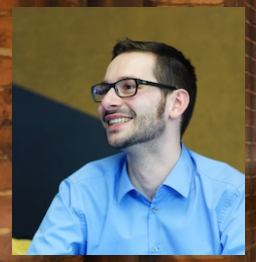
# Hybrid identity design and security considerations in Azure Active Directory



Thomas Naunheim

aOS Germany
1/12/2020

# THANKS TO OUR SPONSORS





# About Me

## Thomas Naunheim

Cloud Solutions Architect
Koblenz, Germany

@Thomas_Live

www.cloud-architekt.net

Microsoft® Most Valuable Professional

Azure Meetup BONN

# Azure Active Directory

## Microsoft Hybrid Identity

(Windows Server)
**AD Domain Services**

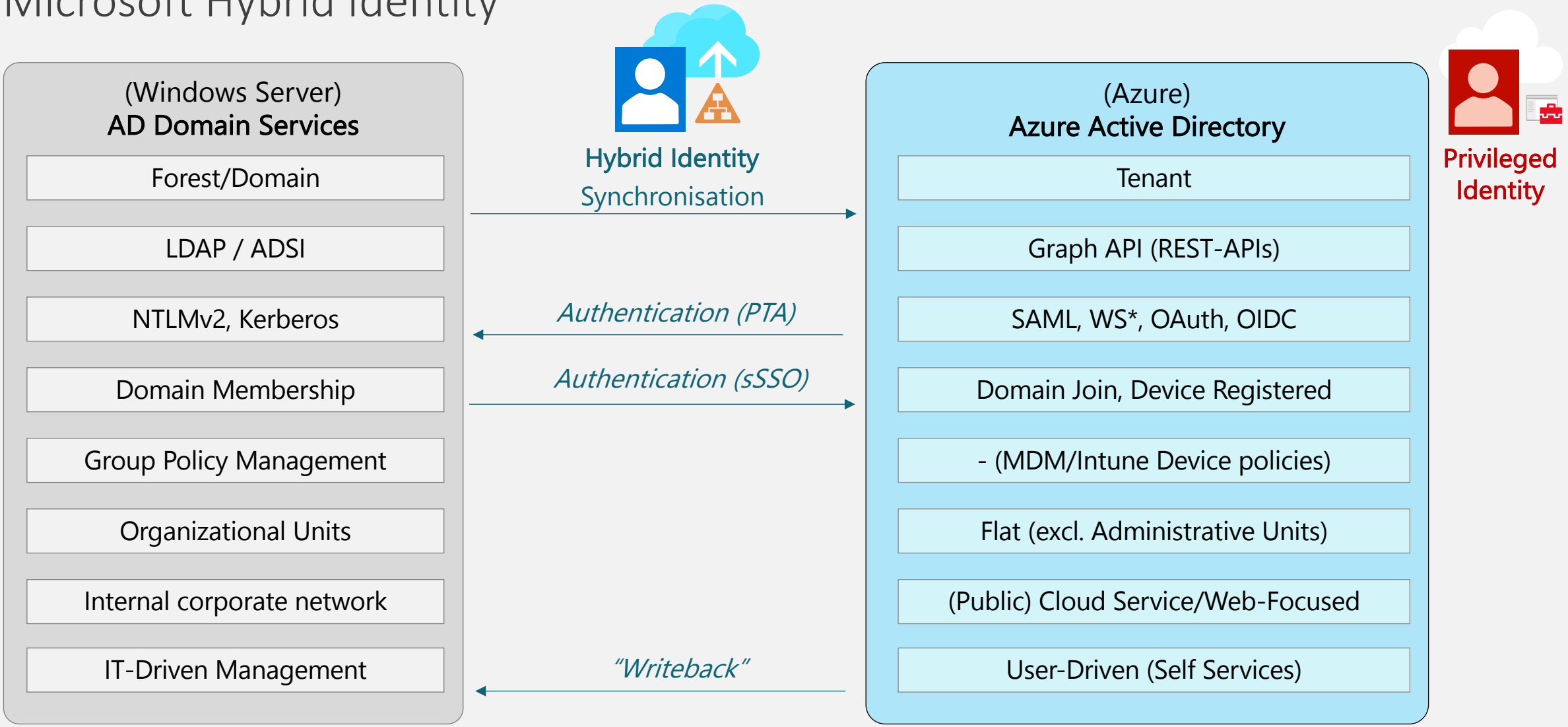
- Forest/Domain
- LDAP / ADSI
- NTLMv2, Kerberos
- Domain Membership
- Group Policy Management
- Organizational Units
- Internal corporate network
- IT-Driven Management

(Azure)
**Azure Active Directory**

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

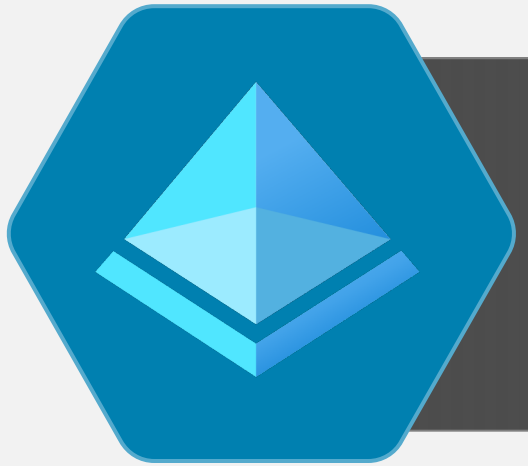
# Azure Active Directory

## Microsoft Hybrid Identity



# Agenda

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

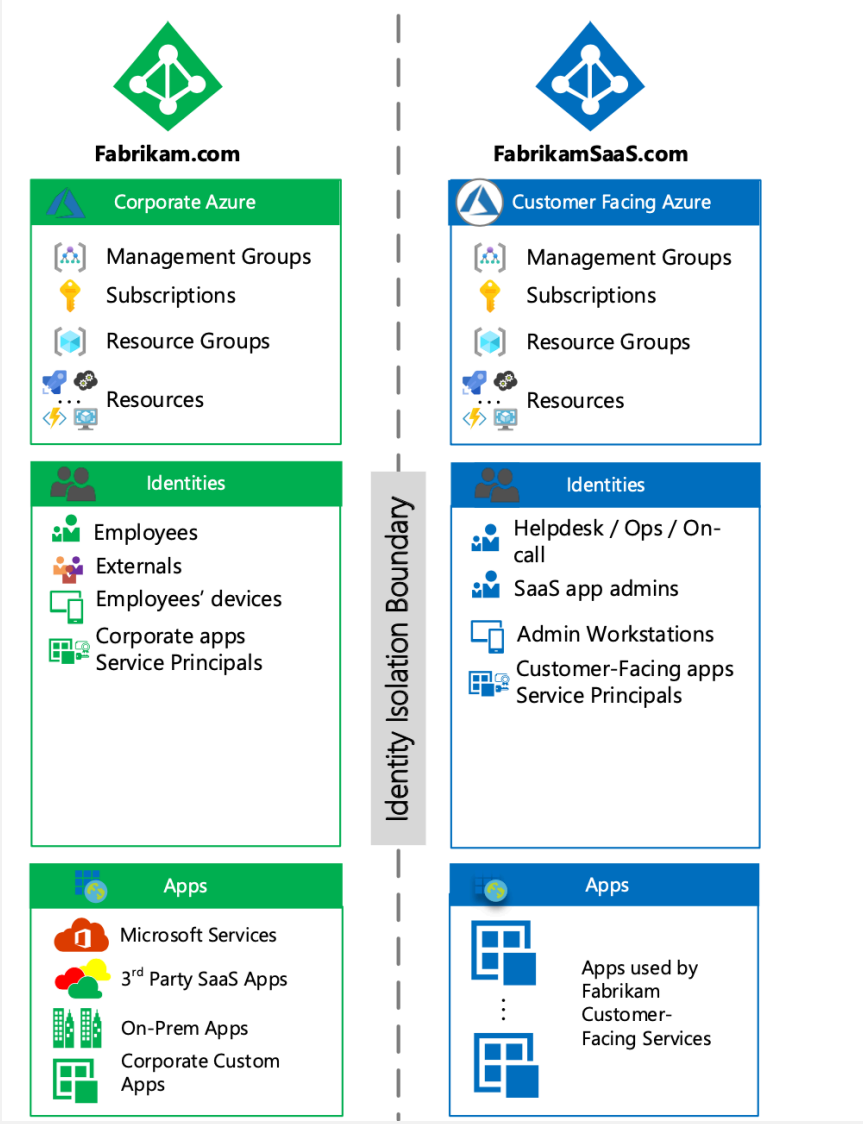


# Azure Active Directory
## Tenant

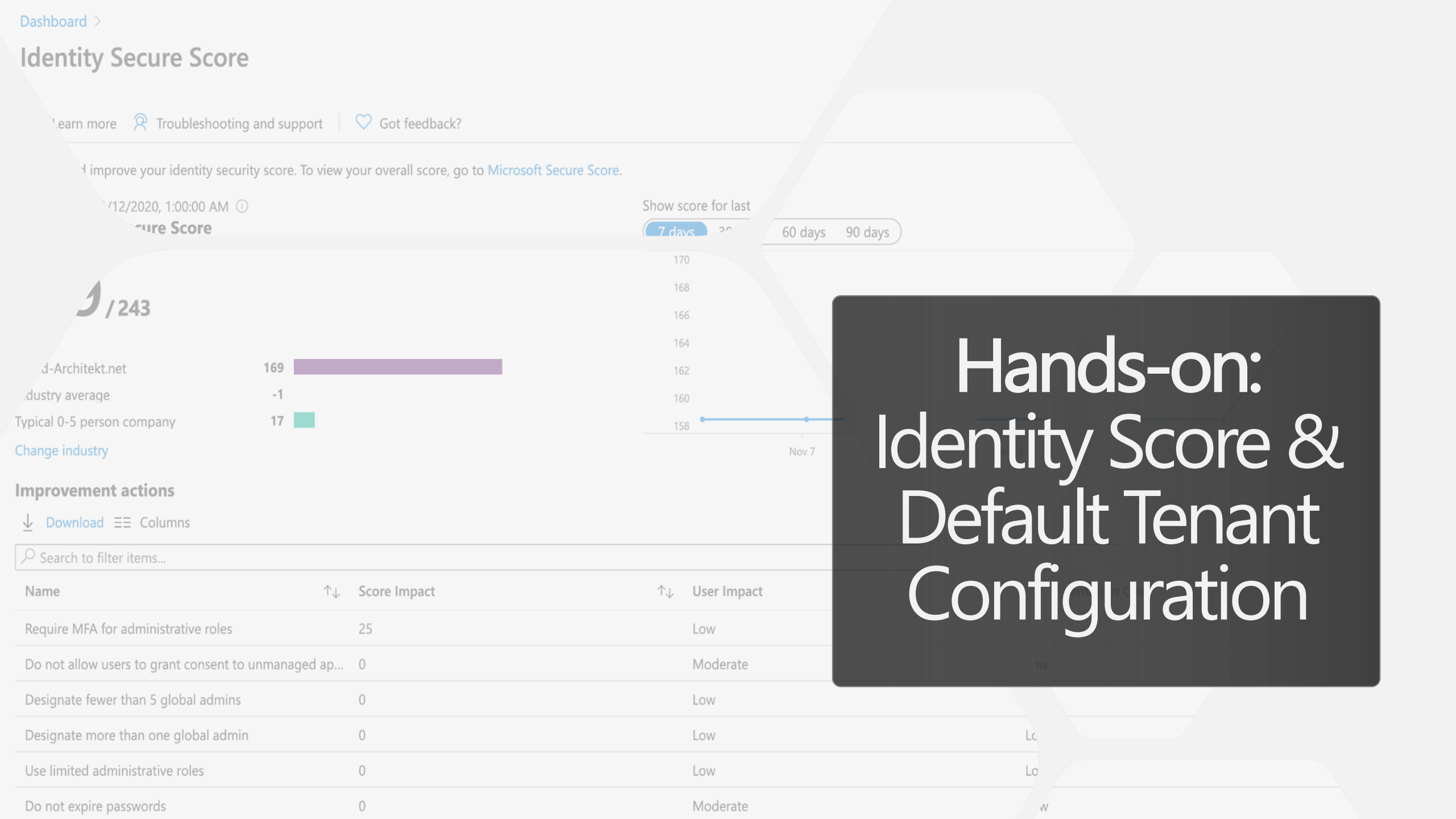
# Azure Active Directory

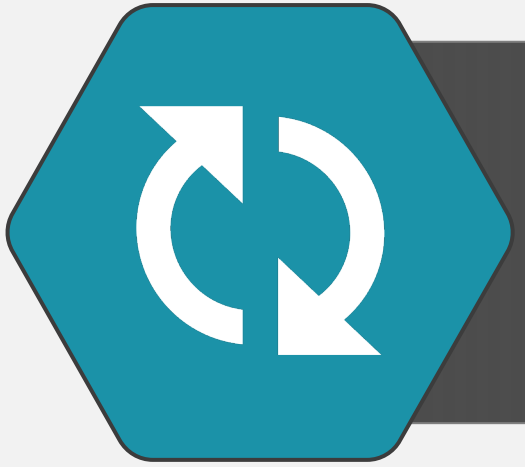
## One tenant to rule them all…?

- **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 (User Type and Scope)
- **Supported topologies for synchronization**
  - Single Forest to single Azure AD Tenant
  - Multiple Forest to single Azure AD Tenant (via single sync service only)




Source: Securing Azure environments with Azure Active Directory

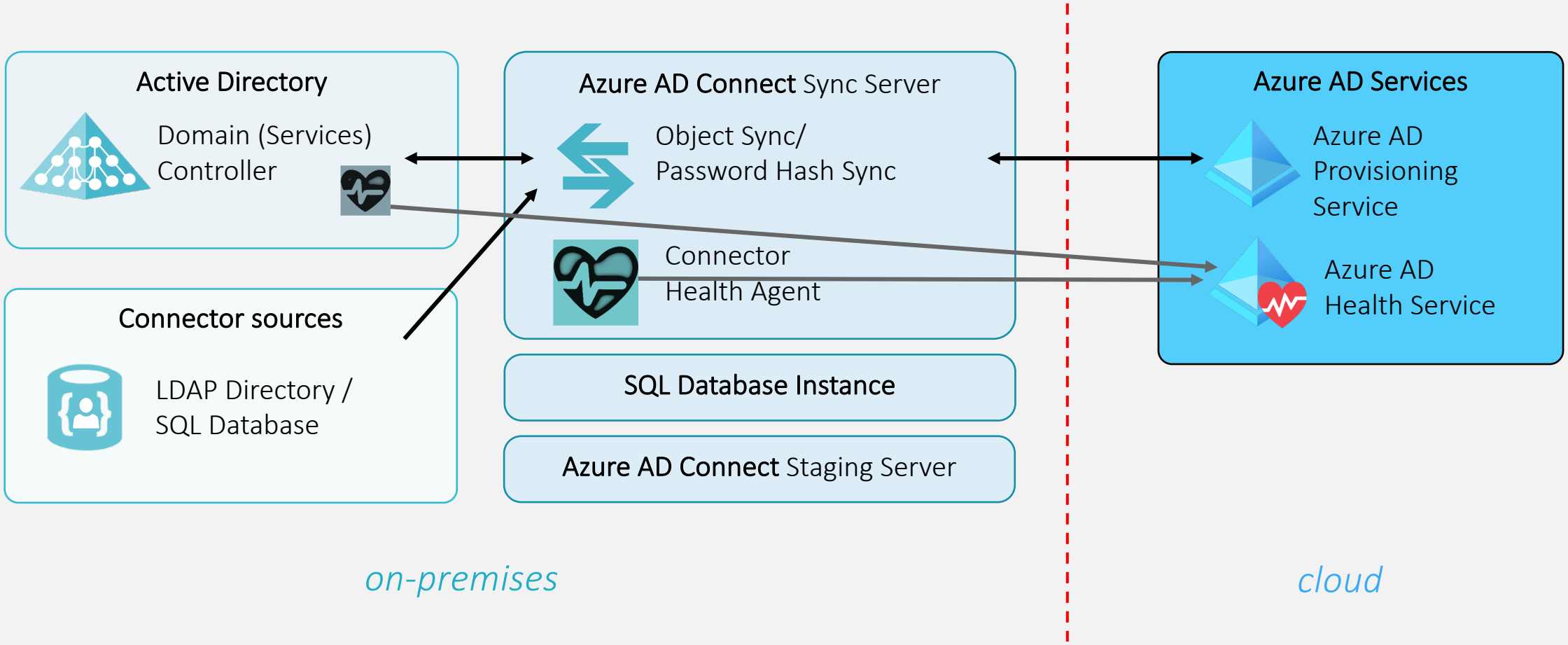

Dashboard
Identity Secure Score
Learn more
Troubleshooting and support
Got feedback?
improve your identity security score. To view your overall score, go to Microsoft Secure Score.
/12/2020, 1:00:00 AM
ure Score
Show score for last
7 days
60 days
90 days
/ 243
170
168
166
164
162
160
158
Nov 7
d-Architekt.net 169
dustry average -1
Typical 0-5 person company 17
Change industry
Improvement actions
Download
Columns
Search to filter items...
Name
Score Impact
User Impact
Require MFA for administrative roles 25 Low
Do not allow users to grant consent to unmanaged ap... 0 Moderate
Designate fewer than 5 global admins 0 Low
Designate more than one global admin 0 Low
Use limited administrative roles 0 Low
Do not expire passwords 0 Moderate
Hands-on:
Identity Score &
Default Tenant
Configuration



# Hybrid Identity Synchronization

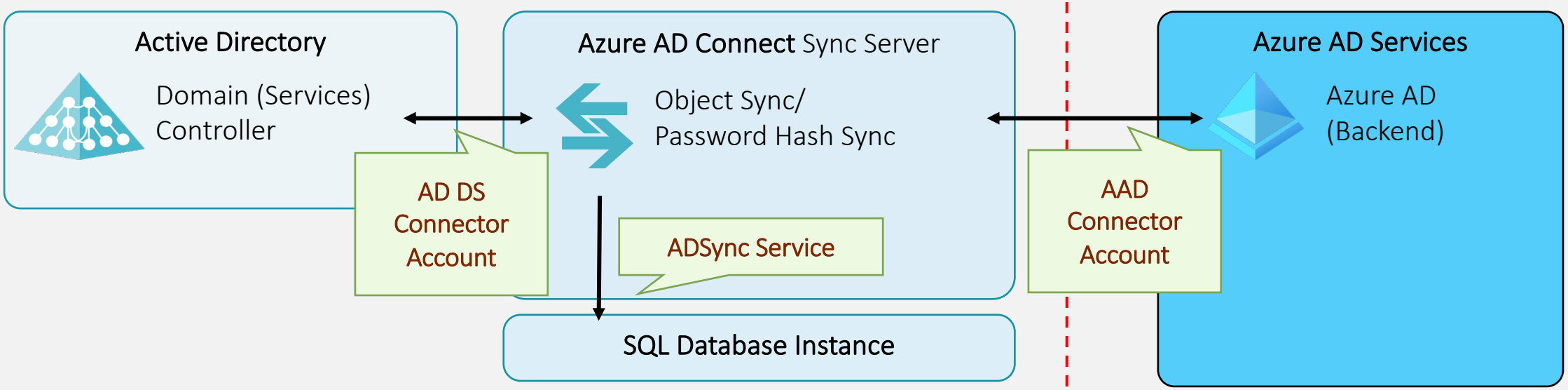
# Azure AD Connect Synchronization

## Architecture and components of „Identity bridge“



# Azure AD Connect Synchronization

## Hardening of Azure AD Connect




- Pre-created AD 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
- **AAD Connector Accounts** needs to be excluded from Conditional Access = Monitoring!

# Azure AD Connect Synchronization

## Design decisions and prerequisites (before implementing)

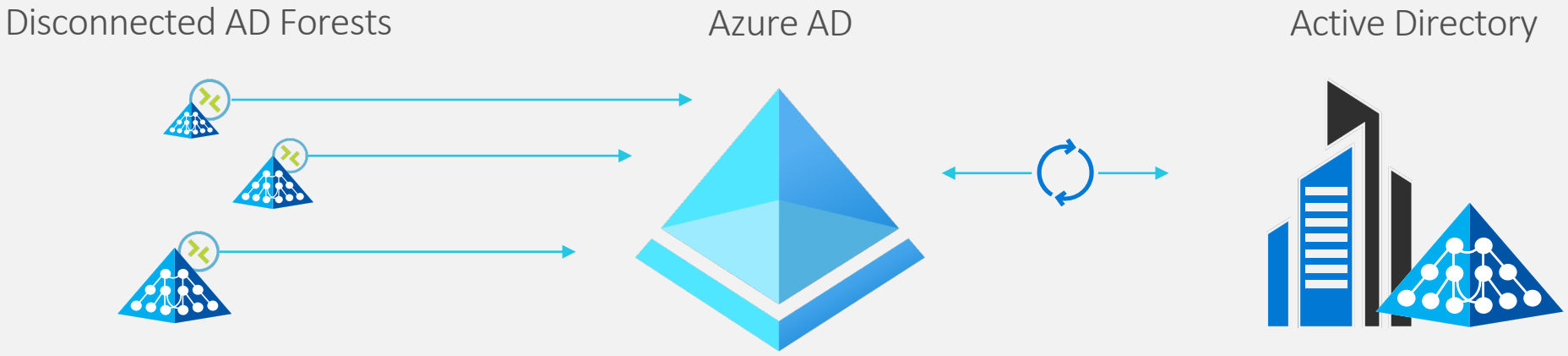
- Review of the synced attributes, filtering and write-back options
  - Scope of objects and filter of attributes that are needed in Azure AD
  - IDFix to prepare and check directory objects and attributes
  - Password Write-back (Self Service Password Reset Service and Auto-Remediation)

- 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

- **Different interval of synchronization** (object and password hash sync)

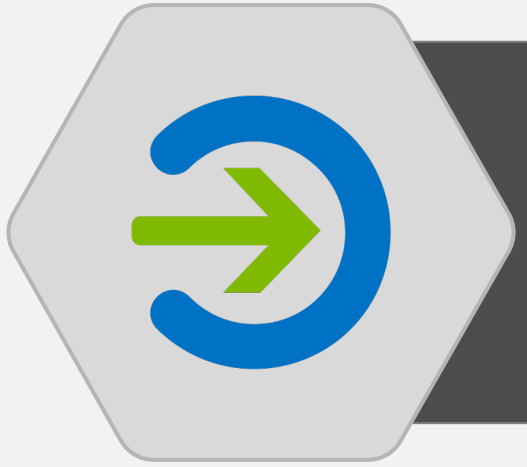
# Azure AD Connect Synchronization

## 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“)



# Hybrid Identity Authentication

# Hybrid Identity Authentication

## How to choose the right model?

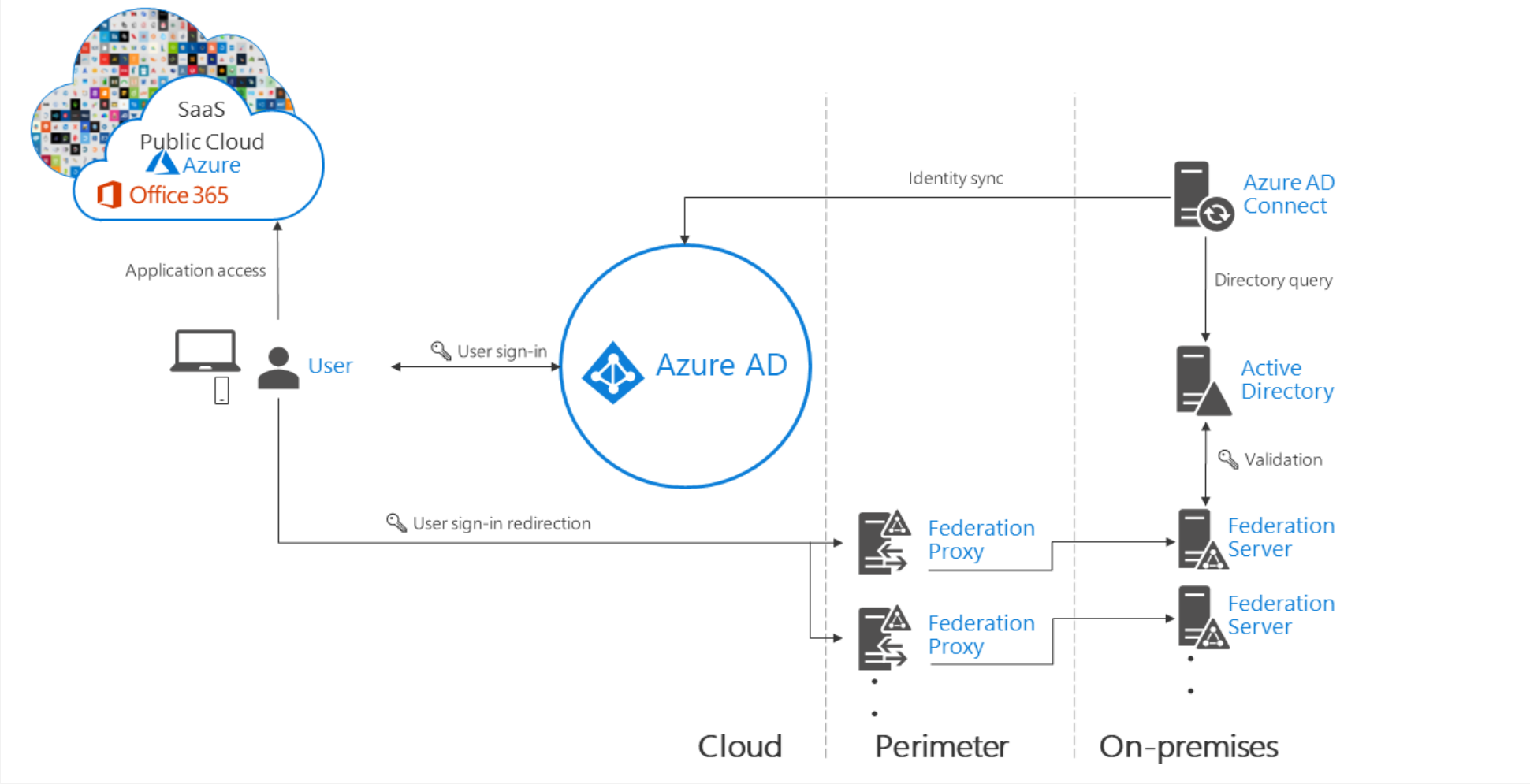
- Decision tree and detailed considerations by Microsoft
- Define **your** (identity) strategy and level of transformation

- **Cloud vs. Federated/On-Prem Authentication?**
  - Defense of initial authentication attacks (brute force and password spray)?
  - Certificate management (Golden SAML)?
  - Hardening of perimeter-network components?
  - Enforcing and validation of local (AD) security policies and identity lifecycle?
    - Example by PHS: "Force Password Change on Next Logon", Account Experation
  - Resilience of IAM Infrastructure (SLA and On-Premises dependency)?

- Identity Protection features (leaked credentials)?

# Hybrid Identity Authentication

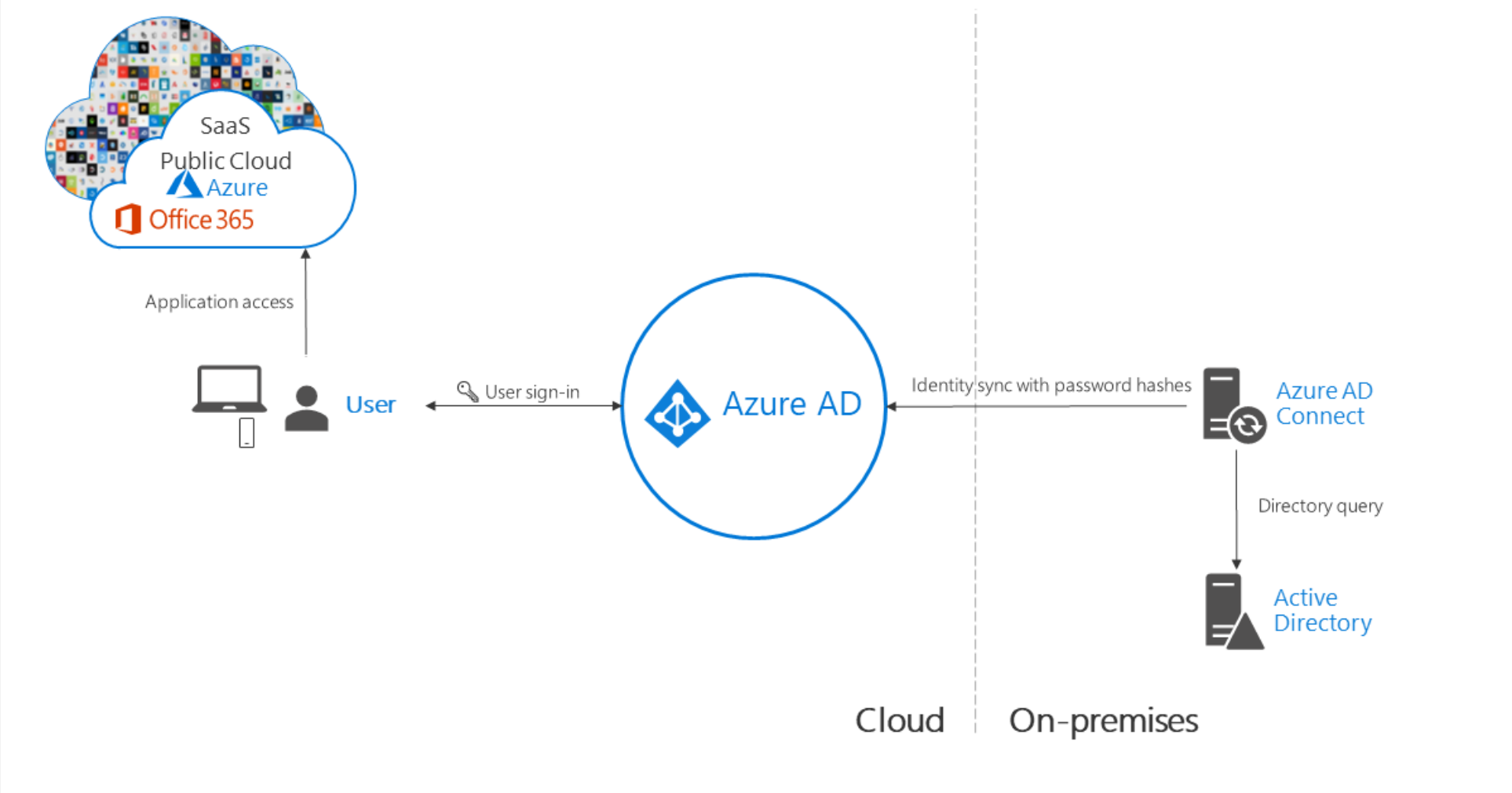
## Hybrid Authentication with Federation Services (AD FS)




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

# Hybrid Identity Authentication

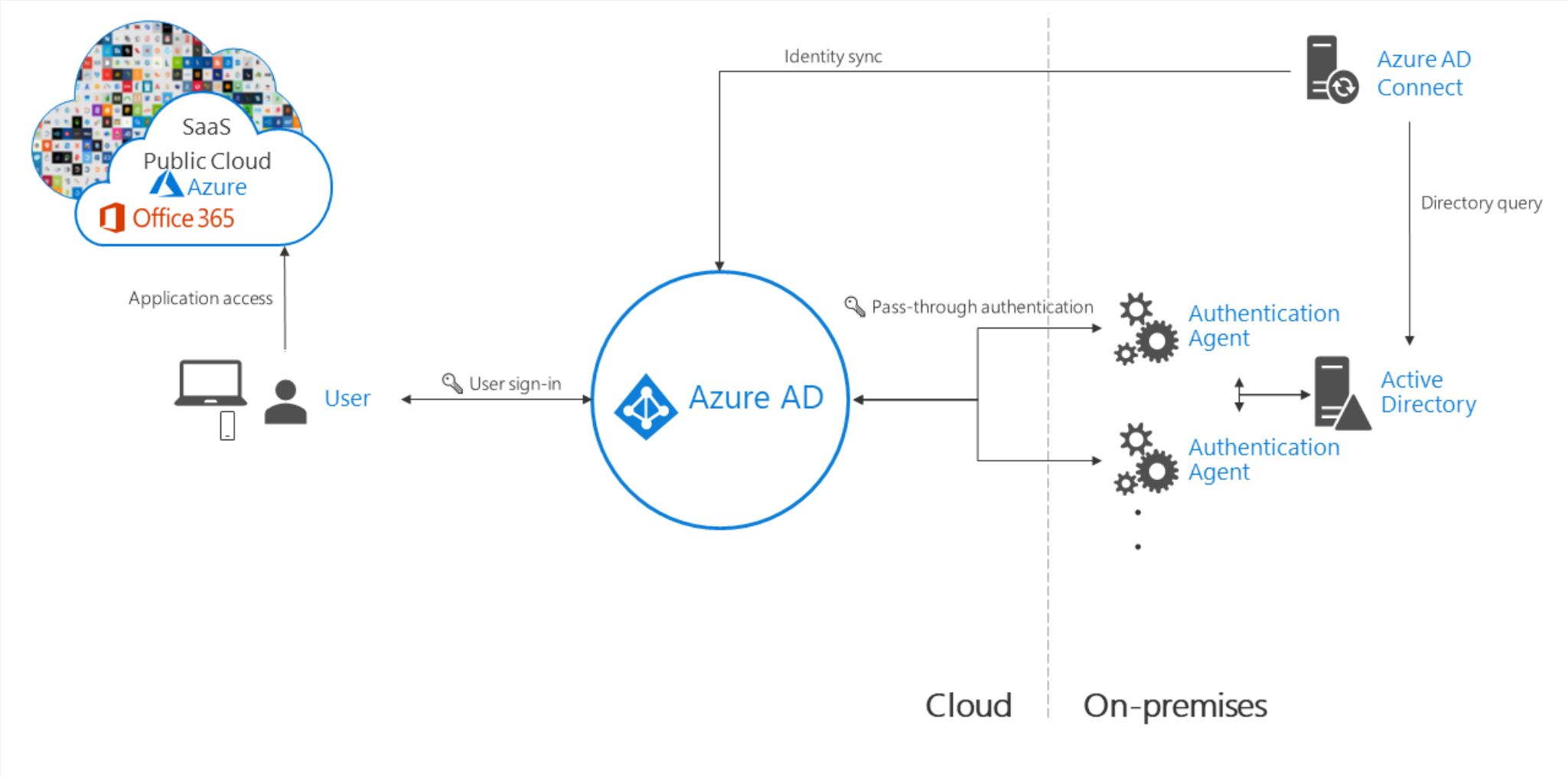
## Hybrid Authentication with Password hash sync (PHS)




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

# Hybrid Identity Authentication

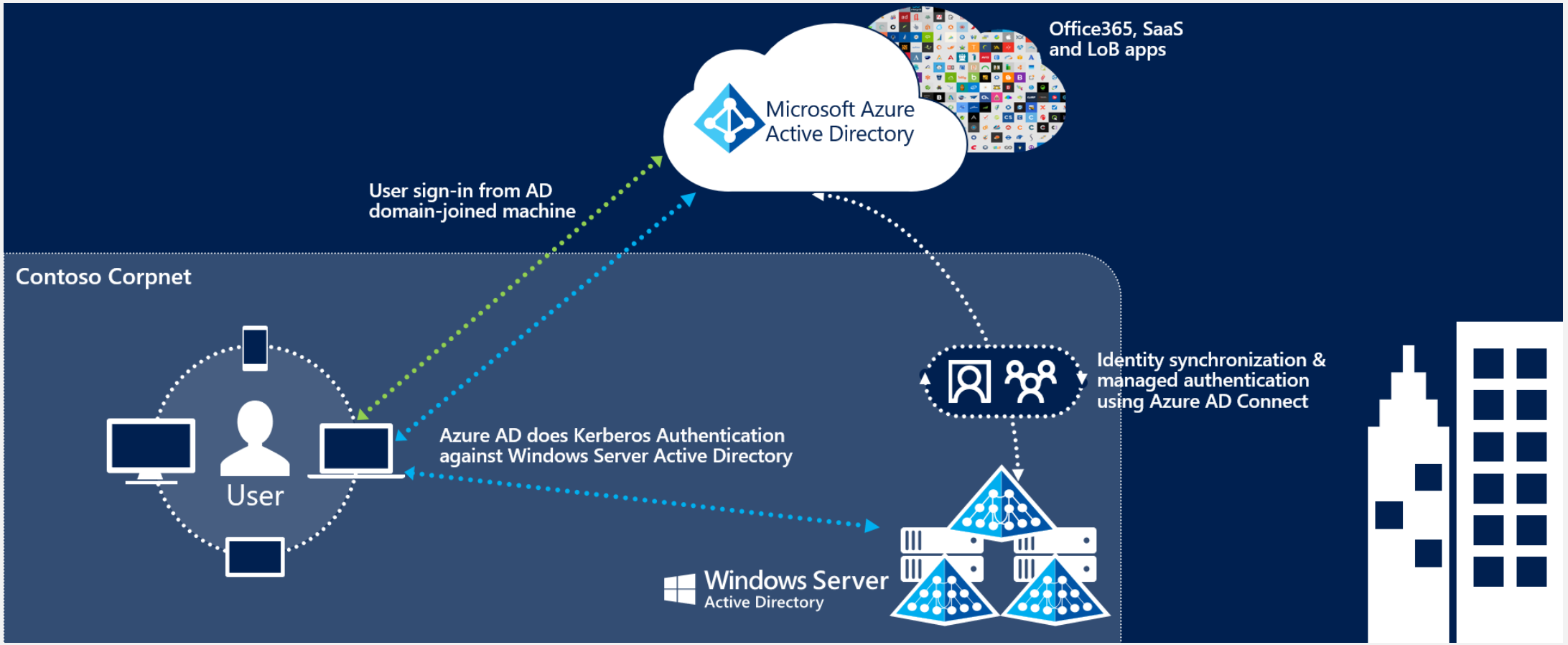
## Hybrid Authentication with Pass-trough Authentication (PTA)




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

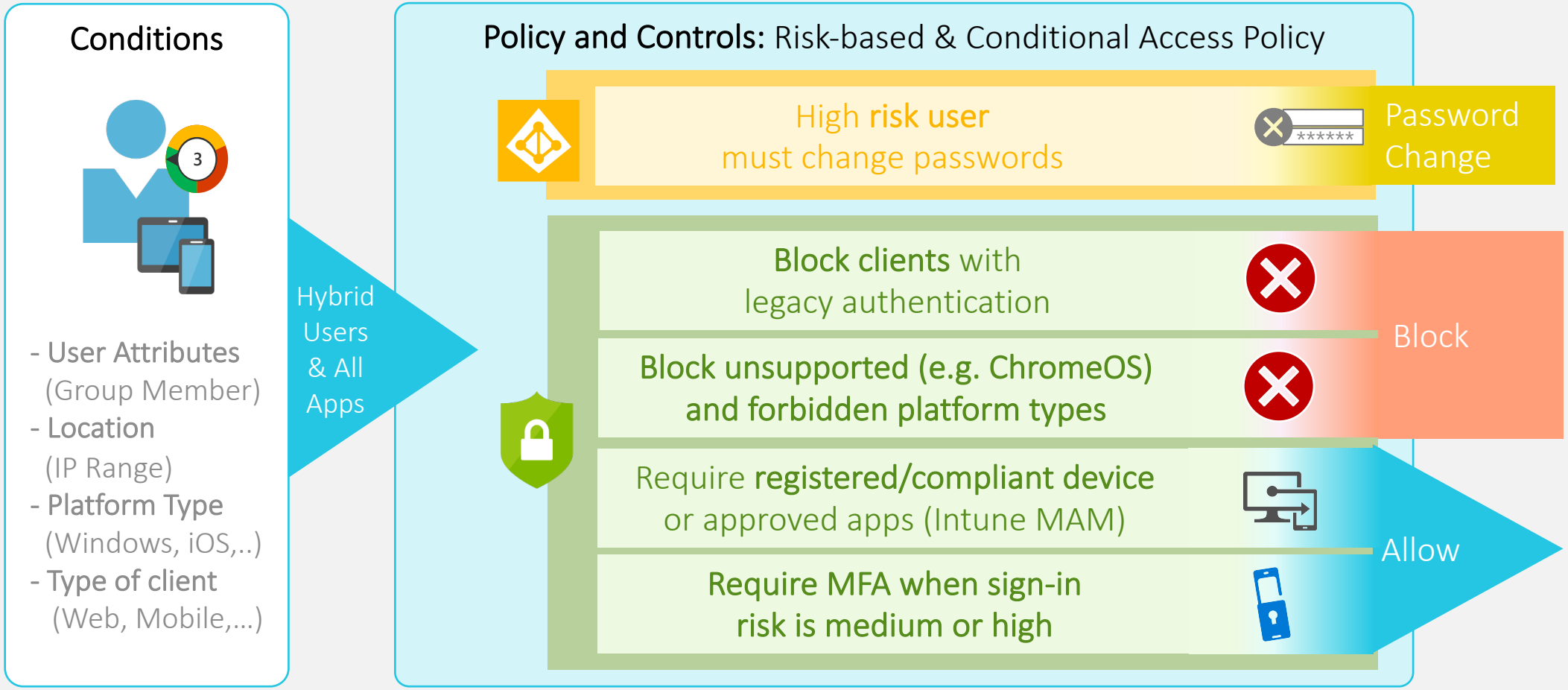
- Limitation of sSSO Kerberos Encryption types in the past:
  - *Support of AES256_HMAC_SHA1 is available (since October 2019), before: RC4_HMAC_MD5 encryption type was only supported*
    Source: https://feedback.azure.com/forums/169401-azure-active-directory/suggestions/36121711-add-support-for-kerberos-aes-and-drop-rc4-hmac-md5

- Known issues and manual roll over Kerberos decyrption key
  - At least every 30 days to mitigate potential compromise of „Computer Account“

# Hybrid Identity Protection

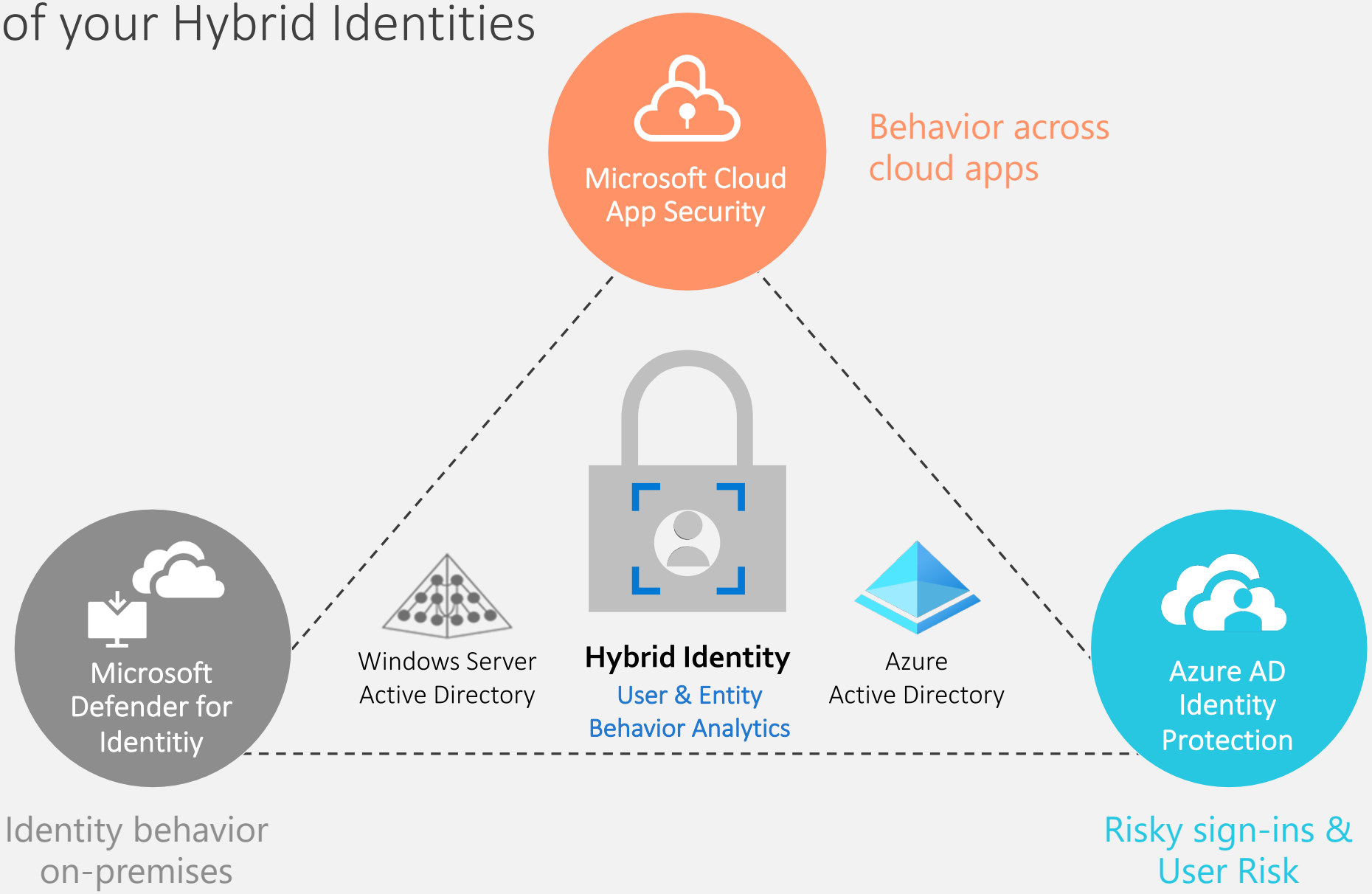
# Hybrid Identity Protection

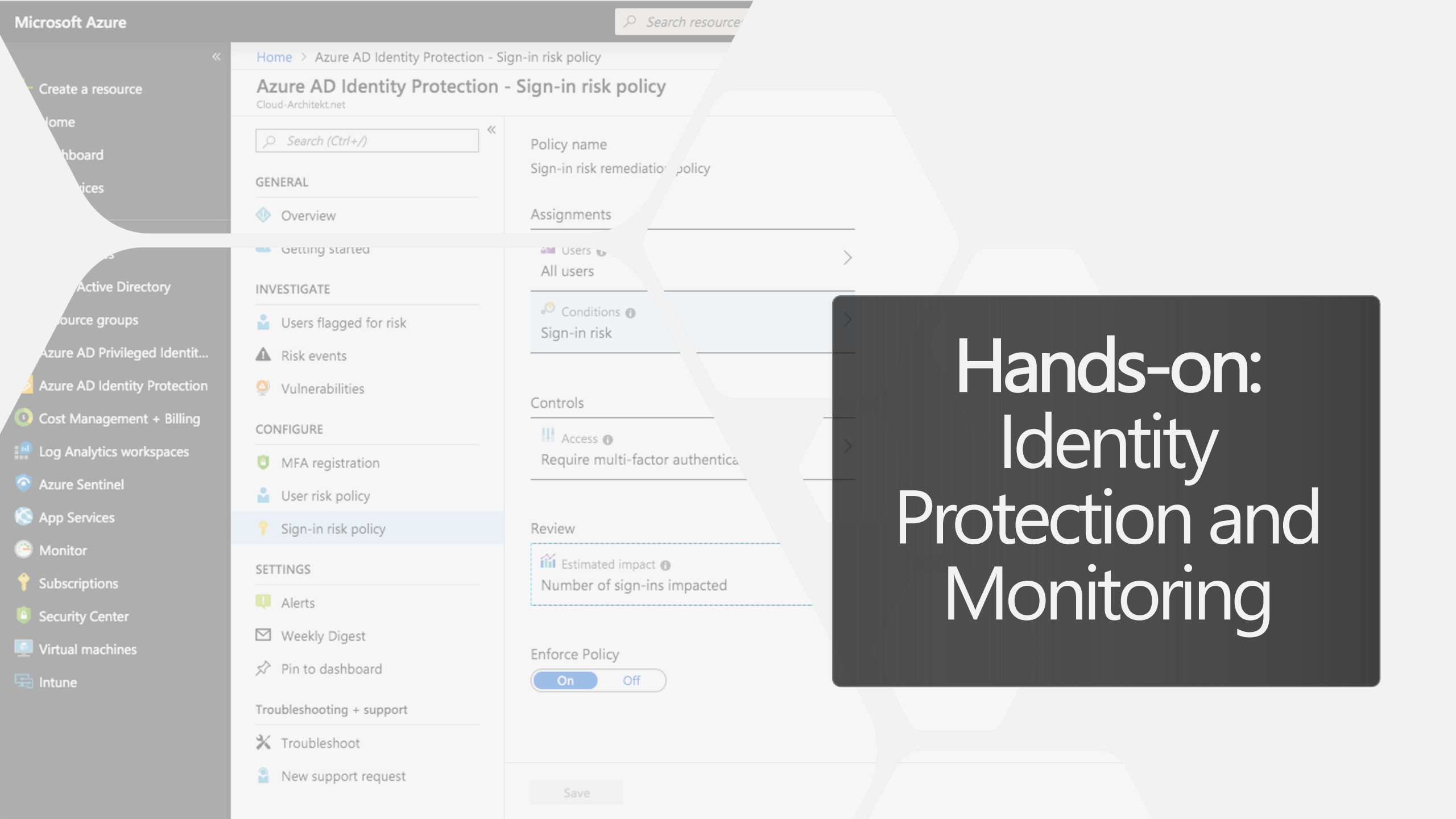
## Design your Identity Protection and Conditional Access Strategy



# Hybrid Identity Protection

## Guards of your Hybrid Identities





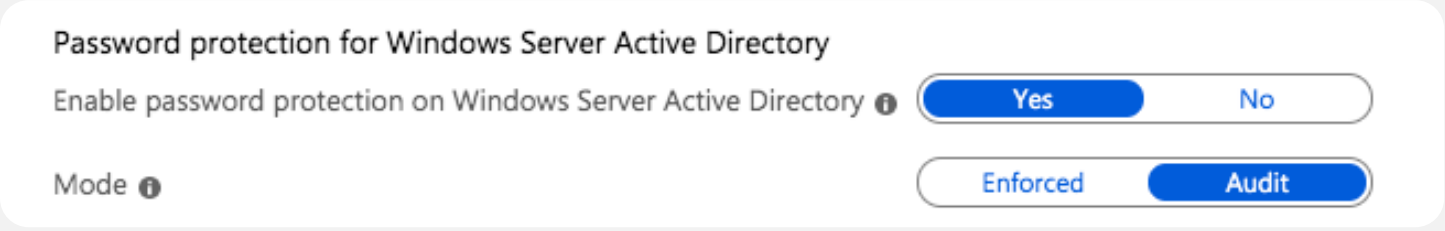

# Hands-on: Identity Protection and Monitoring

# 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)

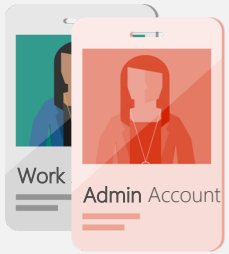



Source: Enforce on-premises Azure AD Password Protection for Active Directory Domain Services

# Privileged Identity Management in Azure AD

# 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, auditing and regular review of access
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

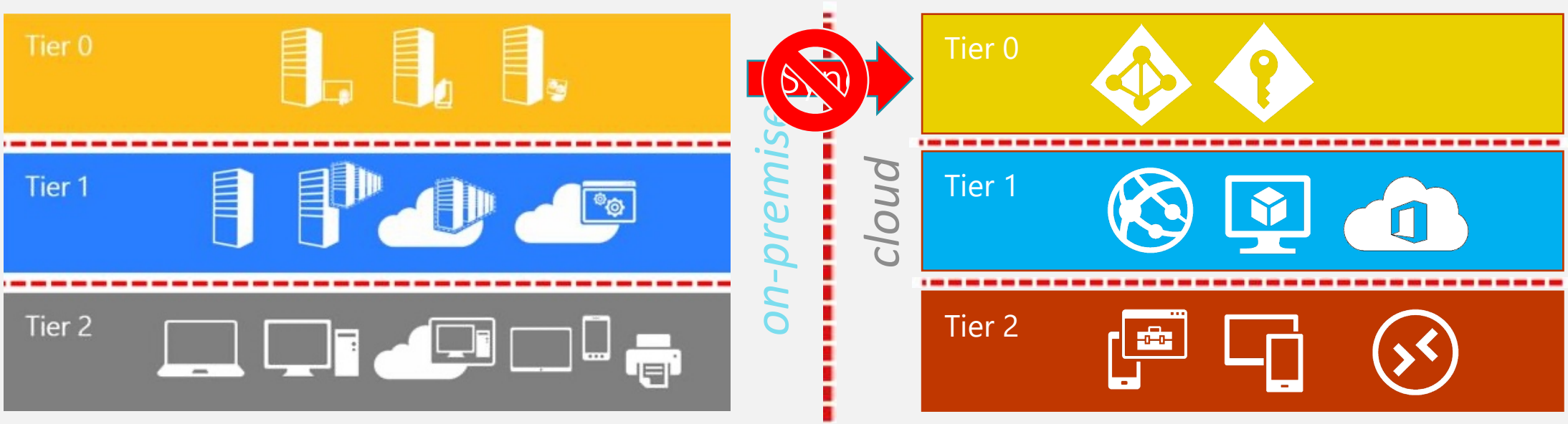
Source: Microsoft Security Blog (“3 investments Microsoft is making to improve identity management”)

# Priviliged Identity Management (PIM)

## Securing privileged access for hybrid and cloud deployments

*„To mitigate risk of identity compromise, or bad actors, implement **tiered administration** and ensure that you **follow principles of least privilege for Azure AD Administrator Roles.**“*

*Source: „Securing Azure Environments with Azure AD (Architecture and Design Guide)“, Page 8*




Source: Active Directory administrative tier model


# DANKESCHÖN!

@Thomas_Live

www.cloud-architekt.net