Azure Meetup
THÜRINGEN

Design and Security
Hybrid Azure AD

Thomas Naunheim

Azure Meetup Thüringen, 16.01.2020

About Me

Thomas Naunheim

Cloud Engineer
Koblenz, Germany

@Thomas_Live

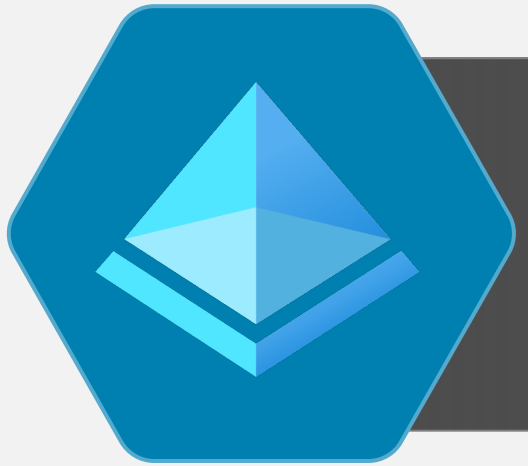
Thomas@Naunheim.net

www.cloud-architekt.net

Azure Meetup
BONN

Agenda

1. Azure Active Directory Tenant
2. Hybrid Identity Synchronization
3. Hybrid Identity Authentication
4. Hybrid Identity Protection
5. Privileged Identity Management



Azure Active Directory
Tenant

Azure Active Directory

Active Directory in Azure?

(Windows Server)
AD Domain Services

- Forest/Domain
- LDAP / ADSI
- NTLMv2, Kerberos
- Domain Membership
- Group Policy Management
- Organizational Units
- Internal corporate network
- IT-Driven Management

Azure Active Directory

Active Directory in Azure?

(Windows Server)

AD Domain	AD Federation Services
Forest/Domain	ADFS Farm
LDAP / ADSI	
NTLMv2, Kerberos	SAML, WS*, OAuth, OIDC
Domain Membership	Workplace Join
Group Policy Management	
Organizational Units	
Internal corporate network	External network (WAP)
IT-Driven Management	

Azure Active Directory

Active Directory in Azure?

(Windows Server)	
AD Domain	**AD Federation Services**
Forest/Domain	ADFS Farm
LDAP / ADSI	
NTLMv2, Kerberos	SAML, WS*, OAuth, OIDC
Domain Membership	Workplace Join
Group Policy Management	
Organizational Units	
Internal corporate network	External network (WAP)
IT-Driven Management	

(Azure)
Azure Active Directory
Tenant
Graph API (REST-APIs)
SAML, WS*, OAuth, OIDC
Domain Join, Device Registered
- (MDM/Intune Device policies)
Flat (excl. Administrative Units)
Cloud-Services/Web-Focused
User-Driven (Self Services)

Azure Active Directory

Active Directory in Azure?

(Windows Server)
AD Domain Services

- Forest/Domain
- LDAP / ADSI
- NTLMv2, Kerberos
- Domain Membership
- Group Policy Management
- Organizational Units
- Internal corporate network
- IT-Driven Management

Options for lift-and-shift:

1. Full Control of AD =
Domain Controllers as IaaS

2. Managed AD in Azure* =
Azure AD Domain Services

3. Third Party Managed AD =
- AWS Directory Service for AD
- GCP Managed Service for AD

*Limited functionality
and comparison of features
strongly recommended

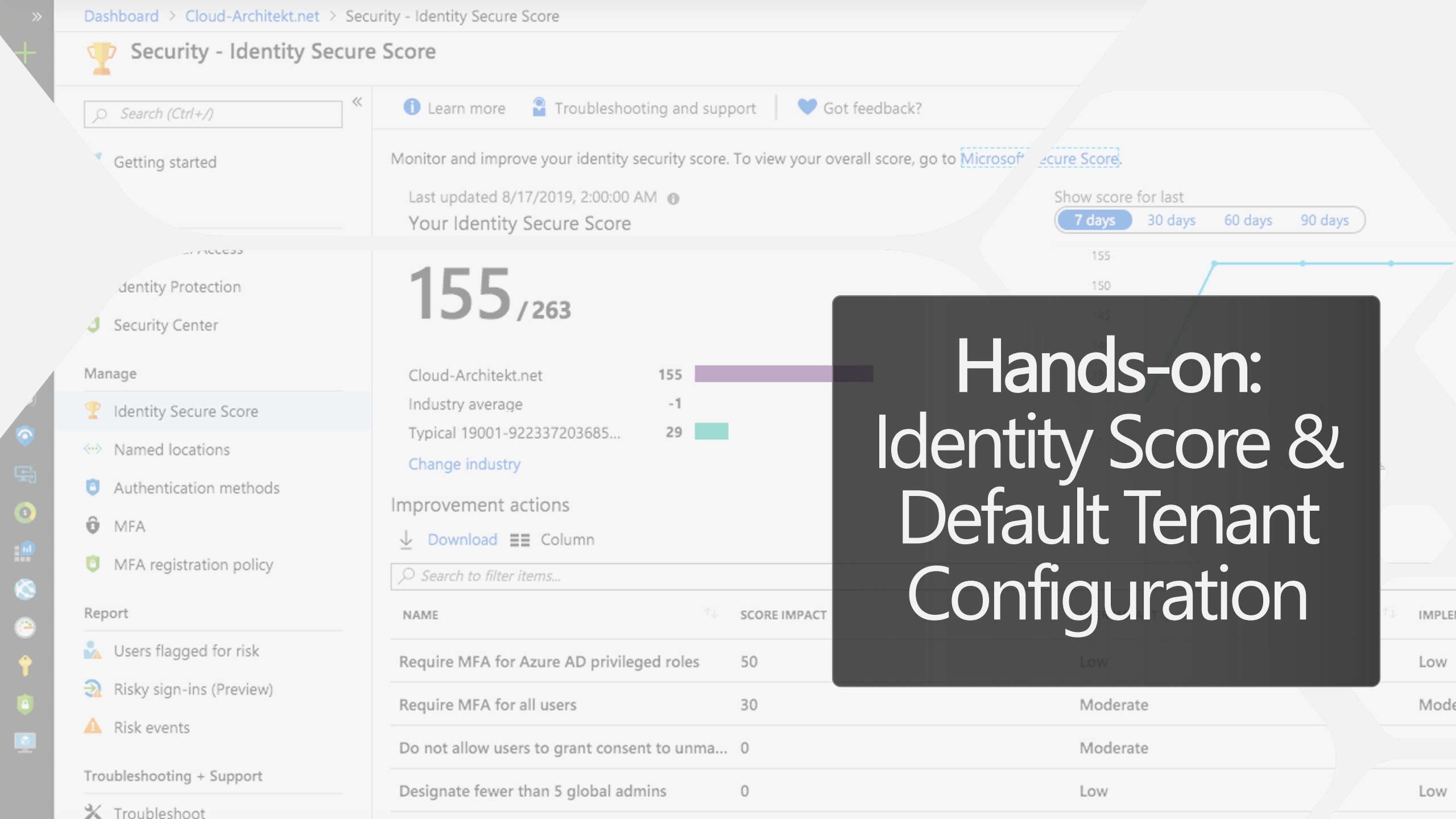
(Azure)
Azure Active Directory

- Tenant
- Graph API (REST-APIs)
- SAML, WS*, OAuth, OIDC
- Domain Join, Device Registered
- - (MDM/Intune Device policies)
- Flat (excl. Administrative Units)
- Cloud-Services/Web-Focused
- User-Driven (Self Services)

Azure Active Directory

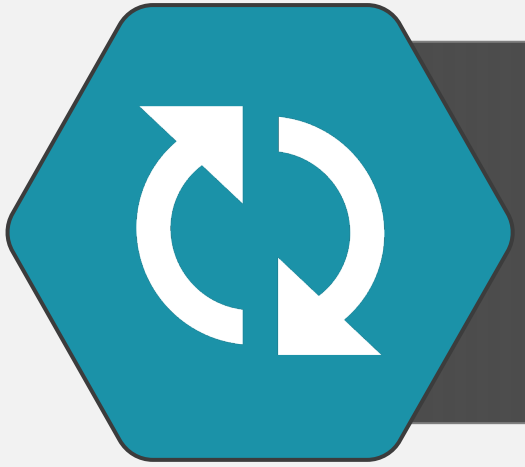
One tenant to rule them all…?

- Tenant isolation (security boundary)
  - Staging environments, (geopolitical/multi-geo) region or B2C (local) accounts
  - Granulator control over admin permissions → Administrative Units, Custom Roles (In Preview)
  - Default user permissions
- Tenant friending / Connected organizations
- Supported topologies for synchronization (multi-forest-support)


Dashboard > Cloud-Architekt.net > Security - Identity Secure Score
Security - Identity Secure Score
Search (Ctrl+/)
Getting started
Identity Protection
Security Center
Manage
Identity Secure Score
Named locations
Authentication methods
MFA
MFA registration policy
Report
Users flagged for risk
Risky sign-ins (Preview)
Risk events
Troubleshooting + Support
Troubleshoot
Learn more
Troubleshooting and support
Got feedback?
Monitor and improve your identity security score. To view your overall score, go to Microsoft Secure Score.
Last updated 8/17/2019, 2:00:00 AM
Your Identity Secure Score
155/263
Show score for last
7 days
30 days
60 days
90 days
155
150
Cloud-Architekt.net 155
Industry average -1
Typical 19001-922337203685... 29
Change industry
Improvement actions
Download
Column
Search to filter items...
NAME
SCORE IMPACT
IMPLE
Require MFA for Azure AD privileged roles 50 Low Low
Require MFA for all users 30 Moderate Mode
Do not allow users to grant consent to unma... 0 Moderate
Designate fewer than 5 global admins 0 Low Low
Hands-on:
Identity Score &
Default Tenant
Configuration

Azure AD Tenant
Checklist

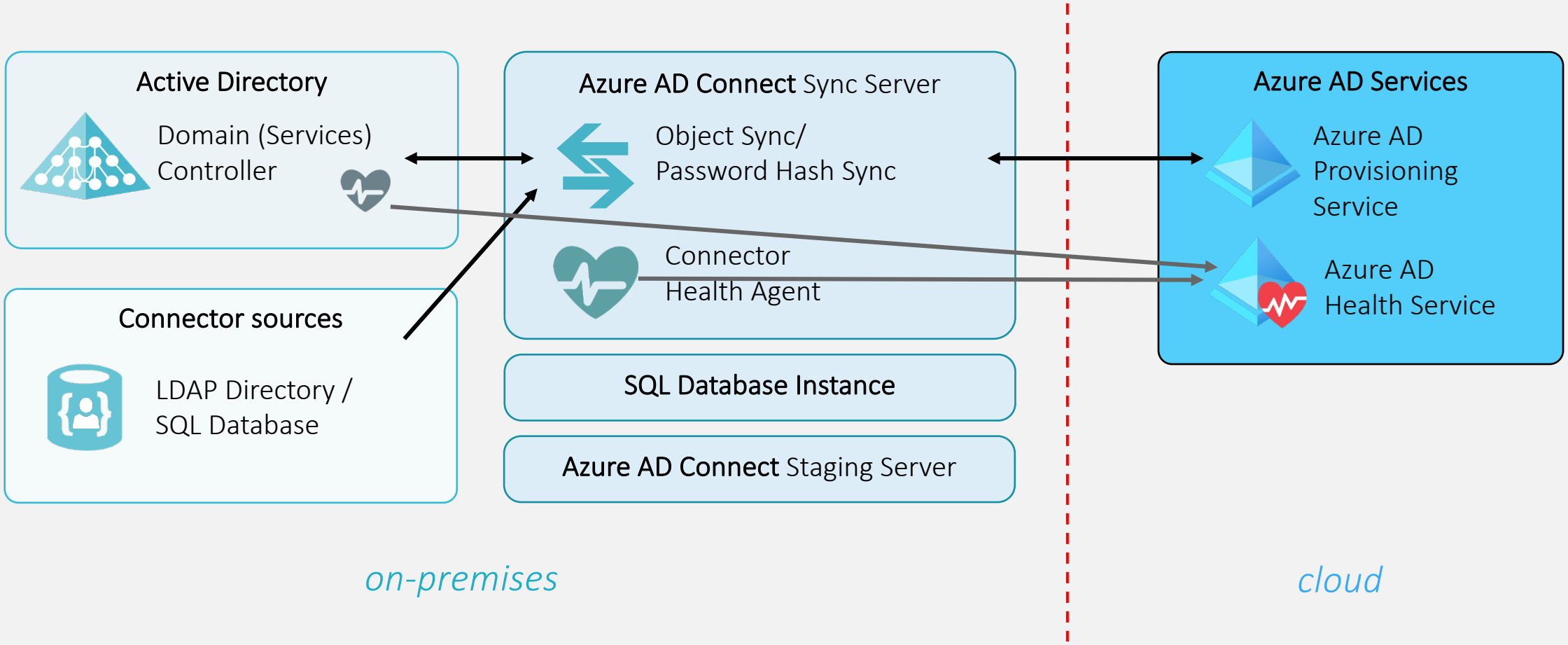
- ✓ *Regular review of (changed) default or new (feature) settings*
- ✓ *Monitor your identity score, usage and insights reports*
- ✓ *Prevent elevated access to manage all Azure ressources as „Global Admin“*
- ✓ *Check technical contact and notification mail address*
- ✓ CSP customers: Verify delegated admin privileges to partners
- ✓ Planning and monitoring assignment of licenses and application/service principals
- ✓ Service Health alerts of Azure AD and MFA service



Hybrid Identity Synchronization

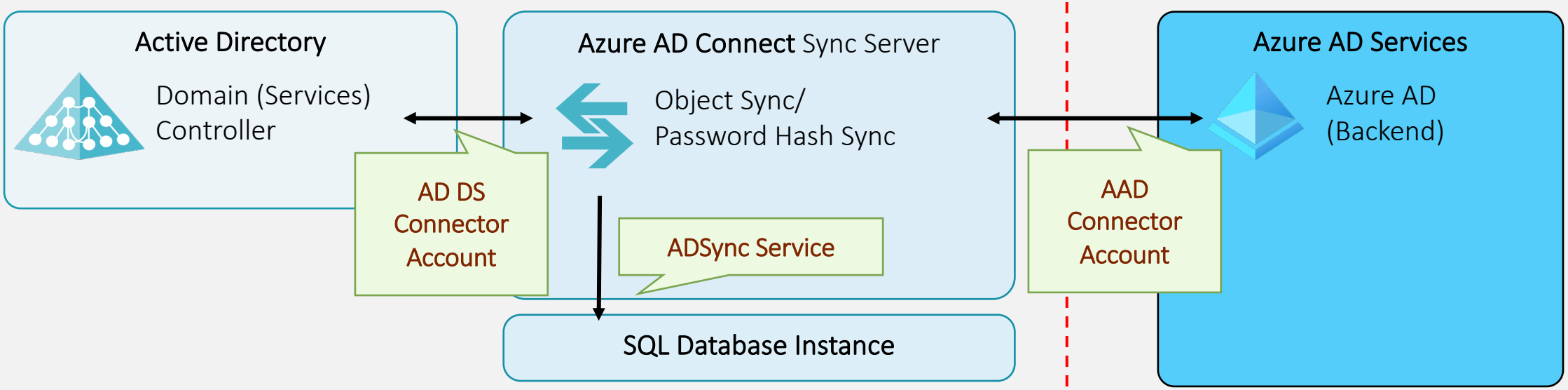
Azure AD Connect Synchronization

Architecture and components of „Identity bridge“



Azure AD Connect Synchronization

Hardening of Azure AD Connect



- Pre-created service accounts and delegated permissions (based on your user scope/filter and write-backs attributes)
  - ADSync service accounts as "(Group) Managed Service Account"
  - Security advisory for AD DS connect service account

Azure AD Connect Synchronization

Design decisions and prerequisites (before implementing)

- Review of the synced attributes, filtering and write-back options
  - IDFix to prepare and check directory objects and attributes

- Placement and protection of Azure AD connect, PTAs servers and databases
  - Hybrid identity components must be protected (similarly high as domain controllers)
  - Supported options for “High availability” of PTA and SQL cluster

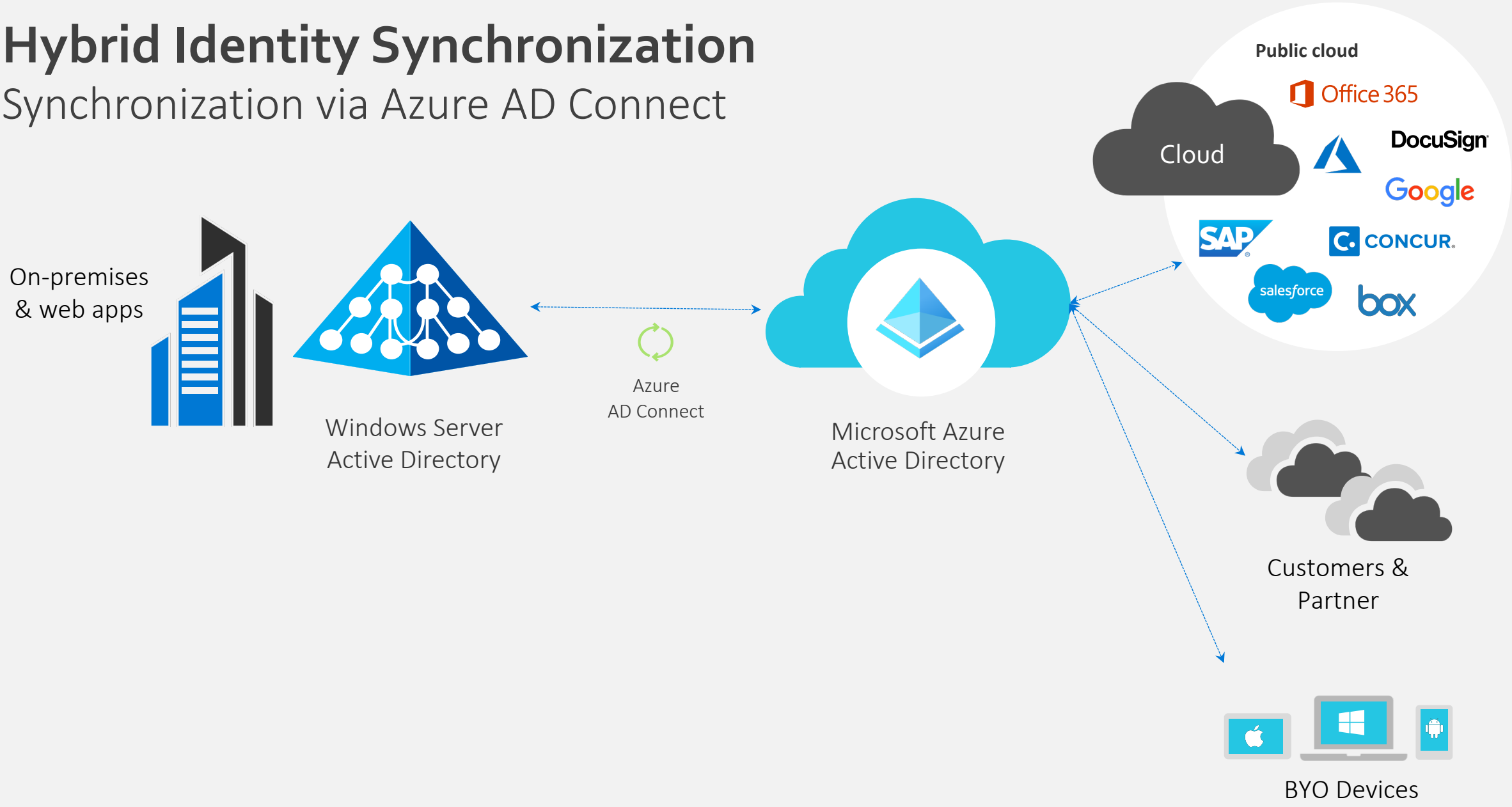
- Identity lifecycle and security use cases that needs to be validated
  - Example by PHS: Expired accounts, Force password reset (Public Preview)

Hybrid Identity Synchronization
Checklist

- ✓ *Least privilege and write-scope of AD DS Connector account*
- ✓ *Monitor your synchronization with Azure AD Connect Health*
- ✓ *Hardening of your hybrid identity components AND database*
- ✓ Exclude „On-Premises Directory Sync Service Accounts“ from CA Policies
- ✓ Consideration for changing default configuration
- ✓ Tip: Use „Azure AD Connect Config Documenter“ (compare configuration)

Hybrid Identity Synchronization

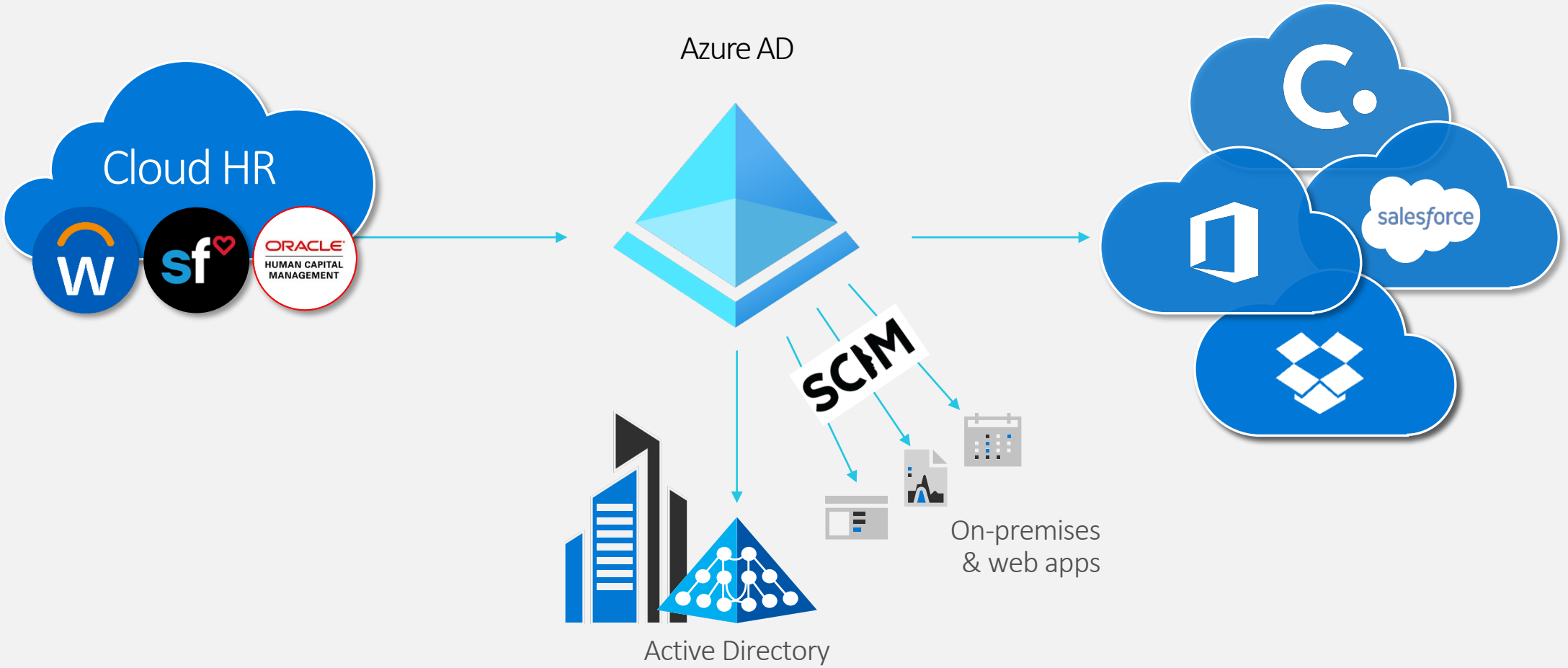
Synchronization via Azure AD Connect



Source: Microsoft (Ignite BRK2126 „Detect, investigate, and respond to identity-based threats in your environment with Azure ATP “)

Hybrid Identity Synchronization

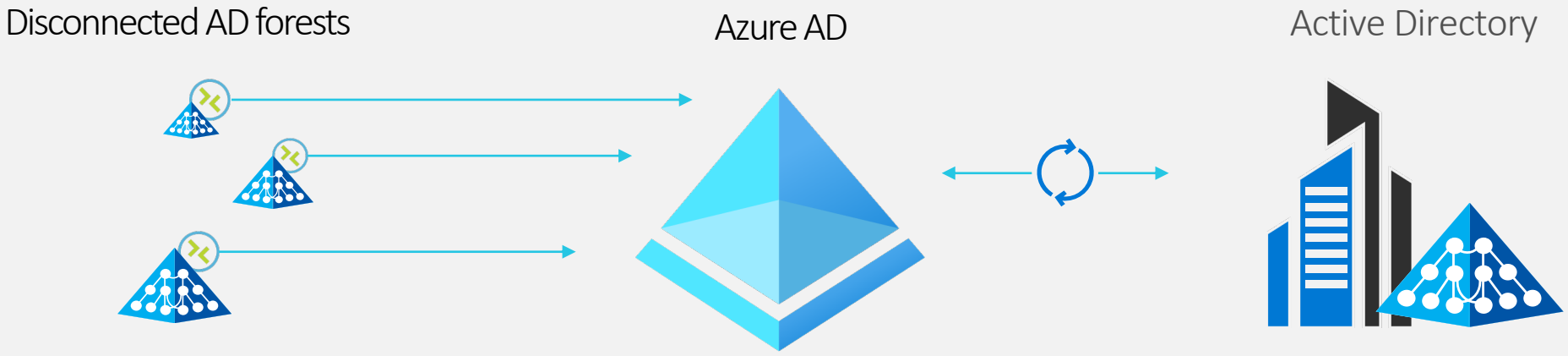
Synchronization via Cloud HR user provisioning (announced)



Source: Microsoft (Ignite BRK2130 „Azure Active Directory: New features and roadmap“)

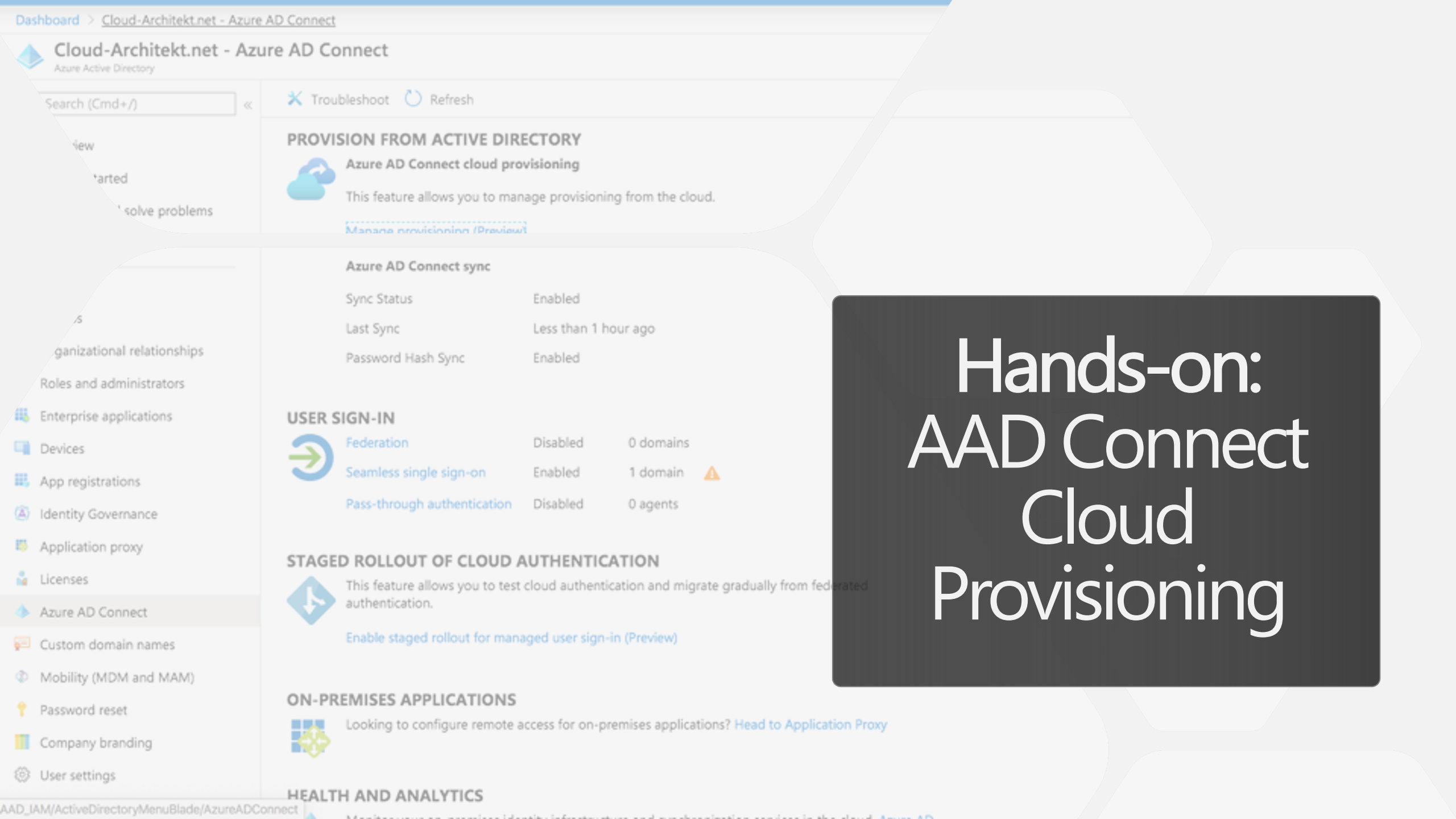
Hybrid Identity Synchronization

Synchronization via Cloud provisioning (in preview)

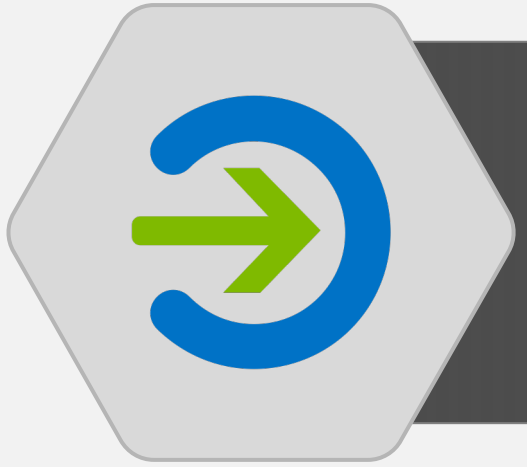


- Easy and lightweight solution
  - Super small on-prem footprint, Configure and manage in the cloud
  - 2-minute sync cycles and active, multiple active agents
  - Support for disconnected forests
- Feature Comparision to Azure AD Connect Sync Service

Source: Microsoft (Ignite BRK2130 „Azure Active Directory: New features and roadmap“)



Hands-on: AAD Connect Cloud Provisioning



Hybrid Identity Authentication

Hybrid Identity Authentication

How to choose the right model?

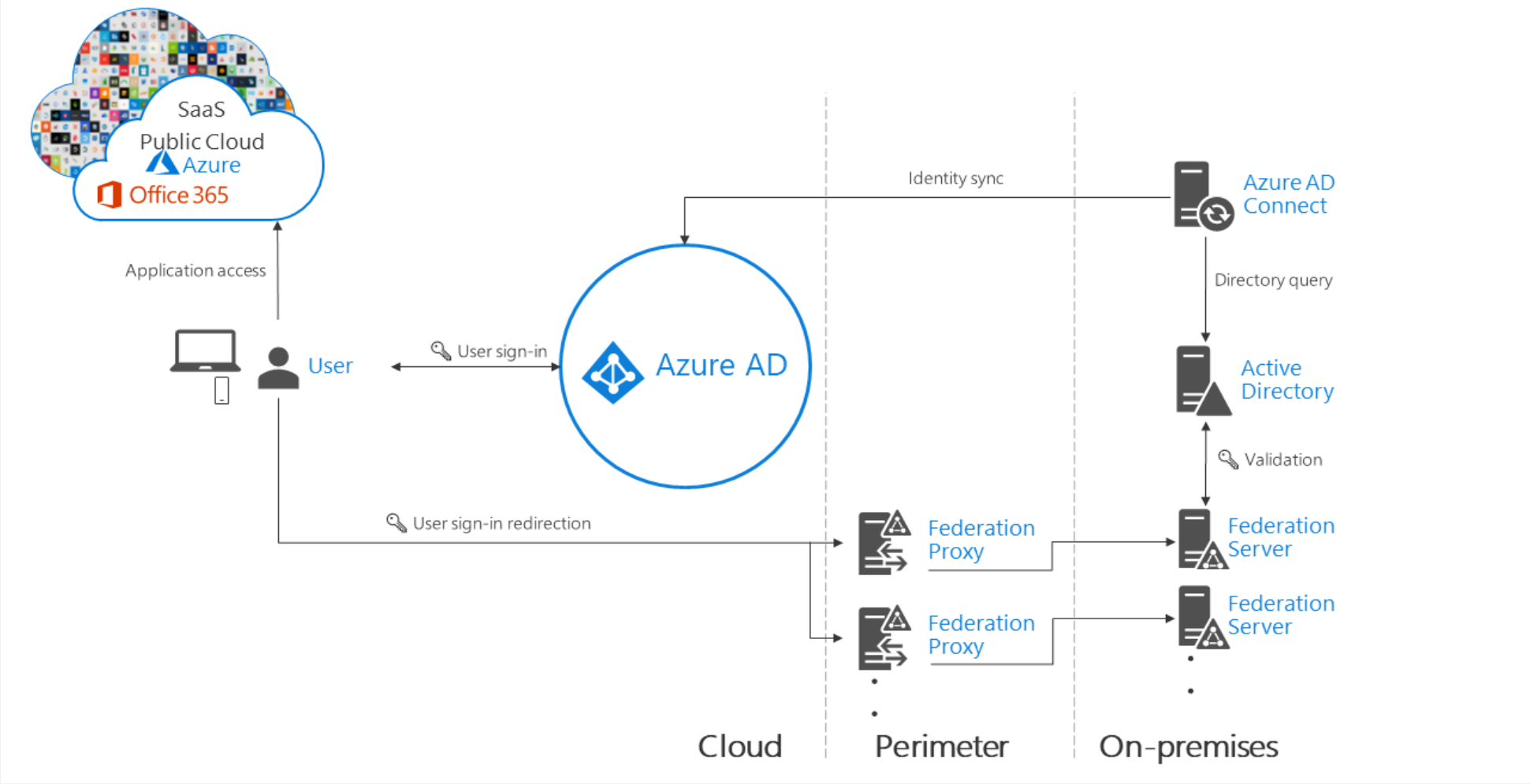
- Decision tree and detailed considerations by Microsoft
- Define **your** (identity) strategy and level of transformation
  - Collect business, security and technical requirements and discuss considerations

- **Cloud vs. Federated/On-Prem Authentication?**
  - Defense of brute force and password spray?
  - Certificate management (Golden SAML)?
  - Hardening of perimeter-network components?
  - Enforcing local (AD) security policies?

- Disaster recovery / SLA (on-premises dependency)?
- Security concerns of password (hashes) in the cloud?
- Identity protection features (leaked credentials)?

Hybrid Identity Authentication

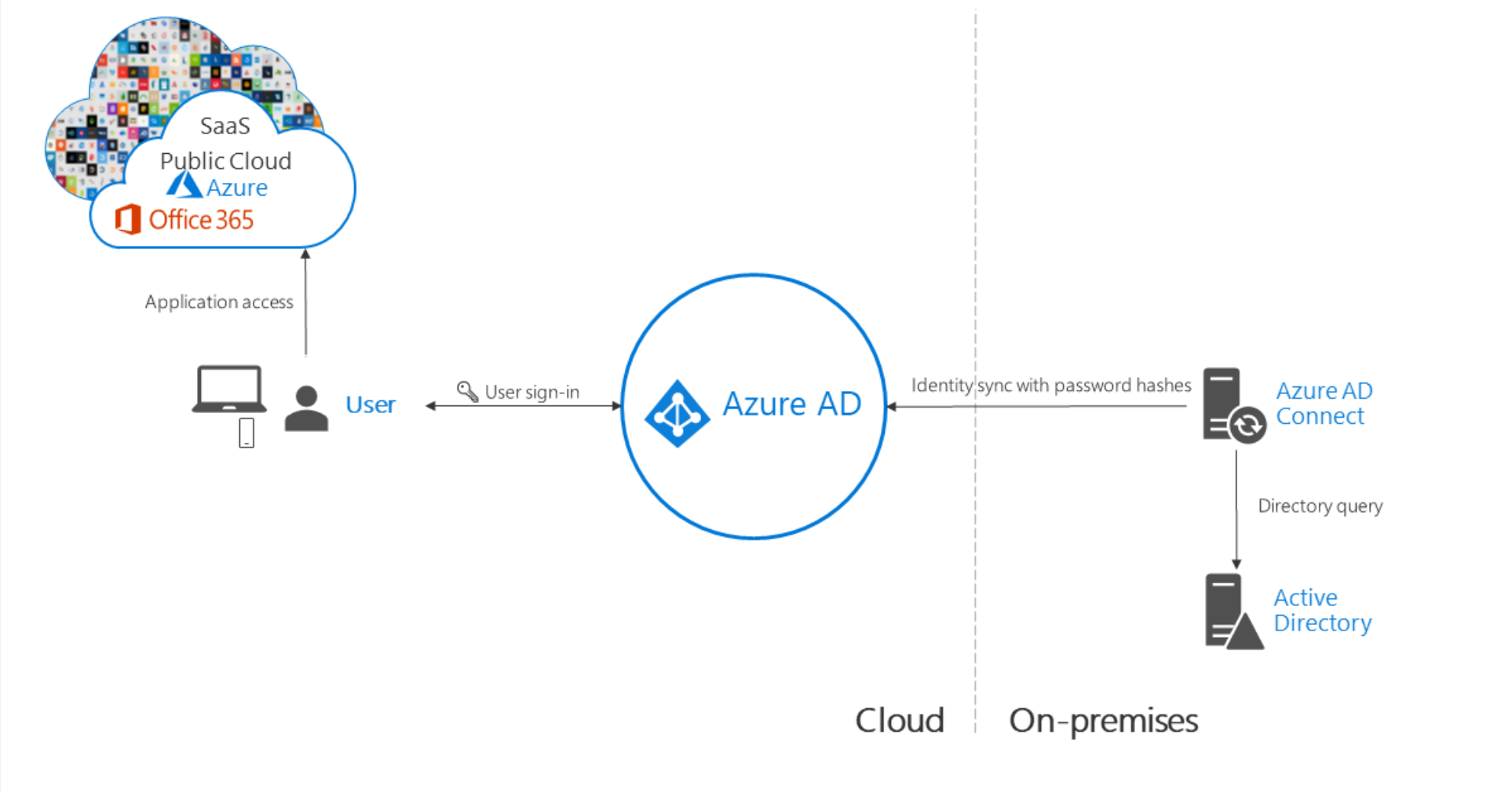
Hybrid Authentication with Federation Services (AD FS)



Source: https://docs.microsoft.com/en-us/azure/security/azure-ad-choose-authn

Hybrid Identity Authentication

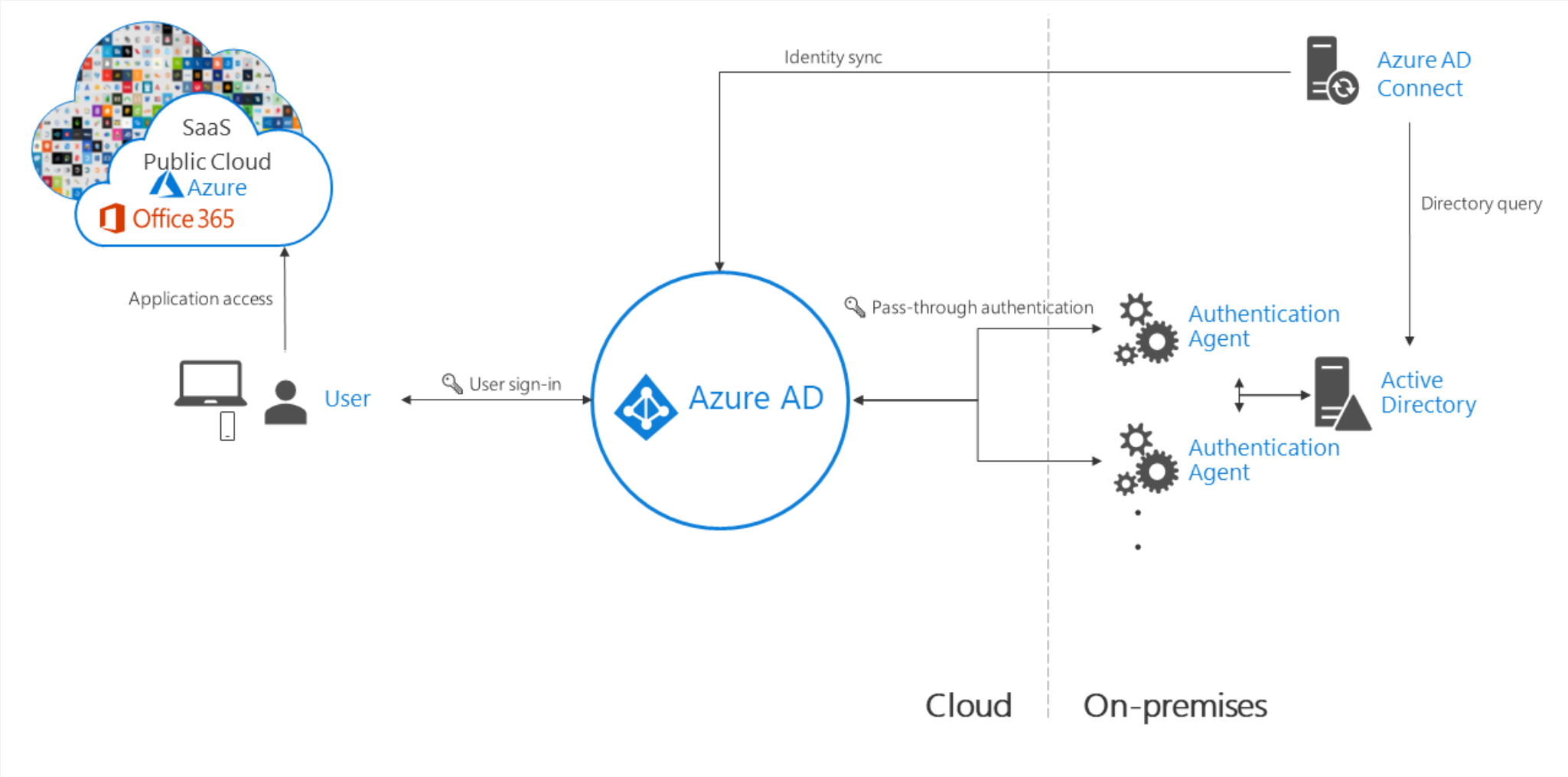
Hybrid Authentication with Password hash sync (PHS)



Source: https://docs.microsoft.com/en-us/azure/security/azure-ad-choose-authn

Hybrid Identity Authentication

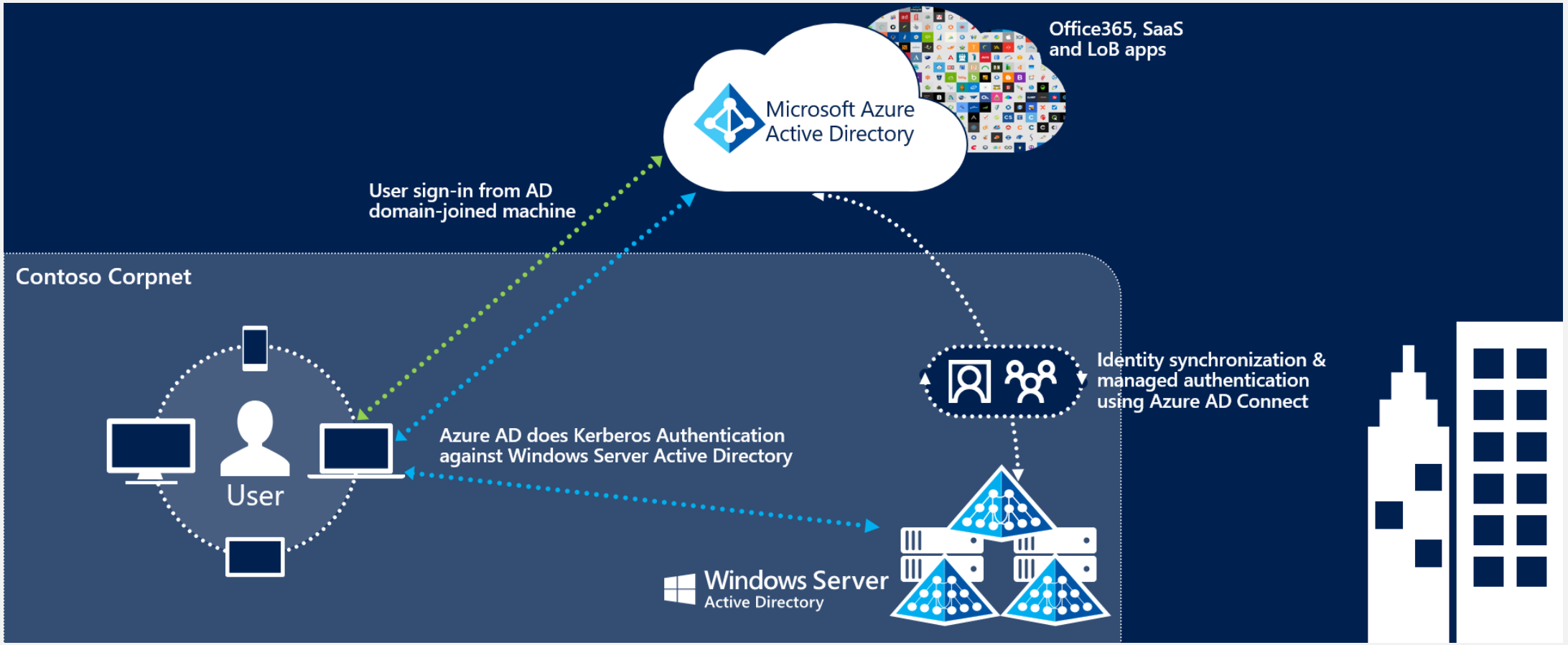
Hybrid Authentication with Pass-trough Authentication (PTA)



Source: https://docs.microsoft.com/en-us/azure/security/azure-ad-choose-authn

Hybrid Identity Authentication

Hybrid Authentication and Seamless Single-Sign On (sSSO)



Source: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso

Hybrid Identity Authentication

Weakness of Seamless SSO (sSSO)

- Kerberos (Silver Ticket) Attacks to AZUREADSSOACCT

- Limitation of sSSO Kerberos Encryption types in the past:
  - *Support of AES256_HMAC_SHA1 in latest versions (October 2019), before RC4_HMAC_MD5 encryption type was only supported*
    Source: https://feedback.azure.com/forums/169401-azure-active-directory/suggestions/36121711-add-support-for-kerberos-aes-and-drop-rc4-hmac-md5

- Known issues and manual Roll over Kerberos decyrption key

- Alternative solution: Windows Hello for Business (Hybrid)
  - Azure AD-joined device + Synchronized „msDS-KeyCredentialLink“ via AAD Connect = Azure AD (PRT) and AD (TGT) → Credential Guard!

Hybrid Identity Authentication
Checklist

- ✓ *Use cloud authentication / password hash synchronization*
- ✓ *Implement of „Windows Hello for Business“ (Hybrid) for employees*
- ✓ Enable all users to register MFA (Fallback WHfB) and SSPR information
- ✓ Revocation behaviour of Password-based and Non-password-based token

Hybrid Identity Protection

Hybrid Identity Protection

Design your Identity Protection and Conditional Access Strategy

Conditions

- User Attributes (Group Member)
- Location (IP Range)
- Platform Type (Windows, iOS,..)
- Type of client (Web, Mobile,...)

All Users & Apps

Policy and Controls: Risk-based & Conditional Access Policy

High **risk user** must change passwords

Password Change

Block clients with legacy authentication

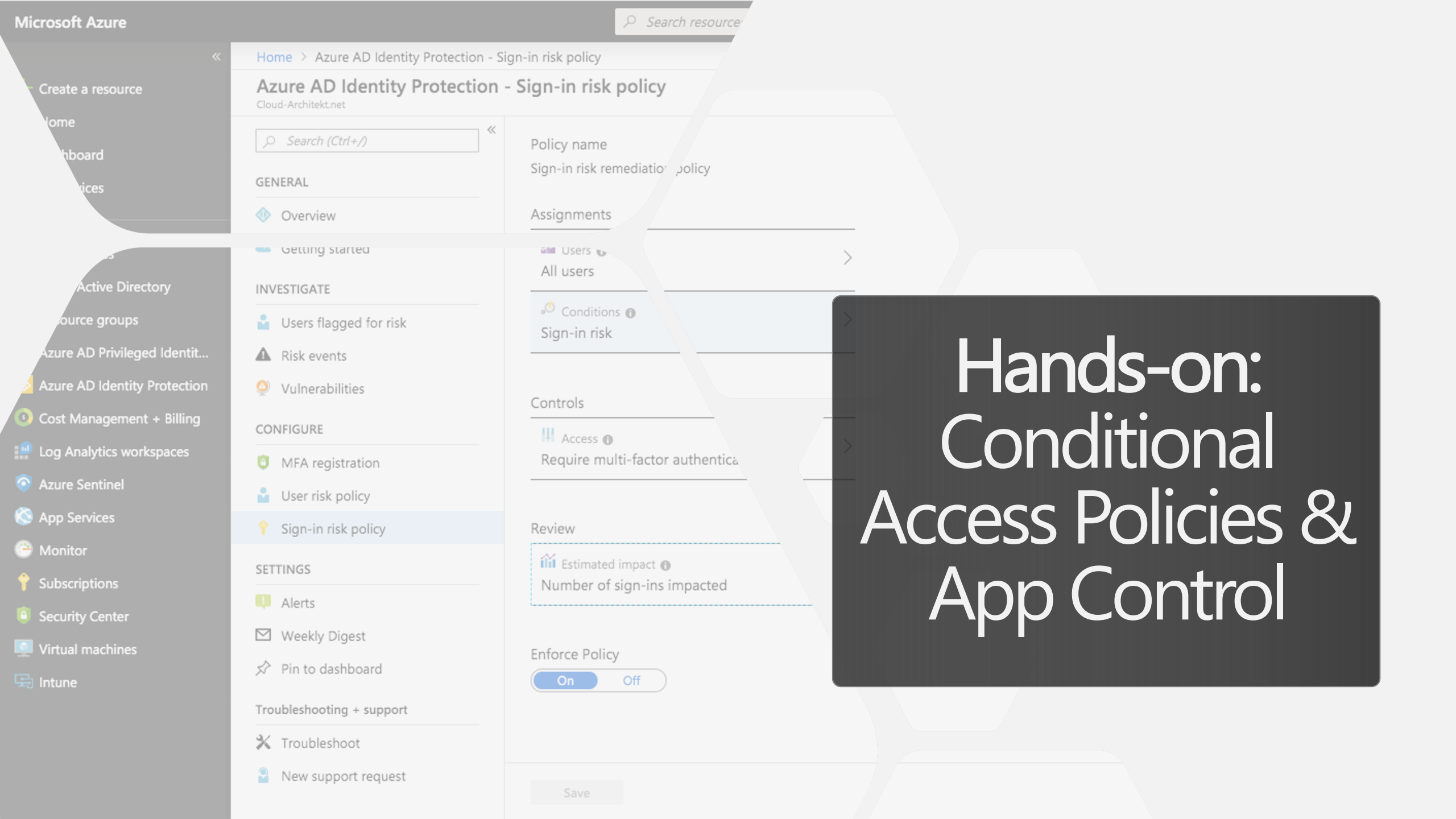
Block unsupported (e.g. ChromeOS) and forbidden platform types

Block

Require **registered/compliant device** or approved apps (Intune MAM)

Require MFA when sign-in risk is medium or high

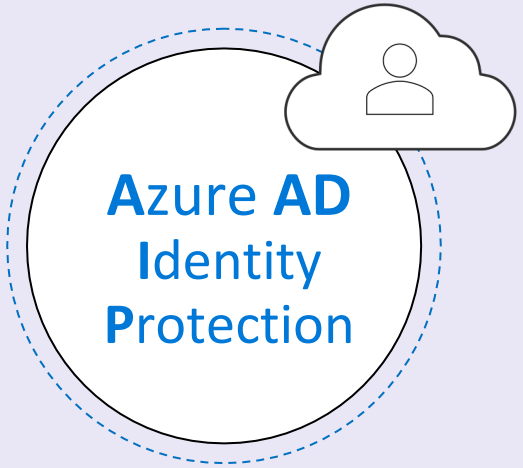
Allow



Hands-on: Conditional Access Policies & App Control

Hybrid Identity Protection

Investigation on cloud identity, on-premises and cloud apps



Risky sign-ins & User Risk

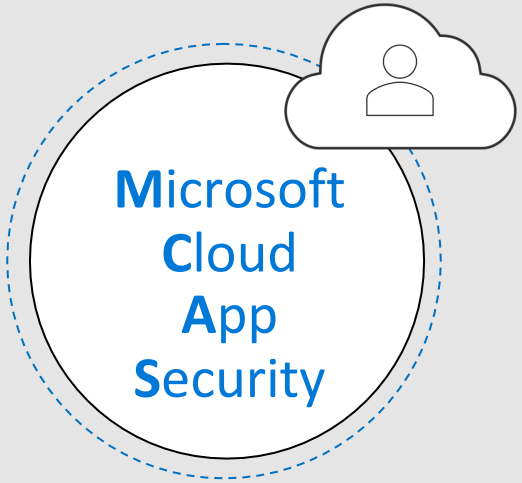
Sign-ins from unfamiliar locations/Leaked credentials

-

Identity behavior on-premises

Suspicious VPN connection/Kerberos Attacks

Data exfiltration over SMB



Behavior across cloud apps

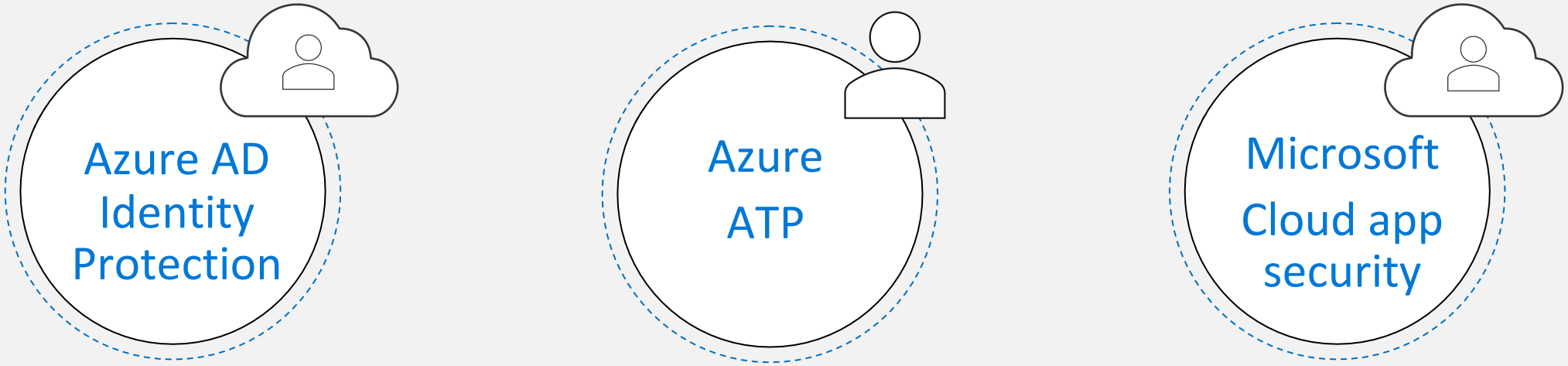
Activity from infrequent country

Data exfiltration to unsanctioned apps

Source: Microsoft Ignite Session BRK3117 (https://mediusproduction.blob.core.windows.net/presentations/Ignite2018/BRK3117.pptx)

Hybrid Identity Protection

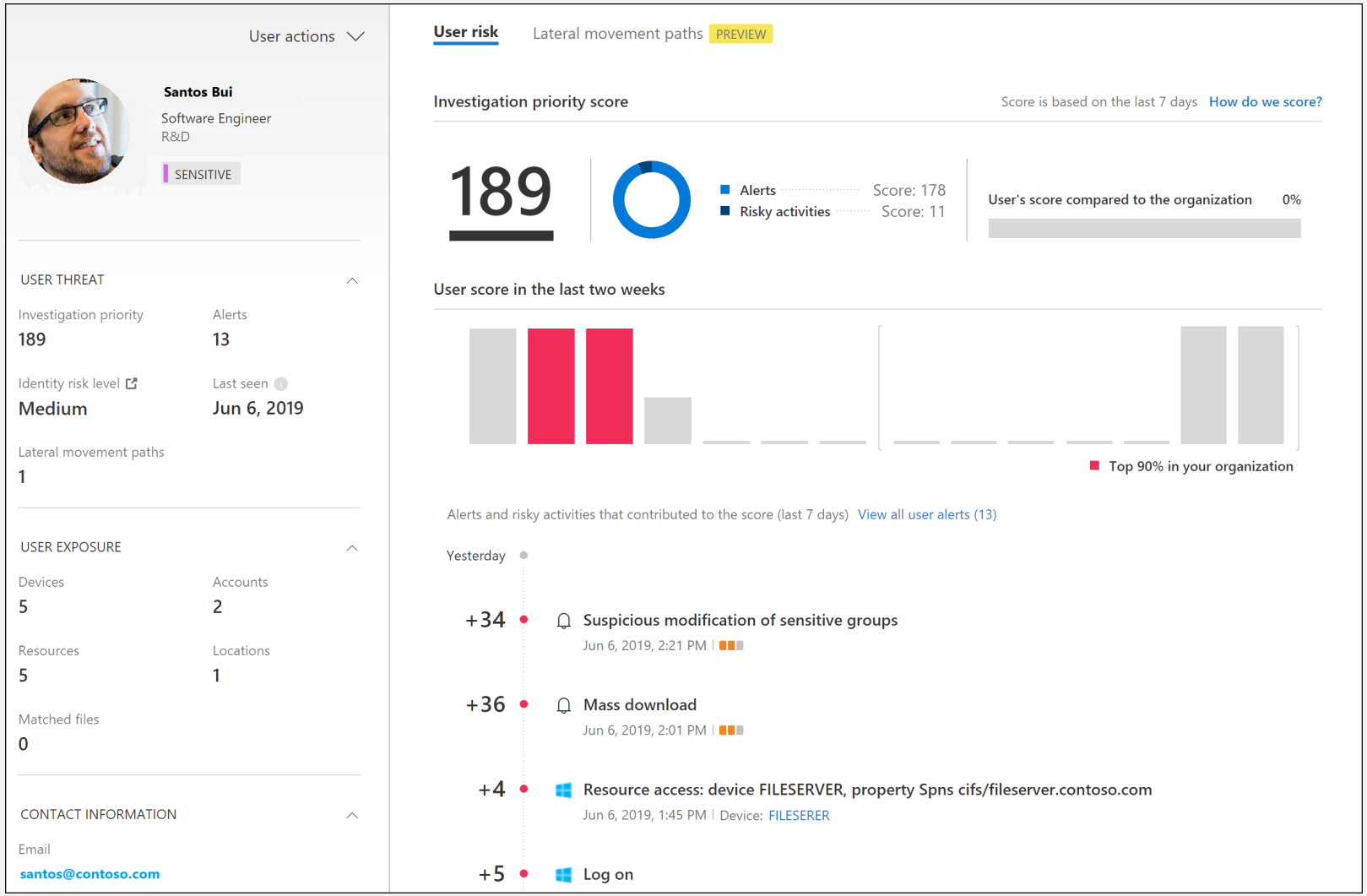
Unified SecOps Investigation of hybrid environments



Source: Microsoft Ignite Session BRK3117 (https://mediusproduction.blob.core.windows.net/presentations/Ignite2018/BRK3117.pptx)

Auditing and Monitoring of Azure Active Directory

Investigation Priority built on User and Entity Behavior Analytics



Source: https://docs.microsoft.com/en-us/cloud-app-security/tutorial-ueba

Advanced protection of identities and access
Smart Lockout

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

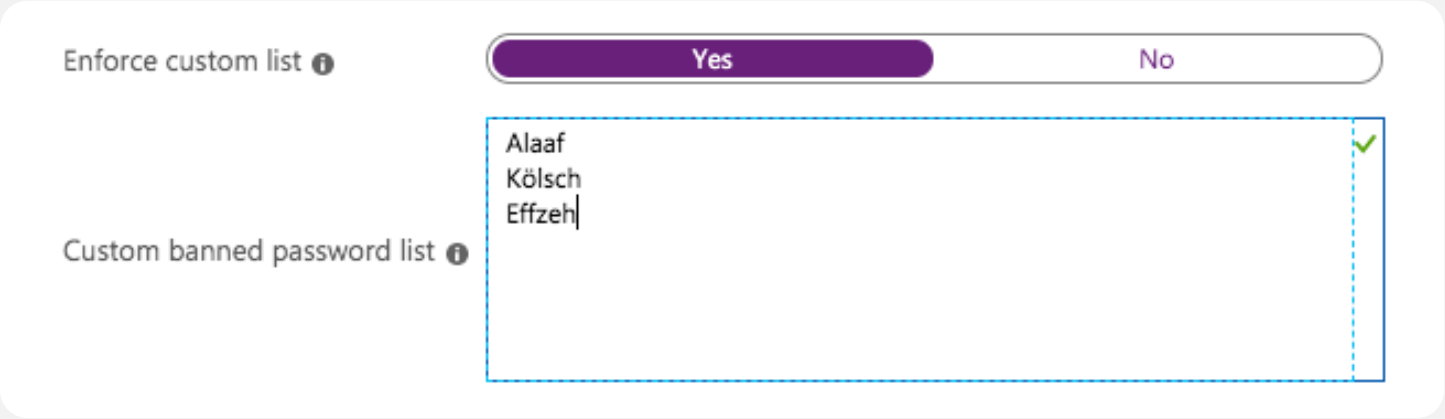
- AAD data center/regions tracks **lockout independently**
- **Consideration** in hybrid environments **with PTA**:
  - **Lockout threshold** in Azure AD should be **less than in AD**
  - **Lockout duration** should be set **longer than AD reset**

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

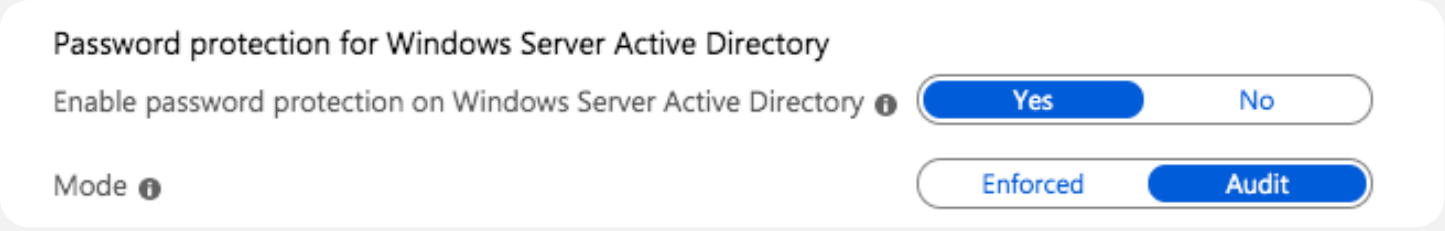
Advanced protection of identities and access

Password Protection

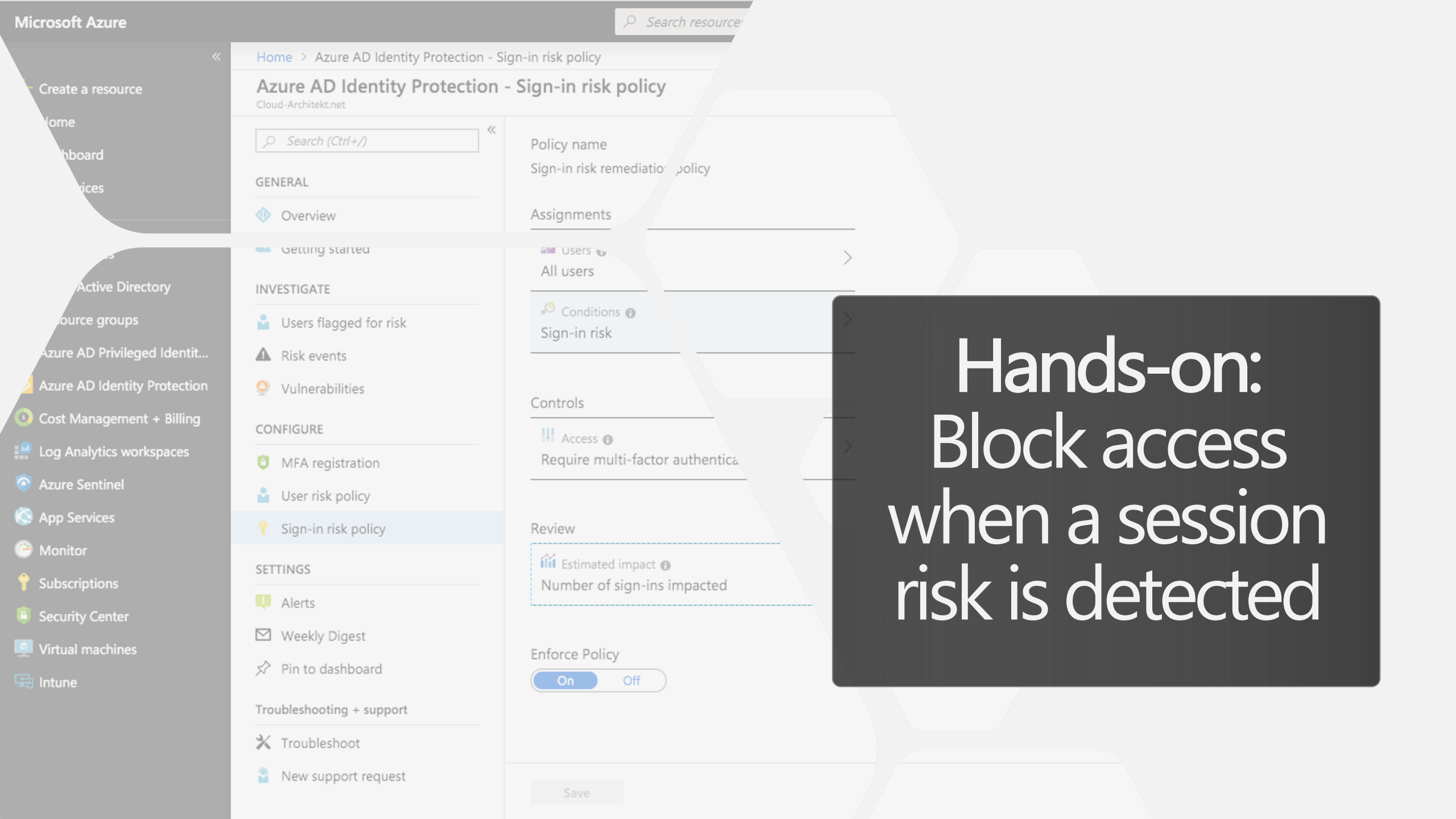
- **Reset or change password checks** current version of „global **banned password list**“
- Based on **known bad patterns** (passw0rds and k3ywords)
- **Custom** banned password **list** (max. 1000 terms and 16 characters)



- On-premises integration with “**Azure AD Password Protection**“ (including monitoring)



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



Hands-on: Block access when a session risk is detected

Hybrid Identity Protection
Checklist

✓ *Securing access with conditional access policies (strong baseline e.g. block legacy auth!)*

✓ *Protect and monitor your identities with Azure ATP, MCAS and Identity protection*

✓ *Strong passwords and authentication (Password Protection, MFA for everyone)*

✓ Case of disruption or lockout: Contingency CA policy
(as part of resilient access control management strategy)

✓ Exclude emergency accounts from every policy and
manage (temporary) exclusions with Azure AD access reviews

✓ Export and document your Conditional Access Policies via Graph API

Privileged Identity Management in Azure AD

Privileged Identity Management (PIM)

Foundation of securing privileged access

Separated privileged identities

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

Non-persistent 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

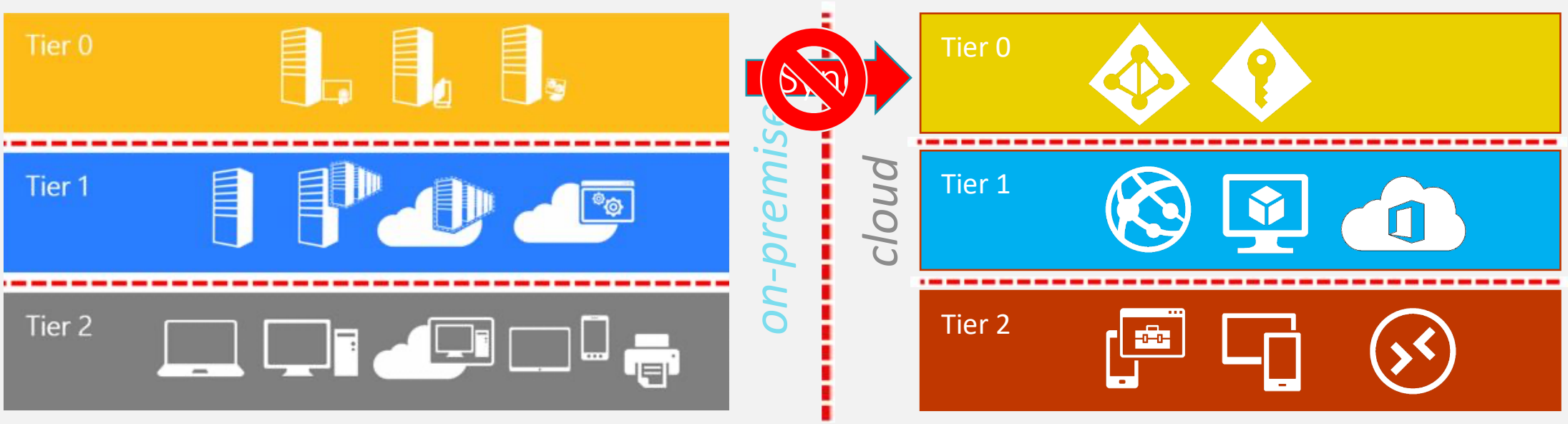
Source: https://www.microsoft.com/security/blog/2019/05/08/3-investments-improve-identity-management-microsoft/

Priviliged Identity Management (PIM)

Securing privileged access for hybrid and cloud deployments

Security isolation level of privileged identities

- Separate your work account and privileged account
- Do not sync on-premises accounts as cloud admins
- Tiering model of **E**nhanced **S**ecurity **A**dministrative **E**nvironment (ESAE)



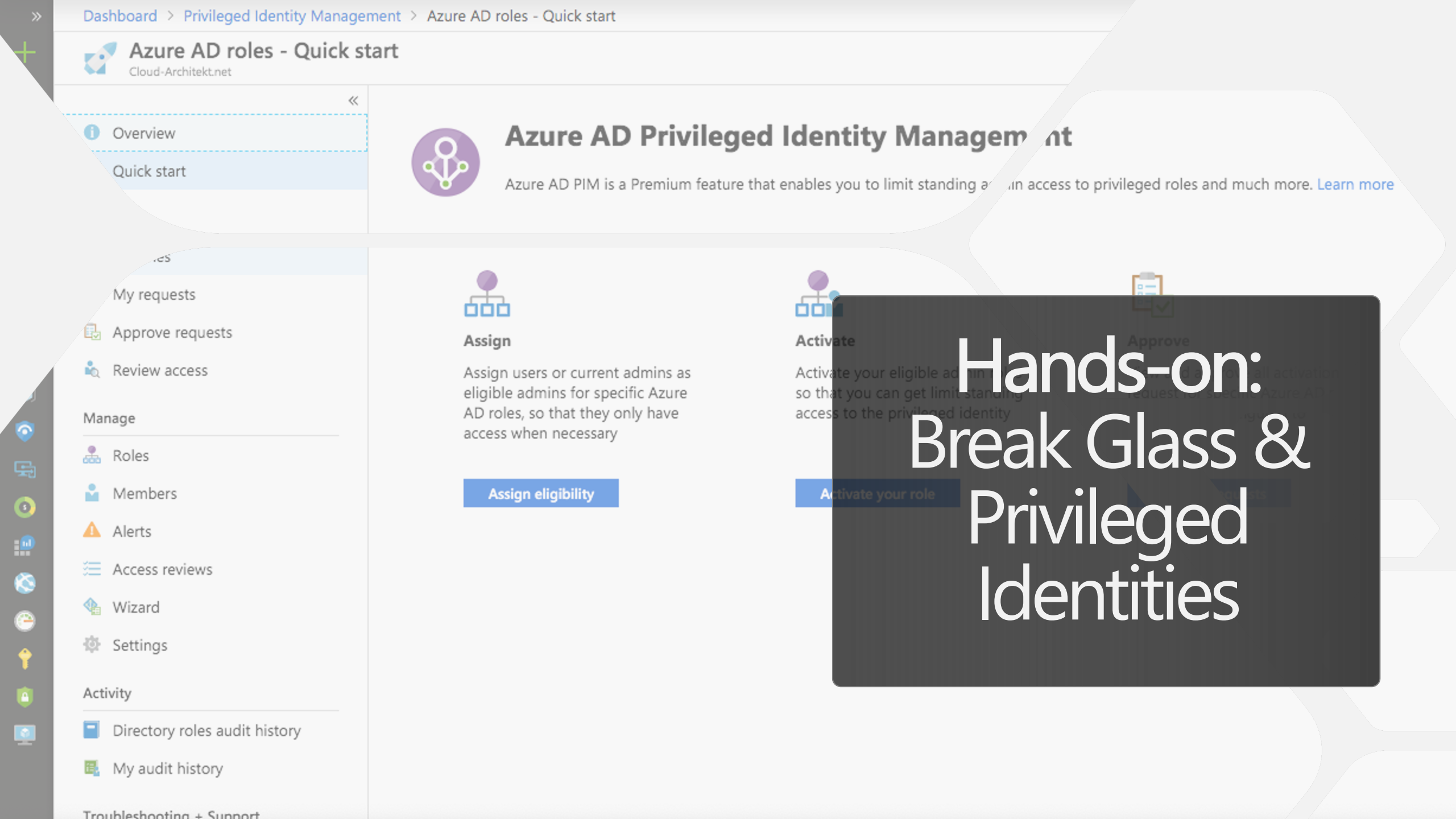
Source: https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

Priviliged Identity Management (PIM)

Design your Azure AD roles

Built-in Azure AD directory roles and limitations

- Azure AD Built-in Directory roles and least-privileged roles by task
- Custom directory roles → Available in public preview for “app registration”
- No support for security group assignment → “Under review” by AAD product group


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:
Break Glass &
Privileged
Identities

Priviliged Identity Management
Checklist

- ✓ *Built your Azure and Azure AD RBAC model with least privilege*
- ✓ *Azure AD PIM to reduce expose of privileged accounts*
  → *Microsoft IT showcase: Elevated access with tools and privileged credentials*
- ✓ *Require strong (or passwordless) authentication and compliant device for admins*
- ✓ *Manage two emergency accounts (alerting by sign-in attempts)*
- ✓ Access to Azure portals and shell from secured device only (Secure Admin Workstation)
- ✓ Prevent lateral movement (Local Admin Password Solution in Azure? SLAPS!)
- ✓ Regularly review of critical accounts and permissions (by Azure AD Access Review)

Thank You

@Thomas_Live

Thomas@Naunheim.net

www.cloud-architekt.net