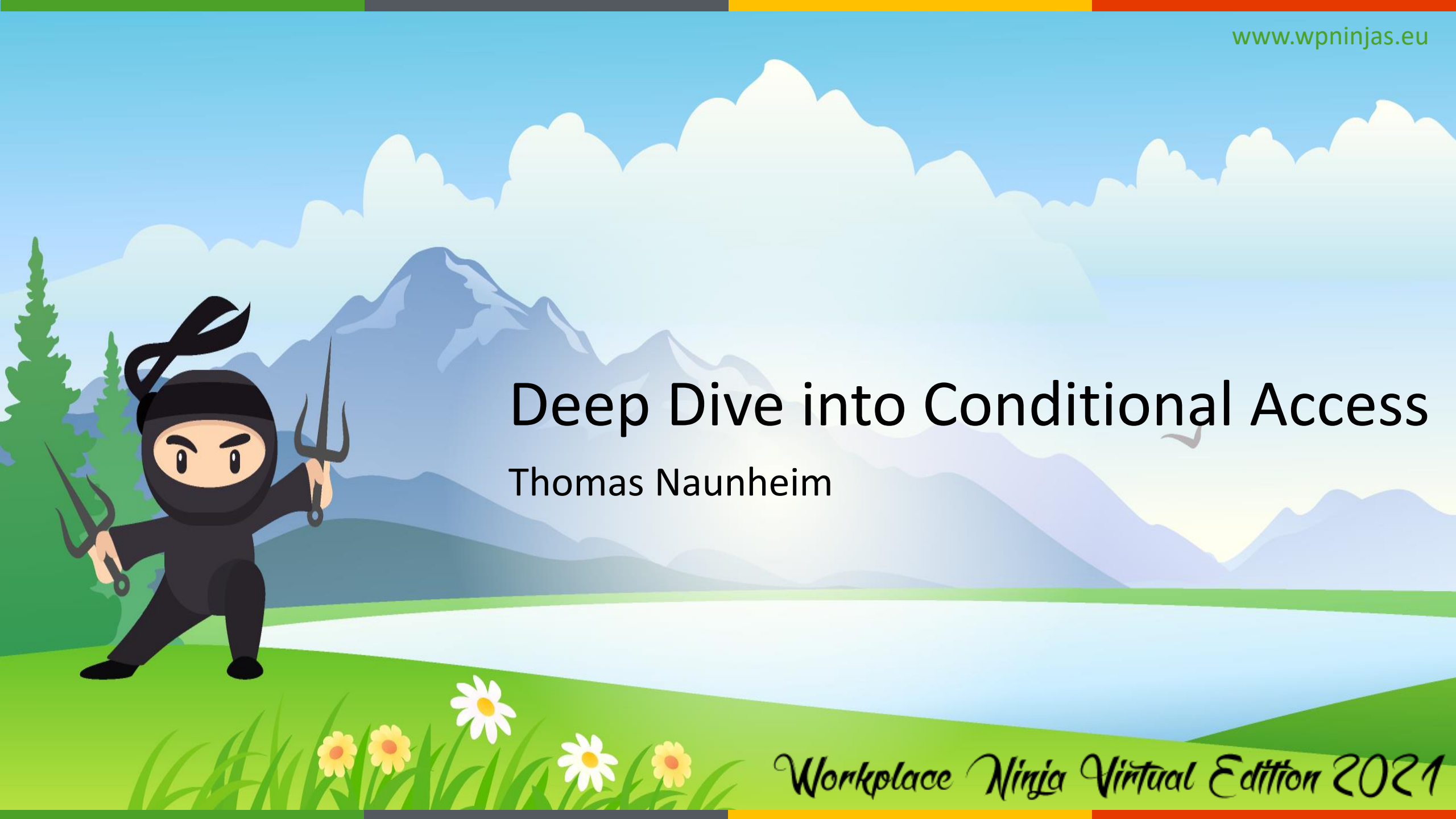
www.wpninjas.eu



Deep Dive into Conditional Access

Thomas Naunheim

Workplace Ninja Virtual Edition 2021

V-Platin Sponsor

nwc services
one step ahead

RECAST SOFTWARE

Patch My PC
PATCH MANAGEMENT MADE EASY

glueckkanja gab

Lenovo

Microsoft

V-Gold Sponsor

scopewyse
we are what's next

sepago®

baseVISION
SECURE & MODERN WORKPLACE

Patron Sponsors

SD:>_
SwissDev Jobs

About Me

Thomas Naunheim

Cloud Security Architect @glueckkanja-gab

Focus

Identity + Security
@Microsoft Azure

From

Koblenz, Germany

My Blog

www.cloud-architekt.net

Certifications

Azure Solutions Architect Expert
Azure DevOps Engineer Expert

Hobbies

Playing Bass Guitar, Hiking, Traveling

Contact

@Thomas_Live

Agenda

Overview of CA Policies

Principals of Signal, Decision and Enforcement

Extension of Conditions and Controls

Integration of Identity Protection and MCAS

Design and Implementation

Best Practices and Common Policies

Policies As Code

Operationalization of Policies, Management at Scale

Monitoring and Reporting

Insights (Workbooks) and Azure Sentinel for SecOps

Key takeaways:

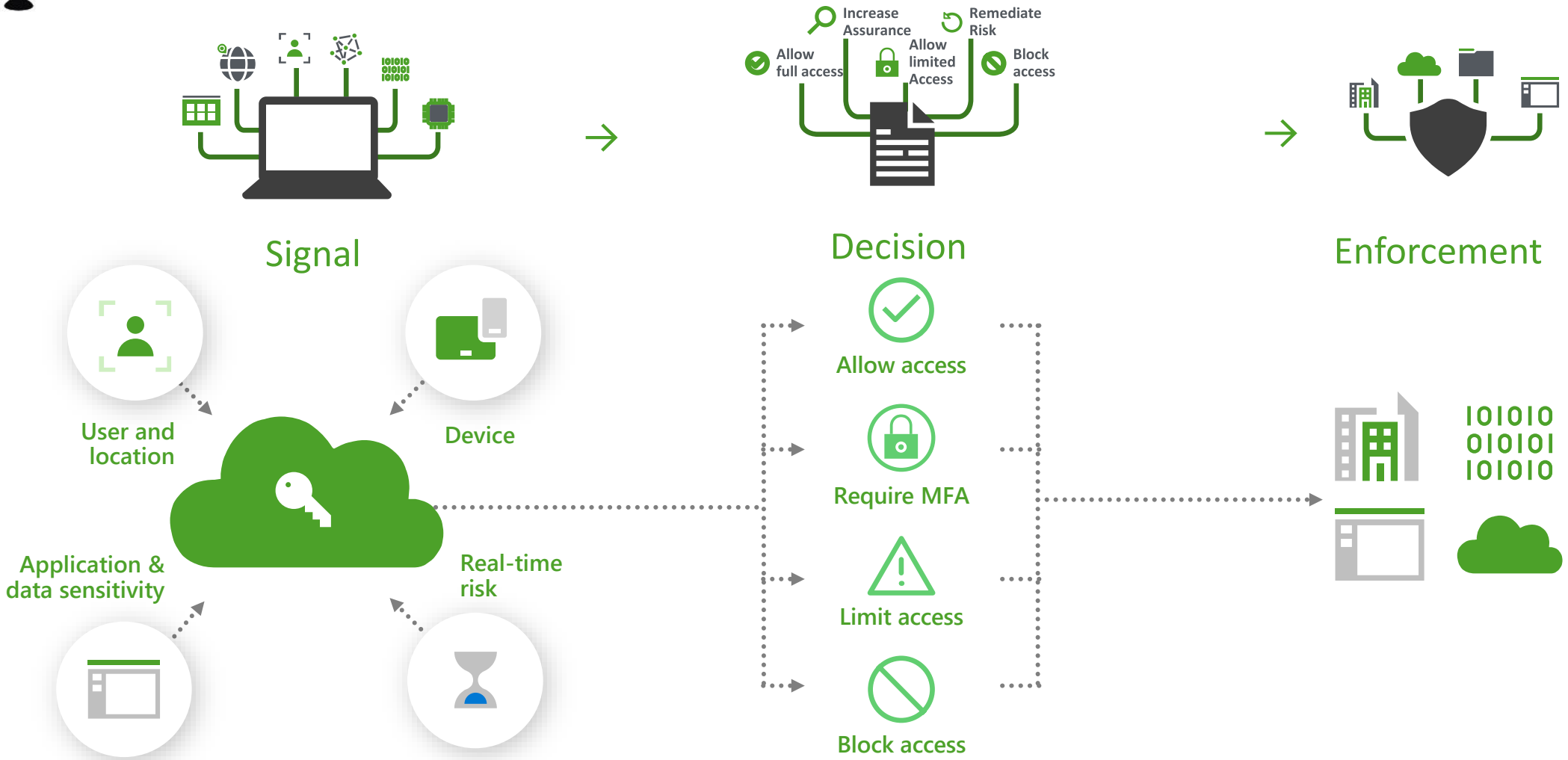
- **Insights of “Policy Engine” and various “Trigger” events**
- **Advanced integration of conditions and control in Microsoft Ecosystem**
- **“Operational” aspects and monitoring of policies are also important**

Overview of Conditional Access

Principals of Signal, Decision and Enforcement

Overview of Conditional Access

www.wpninjas.eu



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

Overview of Conditional Access

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.*

Conditional Access 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: {}
```

Overview of Conditional Access

www.wpninjas.eu

Trigger of Conditional Access Evaluation

Authenticated User
Access Token requested
(App-Level)

Initial access or Refresh Token

Critical Event
Revoke Token, Location change, Identity Risk…

(Continuous) Access Evaluation
Resource Provider listen for events and CA Policies to verify token in case of critical events (and posture change)

Evaluate policies based on specific **authentication context**

Conditional Access
Evaluation
Satisfied?

no

yes

Access token is not issued/rejected

Access token is issued/not rejected

Sensitive Activity
Step-up Authentication

*Access Token expired (default: one hour)

Conditional Access Policy Engine

Conditional Access Policy

- id
- displayName
- state

Conditions
(When this happens)

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

Access Controls
(Then do this)

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

Authentication Context

ID <C1-25> - <DisplayName>

Extension of Conditions & Controls

Integration of Identity Protection and MCAS

CA Integration Capabilities

www.wpninjas.eu

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

Legend
- Full access
- Limited access
- Risk Mitigation
- Remediation Path

Policy is evaluated when
- Initial Access + Token Refresh
- Change in security posture

User risk

- User Threat/ Risk Signals
  - Azure AD Identity Protection
    - Leaked cred protection
    - Behavioral Analytics
    - ...
  - Microsoft Defender for Identity
  - Microsoft Cloud App Security
- User/Session Risk

Microsoft Threat Intelligence
8+ Trillion signals per day of security context & Human Expertise

- Increase Trust by requesting MFA
- Hello for Business
- Azure MFA
- Multi-Factor Authentication

Organization Policy

Conditional Access
- Azure Active Directory (Azure AD)
- Azure AD B2B & B2C

Device risk

- IsCompliant
- Partner MDM: airwatch by vmware, jamf
- Microsoft Intune
- Microsoft Defender for Endpoint
- Device Threat/ Risk Signals
- Active Directory
- IsManaged

Remediate Leaked Credential (Requires MFA)

Azure AD Self Service Password Reset (SSPR)

Lower Access
Restricted session

Monitor & Restrict Access

Approved Apps

Microsoft Cloud App Security
Conditional Access App Control

3rd party VPN and Remote Access Devices: citrix, cisco, f5, ...

- Azure Resource Manager (ARM) → Cloud Infrastructure
  - Azure Portal
  - Linux Login
- Azure AD App Proxy → Legacy Apps (Secure VPN Replacement)
  - Java, JBoss, {LDAP}, php, .NET, HTML, Microsoft .net, ...
- Microsoft Information Protection (MIP) → Documents
- Microsoft Intune (MAM functionality) → Mobile Apps

Microsoft Applications
- Office 365
- Dynamics 365

Modern Applications
- OpenID Connect, SAML, aws, ...

SaaS Applications
- aws, salesforce, box, now, ...

Signal
to make an informed decision

Decision
based on organizational policy

Enforcement
of policy across resources

Extension of Conditions & Controls

Demo: Identity Protection and MCAS

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

Design and Implementation

Best Practices and Common Policies

Design and Implementation

Baseline

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

Design and Implementation

“Common Policies” by Microsoft

Equivalent policies to those 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

Design and Implementation

Policy Fundamentals

- **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, Frontline Workers, CXO, Privileged Users)
  - **Protection level and access paths of „Apps & Data“** (incl. Business / Privileged Interfaces)
  - **Integration level and signals from Endpoints** (AAD-joined + MDM, VDI, BYOD?)

Design and Implementation

“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.

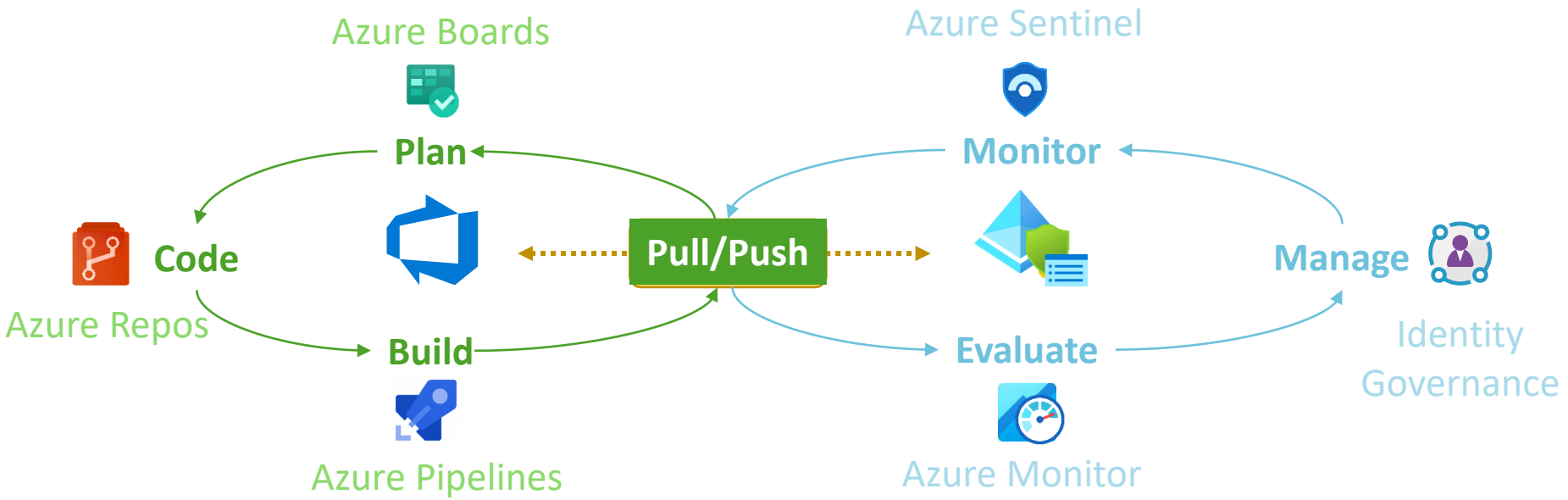
- Repository: „AlexFilipin/ConditionalAccess“ (GitHub)
- 425show episode with talk about the policy templates

Policies As Code

Operationalization of Policies, Management at Scale

Policies As Code

Project “AADOps”



Policies As Code

Demo: AADOps

- Different policy designs
- Advantages in using

  (Azure) Repos and Pipelines
- Templates and Deployment to

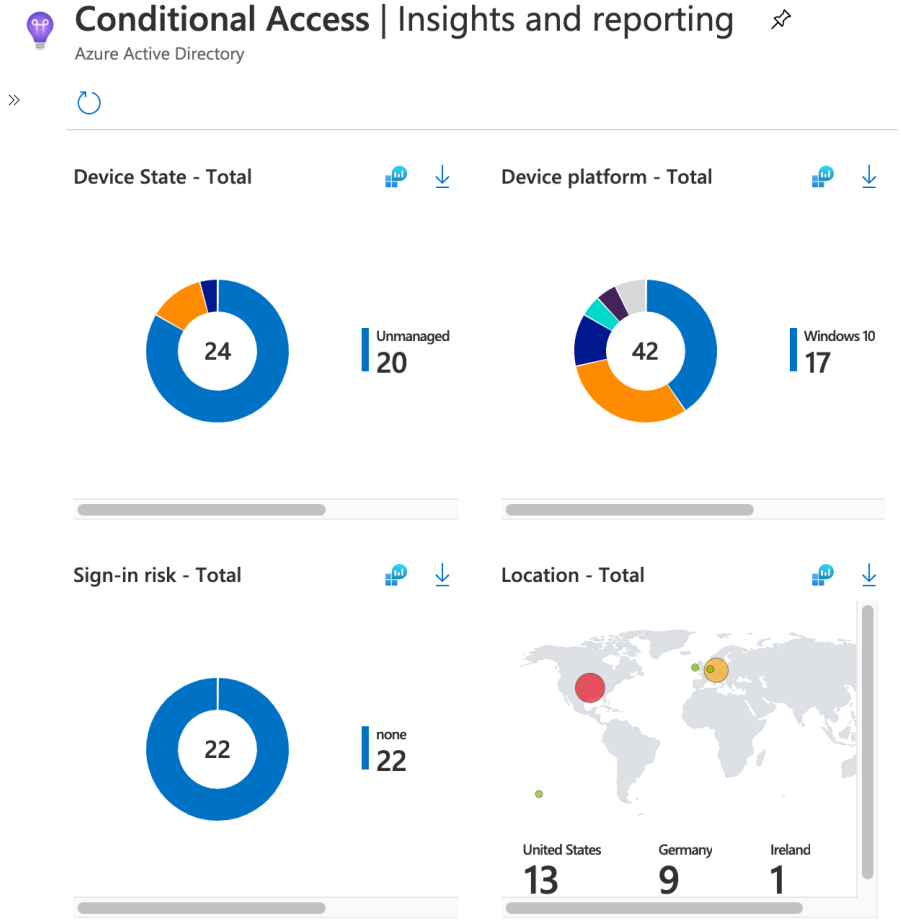
  Intra- vs. Inter-Staging
- Management of Exclusions

Monitoring and Reporting

Insights (Workbooks) and Azure Sentinel for SecOps

Monitoring and Reporting

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

Monitoring and Reporting

Demo: Azure Workbooks and Azure Sentinel

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

Thank You