



Azure AD Hybrid Identity Design and Security

Thomas Naunheim

Glasgow Azure User Group, 28th August 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

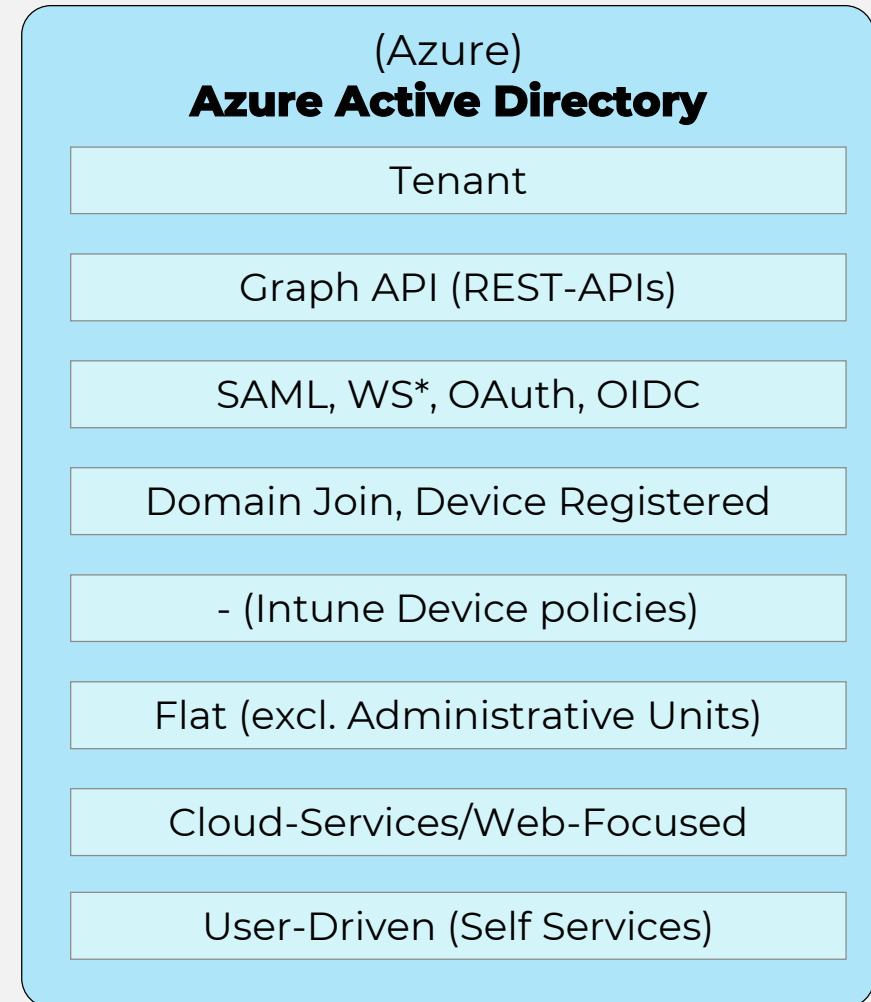
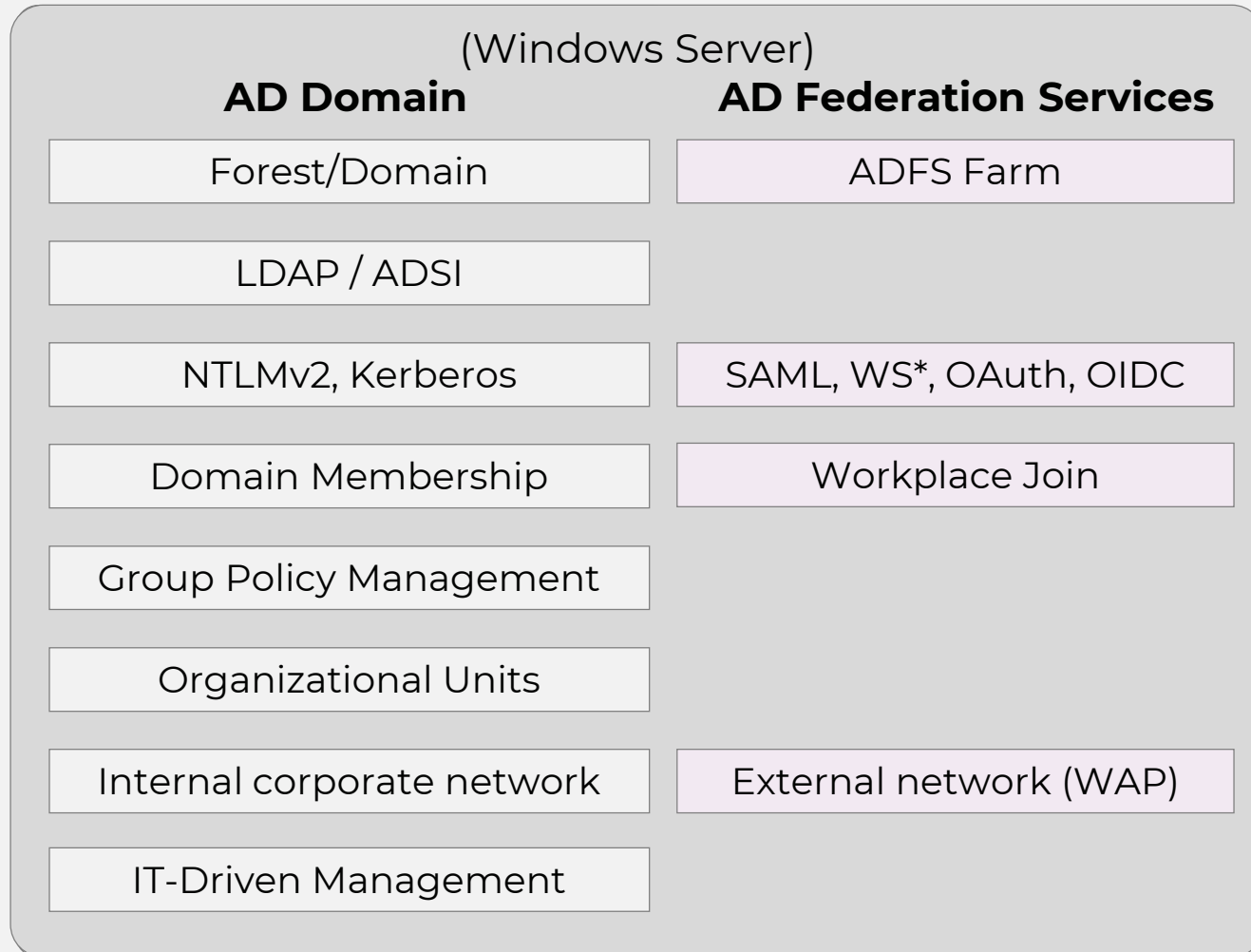
Azure Active Directory

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	

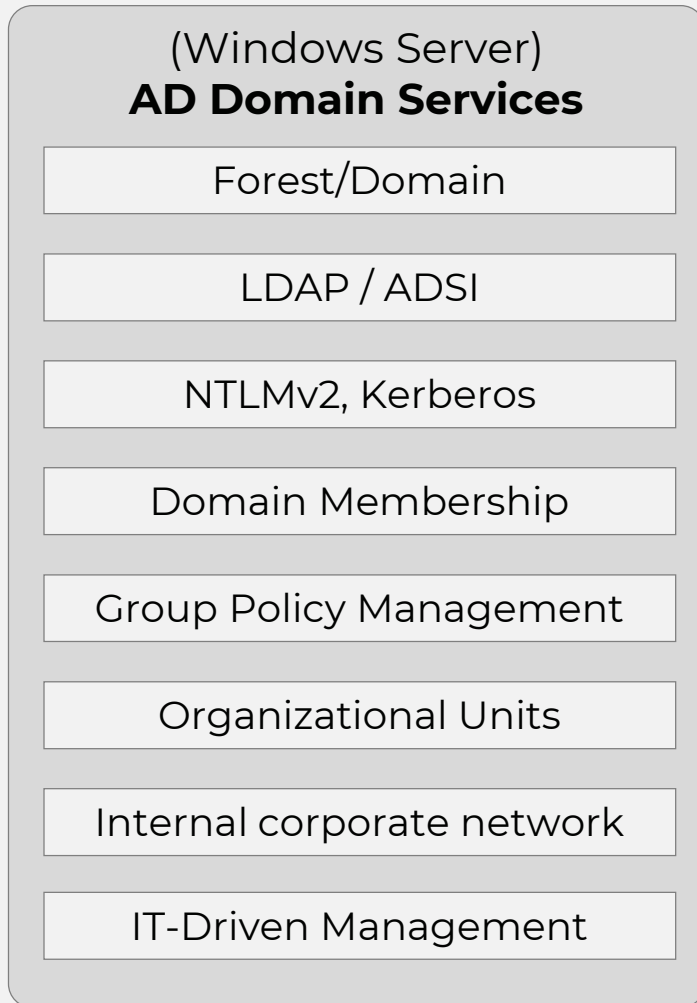
Azure Active Directory

Active Directory in Azure?



Azure Active Directory

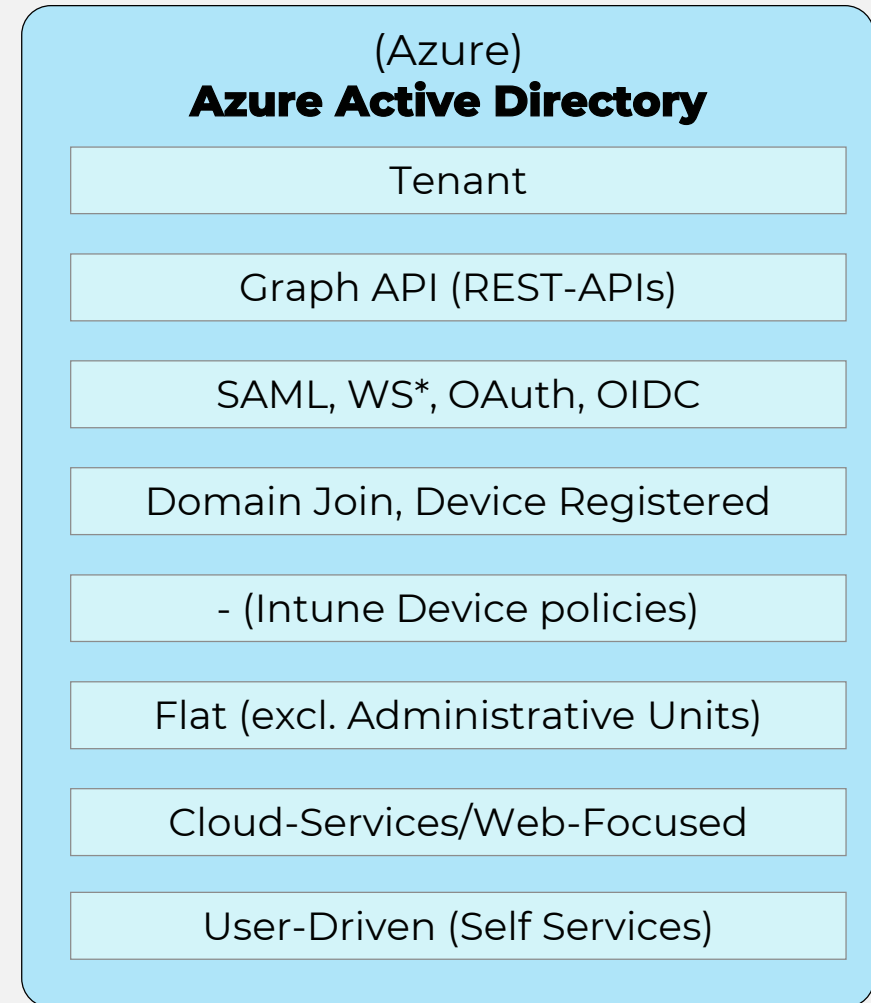
Active Directory in Azure?



Options for lift-and-shift:

1. Full Control of AD = Domain Controllers as IaaS
2. Managed AD in Azure* = Azure AD Domain Services
3. Managed AD in AWS* = AWS Managed Microsoft AD

*Limited functionality and [comparison](#) of features strongly recommended



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)? Where [is my data located](#)?

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

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...

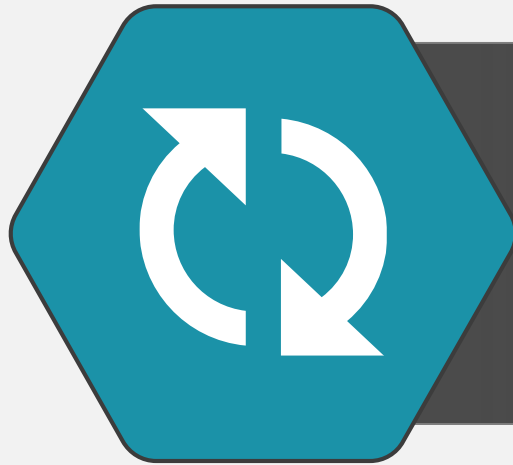
NAME	SCORE IMPACT
Require MFA for Azure AD privileged roles	50
Require MFA for all users	30
Do not allow users to grant consent to unma...	0
Designate fewer than 5 global admins	0

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 Active Directory

Different user types



Member (Work accounts)

- Cloud-only or synchronized (hybrid) identities of your organization
- Prevent usage of Personal Accounts (Microsoft Accounts)



Guest (B2B User accounts)

- Invited external users with Azure AD/MSA accounts or from [federated IDPs](#)
- [Synchronized partner accounts](#) from on-premises AD



Break Glass (Emergency accounts)

- [Guidelines](#) for managing emergency access accounts (“break glass”)

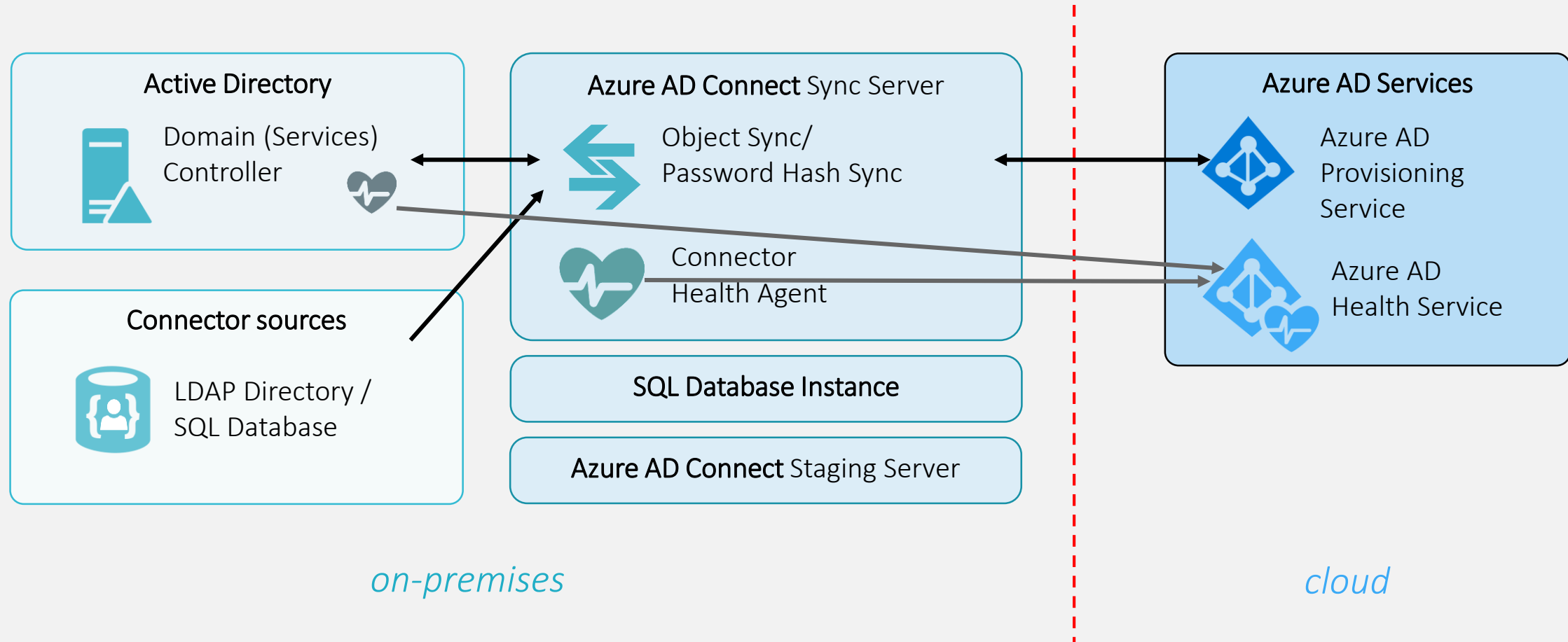


Privileged accounts

- Separated accounts (cloud-only) for administrative tasks

Azure AD Connect Synchronization

Architecture and components of „Identity bridge“



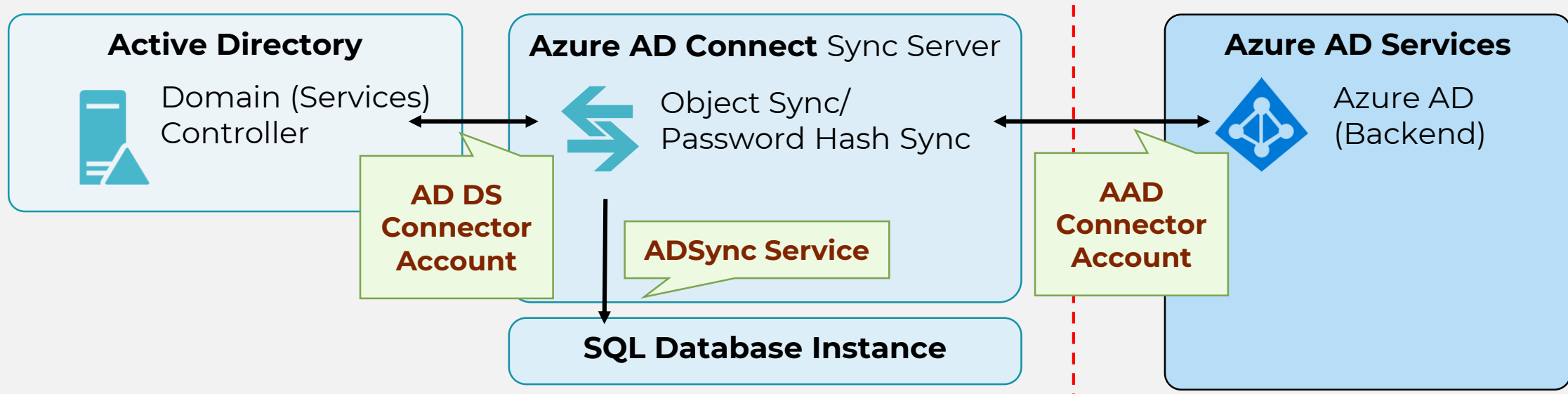
Azure AD Connect Synchronization

Design decisions and prerequisites (before implementing)

- Placing of Azure AD connect, PTAs servers and databases
 - Supported options for “High availability” of PTA and SQL cluster
- Required internet connectivity (direct / proxy)
 - Running tests with „AADConnect-CommunicationsTest.ps1“
- Review of the [synced attributes](#), filtering and write-back options
- Identity lifecycle and security use cases that needs to be validated
 - Example: [Expired user password](#), [nested \(AD\) groups](#), [Force password reset](#)
- [IDFix](#) to prepare and check directory objects and attributes

Azure AD Connect Synchronization

Hardening of Azure AD Connect

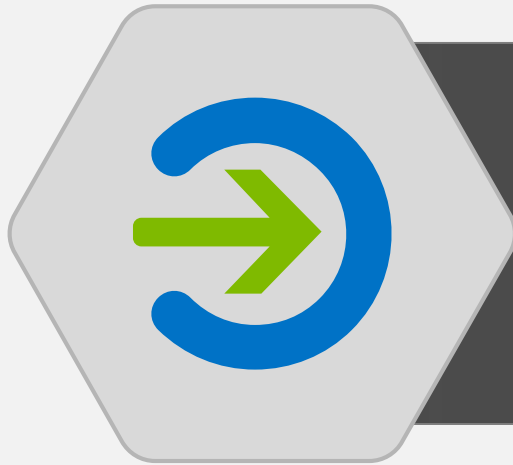


- ◆ Pre-created service accounts and [delegated permissions](#) (based on your user scope/filter and write-backs attributes)
 - ◆ AD Sync service accounts as “Group Managed Service Account”
 - ◆ [Security advisory](#) for AD DS connect service account

Hybrid Identity Synchronization

Checklist

- ✓ *Least privilege and write-scope of AD DS Connector account*
- ✓ *Monitor your synchronization with Azure AD Connect Health*
- ✓ Protect your hybrid identity components AND database (as well as DCs/Tier0-systems)
- ✓ Monitor your application and security logs on all AADC-related servers
- ✓ Use „Azure AD Connect [Config Documenter](#)“ (compare configuration)



Hybrid Identity Authentication



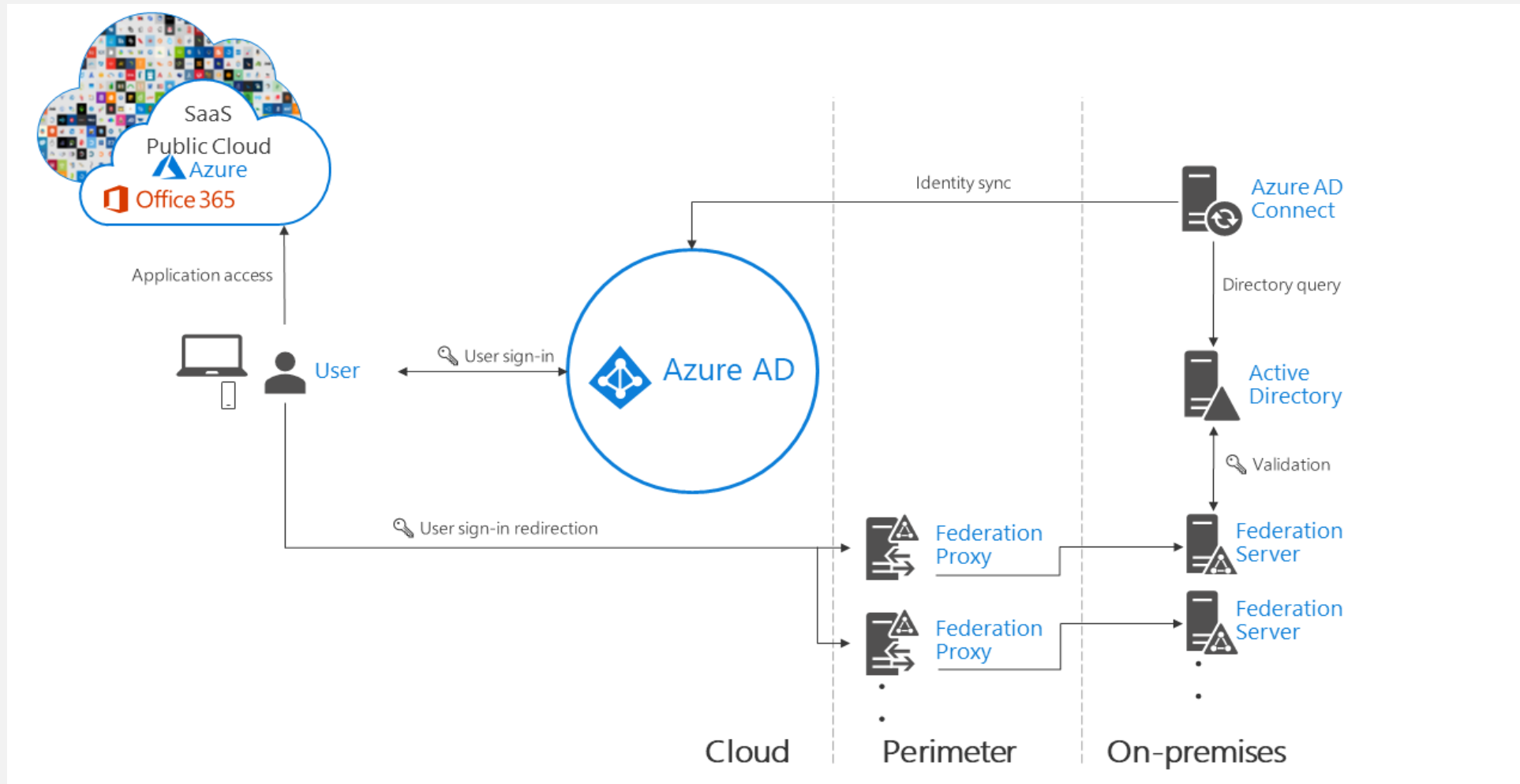
Hybrid Identity Authentication

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](#))?

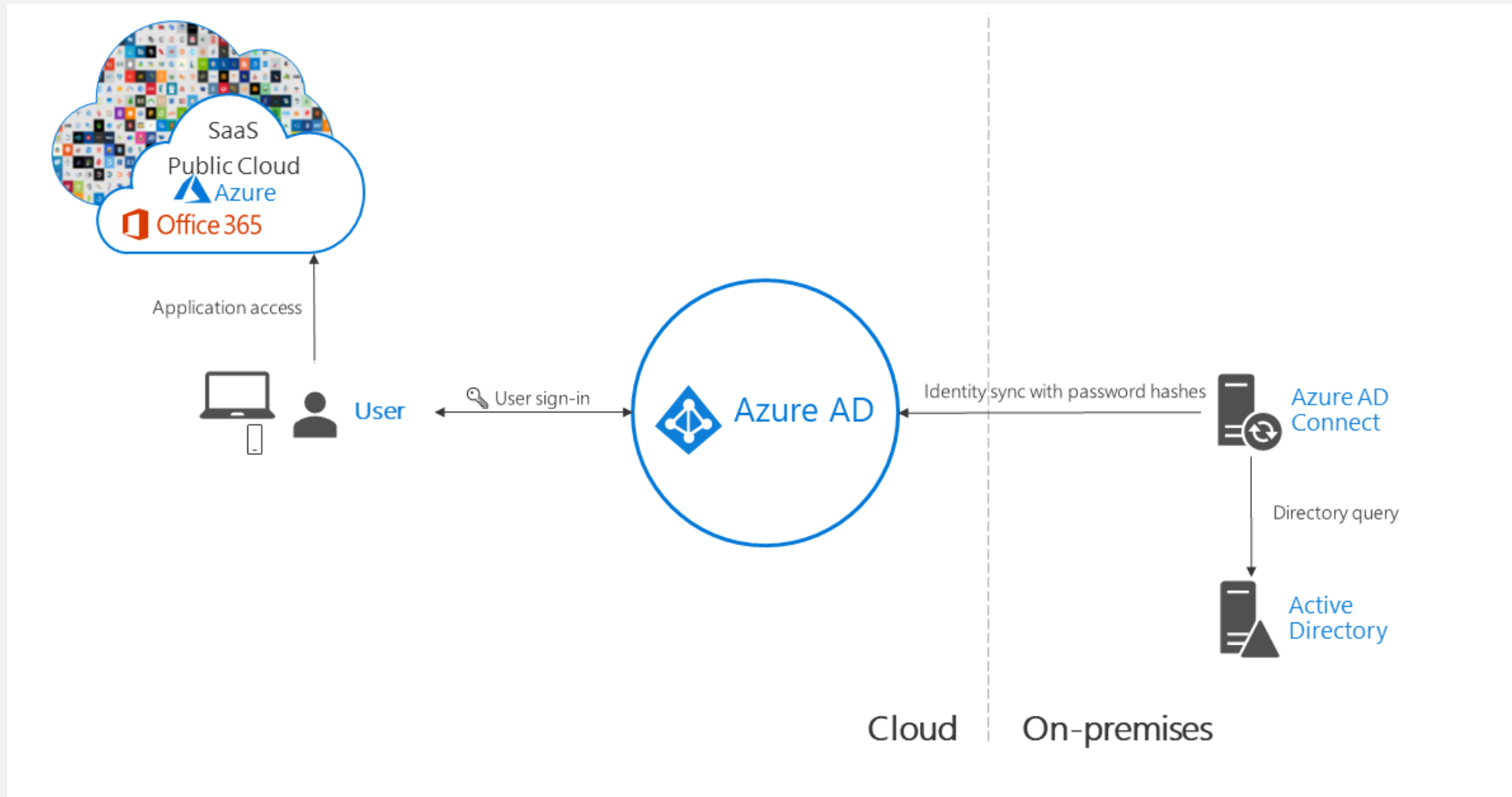
Hybrid Identity Authentication

Hybrid Authentication with Federation Services (AD FS)



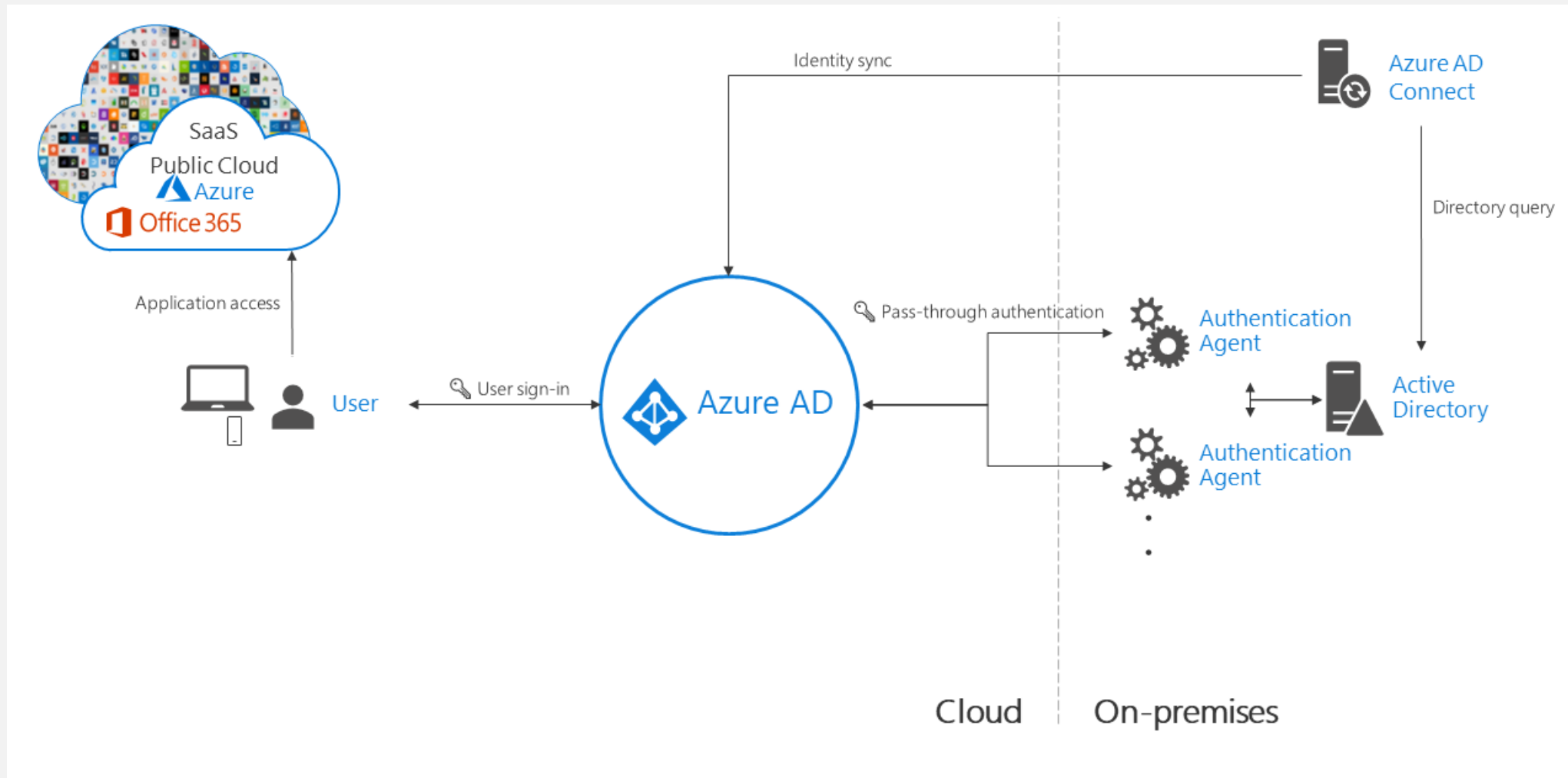
Hybrid Identity Authentication

Hybrid Authentication with Password hash sync (PHS)



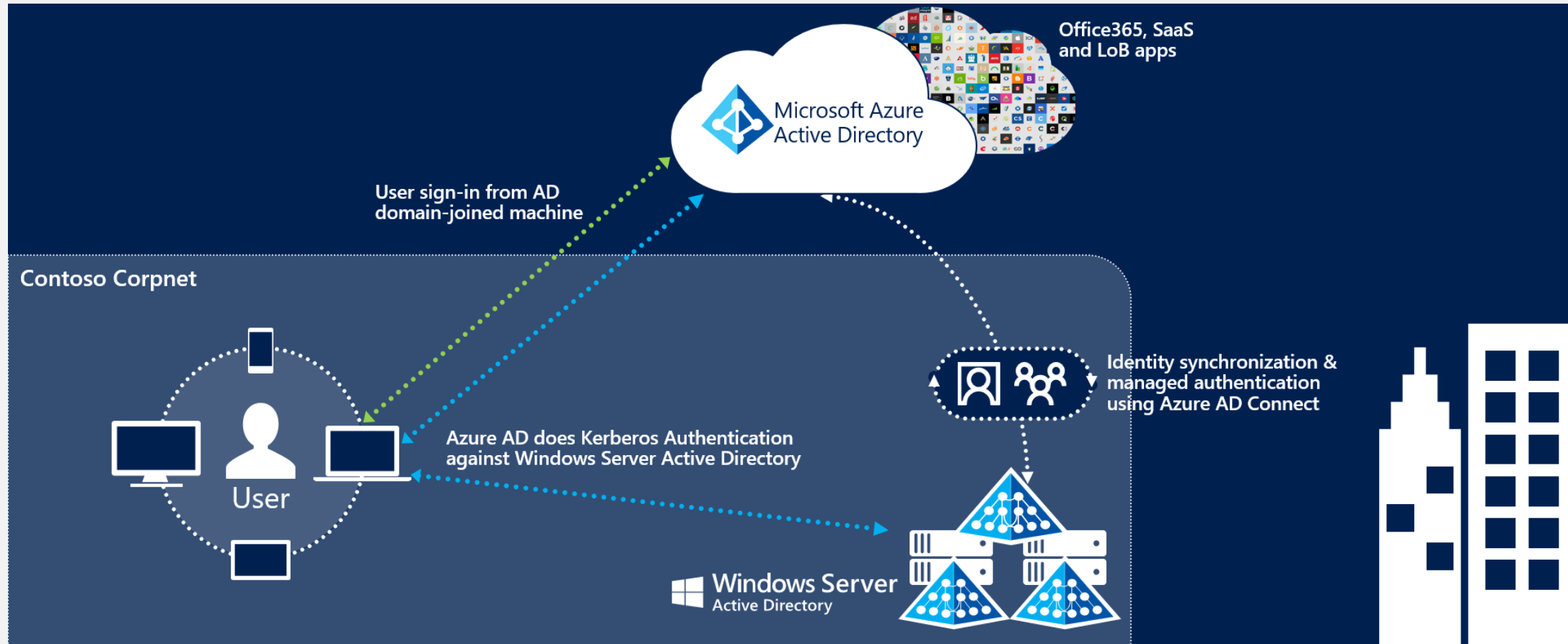
Hybrid Identity Authentication

Hybrid Authentication with Pass-through Authentication (PTA)



Hybrid Identity Authentication

Hybrid Authentication & 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
 - *“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>
- 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*
- ✓ PTA: Configure „[Smart Lockout Policy](#)“ and consider your AD lockout policy
- ✓ Enable all users to register MFA and SSPR information
- ✓ Move „change password“ and „self-service password reset“ (SSPR) process to Azure AD or implement „[Azure AD Password Protection](#)“

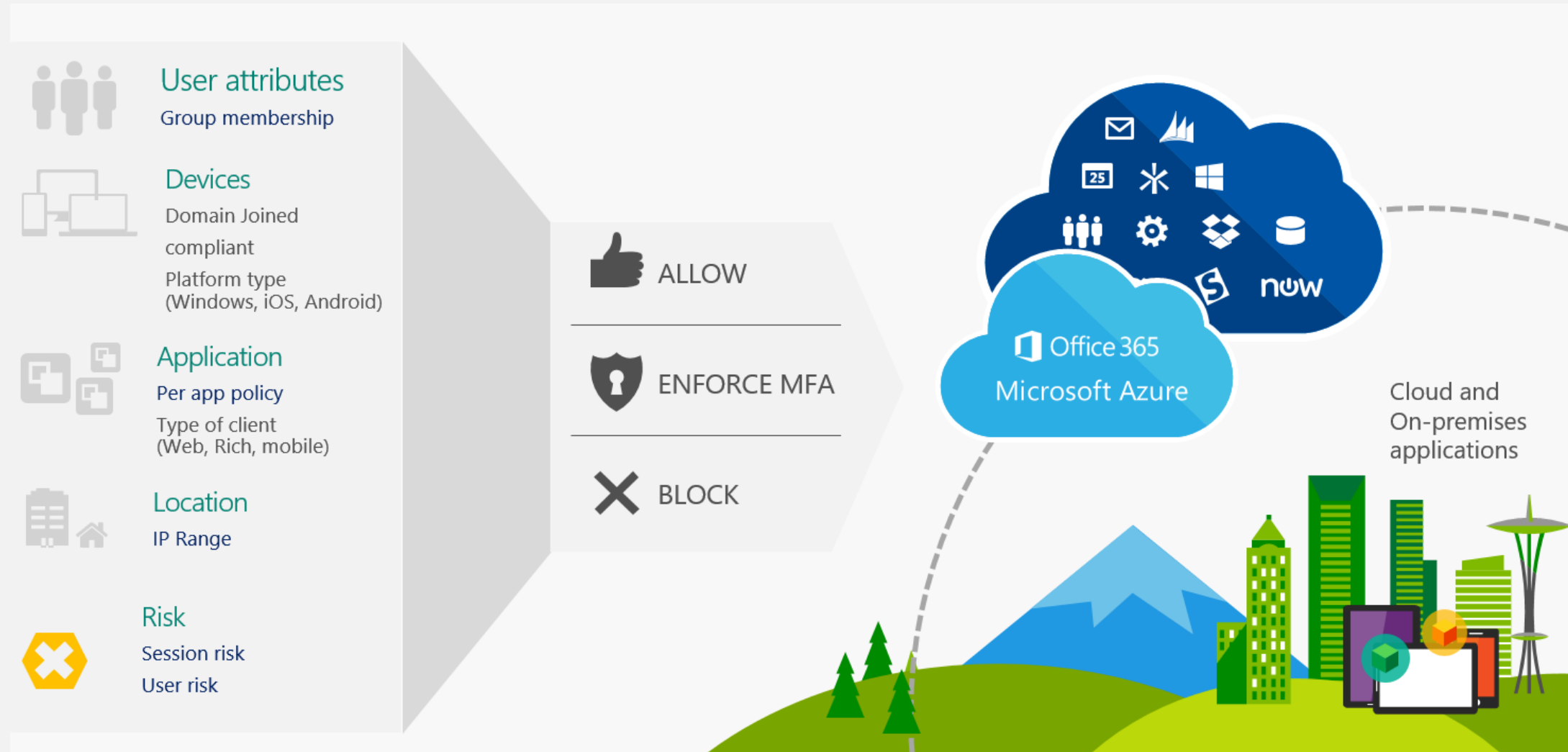


Hybrid Identity Protection









Hybrid Identity Protection

Zero Trust approach with Conditional Access Policies



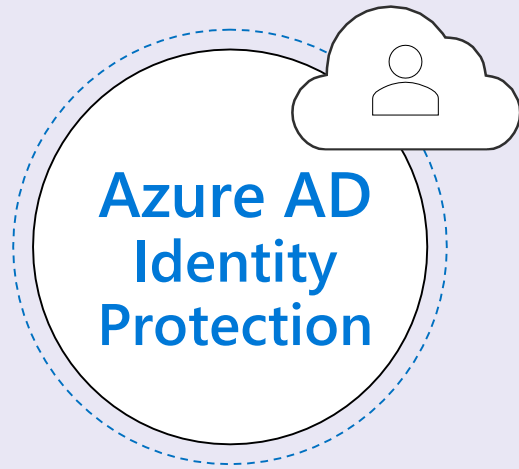
Hybrid Identity Protection

Microsoft's "Golden" Config (aka.ms/M365GoldenConfig)

Protection level	Device type	Azure AD conditional access policies			Azure AD Identity Protection user risk policy	Intune device compliance policy	Intune app protection policies
Baseline		Require multi-factor authentication (MFA) when sign-in risk is <i>medium</i> or <i>high</i>		Block clients that don't support modern authentication (Clients that do not use modern authentication can bypass conditional access rules, so it's important to block these)	Require compliant PCs	High risk users must change password (Forces users to change their password when signing in if high risk activity is detected for their account)	Define compliance policies (One policy for each platform)
			Require approved apps (Enforces mobile app protection for phones and tablets)				Define app protection policies (One policy per platform — iOS, Android)
Sensitive		Require MFA when sign-in risk is <i>low</i> , <i>medium</i> , or <i>high</i>			Require compliant PCs <i>and</i> mobile devices (Enforces Intune management for PCs and phone/tablets)		
							
Highly regulated		Always require MFA					
							

Hybrid Identity Protection

Investigation on cloud authentication, cloud apps and on-premises



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



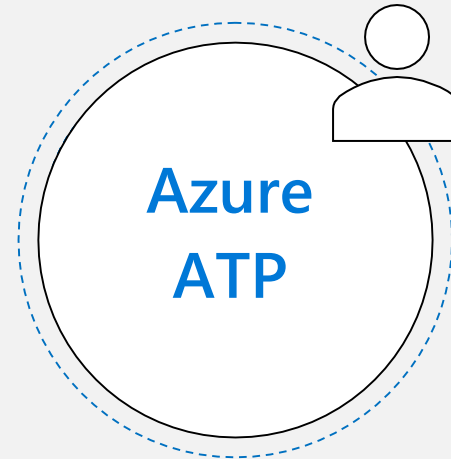
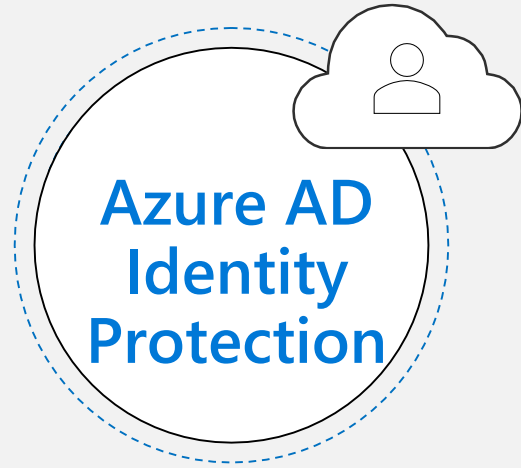
Behavior across
cloud apps

Activity from
infrequent country

Data exfiltration
to unsanctioned apps

Hybrid Identity Protection

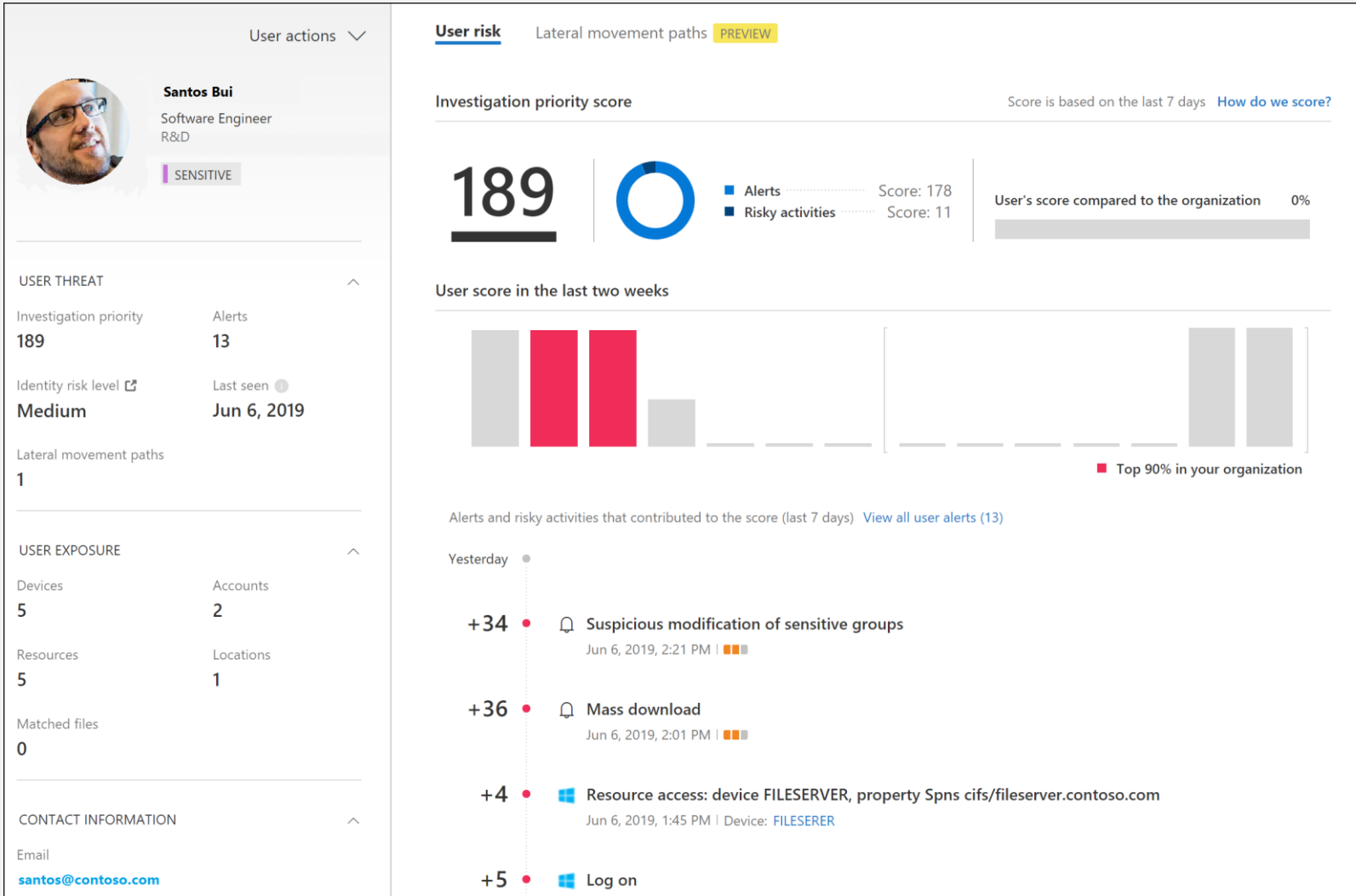
Unified SecOps Investigation of hybrid environments



User and Entity Behavior Analytics (UEBA)

Auditing and Monitoring of Azure Active Directory

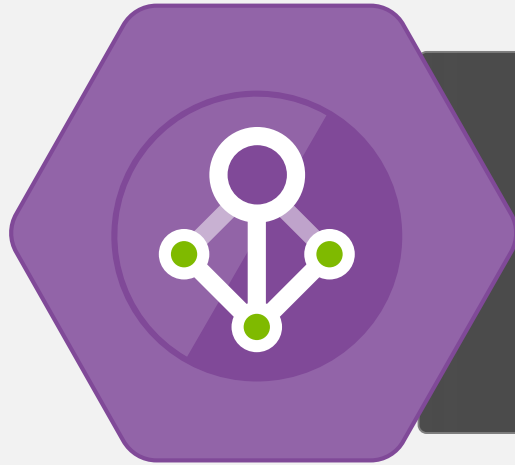
Investigation Priority built on User and Entity Behavior Analytics



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



Privileged Identity Management in Azure AD

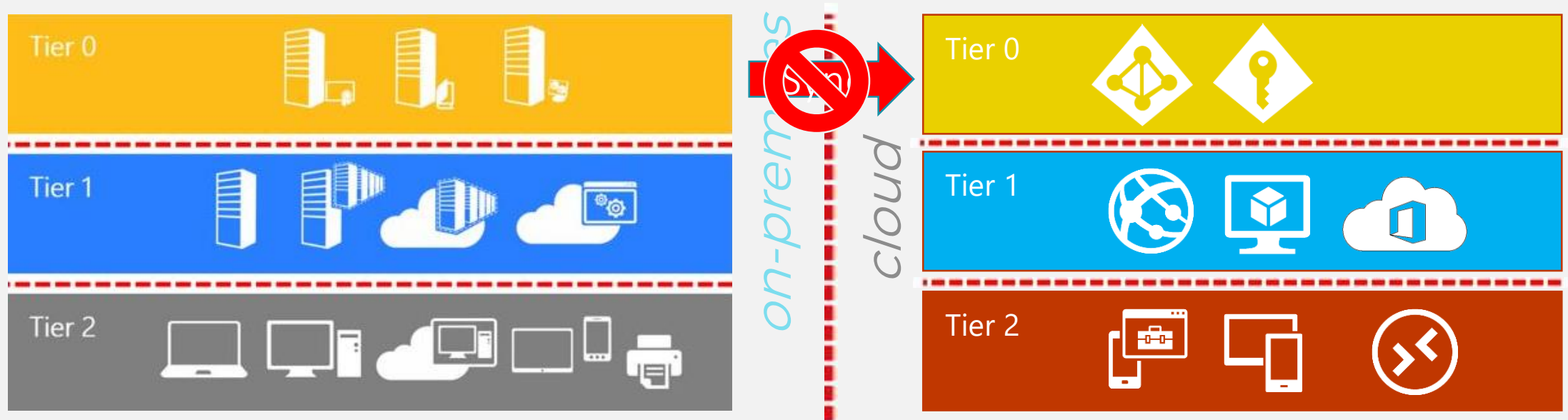



Privileged Identity Management (PIM)

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](#) = Red Forest)



 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](#)



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](#)



Approve


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

My requests

 Approve requests

 Review access

Manage

 Roles

 Members

 Alerts


 Access reviews

 Wizard

 Settings

Activity

 Directory roles audit history

 My audit history

Troubleshooting + Support

Hands-on: Break Glass & Privileged Identities

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

Consideration on default directory roles / least privileges


- Intune Service administrator has the permission to modify security group


Privileged 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