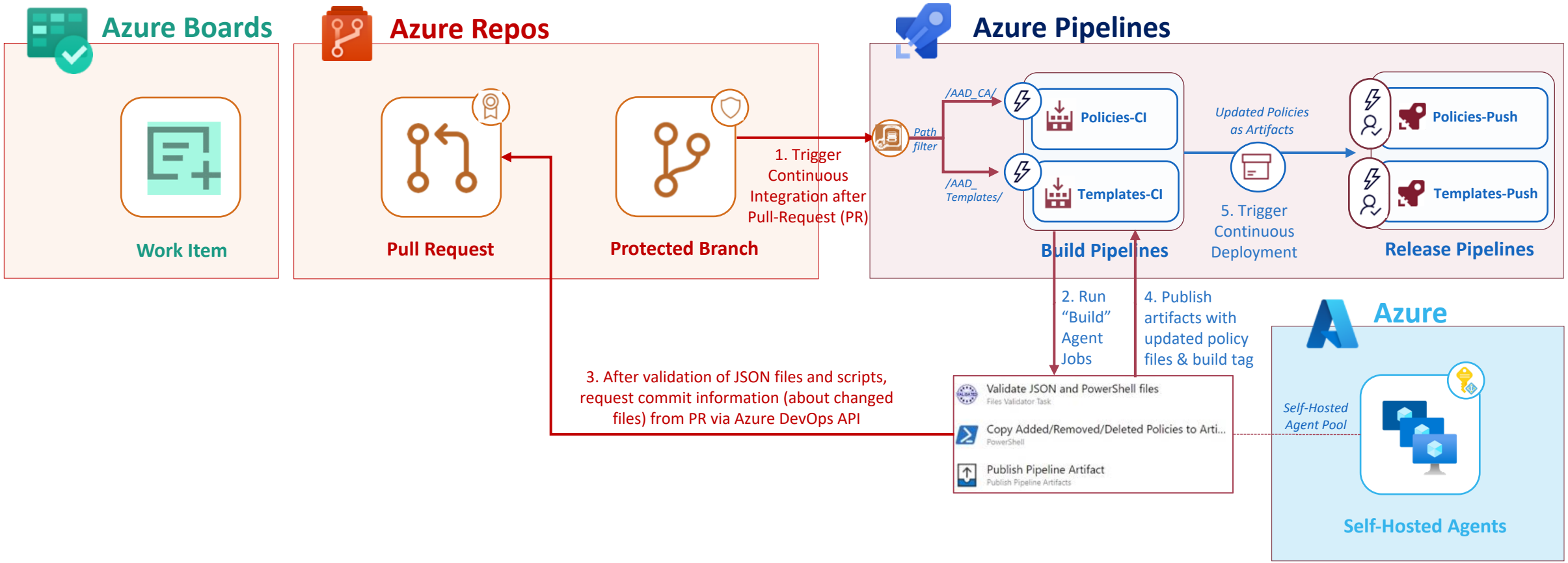


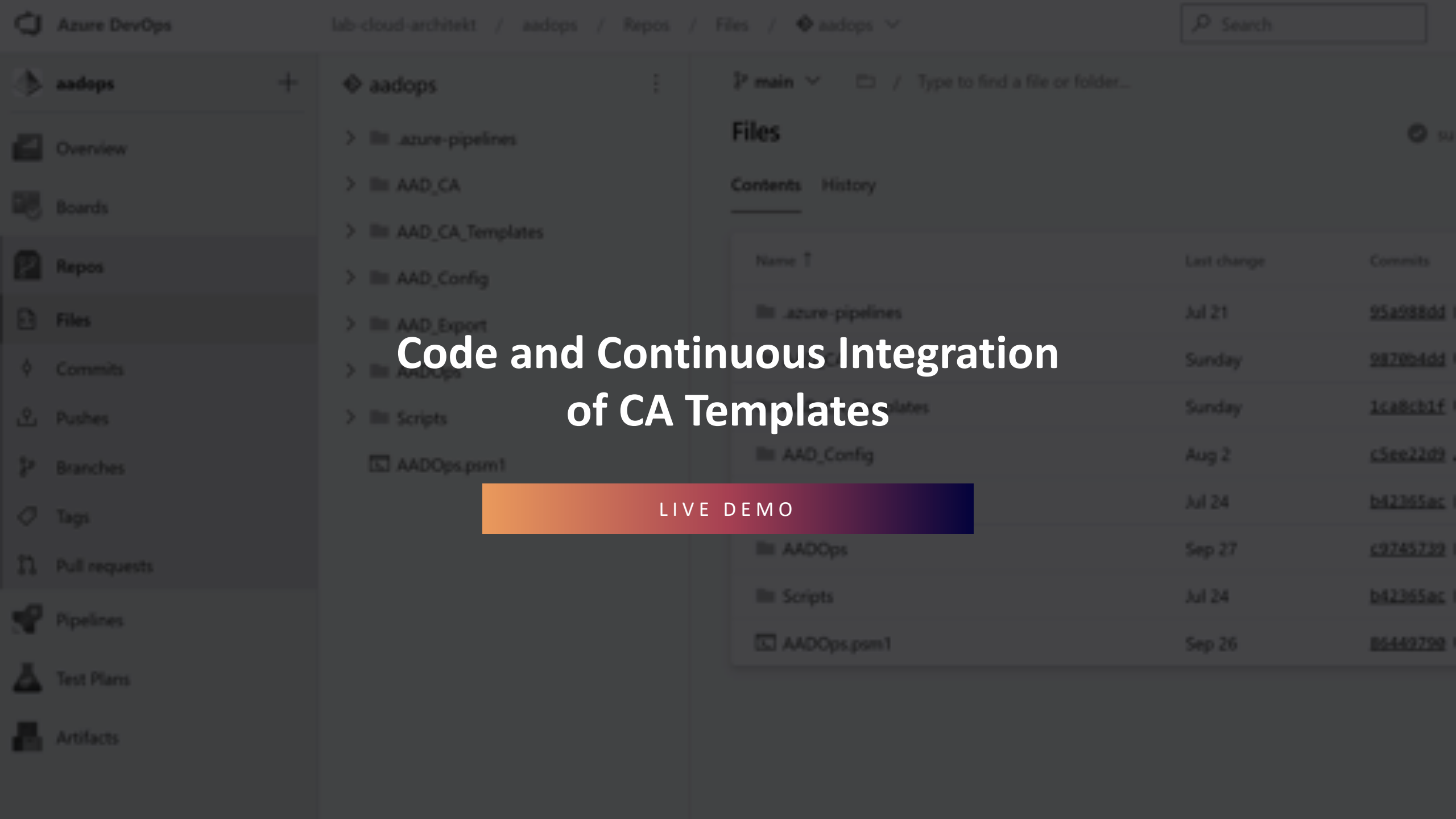
CODING AND CI/CD OF CA TEMPLATES

Process of Coding in “AADOps”

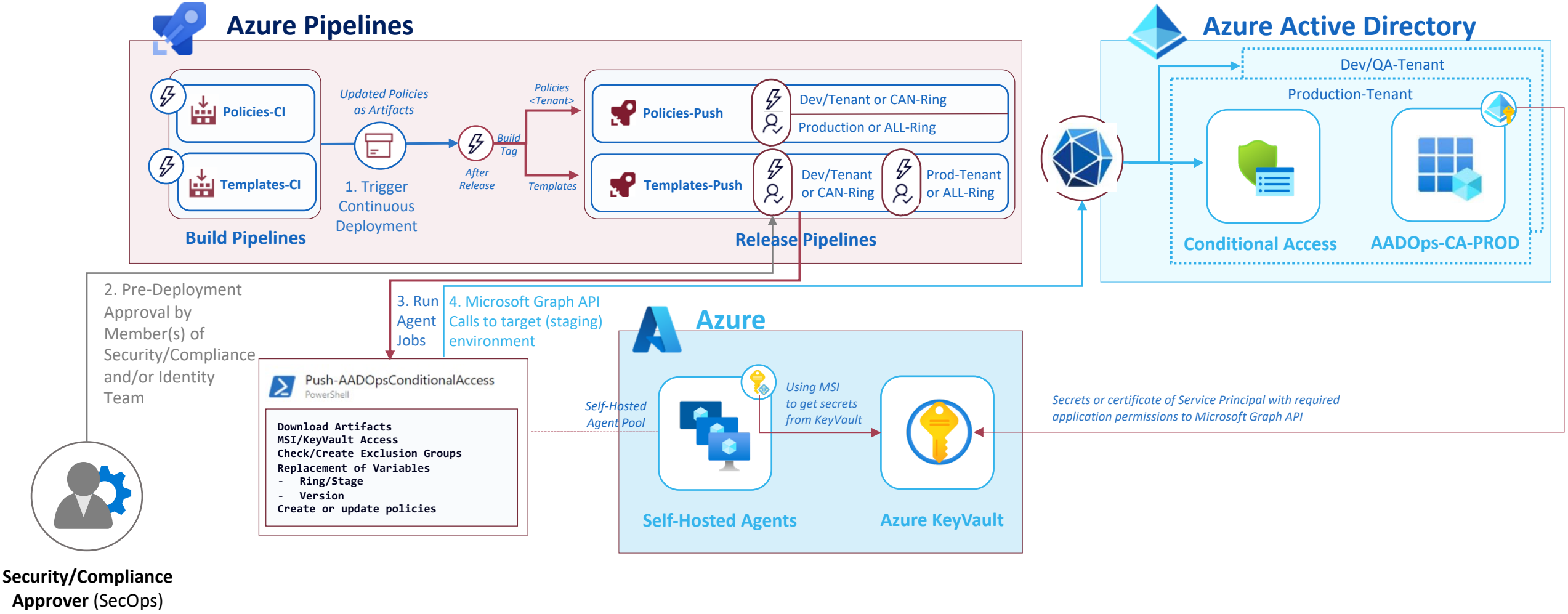


Process of building policies (CI-pipeline)

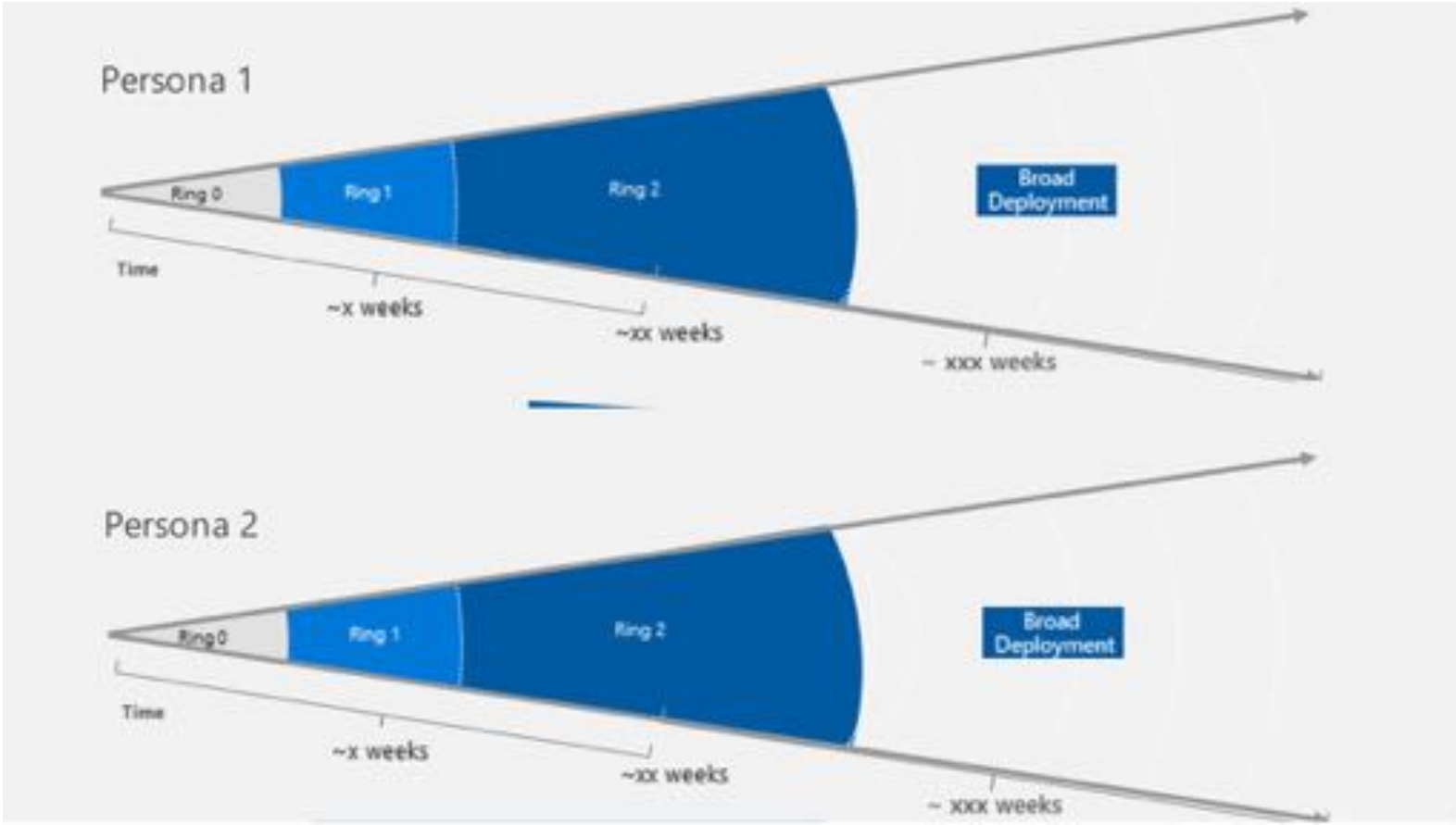



Azure DevOps
lab-cloud-architekt / aadops / Repos / Files / aadops
Search
aadops
Overview
Boards
Repos
Files
Commits
Pushes
Branches
Tags
Pull requests
Pipelines
Test Plans
Artifacts
aadops
.azure-pipelines
AAD_CA
AAD_CA_Templates
AAD_Config
AAD_Export
Scripts
AADOps.psm1
main
Type to find a file or folder...
Files
Contents
History
Name
Last change
Commits
.azure-pipelines
Jul 21
Sunday
Sunday
AAD_Config
Aug 2
Jul 24
AADOps
Sep 27
Scripts
Jul 24
AADOps.psm1
Sep 26
Code and Continuous Integration of CA Templates
LIVE DEMO

Overview of deploy templates (CD-pipeline)



Intra-Staging / Ring-based Deployment



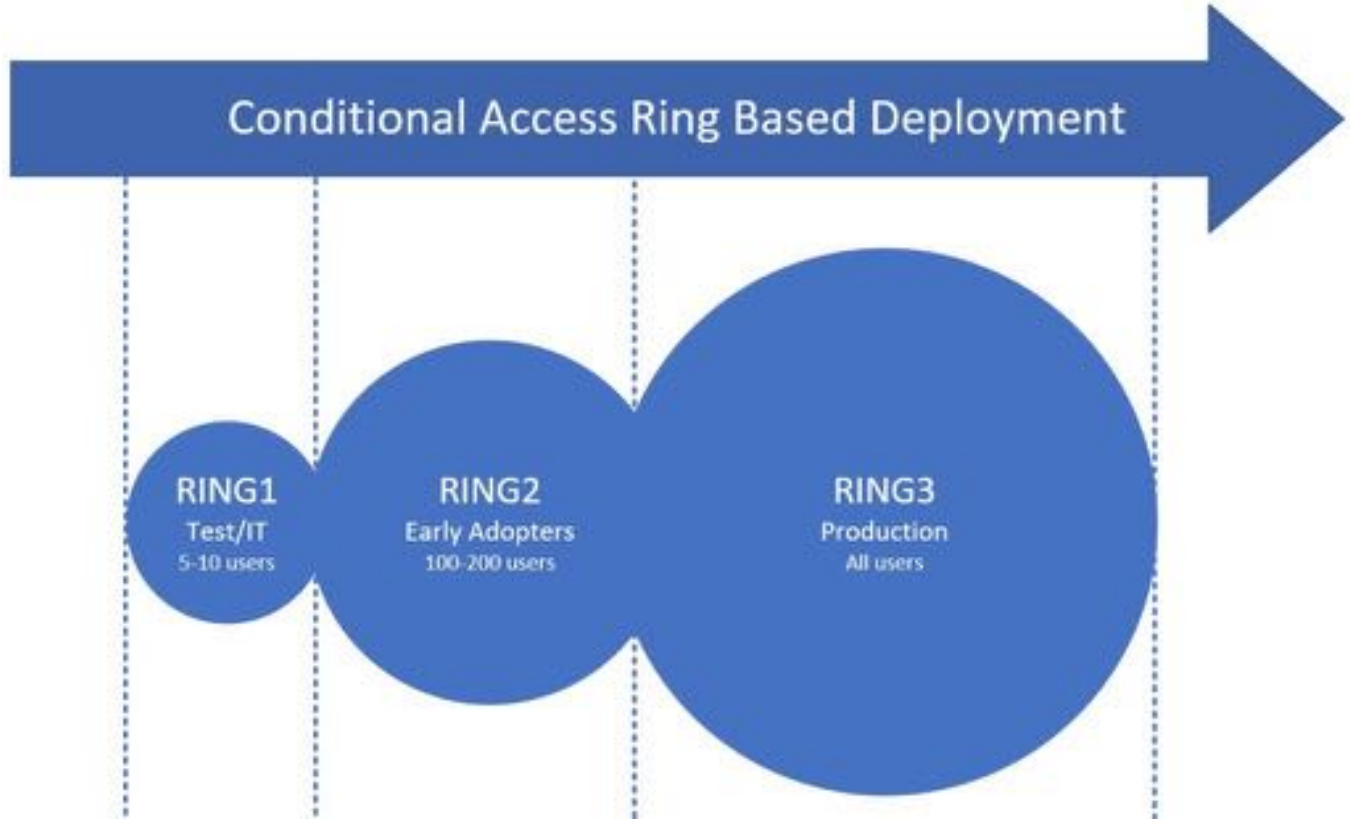
Source: Azure AD Conditional Access guidance by Claus Jaspersen

Intra-Staging / Ring-based Deployment

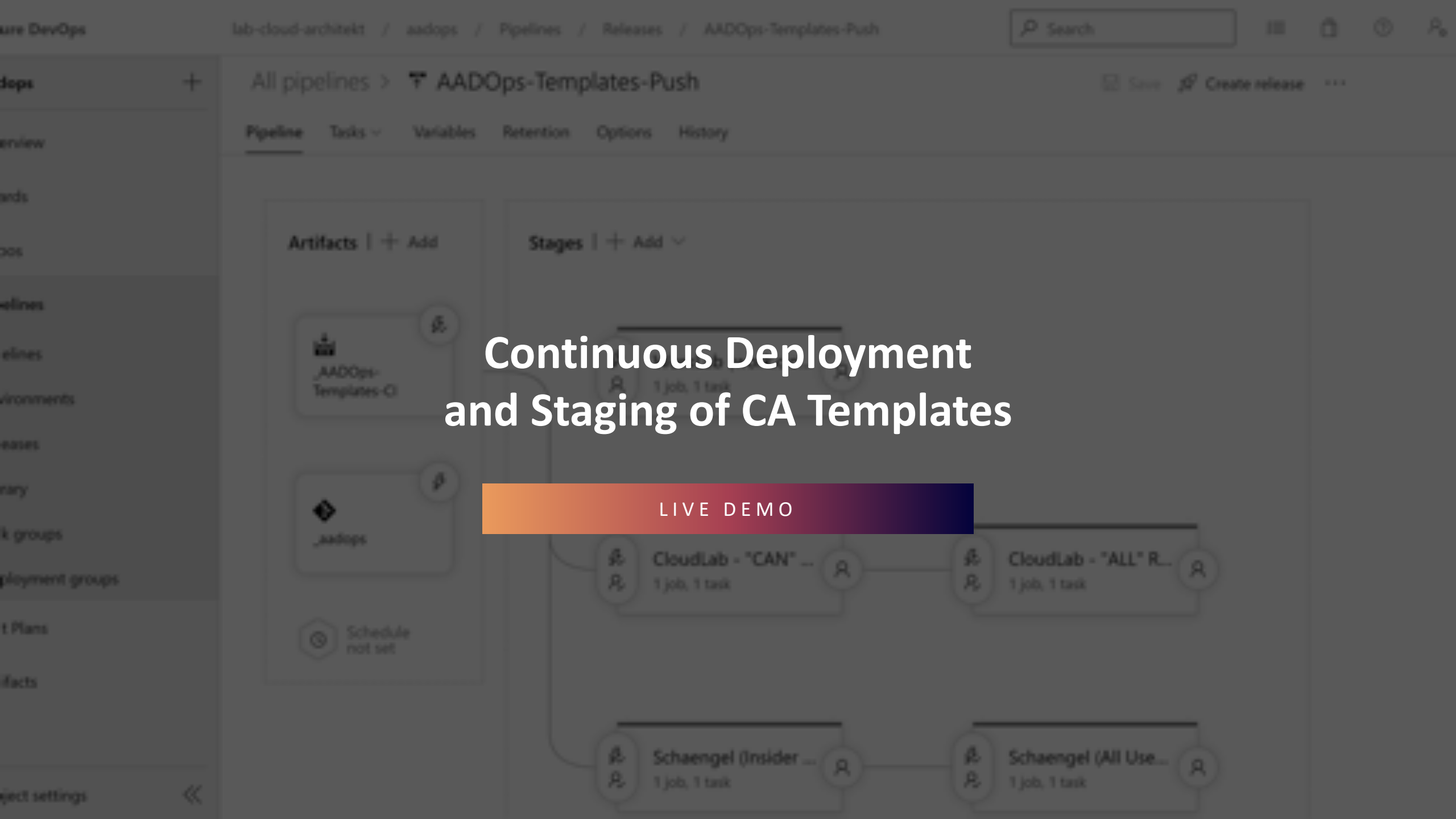
Ring 1 (CAN)
Managed with GUI or as code.
Few users test and troubleshoot before further policy changes

Ring 2 (BETA)
Same policy will be deployed in next stage/ring with pilot users.
Scope to “day-to-day work” evaluation before broad deployment.

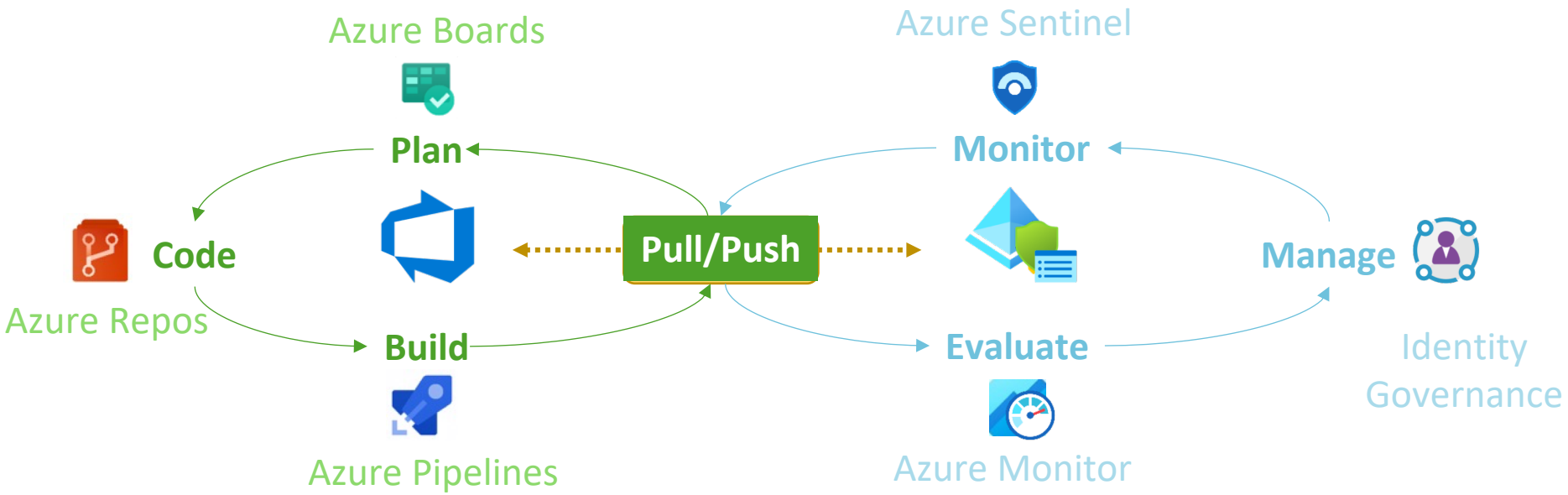
Ring 3 (ALL)
Deployment to “All users”,
in cases of issues:
roll-back to previous policy version/config



Source: Conditional Access Ring Based Deployment with DCToolbox (by Daniel Chronlund)


Continuous Deployment
and Staging of CA Templates
LIVE DEMO

DevOps Lifecycle for Azure AD Conditional Access

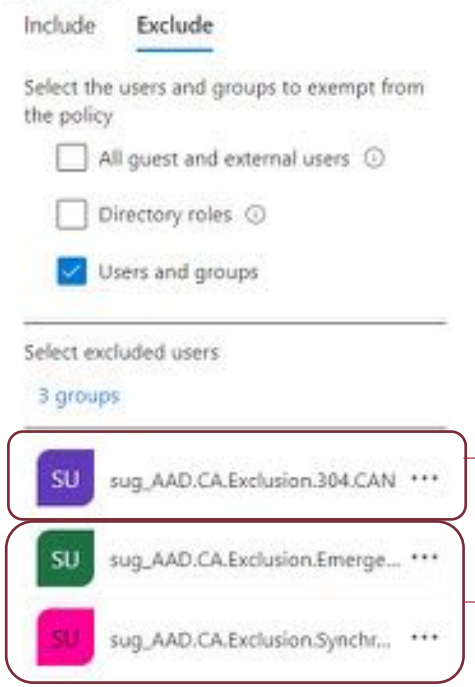


MANAGEMENT OF DEPLOYED CA POLICIES

Integration in Microsoft Cloud Ecosystem

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

Exclusion Management



General approach:

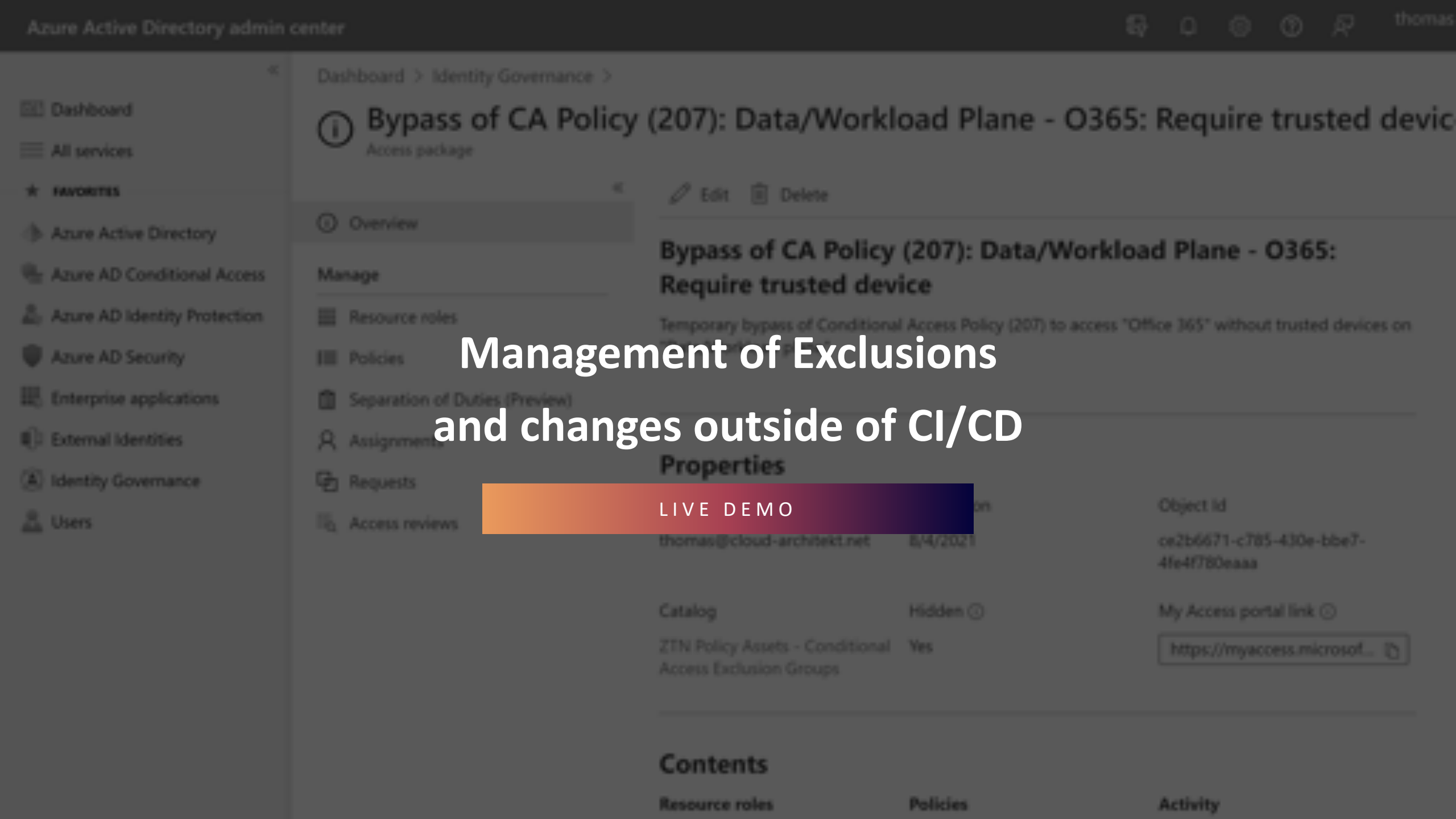
- Exclusion by Security Group (not assigned to user, not synced from on-prem)
- Review of Excluded Groups (Azure AD access reviews)
- Protection of Exclusion Group (Role-Assignable Groups?)

Use Case A: Individual or Incident case

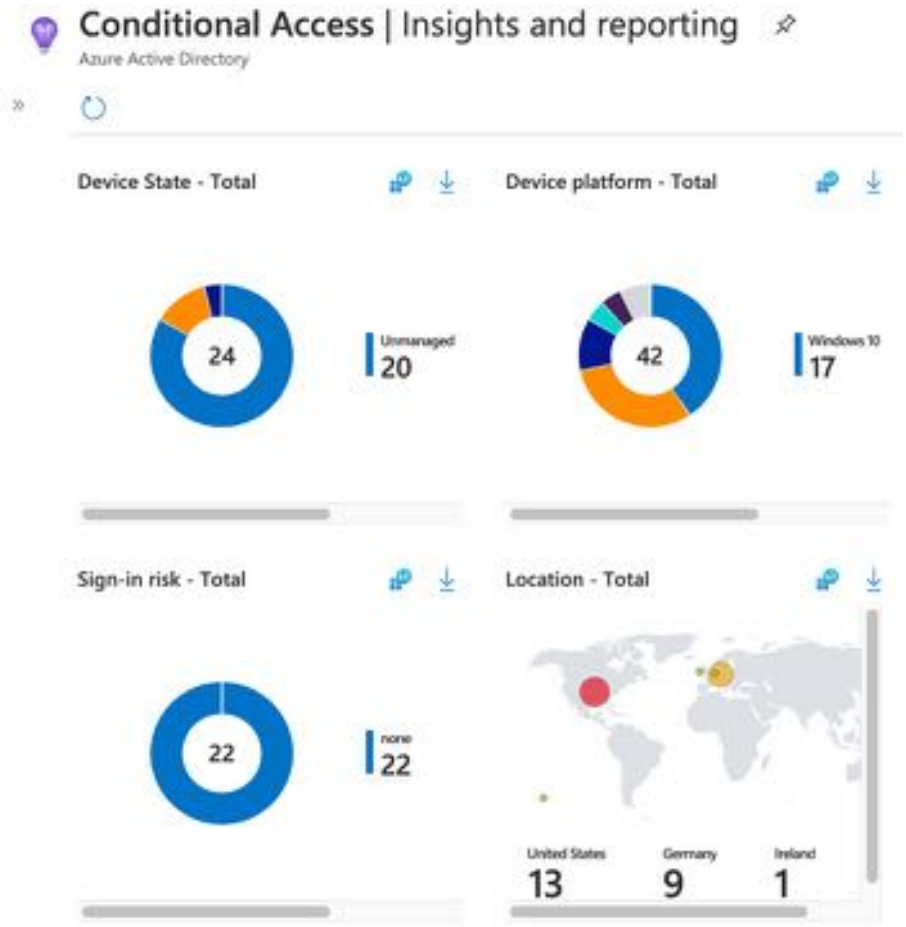
- Temporary or limited Exclusion
- Exclusion for each policy (or group of policies)
- Exclusion after approval process, assignment as Access Package

Use Case B: Break Glass or Sync Account

- Permanent Exclusion
- Assignment to certrain account type, strictly monitored


Azure Active Directory admin center
Dashboard
All services
FAVORITES
Azure Active Directory
Azure AD Conditional Access
Azure AD Identity Protection
Azure AD Security
Enterprise applications
External Identities
Identity Governance
Users
Dashboard > Identity Governance >
Bypass of CA Policy (207): Data/Workload Plane - O365: Require trusted devic
Access package
Overview
Manage
Resource roles
Policies
Separation of Duties (Preview)
Assignments
Requests
Access reviews
Edit
Delete
Bypass of CA Policy (207): Data/Workload Plane - O365: Require trusted device
Temporary bypass of Conditional Access Policy (207) to access "Office 365" without trusted devices on
Management of Exclusions
and changes outside of CI/CD
LIVE DEMO
Properties
Object Id
ce2b6671-c785-430e-bbe7-4fe4f780eaaa
Catalog
Hidden
My Access portal link
ZTN Policy Assets - Conditional Access Exclusion Groups
Yes
https://myaccess.microsof...
Contents
Resource roles
Policies
Activity

Monitoring Capabilities and Requirements



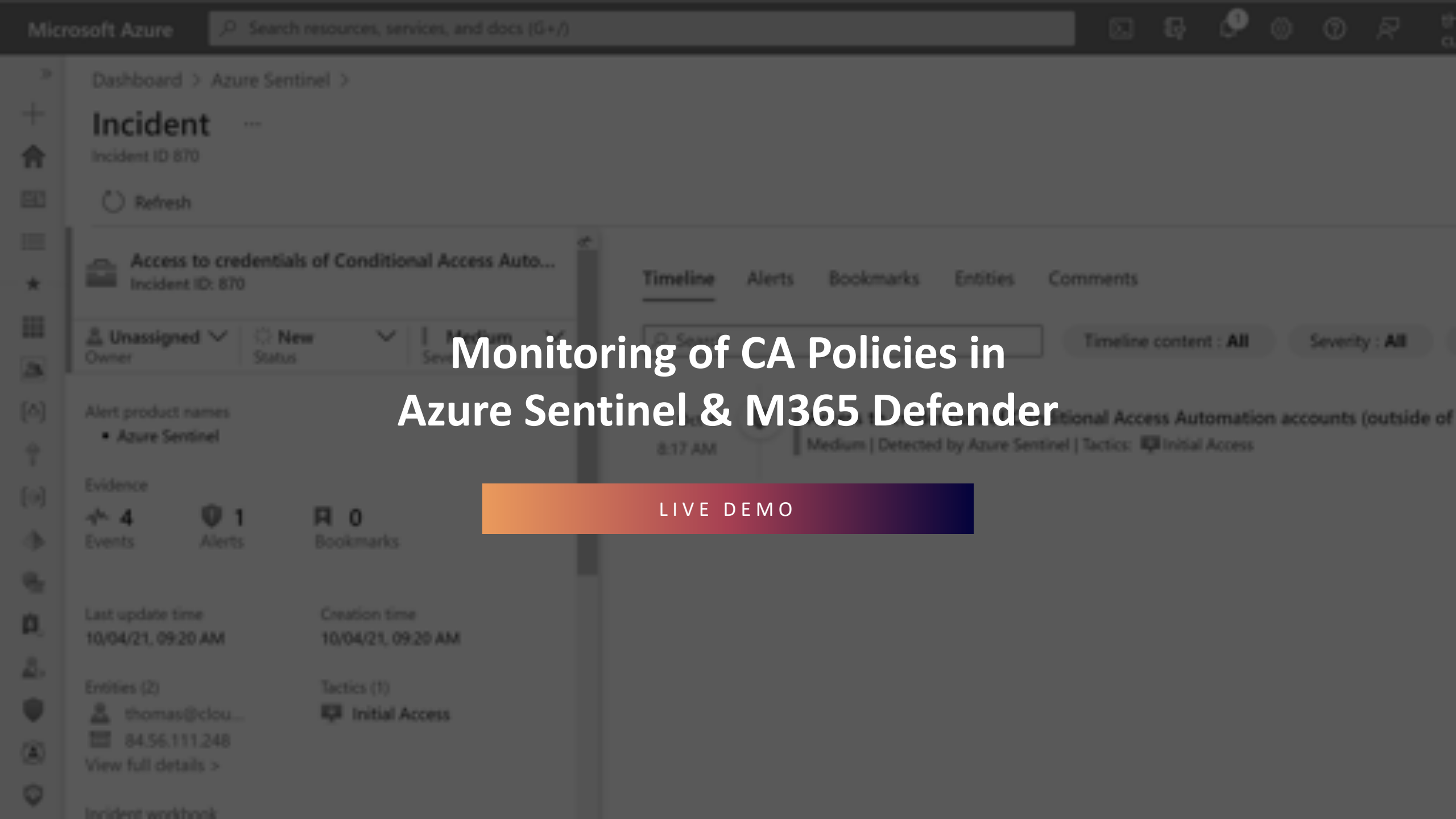
Identity Operations (Azure AD Workbooks)
Analyses and Visualizations to understand impact of Conditional Access Policies and gaps in your environment.

Audit of Management (Azure AD Audit Logs)

- Changes on CA Policies (outside of automated process)
- Changes on Target/Exclusion Groups
- 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



Monitoring of CA Policies in Azure Sentinel & M365 Defender

LIVE DEMO

THANK YOU

@Thomas_Live

Thomas@Naunheim.net

www.cloud-architekt.net