Design and Security Hybrid Azure AD

Thomas Naunheim
cim lingen, 14.09.2019

About Me

Thomas Naunheim

Cloud Engineer
Koblenz, Germany

@Thomas_Live

Thomas@Naunheim.net

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
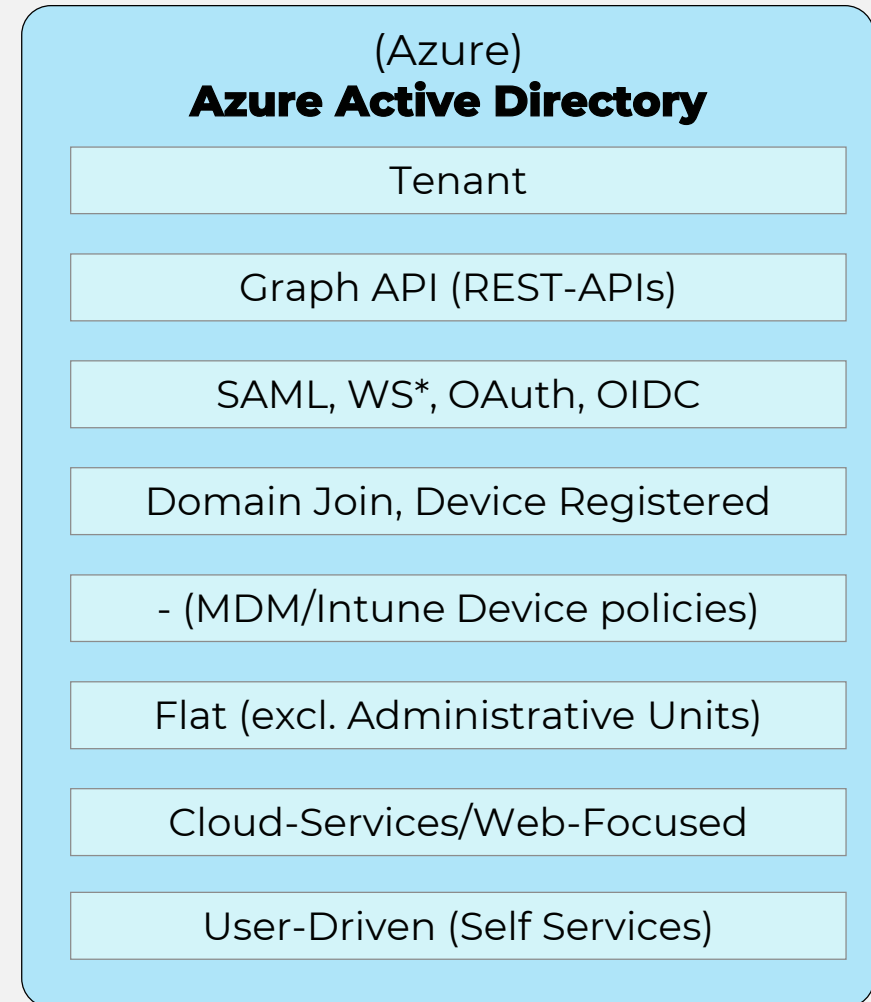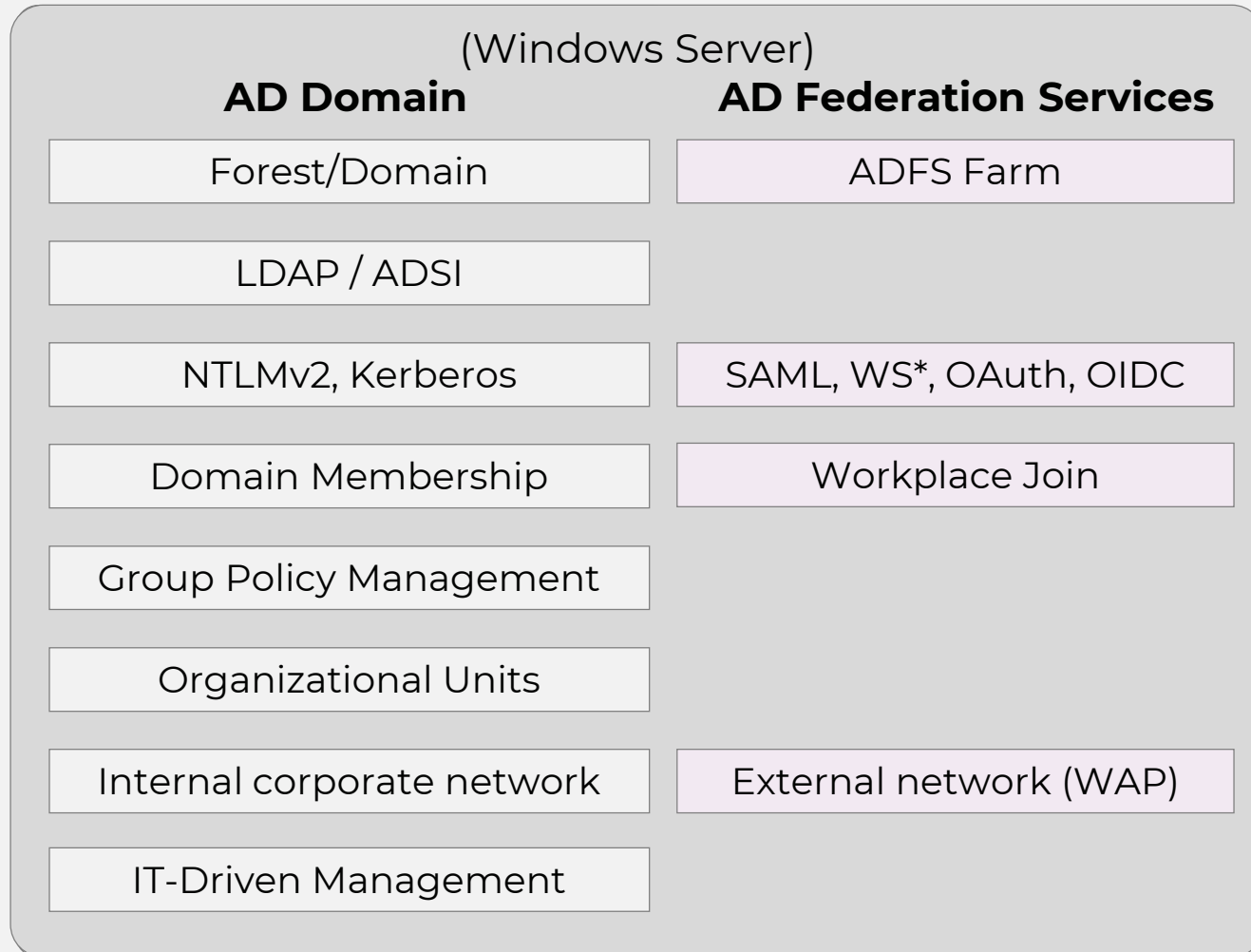- Internal corporate network
- IT-Driven Management

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)

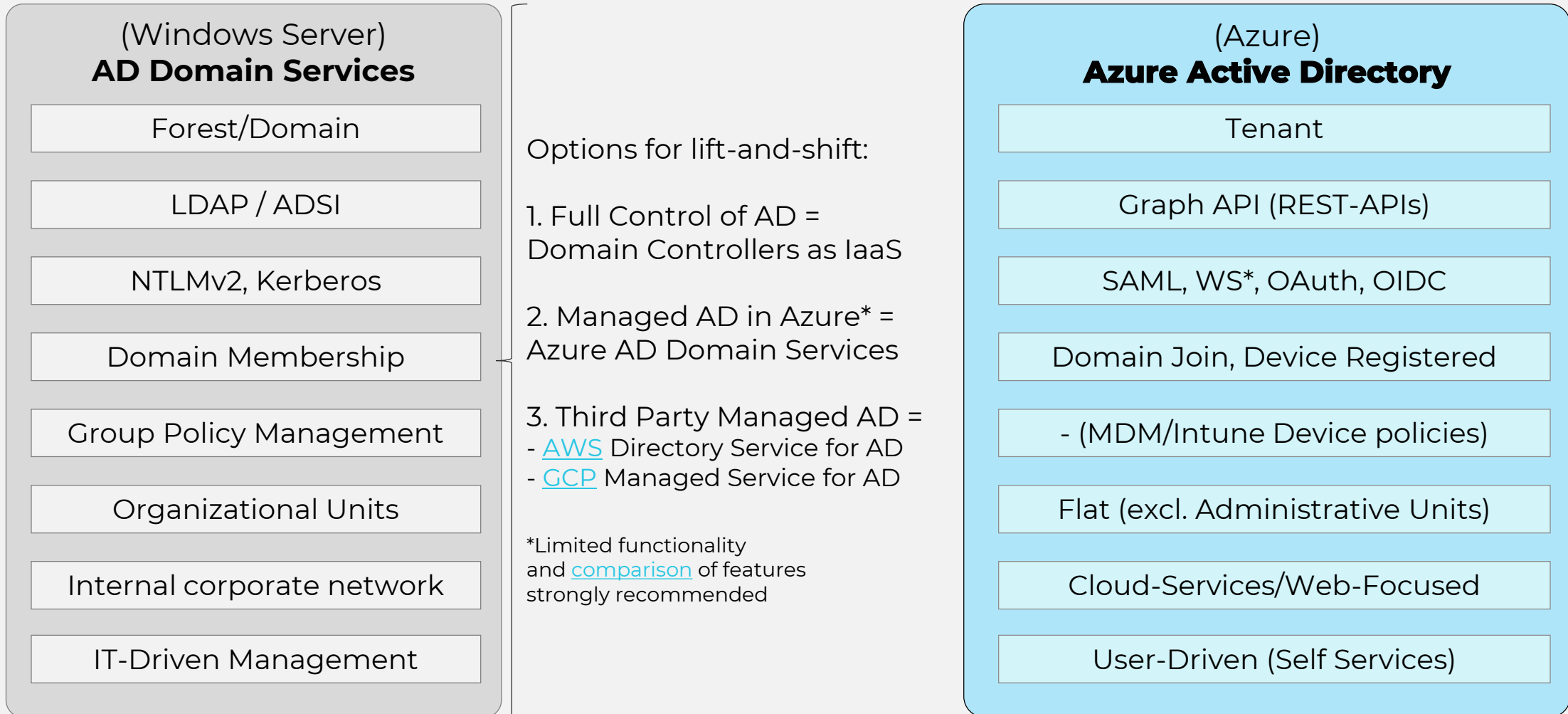| AD Domain	AD Federation Services
Forest/Domain	ADFS Farm
LDAP / ADSI	
NTLMv2, Kerberos	SAML, WS*, OAuth, OIDC
Domain Membership	Workplace Join
Group Policy Management	
Organizational Units	
Internal corporate network	External network (WAP)
IT-Driven Management	

(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
  - Default user permissions

- Tenant friending

- Supported topologies for synchronization (multi-forest-support)

- Location of identity data storage and security considerations
  - Data privacy regulation (workers' council, data privacy)? Where is my data located?

🏆 Security - Identity Secure Score

🔍 Search (Ctrl+/)

ℹ️ 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 ℹ️

Your Identity Secure Score

Show score for last

7 days   30 days   60 days   90 days

... Access

Identity Protection

🛡️ Security Center

155 **/263**

155

150

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

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 resources 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
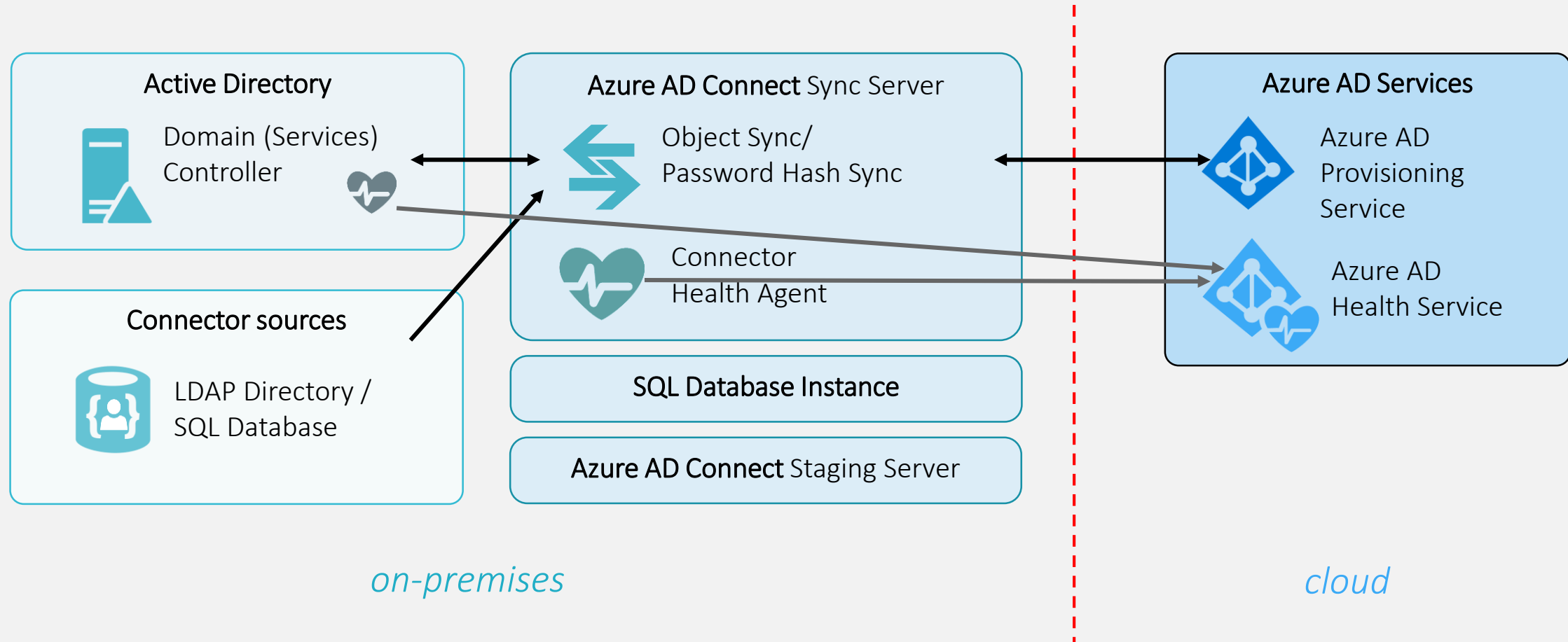
✓ Service Health alerts of Azure AD and MFA service
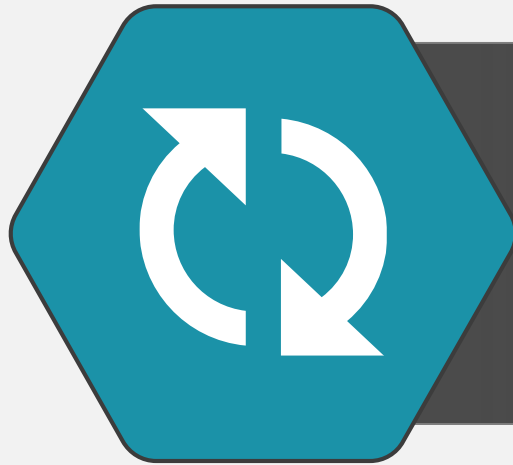
Hybrid Identity
Synchronization

Azure AD Connect Synchronization
Architecture and components of „Identity bridge"

Active Directory

Domain (Services) Controller

Connector sources

LDAP Directory / SQL Database

Azure AD Connect Sync Server

Object Sync/ Password Hash Sync

Connector Health Agent

SQL Database Instance

Azure AD Connect Staging Server

Azure AD Services

Azure AD Provisioning Service

Azure AD Health Service

on-premises

cloud

Azure AD Connect Synchronization
Hardening of Azure AD Connect

Active Directory	**Azure AD Connect** Sync Server	**Azure AD Services**
Domain (Services) Controller	Object Sync/ Password Hash Sync	Azure AD (Backend)

AD DS Connector Account

ADSync Service

AAD Connector Account

SQL Database Instance
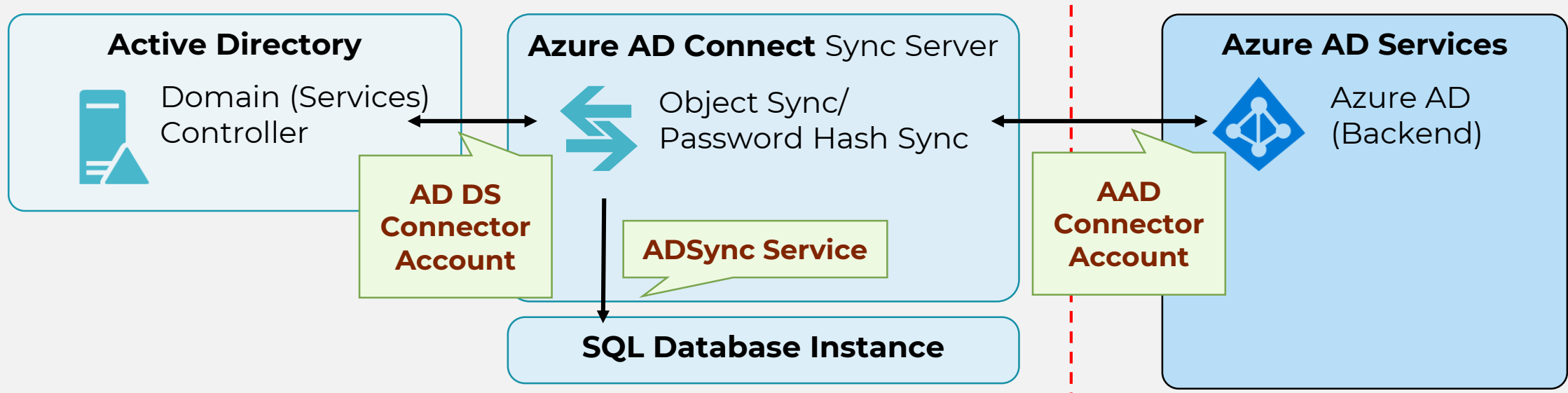
- Pre-created service accounts and delegated permissions (based on your user scope/filter and write-backs attributes)

  - 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 <u>and</u> databases
  - Hybrid identity components must be protected (similarly high as domain controllers)
  - Supported options for "High availability" of PTA and SQL cluster

- Required internet connectivity (direct / proxy)
  - Running tests with „AADConnect-CommunicationsTest.ps1"

- Identity lifecycle and security use cases that needs to be validated
  - Example: Expired user password, nested (AD) groups, Force password reset

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*

✓ Consideration for changing default configuration

✓ Use „Azure AD Connect Config Documenter" (compare configuration)
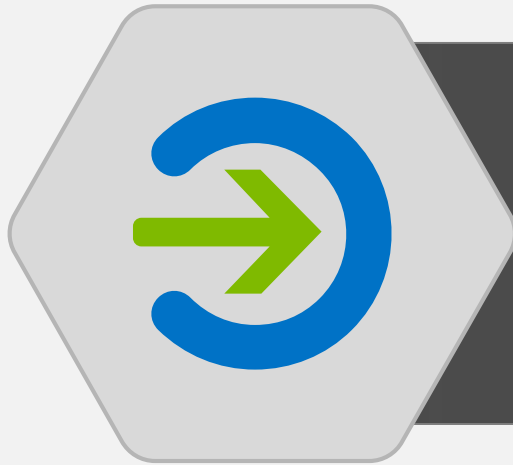
Hybrid Identity Authentication

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 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)
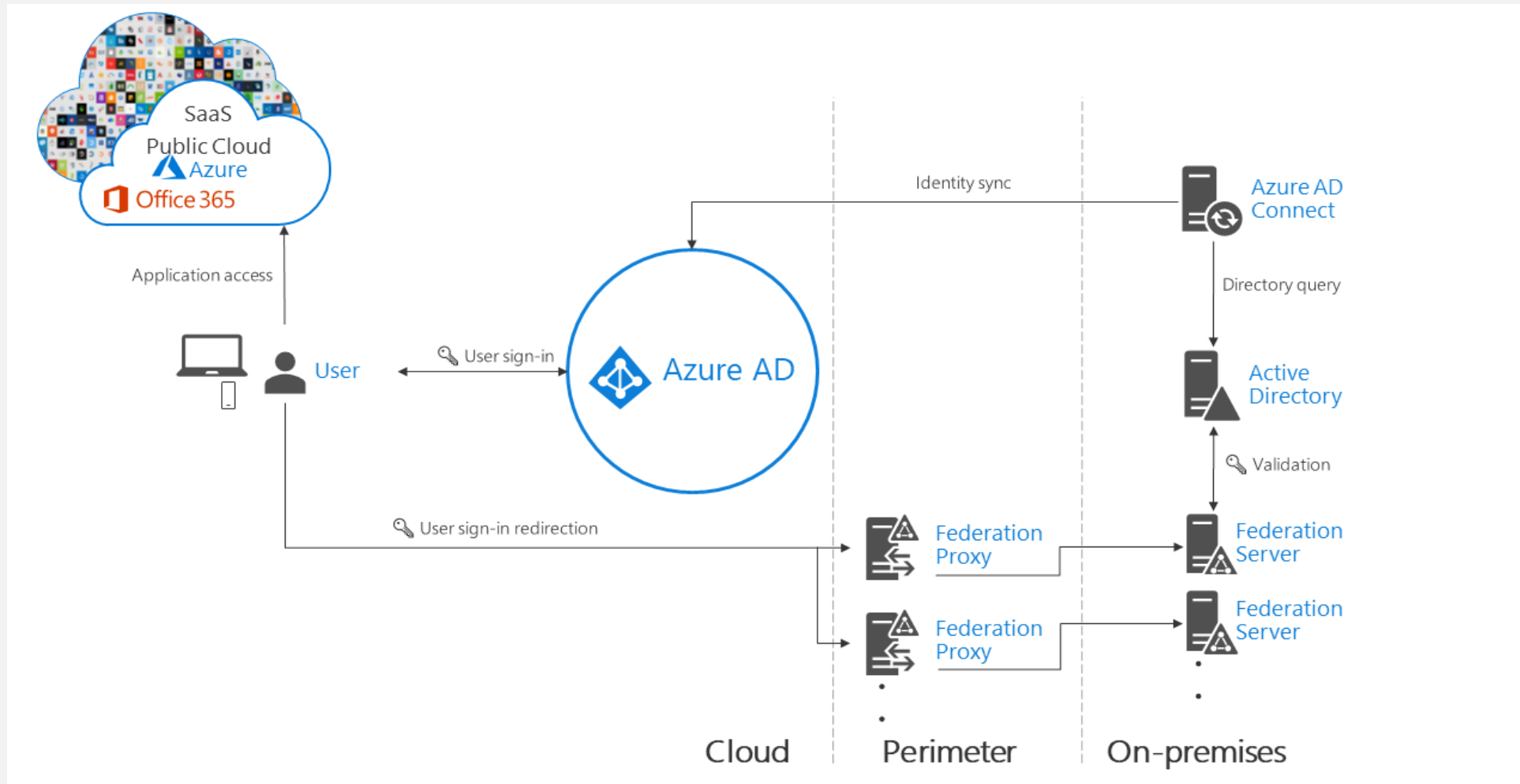
Hybrid Identity Authentication
Hybrid Authentication with Password hash sync (PHS)
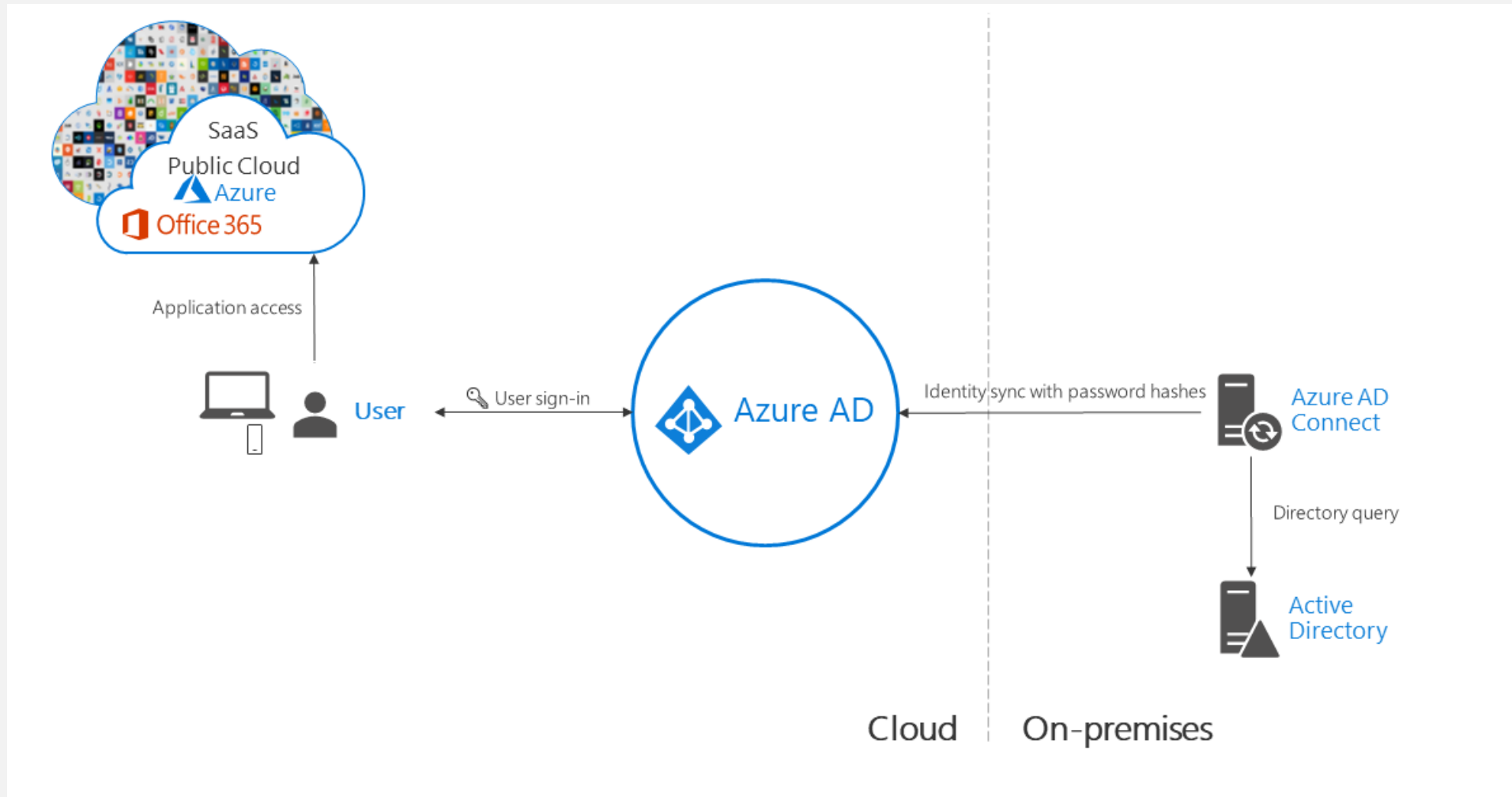
Hybrid Identity Authentication
Hybrid Authentication with Pass-trough Authentication (PTA)
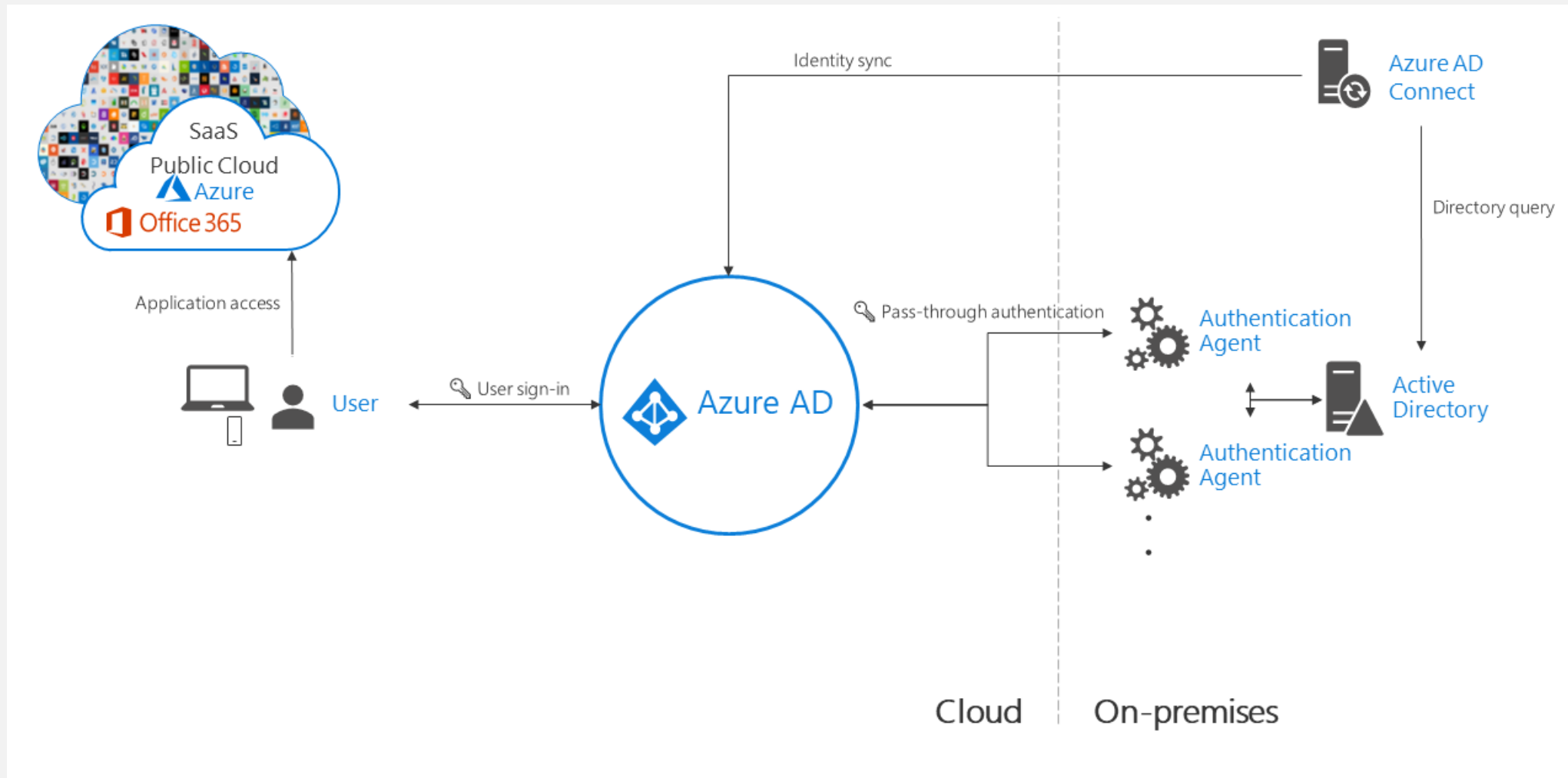
Hybrid Identity Authentication
Hybrid Authentication & Seamless Single-Sign On (sSSO)

Source: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso
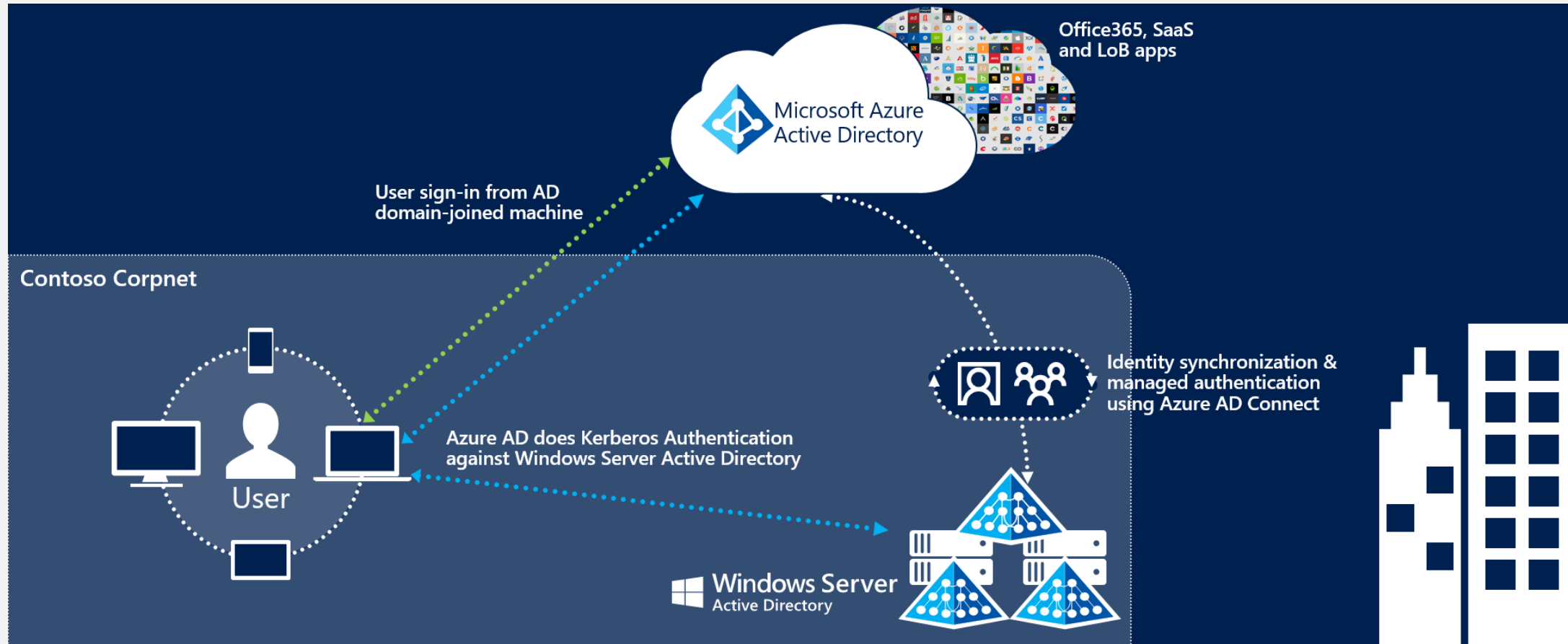
Hybrid Identity Authentication
Weakness of Seamless SSO (sSSO)

- Kerberos (Silver Ticket) Attacks to AZUREADSSOACCT

- Limitation of sSSO Kerberos Encryption types
  - *"Seamless SSO uses the **RC4_HMAC_MD5** encryption type for Kerberos. Disabling the use of the **RC4_HMAC_MD5** encryption type in your Active Directory settings will break Seamless SSO."*
    Source: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/tshoot-connect-sso#manual-reset-of-the-feature&quot

- Roll over the Kerberos decryption key (min. every 30 days)
  Update-AzureADSSOForest (Automated rollover in work)

- 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

- ✓ PTA: Configure „Smart Lockout Policy" and consider your AD lockout policy

- ✓ Move „change password" and „self-service password reset" (SSPR) process to Azure AD or implement "Azure AD Password Protection"
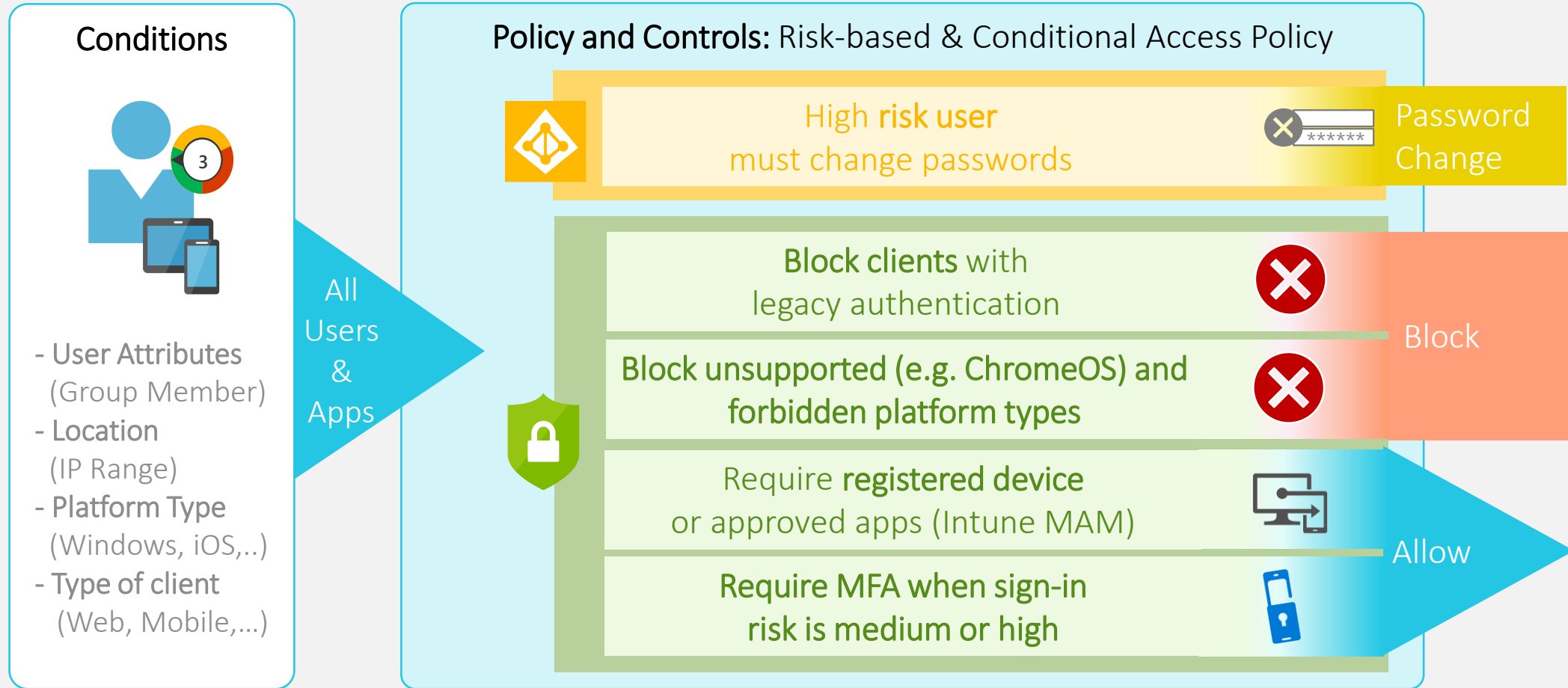
Hybrid Identity Protection

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 device**
or approved apps (Intune MAM)

Require MFA when sign-in
risk is medium or high

Allow

Hybrid Identity Protection
Microsoft's recommendation on Conditional Access Policies

- Microsoft 365 „Golden Config"
  (recommendation on identity and device access configuration)

Protection level	Azure AD conditional access policies	Include	Exclude
Baseline	Require multi-factor authentication (MFA) when sign-in risk is *medium* or *high*	All users	Conditional access exclusion group
Sensitive	Require MFA when sign-in risk is *low, medium,* or *high*	Executive staff	Conditional access exclusion group
Highly regulated	*Always* require MFA	Top secret project X team	Conditional access exclusion group

Hybrid Identity Protection
Investigation on cloud authentication, cloud apps and on-premises

Azure AD Identity Protection
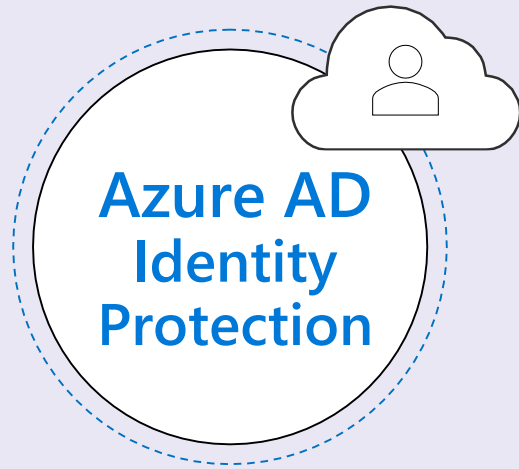
Risky sign-ins & User Risk

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

Hybrid Identity Protection
Unified SecOps Investigation of hybrid environments

Azure AD Identity Protection

Azure ATP

Microsoft Cloud app security
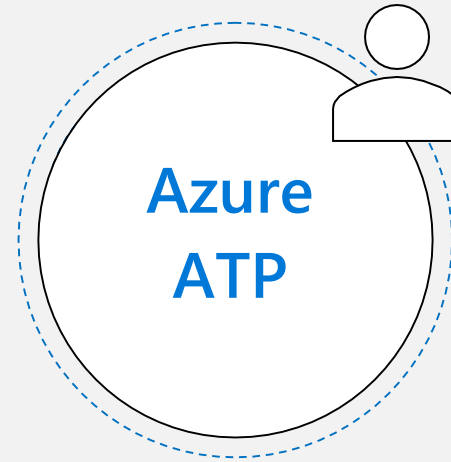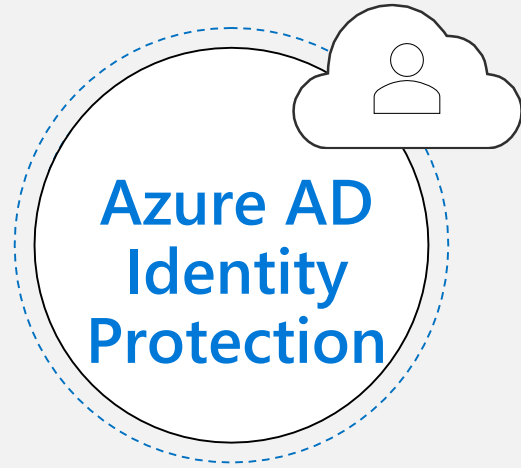
User and **E**ntity **B**ehavior **A**nalytics (UEBA)

Auteri 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
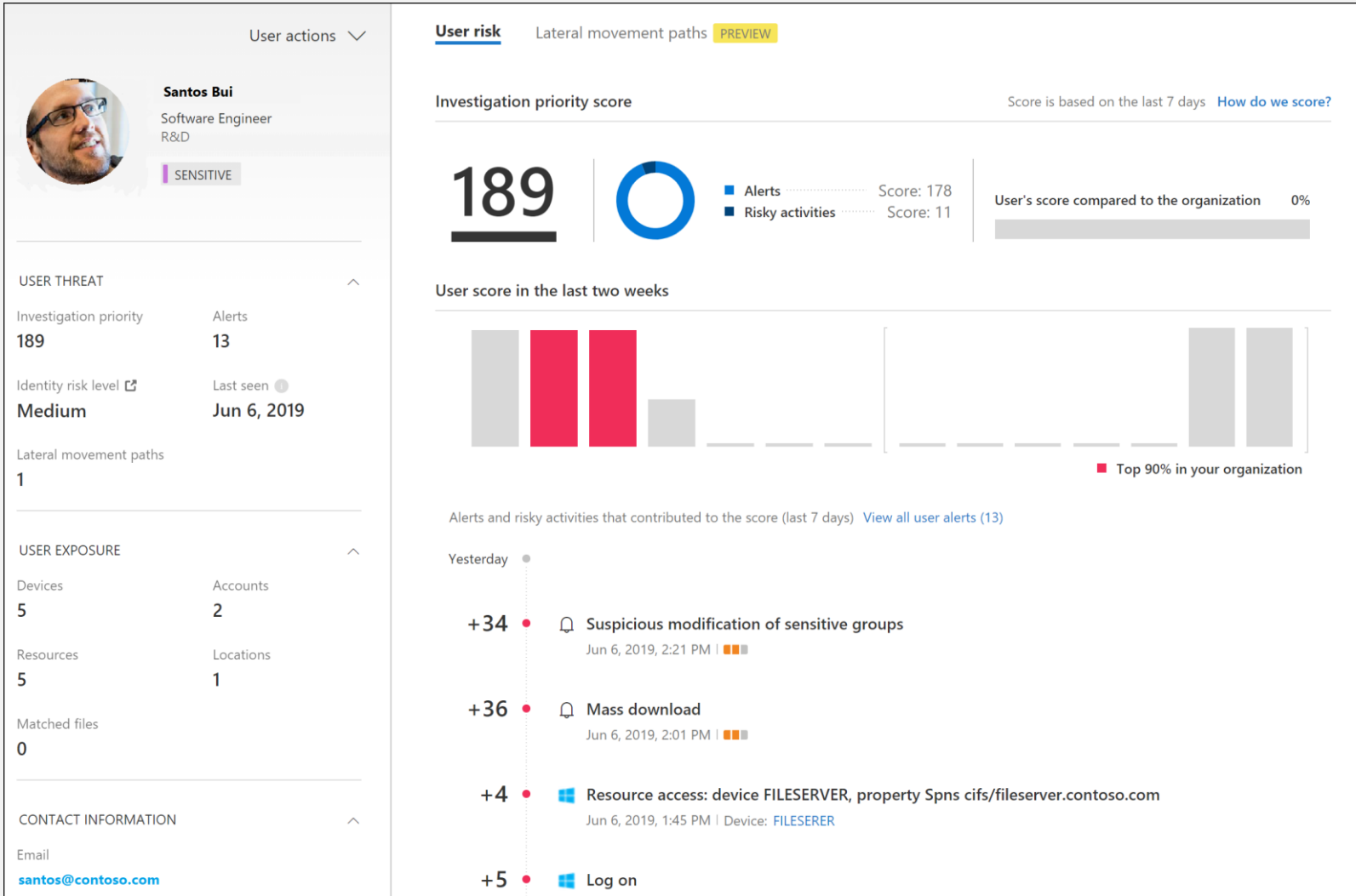
Hybrid Identity Protection
Checklist

✓ *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*

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

✓ Monitoring your audit, sign-in and security logs (part of your SecOps)
  → Plan an reporting and monitoring deployment
  → Integration in SIEM products or Microsoft's Azure Sentinel

Priviliged Identity Management in Azure AD

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 Enhanced Security Administrative Environment (ESAE)
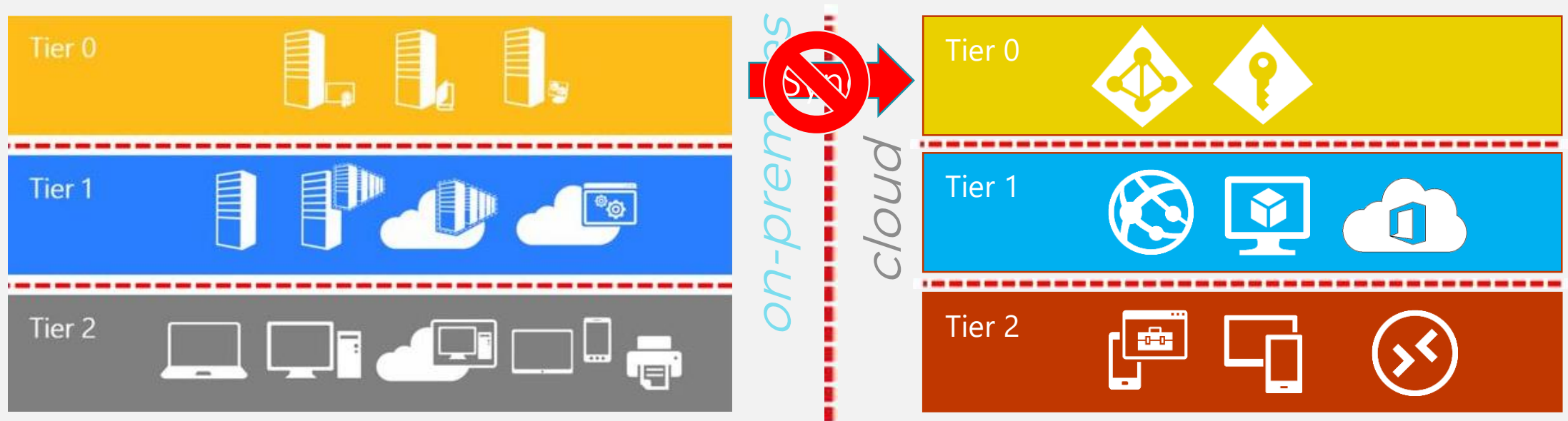
Priviliged Identity Management (PIM)
Design your Azure AD roles

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

Azure AD roles - Quick start
Cloud-Architekt.net

Overview

Quick start

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

My requests

Approve requests

Review access

Manage

Roles

Members

Alerts

Access reviews

Wizard

Settings

Activity

Directory roles audit history

My audit history

Troubleshooting + Support

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 so that you can get limited standing access to the privileged identity

Activate your role

Approve

Hands-on:
Break Glass &
Privileged
Identities

Priviliged Identity Management
Checklist

✓ *Built your Azure and Azure AD RBAC model with least privilege*

✓ *Adapt 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

Thank You

- @Thomas_Live

- ✉ Thomas@Naunheim.net
- 🔗 www.cloud-architekt.net