



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



Thanks to our SPONSORS

Vielen Dank an unsere Partner!



M365Kaffeepause

Learning in the flow of work.

logitech®

MARTELLO

**DIAMOND
sponsors**

**PLATINUM
sponsor**

Organizing sponsor

Granikos



***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**

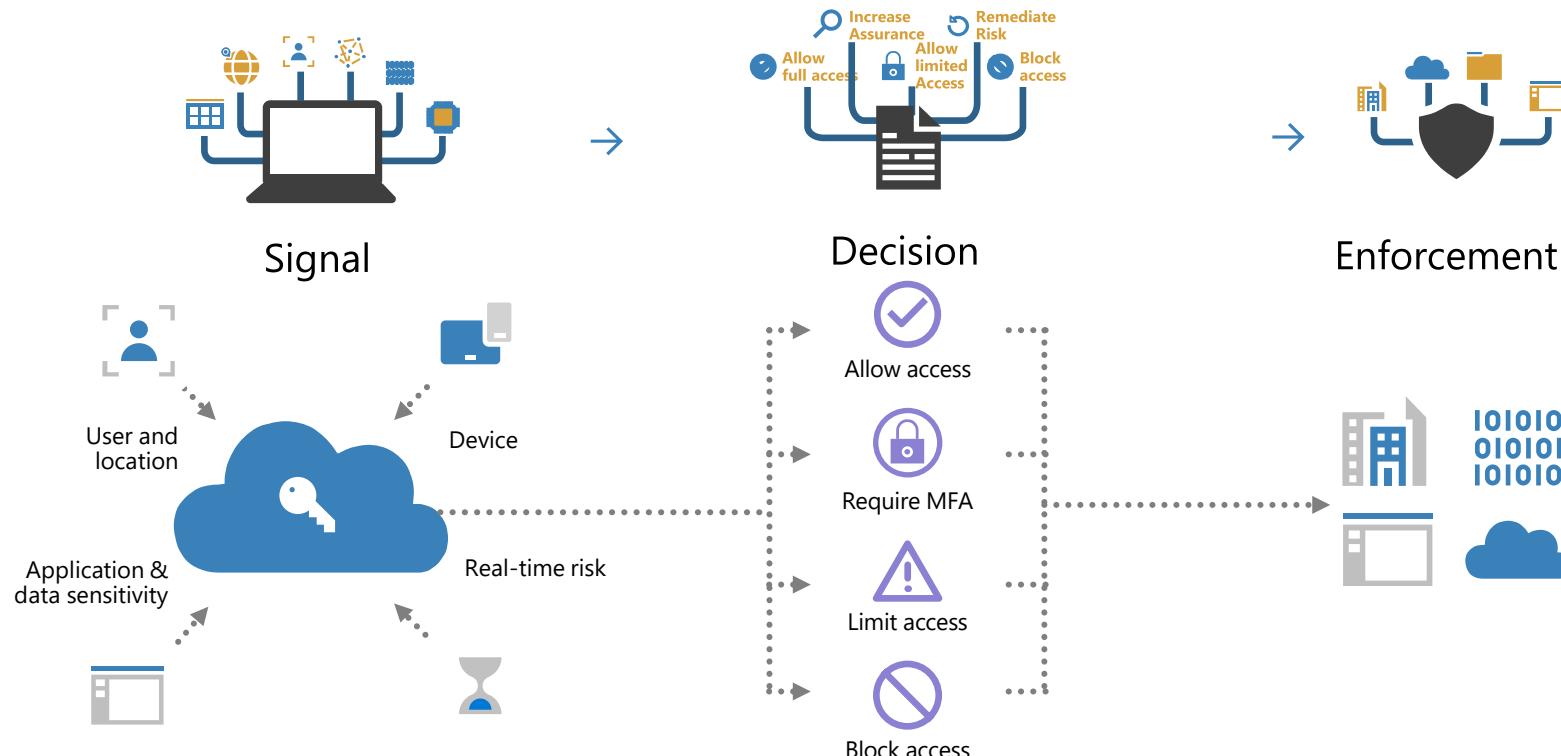


**Monitoring and
Reporting of
“Zero Trust Policies”**

Overview of Conditional Access

Principals of Signal, Decision and Enforcement

Conditional Access - Zero Trust Policy Engine



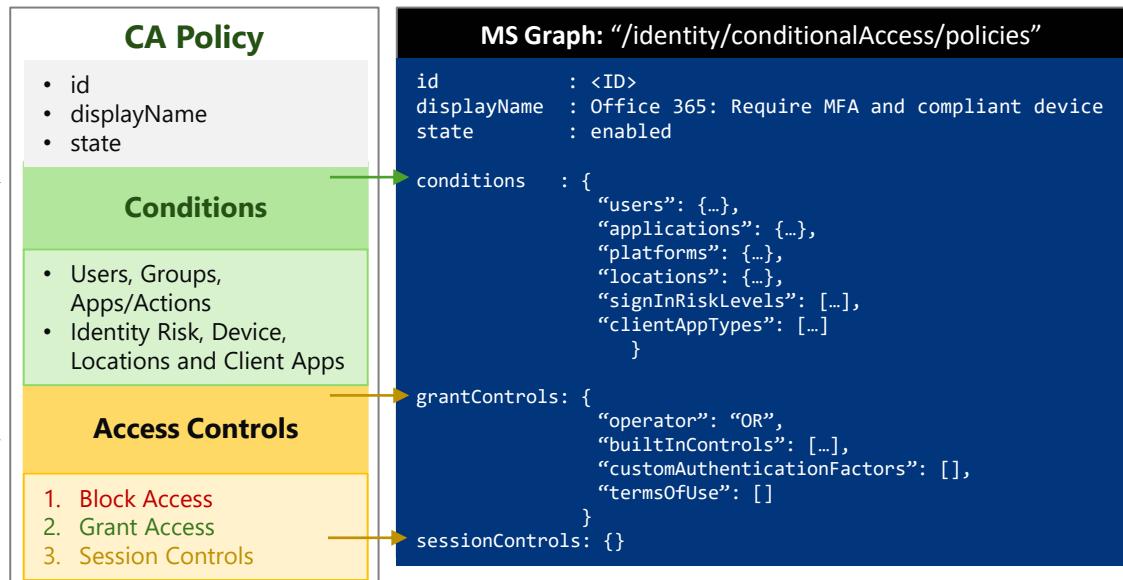
Conditional Access Policy

When this happens...

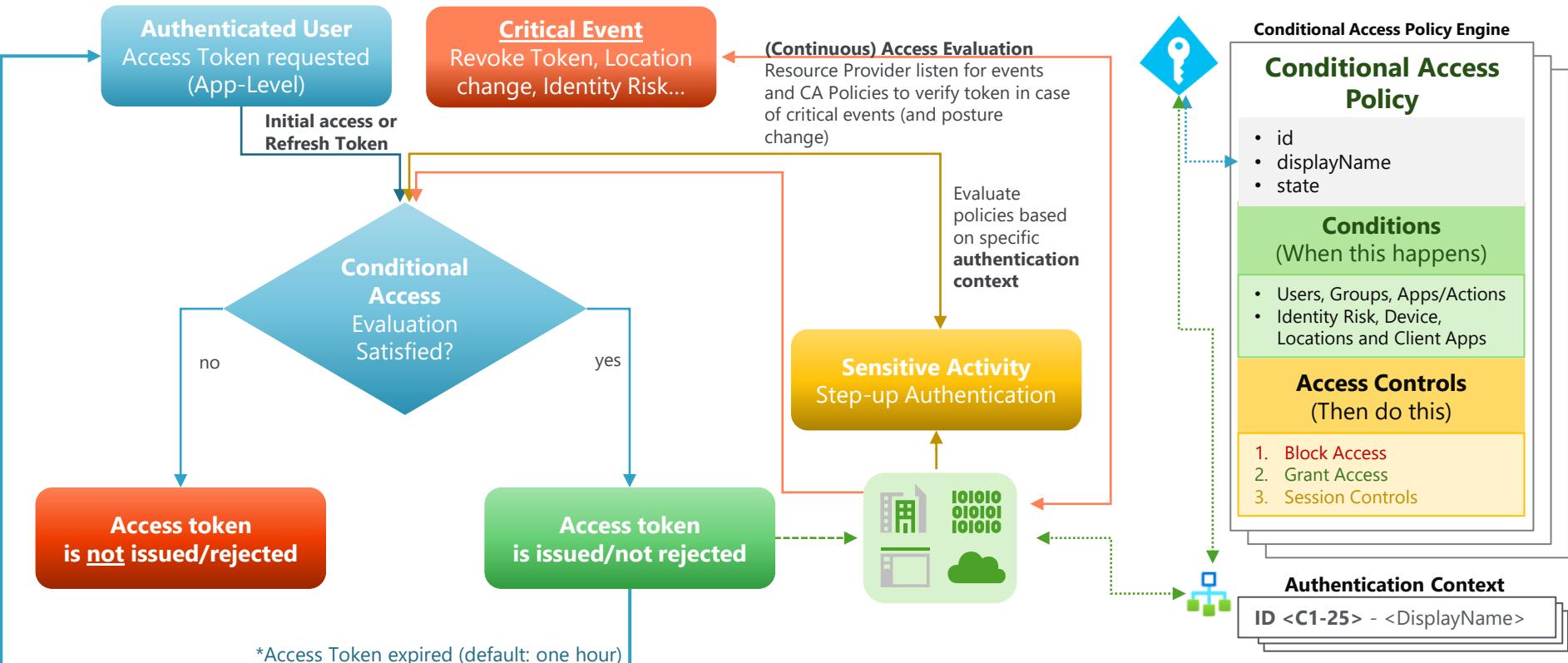
A user from (group) "Marketing employees" is accessing "Office 365" from a browser on a Windows device from any location and no sign-in risk was detected.

...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.



Trigger of Conditional Access Evaluation



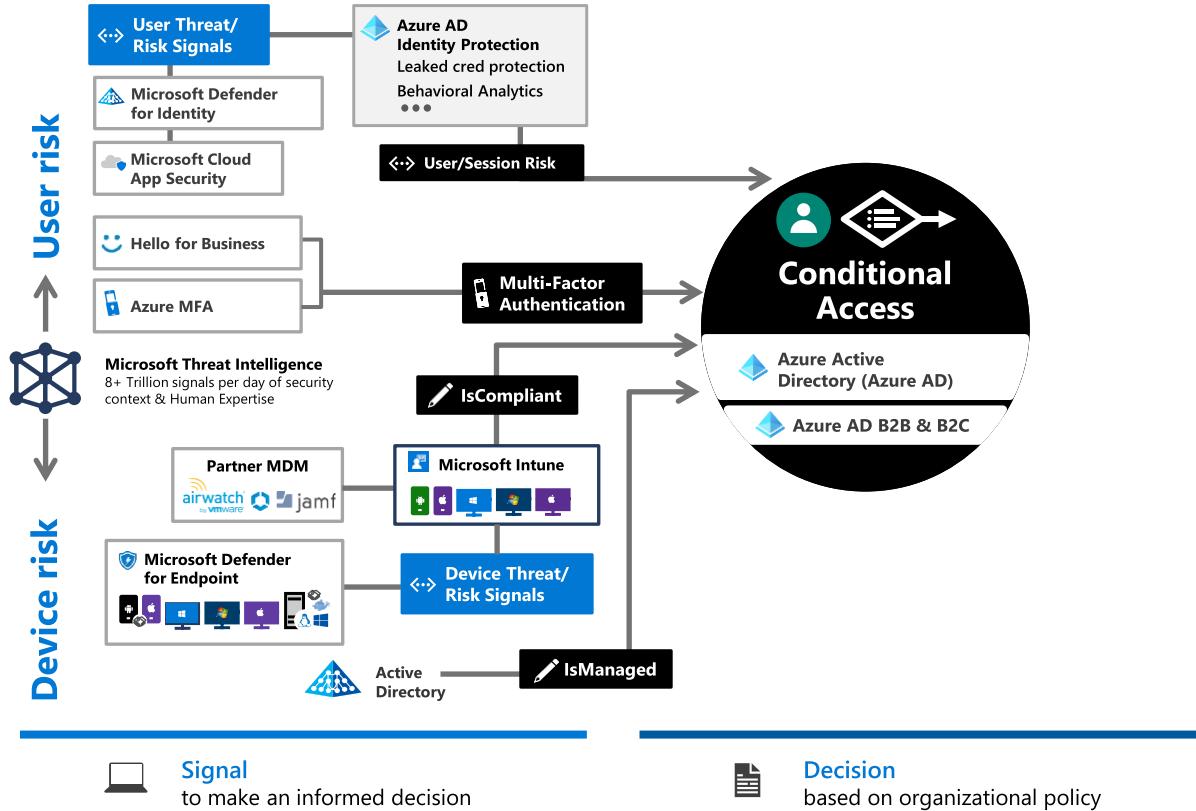


Extension of Conditions & Controls

Integration of Identity Protection and Defender for Cloud Apps

Conditional Access Integration Capabilities

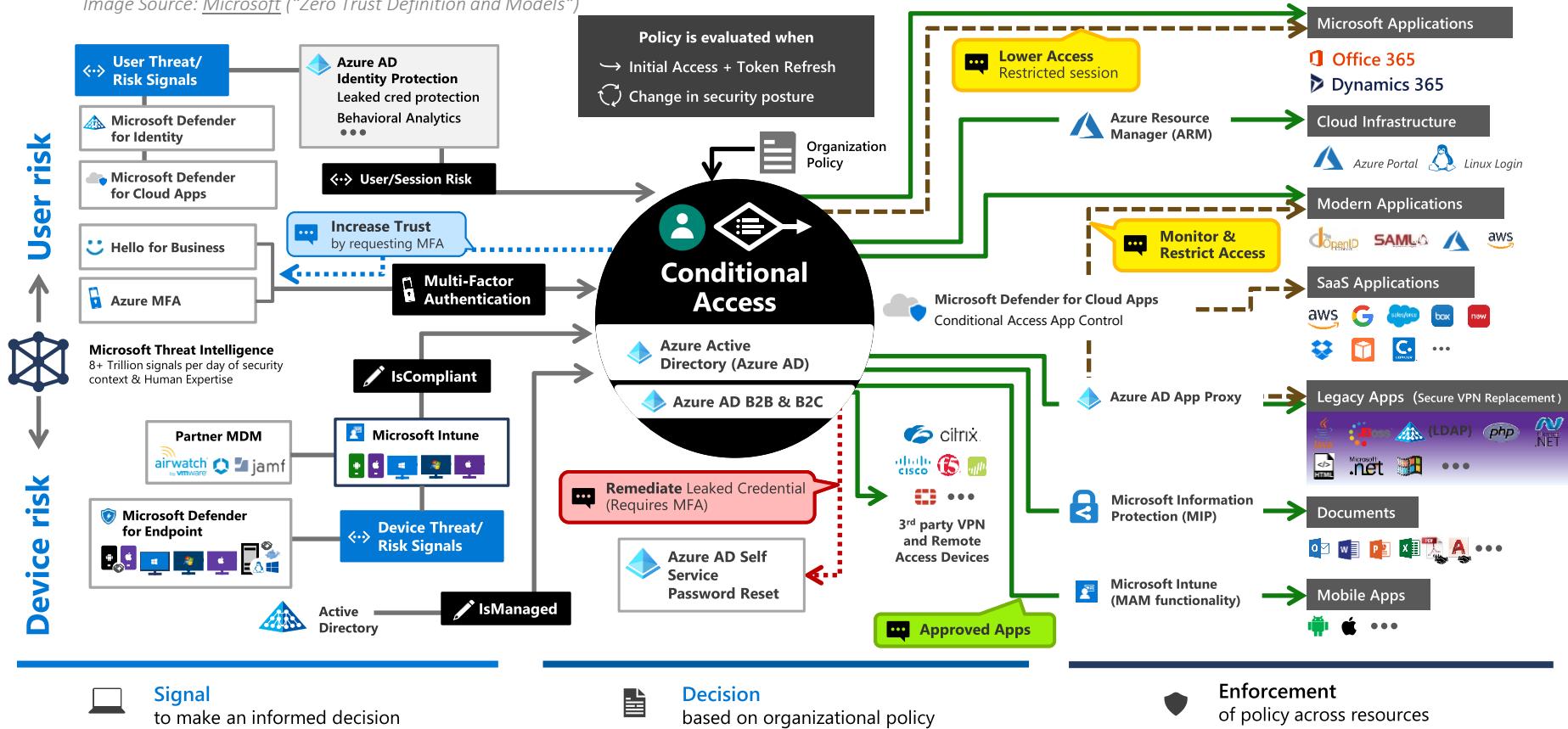
Image Source: Microsoft ("Zero Trust Definition and Models")





Conditional Access Integration Capabilities

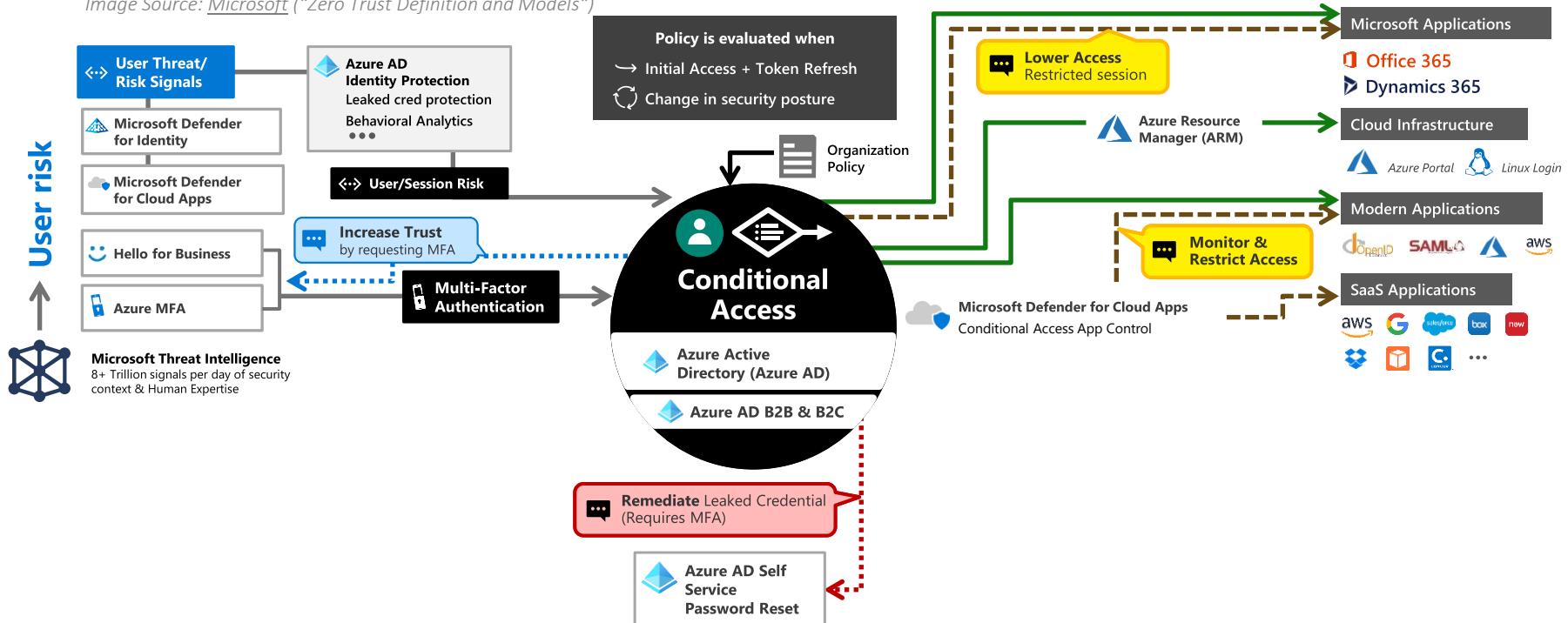
Image Source: Microsoft ("Zero Trust Definition and Models")





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

Wat detection

Information protection

Conditional access

Shadow IT

All policies

- Realtime Sign-in Risk and CAE

- CA App Control in Microsoft Defender for Cloud (MDA)

Policy

Count

Severity

Category

Action

Modified



Block upload of potential malware (based on Microsoft T...
Alert when a user uploads files to the cloud that might be infected with...

0 open alerts



Threat detection



Mar 8, 2021



Block privileged access outside of Secure Admin Worksta...

1 open alerts



Access control



Feb 3, 2021



CA App Control - 3 - Block cut/copy and paste base...
Security will evaluate the content of items that are cut/copi...

5 open alerts



Mar 8, 2021



204 - CA App Control - 1 - Block download based on real...
Cloud App Security will evaluate the content of files being downloaded...

5 open alerts



204 - CA App Control - 0 - Monitor all activities
Cloud App Security will monitor all available activities.

0 open alerts

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*

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

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, AVD/VDI, BYOD?)

Demo: Analyze and implement CA baseline

- Integrated coverage analysis and recommendations



Users

1 off

9 no policies applied
[Monitor user coverage](#)



Devices

99% sign-ins from unmanaged or non-compliant devices
[View devices coverage](#)

[Browse a list of applicable policies](#)

[View top unprotected apps](#)

- Usage & Insights of Authentication Methods/Auth. Prompts

- Built-in Policy Templates

Description

3% of sign-ins out of scope of Conditional Access policies in the last 7 days. [Learn more](#)

Recent sign-ins with medium or above sign-in risk in the last 7 days. [Learn more](#)

Sign-ins lack MFA requirement in the last 7 days. [Learn more](#)

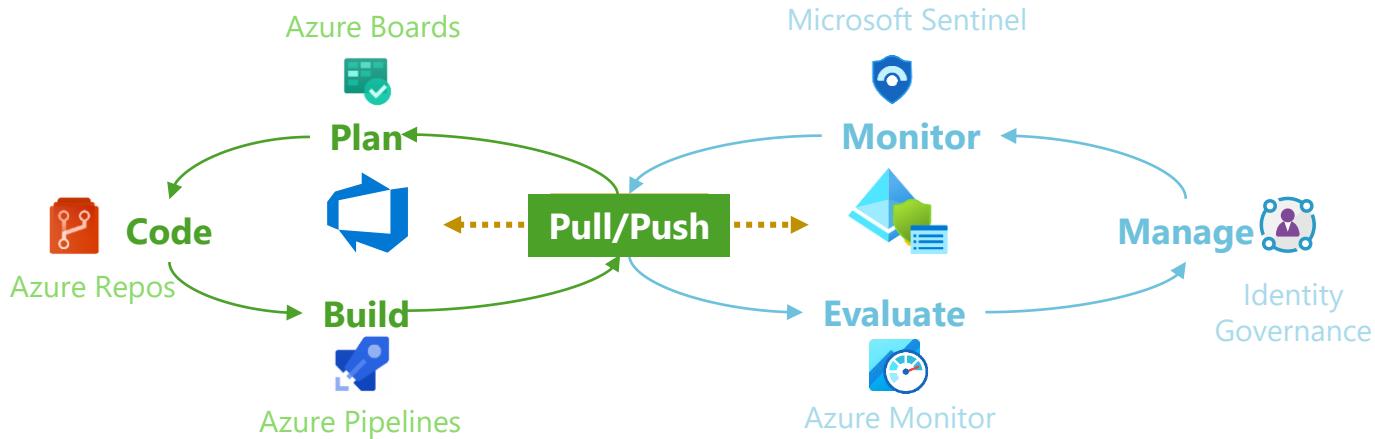
Recommendations

[Create policy to require multi-factor authentication for all users](#)

[Create policy to require multi-factor authentication for risky sign-ins](#)

[Create policy to require multi-factor authentication for users who don't have MFA enabled](#)

Policies As Code - Project "AADOps"



Demo: AADOps

schaengel...

A_Extras

Templates

Components

AADOps-Sa...

AADOps.psm1

Deploy-Nam...

Pull-AADOp...

Push-AADOp...

Reset-AADO...

- Management of Exclusions

cae99da6 (previous) ▾

aef5696e (head)

```

1/03      ,,
1784      {
1785      "id": "e9ca7d28-781e-4eb1-b5af-aa1fb08ae375",
1786      "displayName": "203 - ALL - Data/Workload Plane - Sensitiv
1787      "state": "enabled",
1788      "signInRiskLevels": [
1789      "conditions": {
1790          "userRiskLevels": [
1791          ],
1792          "signInRiskLevels": [
1793          ],
1794          "clientAppTypes": [
1795          ],
1796          "platforms": null,
1797          "locations": null,
1798          "deviceStates": null,
1799          "devices": null,
1800          "clientApplications": null,
1801          "applications": {
1802              "includeApplication": [
1803                  "includeApplication": [
1804                      "includeApplication": [
1805                          "includeApplication": [
1806                              "includeApplication": [
1807                                  "includeApplication": [
1808                                      "includeApplication": [
1809                                          "includeApplication": [
1810                                              "includeApplication": [
1811

```

```

1/04      ,,
1785      {
1786      "id": "e9ca7d28-781e-4eb1-b5af-aa1
1787      "displayName": "203 - ALL - Data/
1788      "state": "enabledForReportingButN
1789      "signInRiskLevels": [
1790      "conditions": {
1791          "userRiskLevels": [
1792          ],
1793          "signInRiskLevels": [
1794          ],
1795          "clientAppTypes": [
1796          ],
1797          "platforms": null,
1798          "locations": null,
1799          "deviceStates": null,
1800          "devices": null,
1801          "clientApplications": null,
1802          "applications": {
1803              "includeApplication": [
1804                  "includeApplication": [
1805                      "includeApplication": [
1806                          "includeApplication": [
1807                              "includeApplication": [
1808                                  "includeApplication": [
1809                                      "includeApplication": [
1810                                          "includeApplication": [
1811

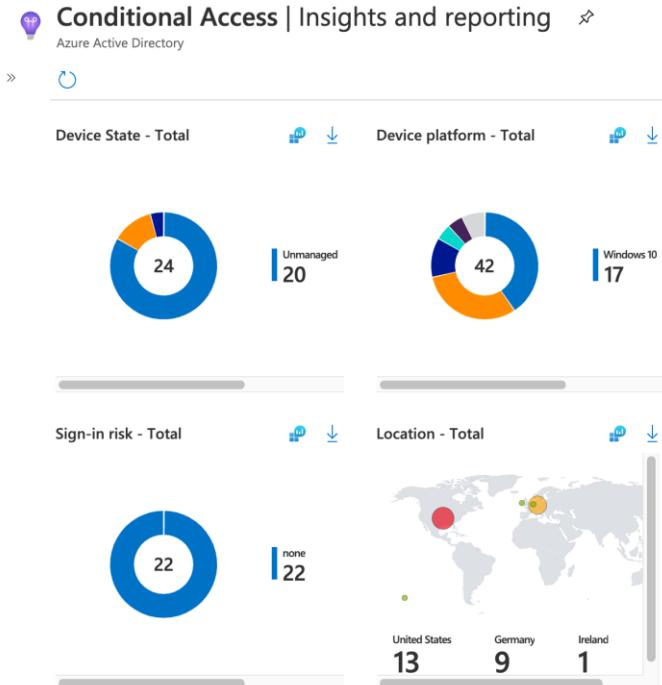
```

1813
1814

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

Microsoft Azure Search resources, services, and docs (G+) thomas@cloud-architek... CLOUDLAB

Home > Conditional Access | Overview (Preview) ...

Overview (Preview) Policies Insights and reporting Diagnose and solve problems

Getting started Overview Coverage Monitoring Tutorials

Got feedback?

Sign-ins by Conditional Access result

Add filter Date range: Last 1 month Policy evaluated: All enabled policies Reset filters

800
600
400
200
0

Apr 8 Apr 9 Apr 10 Apr 11 Apr 12 Apr 14 Apr 16 Apr 18 Apr 20 Apr 22 Apr 24 Apr 27 Apr 30 May 1 May 2 May 3 May 4 May 5

Total sign-ins 5.5K Access granted Controls applied 2.9K Access granted No controls applied 2.4K Access denied Controls applied 29 Access granted No Policy applied 232

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 Microsoft Sentinel



- Audit Logs in Azure AD and M365 Defender

- Analytics Rules in Microsoft Sentinel

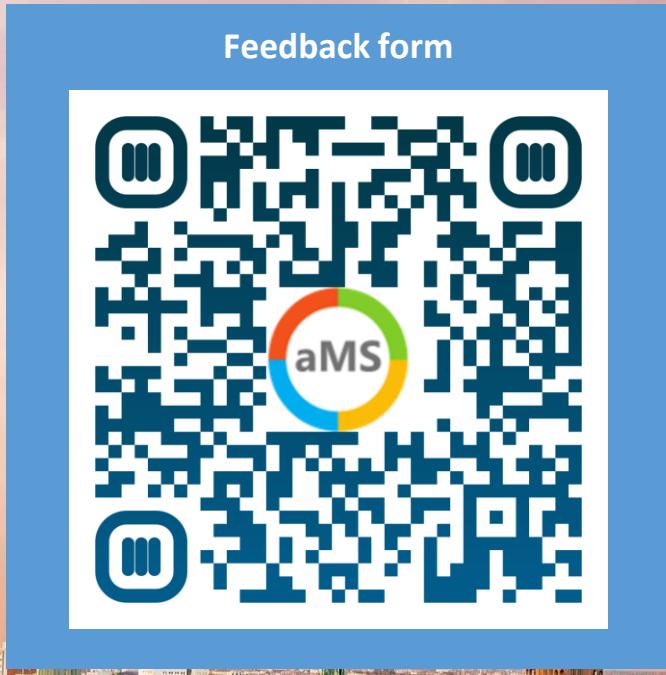
Breakdown per condition and sign-in status

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

Unmanaged
4





THANK YOU!
Danke Schön!