Virtual

Cologne

Securing and monitoring your Azure AD user and privileged accounts

Thomas Naunheim

About Me

Thomas Naunheim

Cloud Engineer
Koblenz, Germany

@Thomas_Live

Thomas@Naunheim.net

www.cloud-architekt.net

Securing and monitoring your Azure AD accounts

Protection and defense of identites across platforms and perimeters

Identity Protection and Strong Authentication

Reduced attack surface of Azure AD

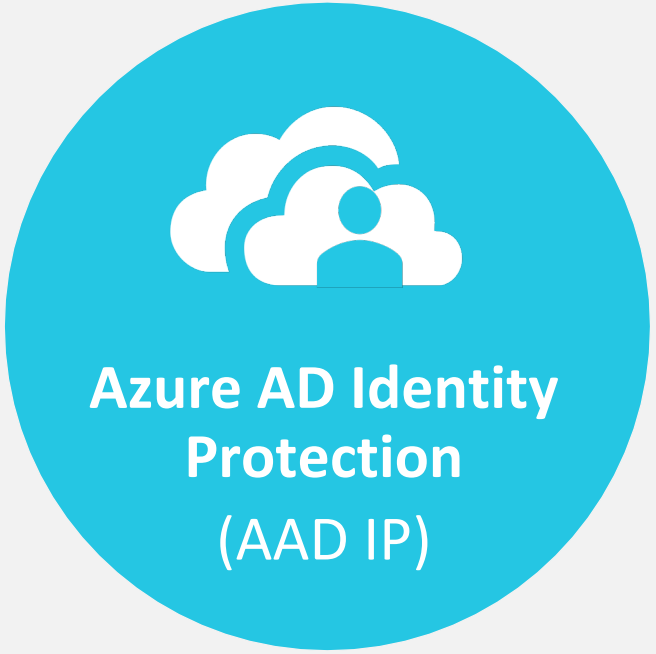
Lower exposure of privileged accounts

Detect, investigate and response of identity threats

Identity Protection and Strong Authentication

Prevent, detect and remediate identity risks

End-to-end Identity Protection



Cloud Identity

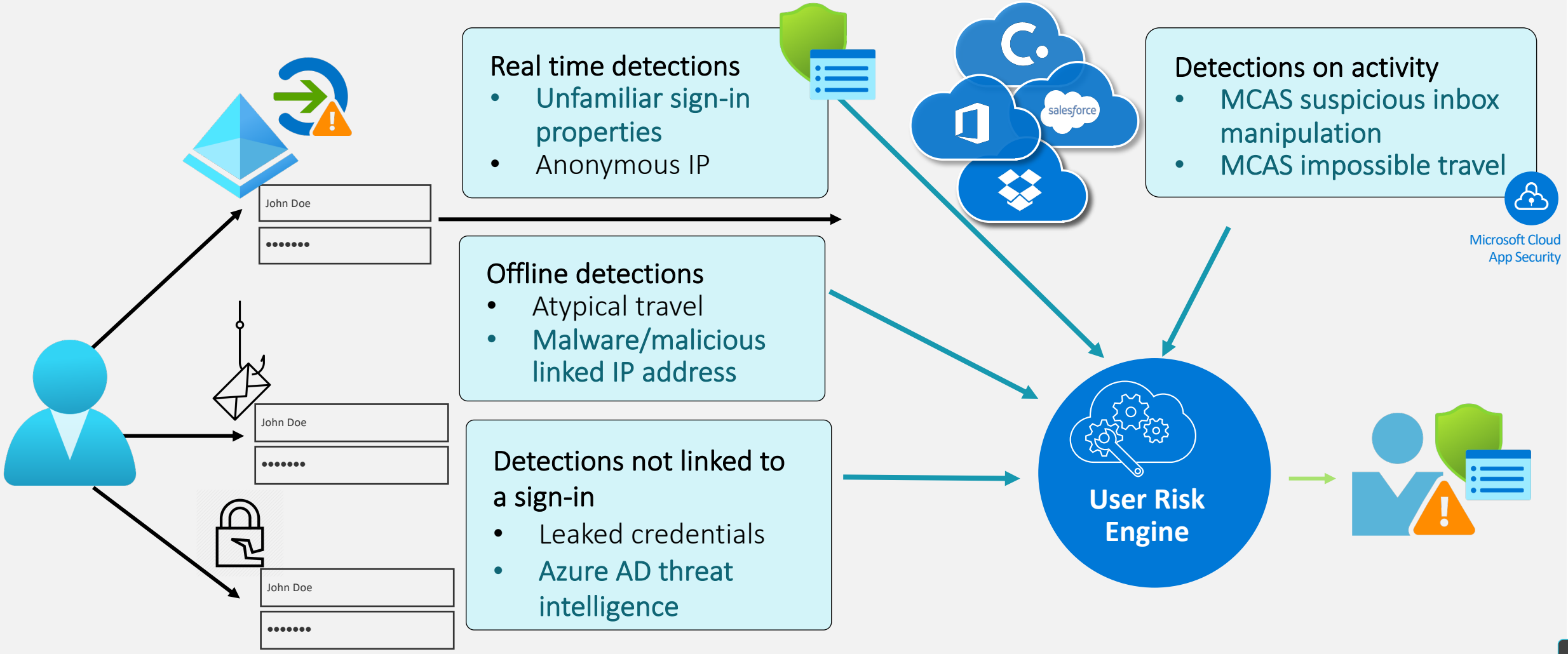
On-Premises Identity

Cloud App (Sessions)

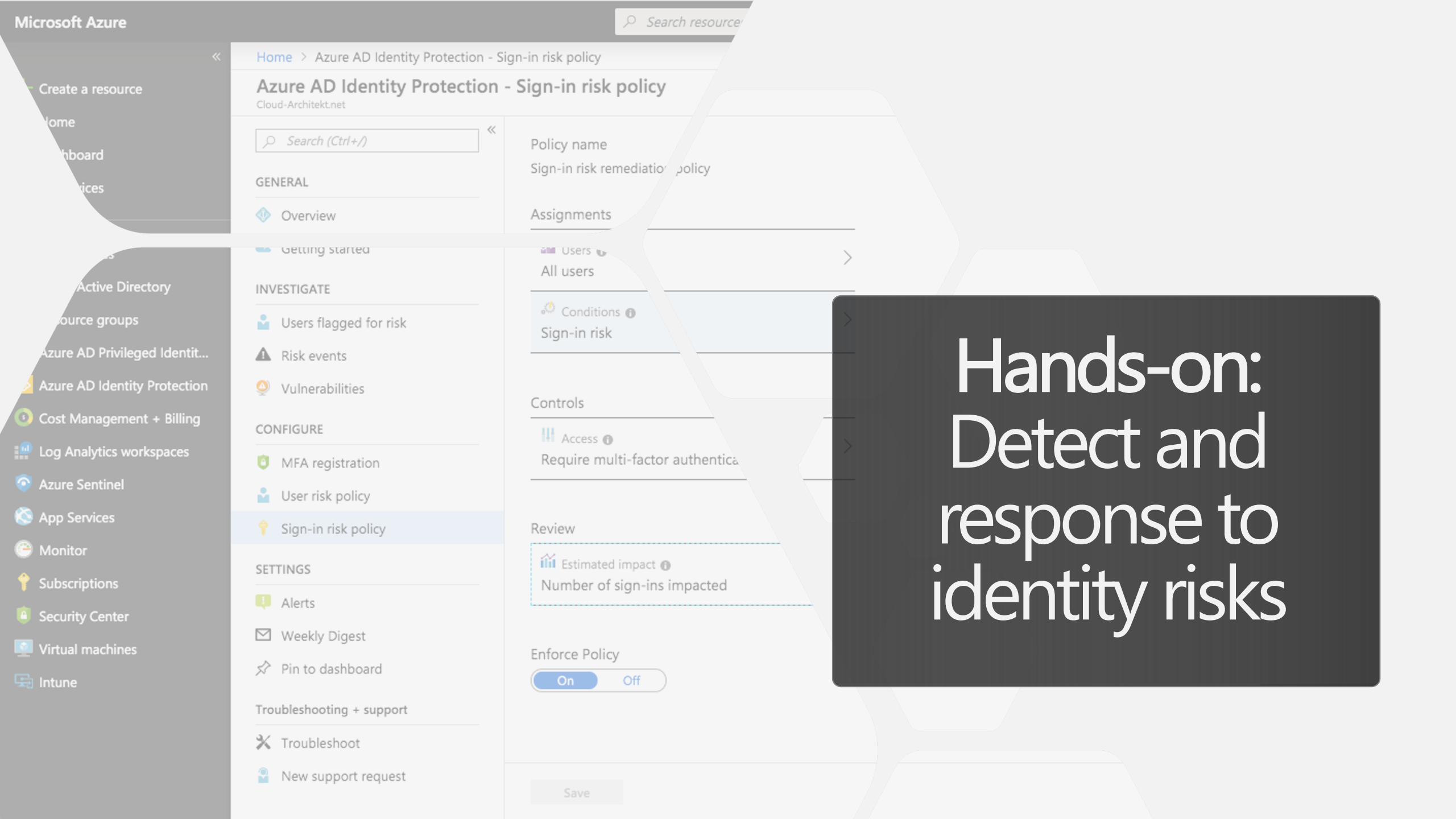
Aggregation + User and Entity Behavior Analytics (UEBA)

Prevent, detect and remediate identity risks

Automate response with Identity Protection and MCAS signals



Source: [Microsoft Ignite Session ("The science behind Azure Active Directory Identity Protection")]



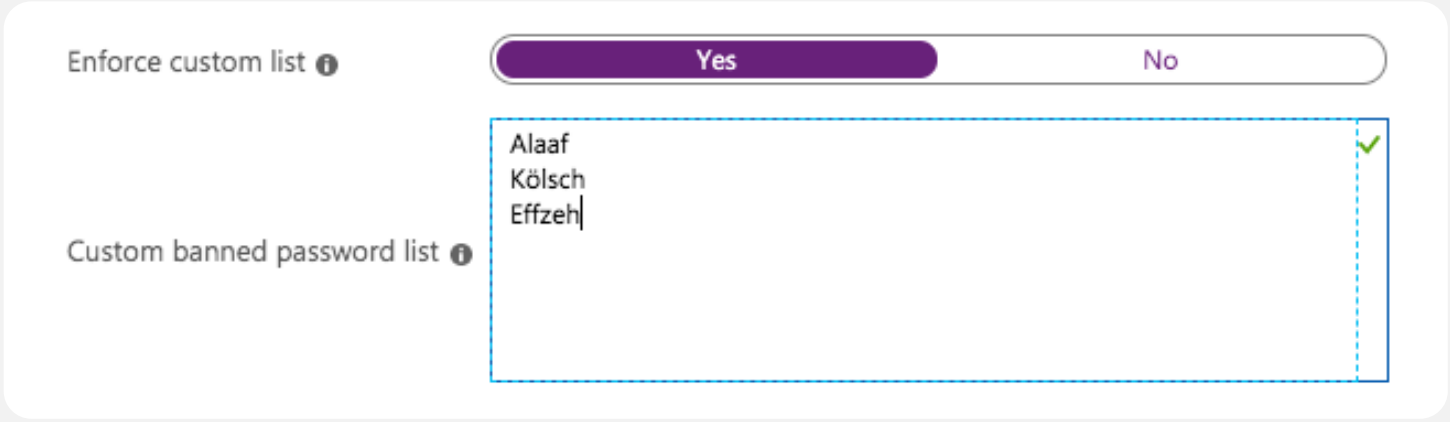
Hands-on: Detect and response to identity risks

Reduce weakness of password-based authentication

Smart Lockout and Password Protection

- Assists in locking out attackers to use **brute-force methods**:

- Avoid creating **weak passwords** with global and custom banned password list



Source: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises

Strong authentication

Options of „Passwordless“ authentication

Image Source: [Identity and access management best practices from around the world]

Reduced attack surface of Azure AD

Conditional Access

Design and Implementation of policies

- **Build strong baselines for users** (hybrid, guest and admins) **and apps** (protection needs)
- Define a standard **naming** convention for policies

  CA01 - Dynamics CRP: Require MFA for marketing When on external networks

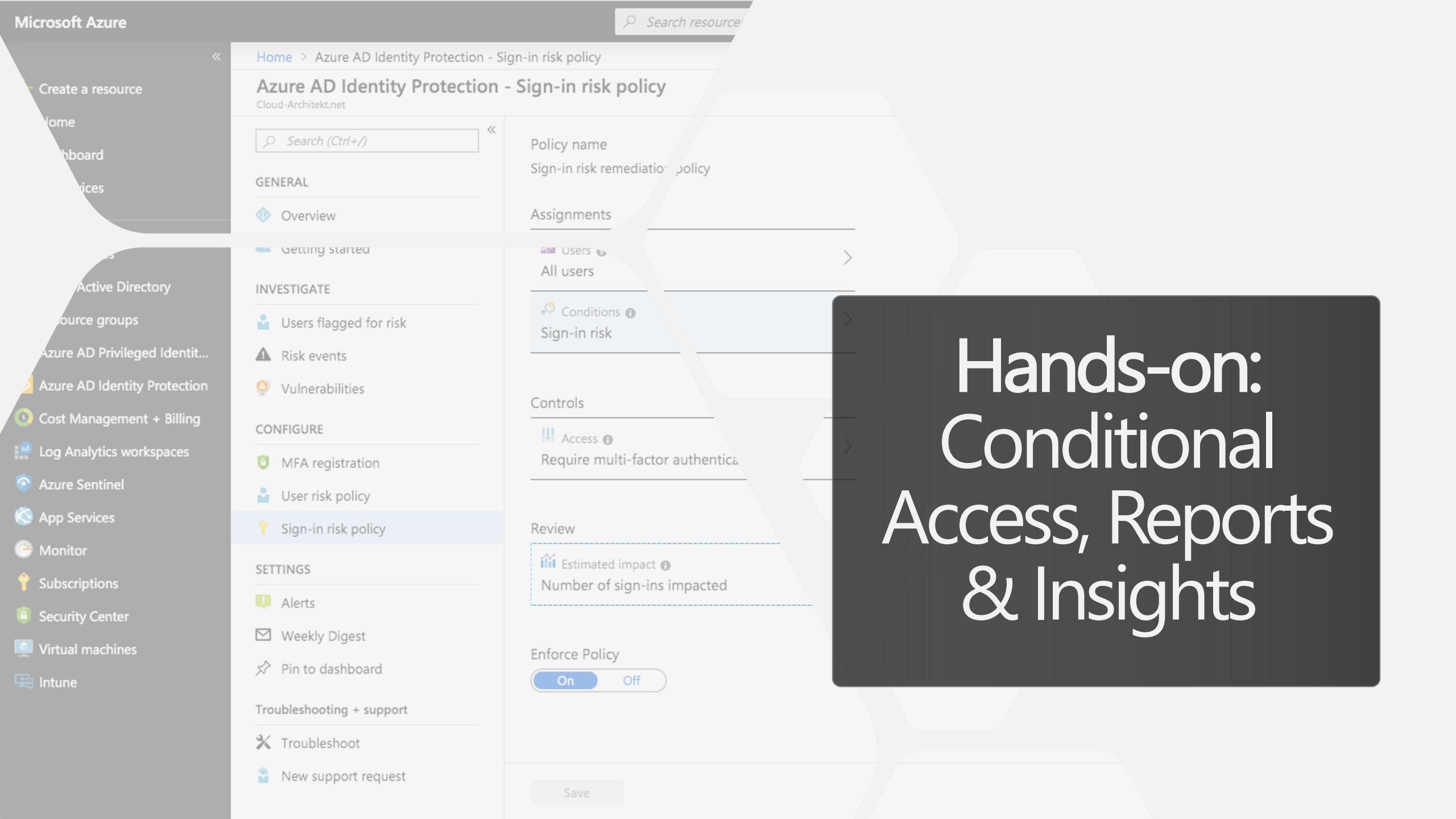
<SN>-	<Cloud app>:	<Response>	For	<Principal>	When	<Conditions>

- **Draft policies** (when this happens → do this)

When this happens	Then do this

- **Consider your environment** (types of devices and authentication methods)
- **Exclude „emergency access accounts“** and **regular review** of other exclusions
- **„Conditional Access as Code“** (Automation and policy sets by Alexander Filipin)

Source: Microsoft Docs („How To: Plan your Conditional Access deployment in Azure Active Directory“)

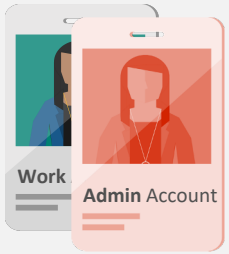


Hands-on: Conditional Access, Reports & Insights

Lower exposure of privileged accounts

Lower exposure of privileged accounts

Foundation of securing privileged access



Separated privileged identities

Issue managed and separated accounts for (least) privileged access
strong or password less authentication

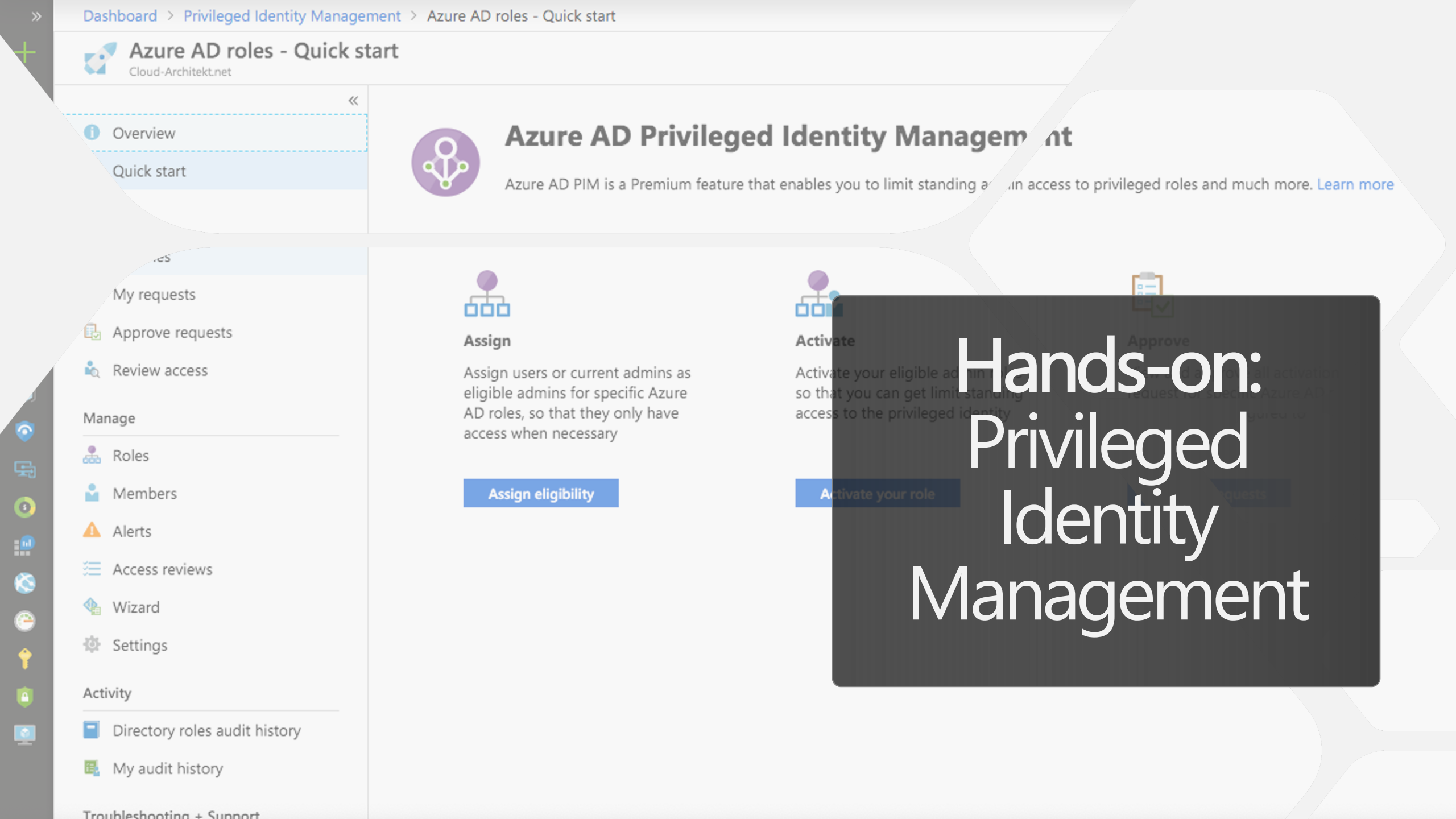
Non-persistent and audited access

Provide zero rights by default to administration accounts
Just-in-time (JIT) privileges based on a standardized RBAC model

Secure devices

Establish a separate device/workstation for administrative tasks
Various kinds of security levels and implementations

Source: Microsoft Security Blog (“3 investments Microsoft is making to improve identity management”)


Dashboard > Privileged Identity Management > Azure AD roles - Quick start
Azure AD roles - Quick start
Cloud-Architekt.net
Overview
Quick start
My requests
Approve requests
Review access
Manage
Roles
Members
Alerts
Access reviews
Wizard
Settings
Activity
Directory roles audit history
My audit history
Azure AD Privileged Identity Management
Azure AD PIM is a Premium feature that enables you to limit standing access to privileged roles and much more. Learn more
Assign
Assign users or current admins as eligible admins for specific Azure AD roles, so that they only have access when necessary
Assign eligibility
Activate
Approve
Hands-on: Privileged Identity Management

Privileged Identity Management (PIM)

Considerations of Azure AD Privileged Identities

- **Built-in directory roles and effective permissions**
  - Intune Service administrator: Modify security groups
  - Authenticator Admin: Reset passwords of “non-admins” (Azure?)
- **Limitation of custom directory roles and scoped permissions**
  - Administrative Units still in preview and very limited
  - Custom roles available for App Registrations only
- **No support for security group** assignment yet (UserVoice)

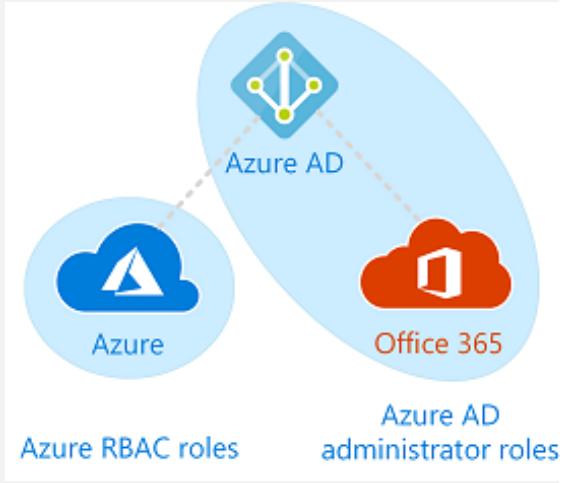
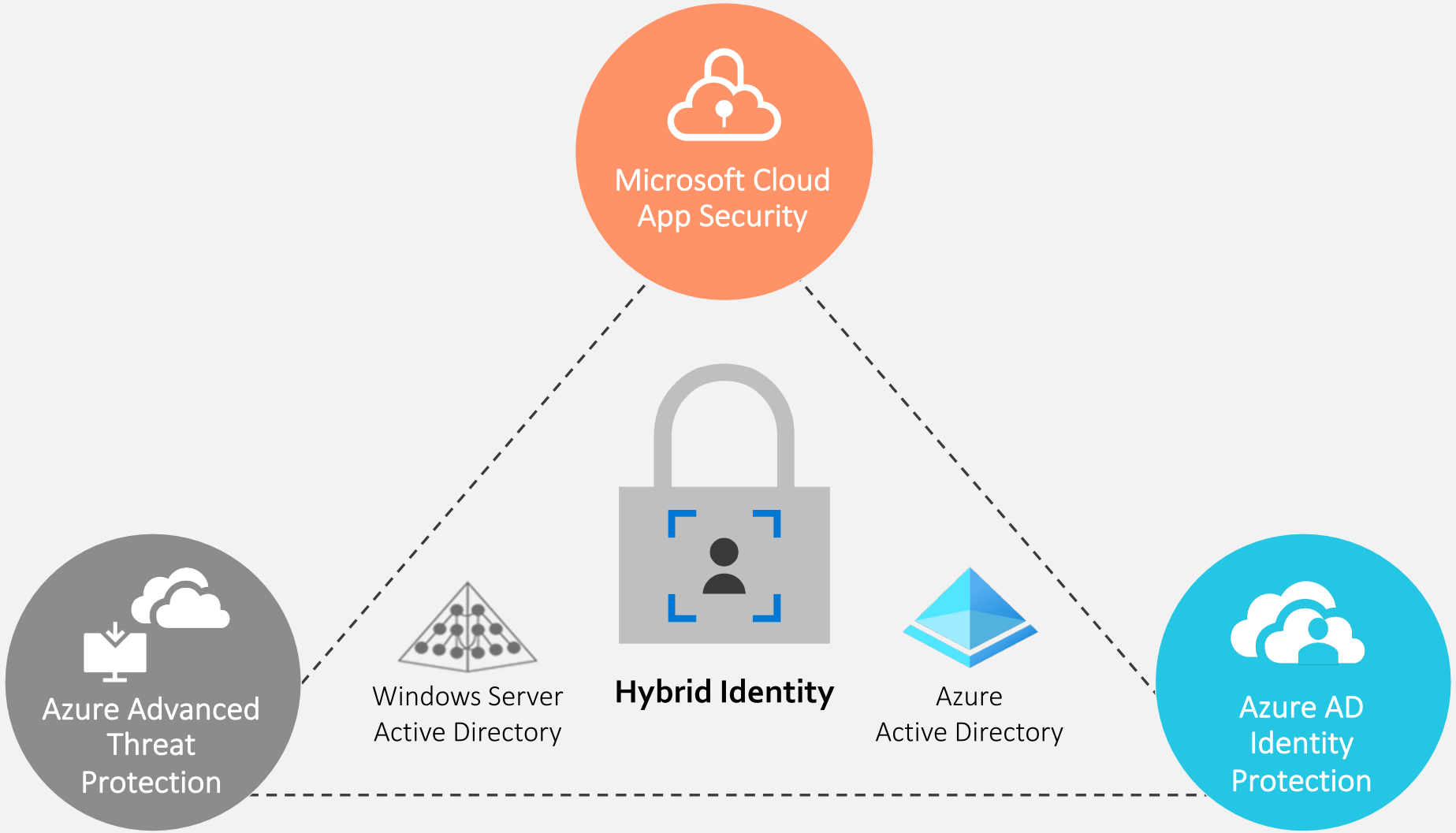


Image source: Microsoft Docs („Classic subscription administrator roles, Azure RBAC roles, and Azure AD administrator roles “)

Detect, investigate and response of identity threats

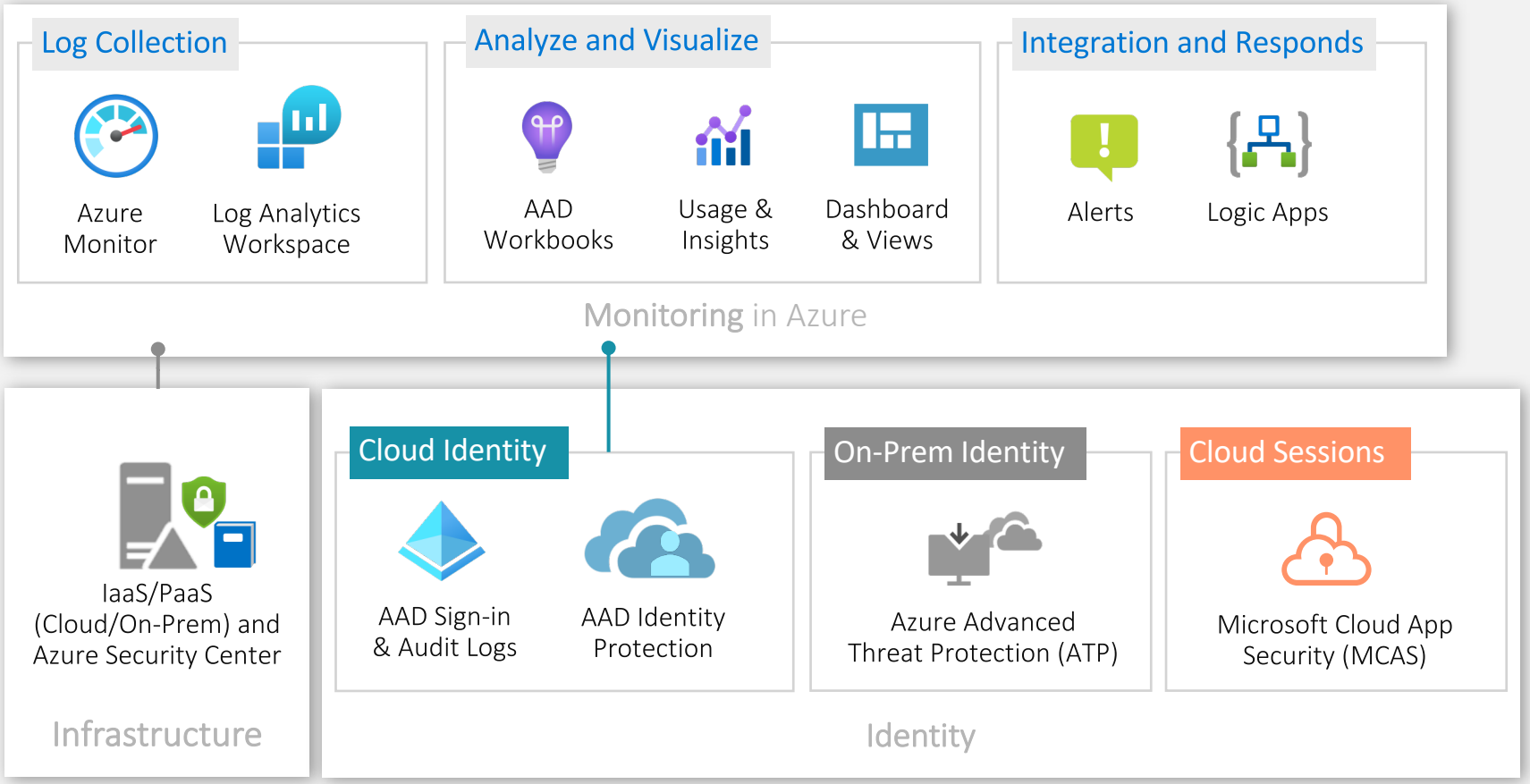
Detect, investigate and response of identity threats

Identity Operations: Azure Monitor and other portals



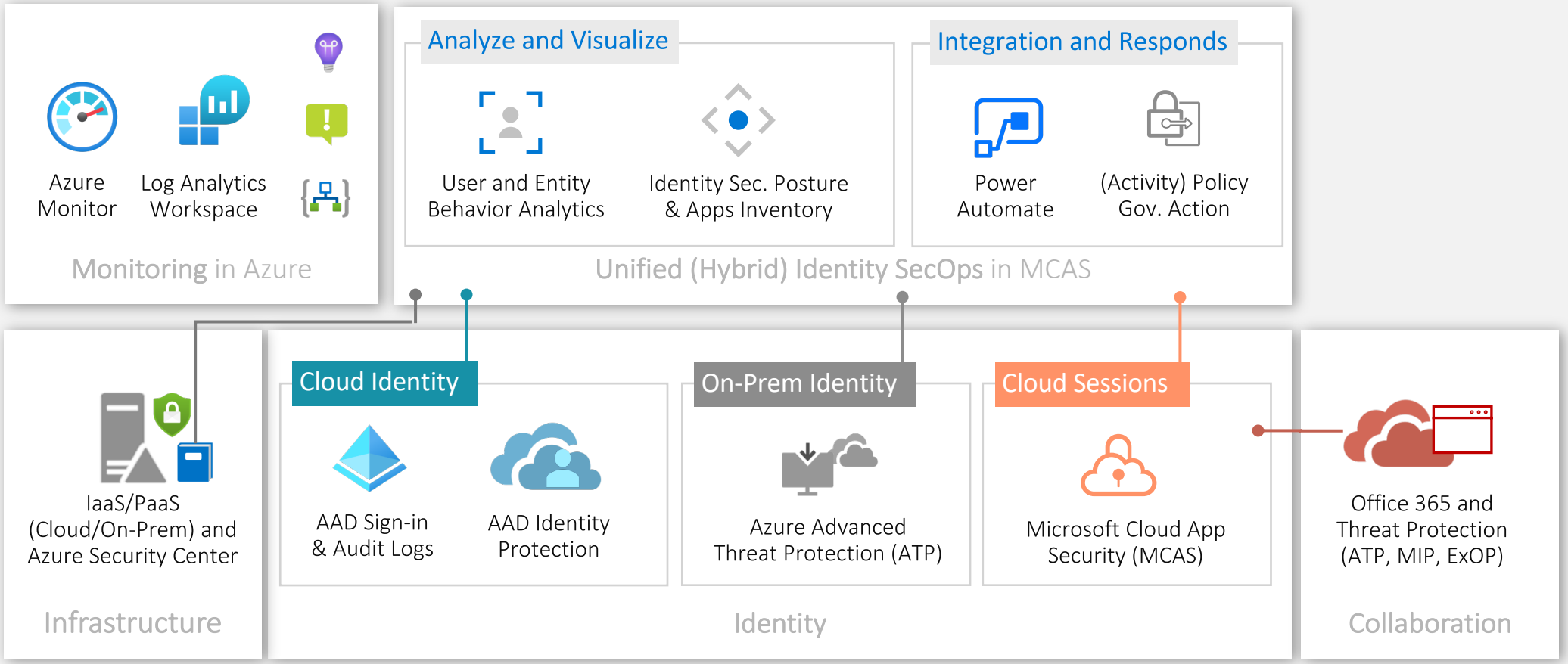
Detect, investigate and response of identity threats

Azure Monitor: Forwarded logs of Azure IaaS/PaaS and Azure AD reports



Detect, investigate and response of identity threats

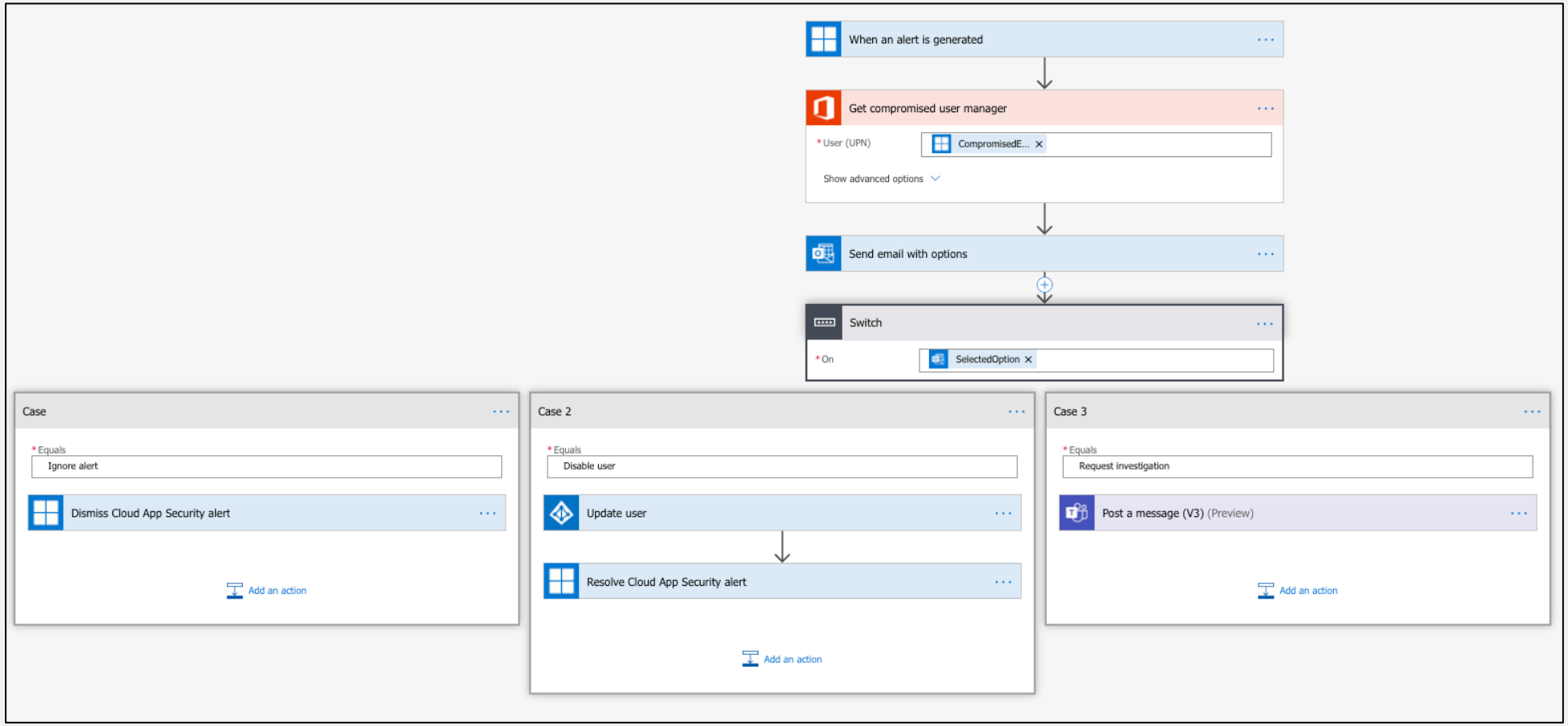
MCAS: Unified Identity SecOps



Detect, investigate and response of suspicious user behavior

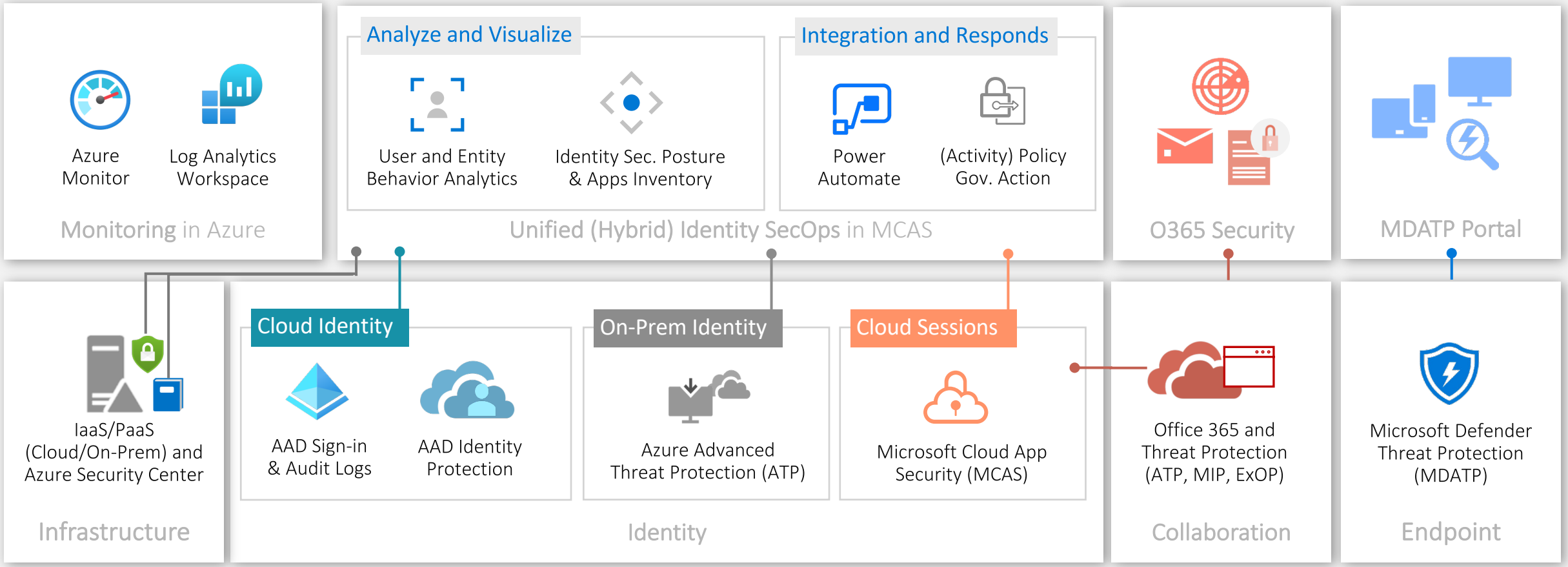
Automate of MCAS Alert response with PowerAutomate (Flow)

- Automating Security workflows with PowerAutomate (various use cases)



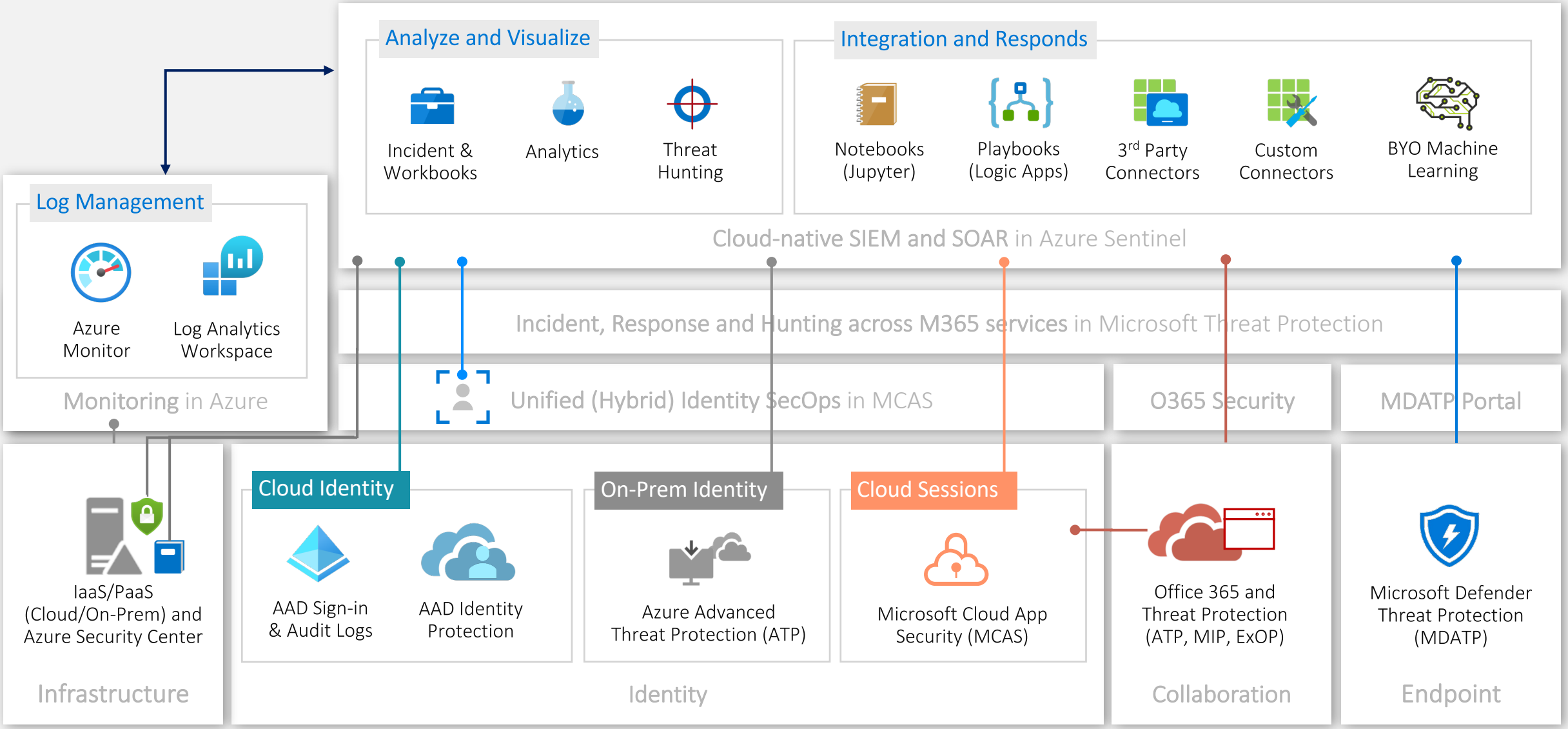
Detect, investigate and response of identity threats

Unified Identity SecOps with MCAS, Microsoft & Office ATP Portals



Detect, investigate and response of identity threats

„Single pane of glass“ with Azure Sentinel (Microsoft‘s cloud-native SIEM)

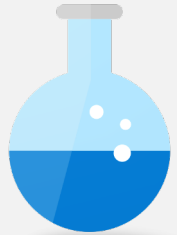


Detect, investigate and response of identity threats

Automate of Azure Sentinel Analytic/Incident with Logic Apps

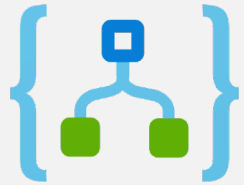
Hunting

- Azure Active Directory signins from new locations
- Inactive or new account signins
- …



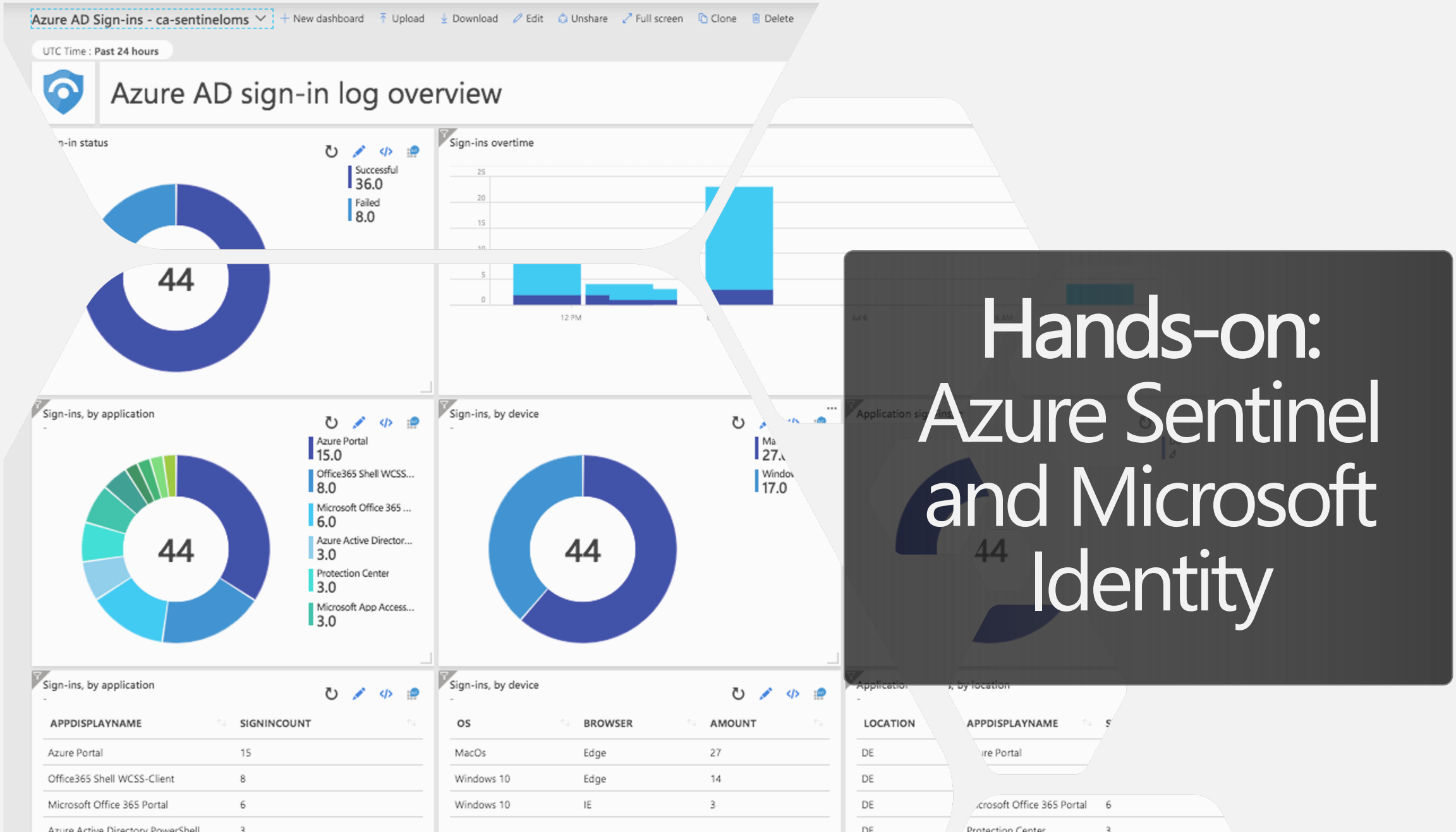
Analytics/Detections

- Attempt to bypass conditional access rule in Azure AD
- Cisco Firewall block but success logon to AAD
- …



Response/Playbooks

- Block-AADUser
- Confirm-AADRiskyUser
- Isolate-MDATPMachine
- Revoke-AADSignInSessions
- Reset-AADUserPassword


Azure AD Sign-ins - ca-sentineloms
New dashboard
Upload
Download
Edit
Unshare
Full screen
Clone
Delete
UTC Time : Past 24 hours
Azure AD sign-in log overview
Sign-ins overtime
Successful
36.0
Failed
8.0
44
Sign-ins, by application
Azure Portal
15.0
Office365 Shell WCSS...
8.0
Microsoft Office 365 ...
6.0
Azure Active Director...
3.0
Protection Center
3.0
Microsoft App Access...
3.0
Sign-ins, by device
17.0
Sign-ins, by application
APPDISPLAYNAME
SIGNINCOUNT
Azure Portal
15
Office365 Shell WCSS-Client
8
Microsoft Office 365 Portal
6
Sign-ins, by device
OS
BROWSER
AMOUNT
MacOs
Edge
27
Windows 10
Edge
14
Windows 10
IE
3
LOCATION
APPDISPLAYNAME
DE
DE
DE
6
Hands-on:
Azure Sentinel
and Microsoft
Identity

Prevent, detect and remediate identity risks

Automate of Azure Sentinel Analytic/Incident with Logic Apps

Detection, Queries, Playbooks and Workbooks in Azure Sentinel Repository

Advanced **multistage attack detection** („Fusion features“)

- Suspicious sign-in activity followed by anomalous Office 365 activity

Build your **own advanced use cases and auto-remediation scenarios**:

- Reducing false positive of impossible travel („Azure Sentinel webinar: Tackling Identity“)

Thank you to our sponsors

pmOne

#GLOBALAZURE 2020
BY COMMUNITY • FOR COMMUNITY
Cologne

Virtual

Azure Meetup
KÖLN

Feedback:

http://feedback.azurecgn.de/

Cologne

Virtual

Azure Meetup
KÖLN

Thank You

@Thomas_Live

Thomas@Naunheim.net

www.cloud-architekt.net