

A blurred background image shows a person's hands typing on a laptop keyboard. The image is overlaid with several large, semi-transparent hexagonal shapes in white, light orange, and black, which frame the title and author information.

Design and Security Hybrid Azure AD

Thomas Naunheim

Virtualization Community NRW, 23.01.2020

About Me

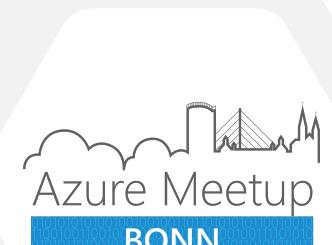
Thomas Naunheim

Cloud Engineer
Koblenz, Germany

 @Thomas_Live

 Thomas@Naunheim.net

 www.cloud-architekt.net



Agenda

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

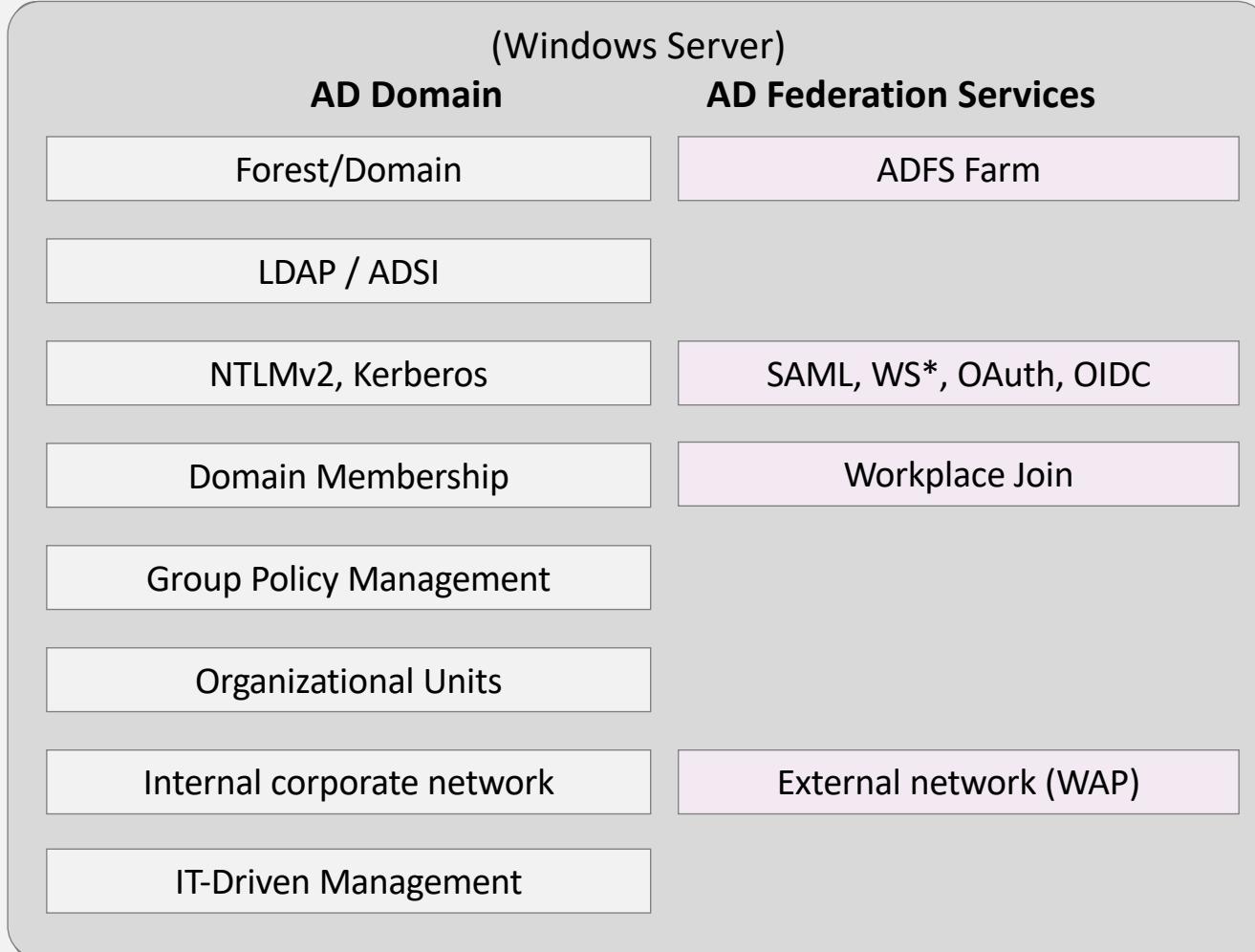




Azure Active Directory Tenant

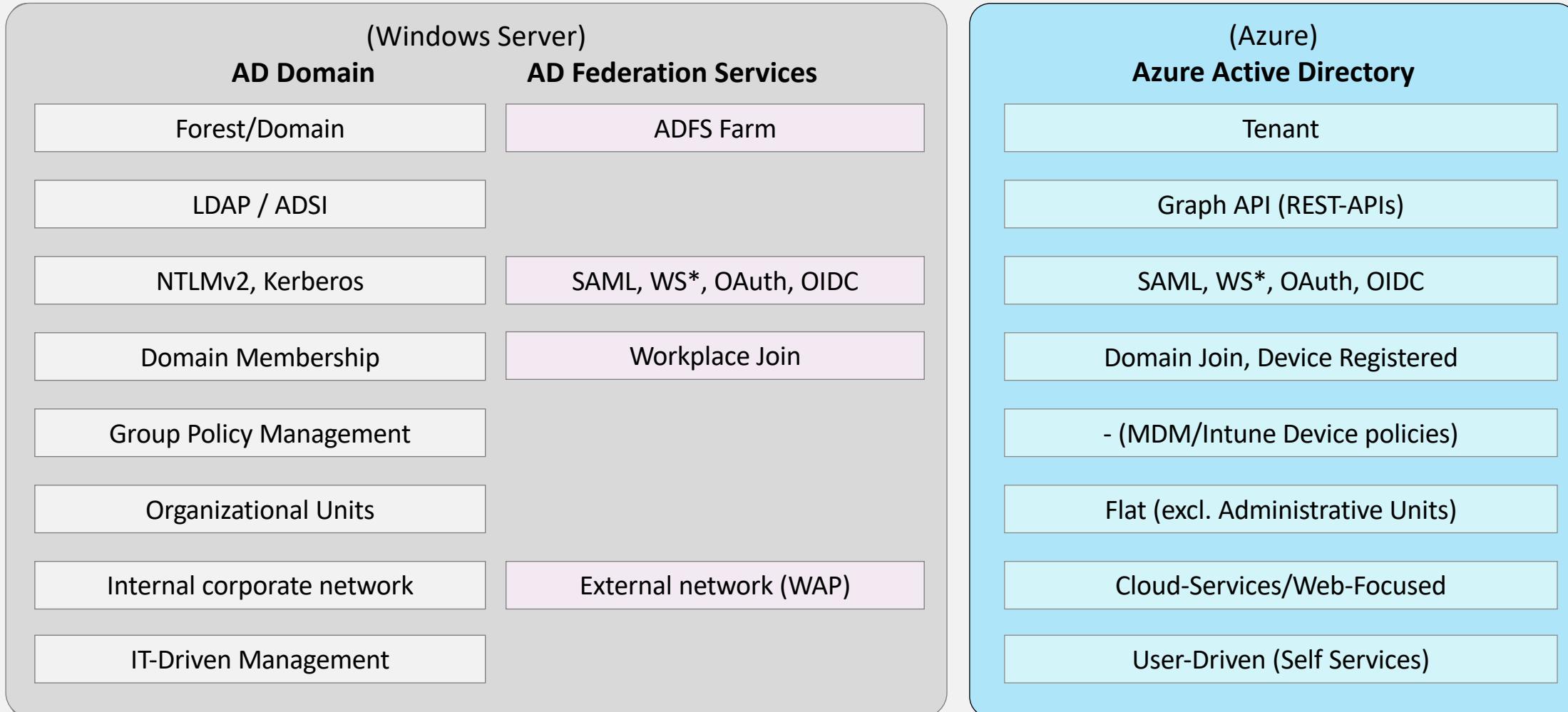
Azure Active Directory

Active Directory in Azure?



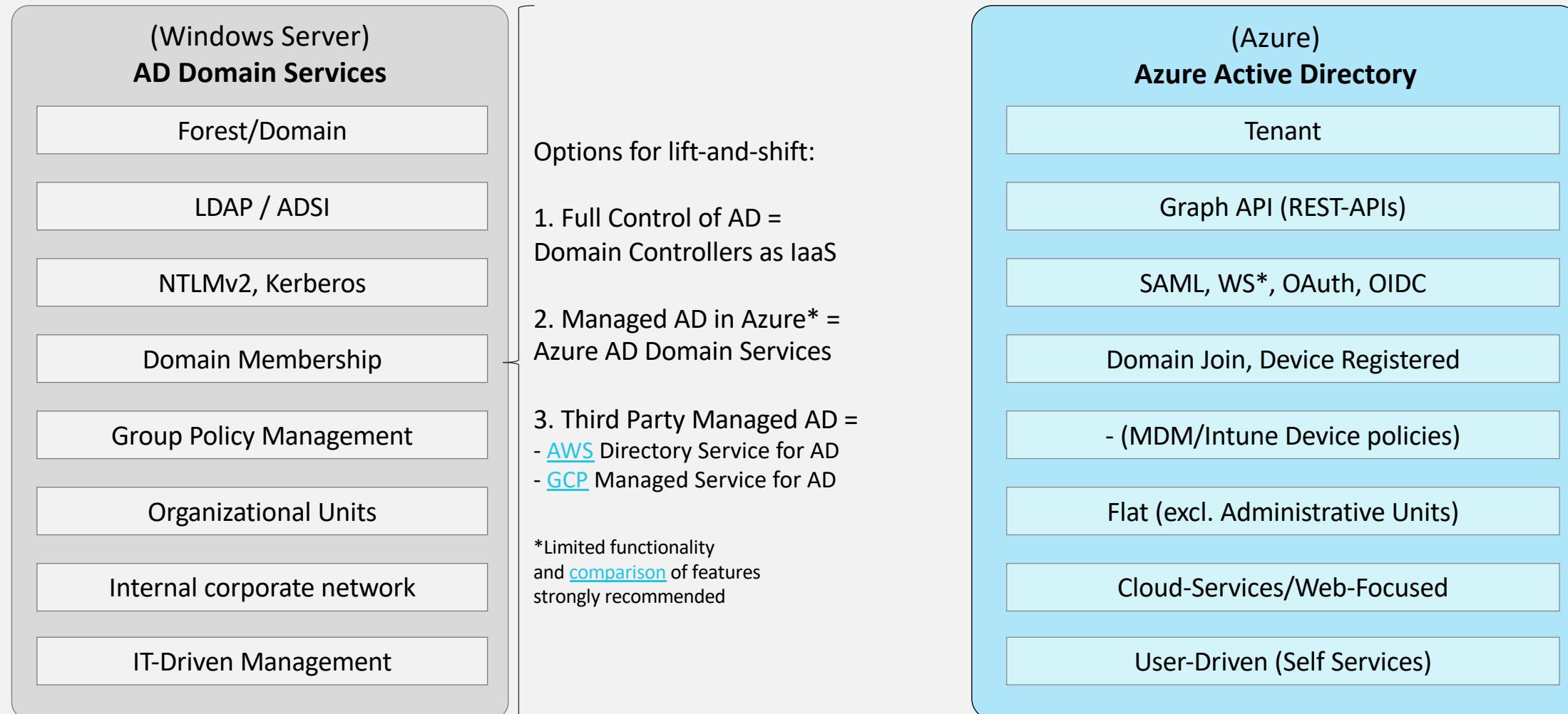
Azure Active Directory

Active Directory in Azure?



Azure Active Directory

Active Directory in Azure?



Azure Active Directory

One tenant to rule them all...?

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

Security - Identity Secure Score

Search (Ctrl+)

[Learn more](#) [Troubleshooting and support](#) [Got feedback?](#)

Getting started

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 [i](#)

Your Identity Secure Score

Show score for last

7 days

30 days

60 days

90 days

155 / 263

Cloud-Architekt.net

155



Industry average

-1

Typical 19001-922337203685...

29



[Change industry](#)

Improvement actions

[Download](#) [Column](#)

[Search to filter items...](#)

NAME	SCORE IMPACT
Require MFA for Azure AD privileged roles	50
Require MFA for all users	30
Do not allow users to grant consent to unma...	0
Designate fewer than 5 global admins	0

Require MFA for Azure AD privileged roles

50

Low

Require MFA for all users

30

Moderate

Do not allow users to grant consent to unma...

0

Moderate

Designate fewer than 5 global admins

0

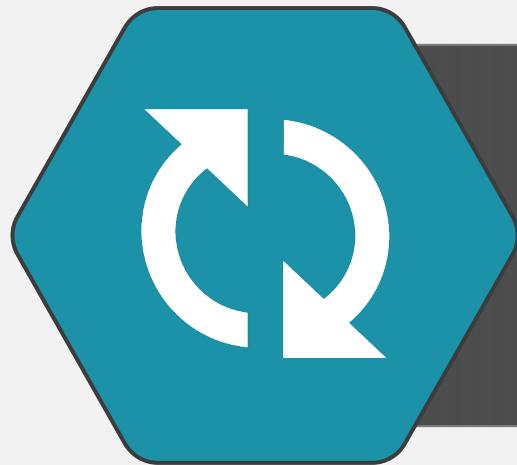
Low

Hands-on: Identity Score & Default Tenant Configuration

Azure AD Tenant

Checklist

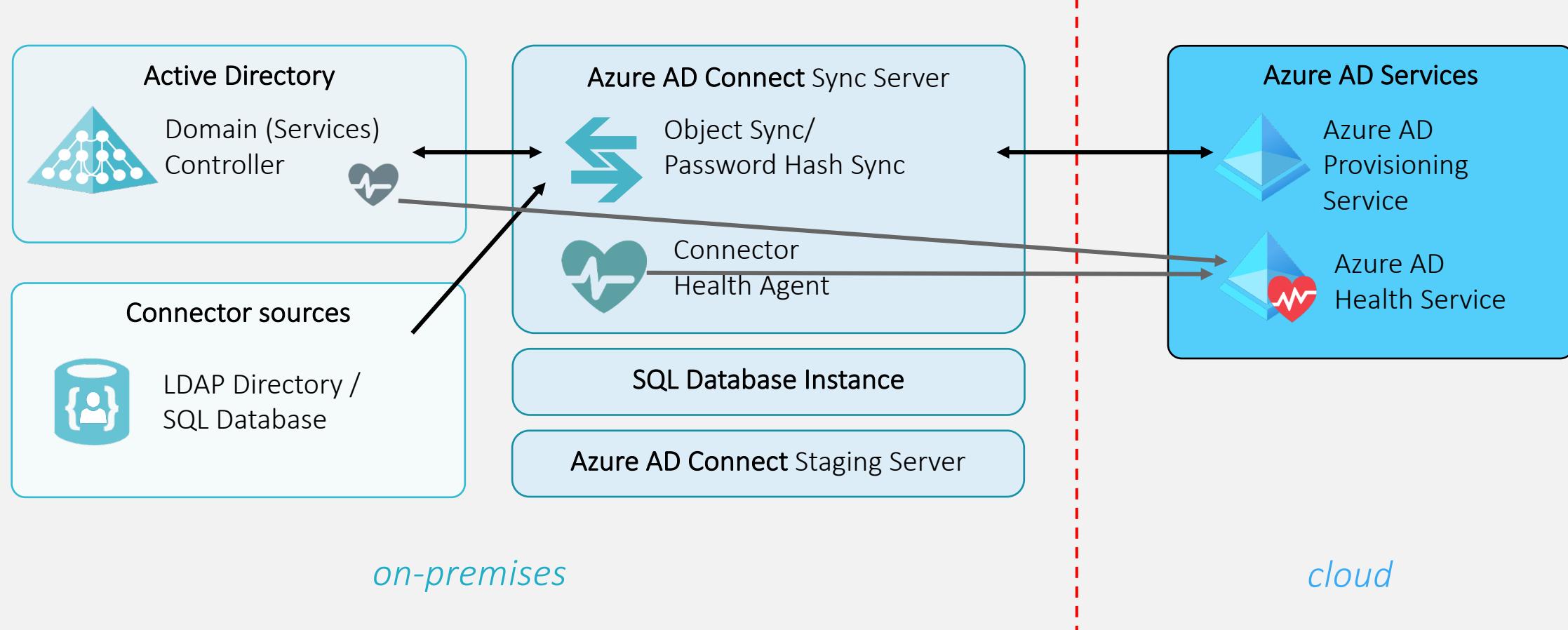
- ✓ *Regular review of (changed) default or new (feature) settings*
- ✓ *Monitor your identity score, usage and insights reports*
- ✓ *Prevent elevated access to manage all Azure resources as „Global Admin“*
- ✓ *Check technical contact and notification mail address*
- ✓ Planning and monitoring assignment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



Hybrid Identity Synchronization

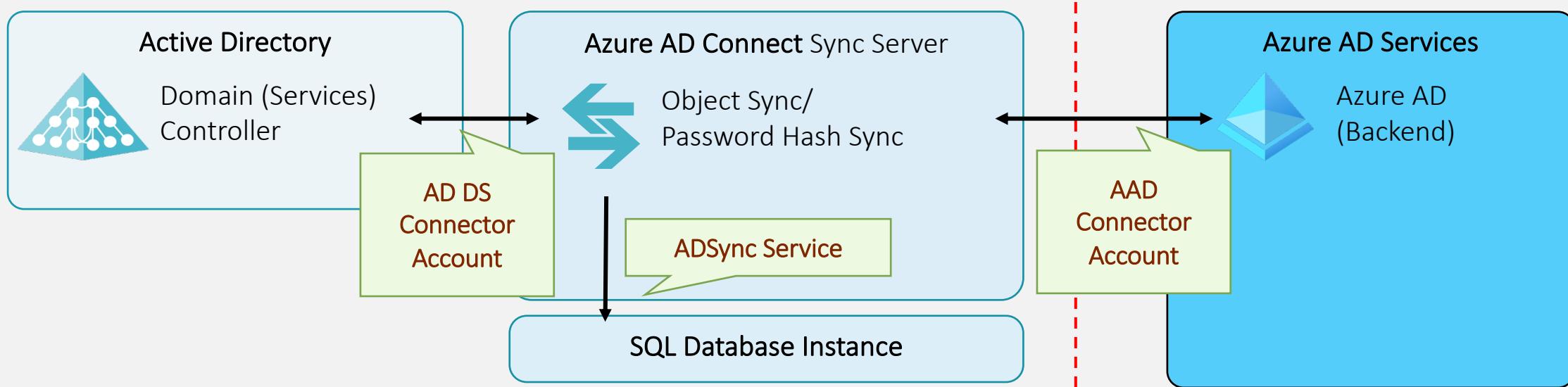
Azure AD Connect Synchronization

Architecture and components of „Identity bridge“



Azure AD Connect Synchronization

Hardening of Azure AD Connect

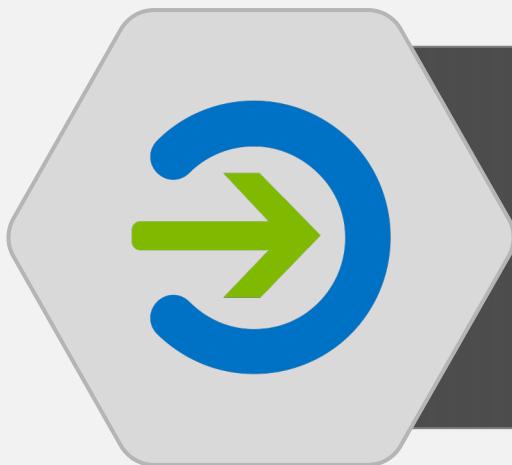


- Pre-created service accounts and delegated permissions
(based on your user scope/filter and write-backs attributes)
 - ADSync service accounts as “(Group) Managed Service Account”
 - Security advisory for AD DS connect service account

Hybrid Identity Synchronization

Checklist

- ✓ *Least privilege and write-scope of AD DS Connector account*
- ✓ *Monitor your synchronization with Azure AD Connect Health*
- ✓ *Placement and protection of Azure AD connect, PTAs servers and databases*
 - ✓ *Hybrid identity components must be protected (similarly high as domain controllers)*
- ✓ Supported changes and recommendation in [changing default configuration](#)
- ✓ Tip: Use „Azure AD Connect [Config Documenter](#)“ (compare configuration)



Hybrid Identity Authentication

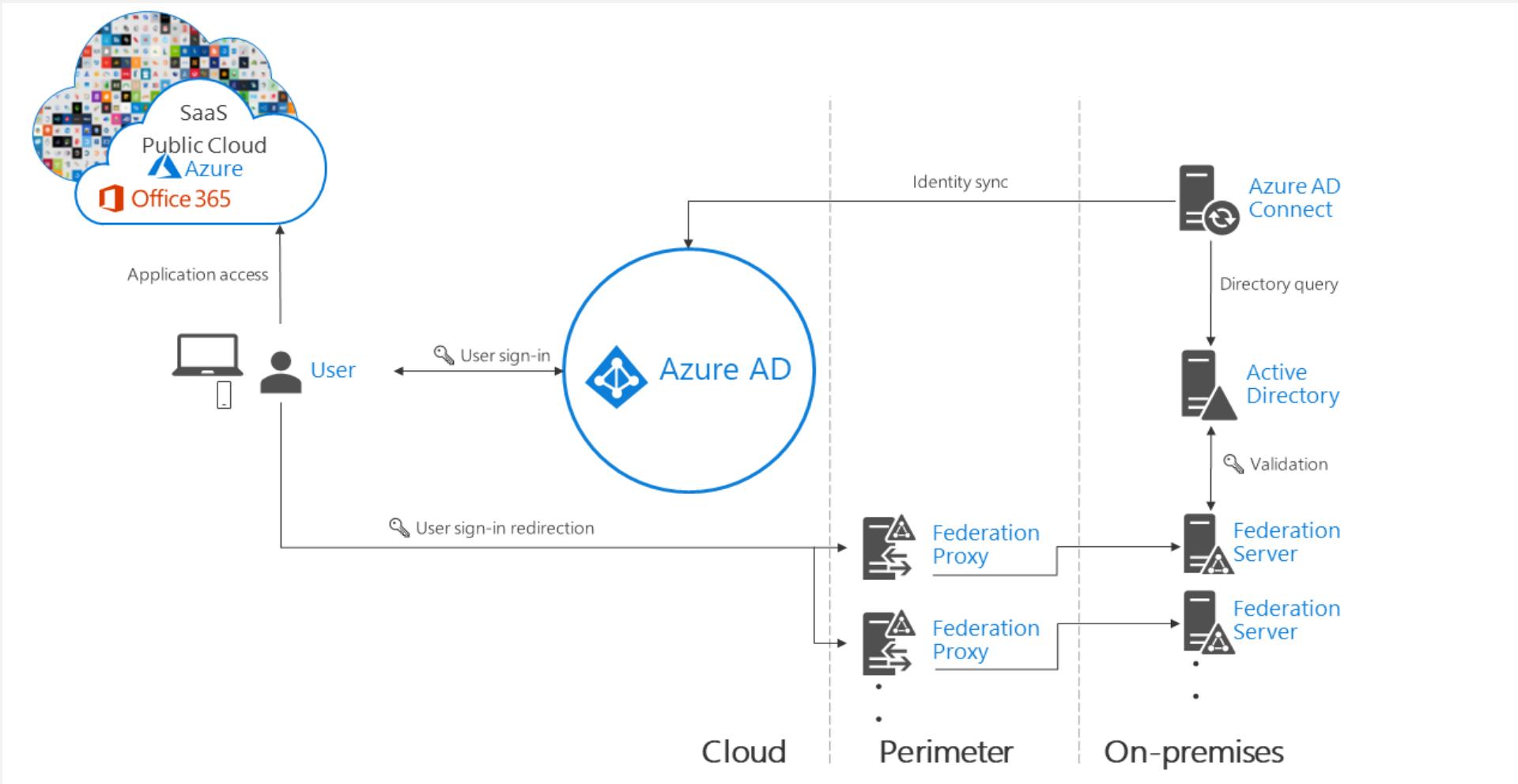
Hybrid Identity Authentication

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 and validation of local (AD) security policies and identity lifecycle?
 - Example by PHS: [Expired accounts](#), [Force password reset \(Public Preview\)](#)
- Disaster recovery / SLA (on-premises dependency)?
- Security concerns of password [hashes](#) in the cloud?
- Identity protection features ([leaked credentials](#))?

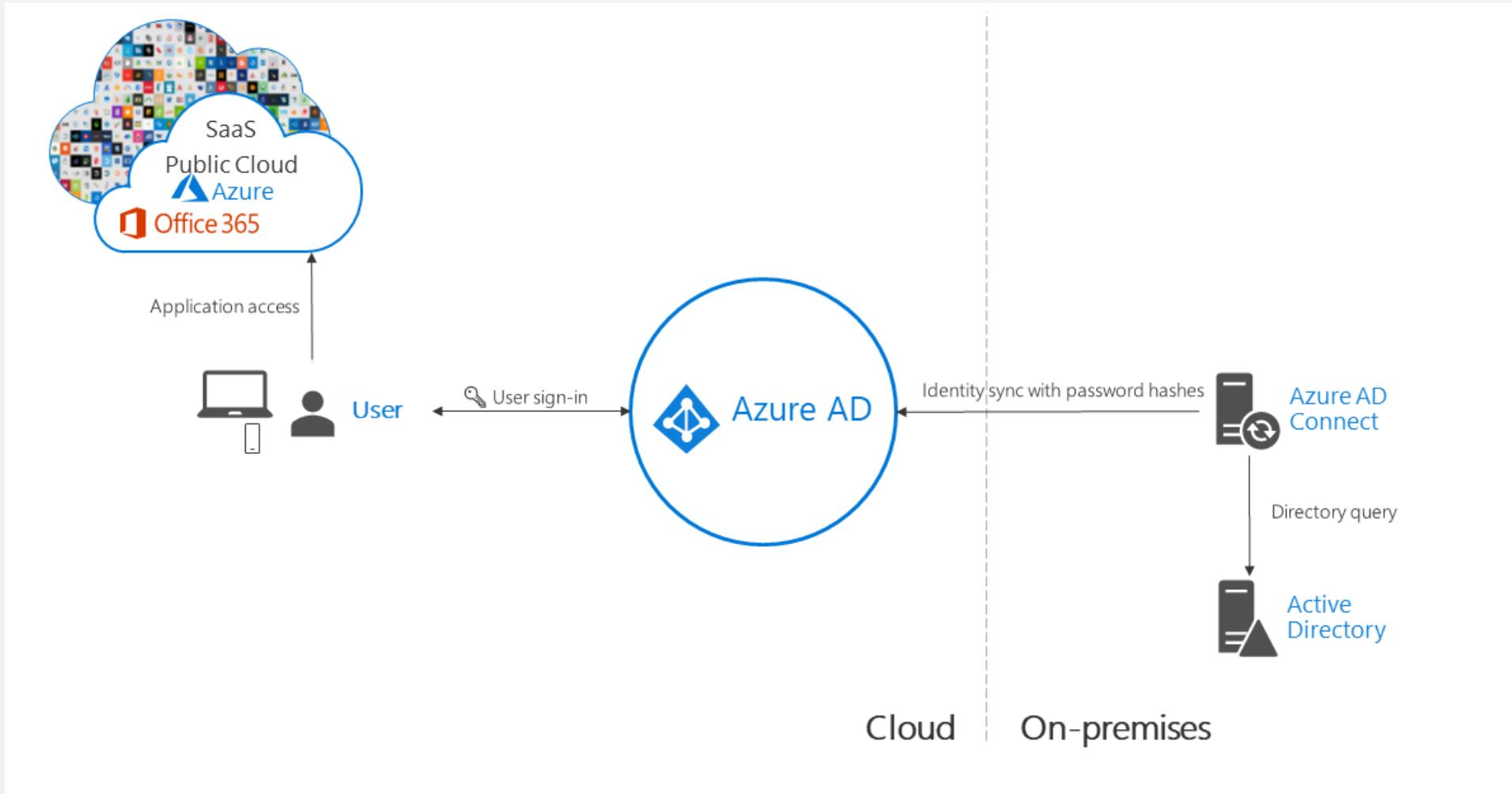
Hybrid Identity Authentication

Hybrid Authentication with Federation Services (AD FS)



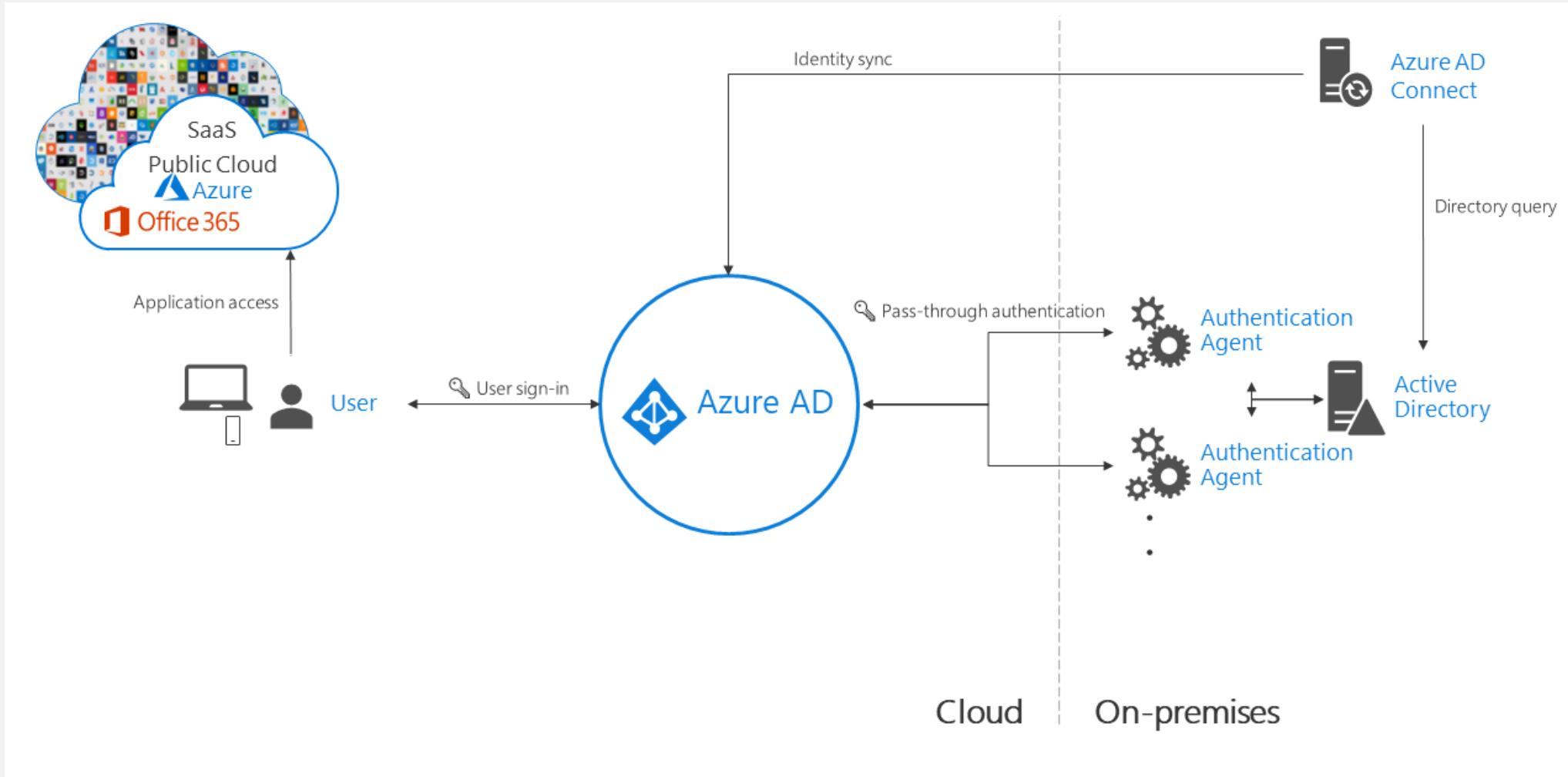
Hybrid Identity Authentication

Hybrid Authentication with Password hash sync (PHS)



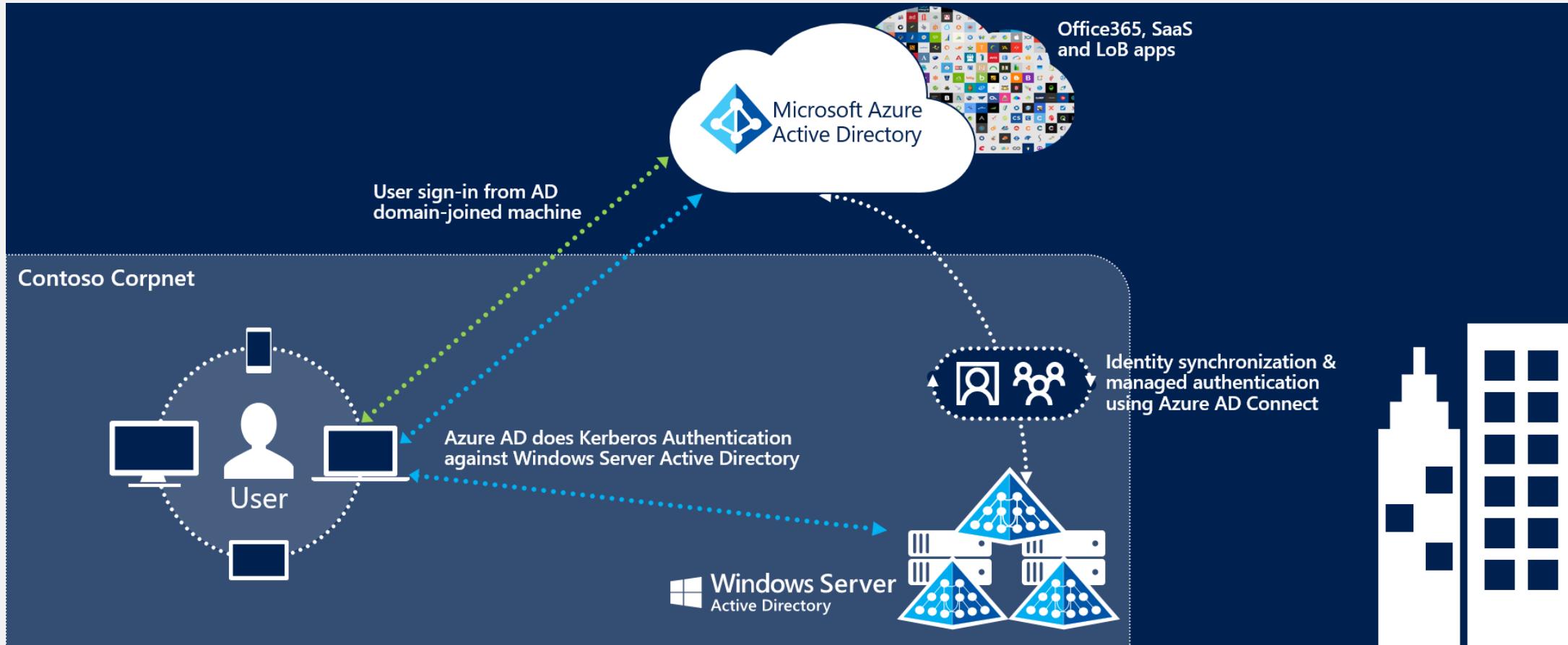
Hybrid Identity Authentication

Hybrid Authentication with Pass-through Authentication (PTA)



Hybrid Identity Authentication

Hybrid Authentication and Seamless Single-Sign On (sSSO)



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 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
- 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

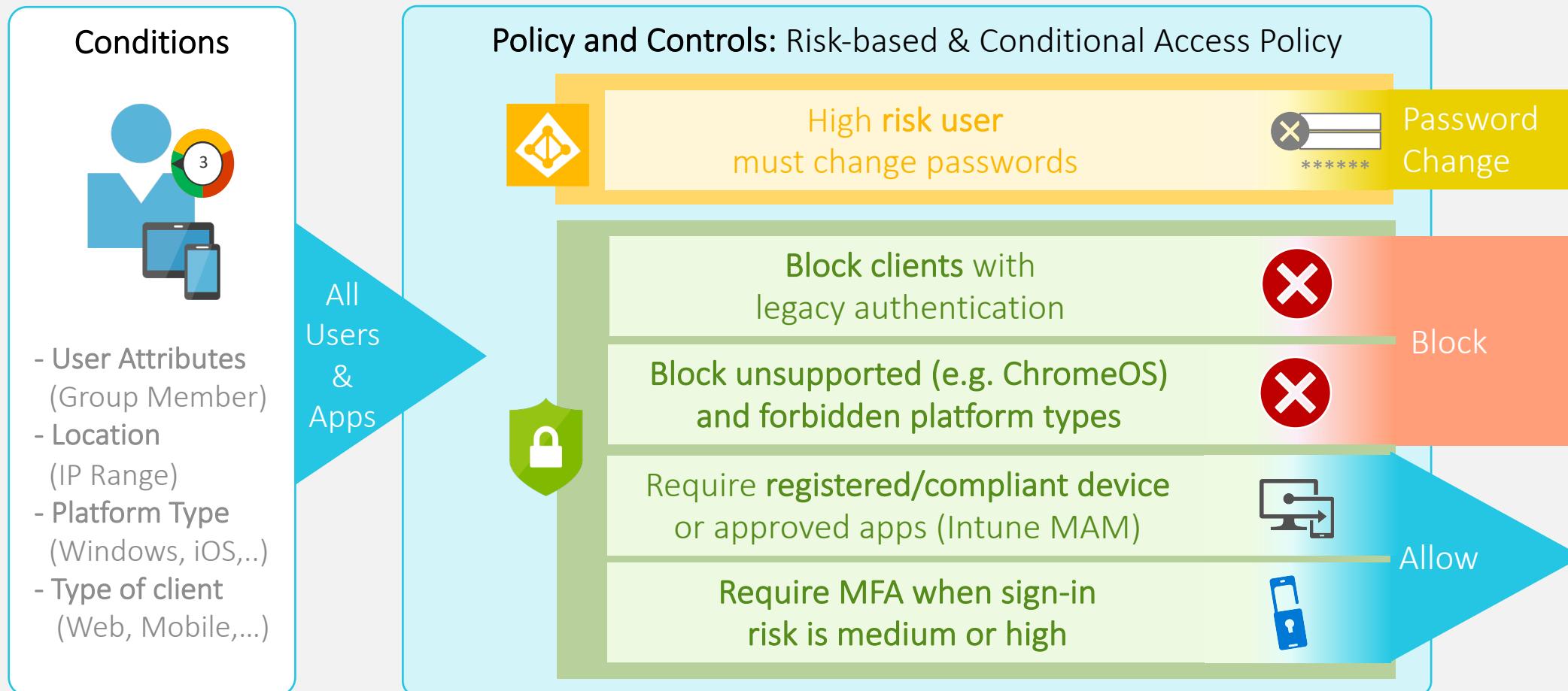
- ✓ *Use cloud authentication / password hash synchronization*
- ✓ *Implement of „Windows Hello for Business“ (Hybrid) for employees*
- ✓ Enable all users to register MFA (Fallback WHfB) and SSPR information
- ✓ Revocation behaviour of „Password-based“ vs. „Non-password-based“ token



Hybrid Identity Protection

Hybrid Identity Protection

Design your Identity Protection and Conditional Access Strategy



Hybrid Identity Protection

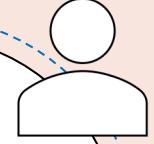
Investigation on cloud identity, on-premises and cloud apps



Azure AD
Identity
Protection

Risky sign-ins &
User Risk

Sign-ins from unfamiliar
locations/Leaked credentials



Azure
Advanced
Threat
Protection

Identity behavior
on-premises

Suspicious VPN
connection/Kerberos Attacks

Data exfiltration
over SMB



Microsoft
Cloud
App
Security

Behavior across
cloud apps

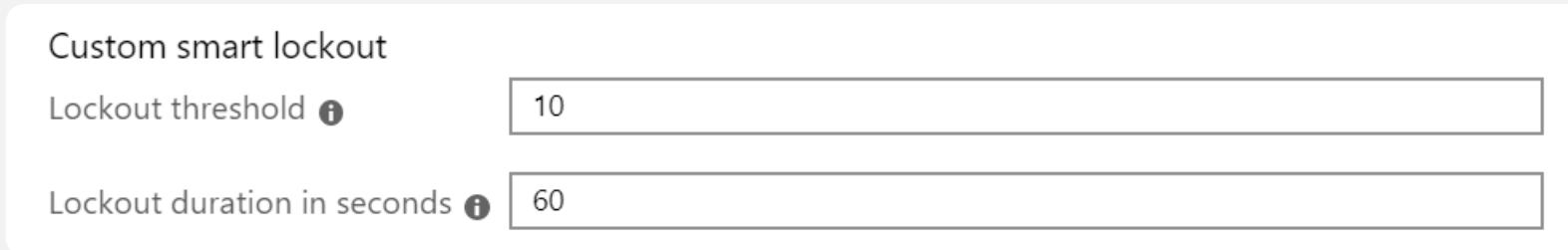
Activity from
infrequent country

Data exfiltration
to unsanctioned apps

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

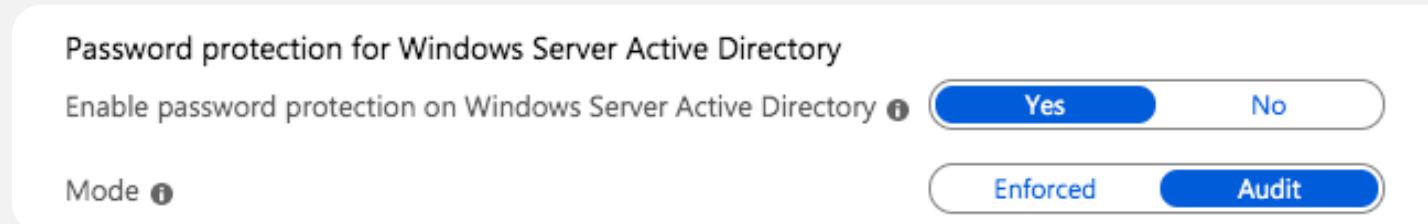
Advanced protection of identities and access

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](#))



Microsoft Azure

Home < Home > Azure AD Identity Protection - Sign-in risk policy

Azure AD Identity Protection - Sign-in risk policy

Cloud-Architekt.net

Search (Ctrl+ /)

GENERAL

- Overview
- Getting started

INVESTIGATE

- Users flagged for risk
- Risk events
- Vulnerabilities

CONFIGURE

- MFA registration
- User risk policy
- Sign-in risk policy**

SETTINGS

- Alerts
- Weekly Digest
- Pin to dashboard

Troubleshooting + support

- Troubleshoot
- New support request

Policy name: Sign-in risk remediation policy

Assignments:

- All users

Conditions:

- Sign-in risk

Controls:

- Require multi-factor authentication

Review:

- Estimated impact: Number of sign-ins impacted

Enforce Policy: **On**

Save

Hands-on: Identity and Password Protection

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 and „On-Premises Directory Sync Service Accounts“ from every policy, 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

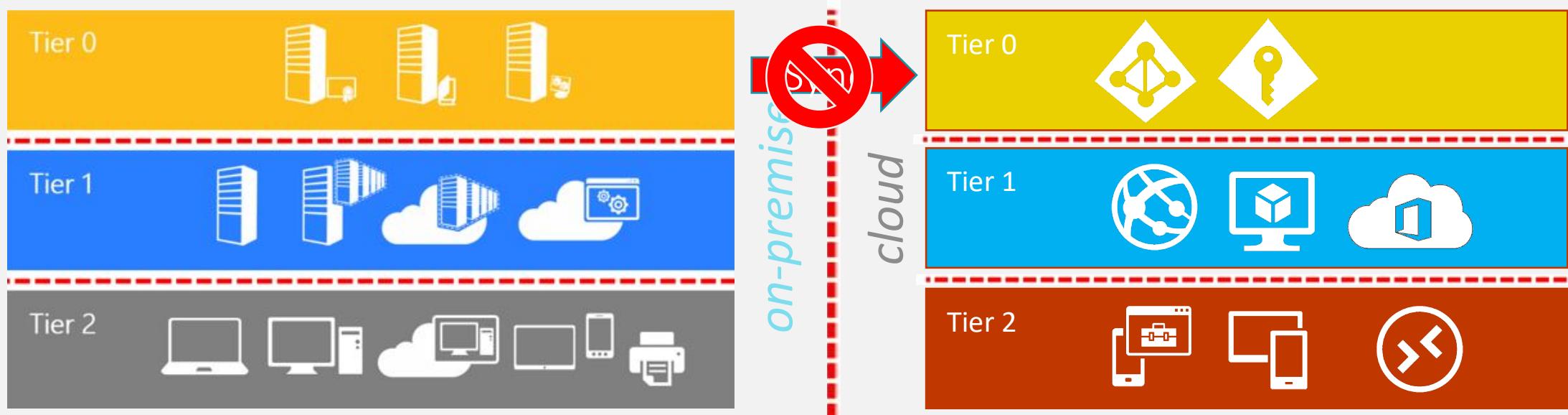
Establish a separate device/workstation for administrative tasks
Various kinds of security levels and implementations

Privileged 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 Enhanced Security Administrative Environment (ESAE)



Privileged 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

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

Troubleshooting + Support



Azure AD Privileged Identity Management

Azure AD PIM is a Premium feature that enables you to limit standing admin 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

Activate your eligible admin role so that you can get limited standing access to the privileged identity

[Activate your role](#)

**Hands-on:
Securing
Privileged
Identities**

Privileged Identity Management

Checklist

- ✓ *Built your Azure and Azure AD RBAC model with least privilege*
- ✓ *Azure AD PIM to reduce expose of privileged accounts*
- ✓ *Require strong (or passwordless) authentication and compliant device for admins*
- ✓ *Manage two emergency accounts (alerting by sign-in attempts)*
- ✓ CSP customers: Verify delegated admin privileges to partners

A close-up photograph of a person's hands typing on a silver laptop keyboard. The background is blurred, showing what appears to be a window or a bright light source.

Thank You

 @Thomas_Live

 Thomas@Naunheim.net

 www.cloud-architekt.net