DICE

Debeka Innovation Center

Azure Active Directory Implementation

Architecture, Design Considerations and Hybrid Identity

Thomas Naunheim

Cloud Architect

#AzureOps

#Koblenz

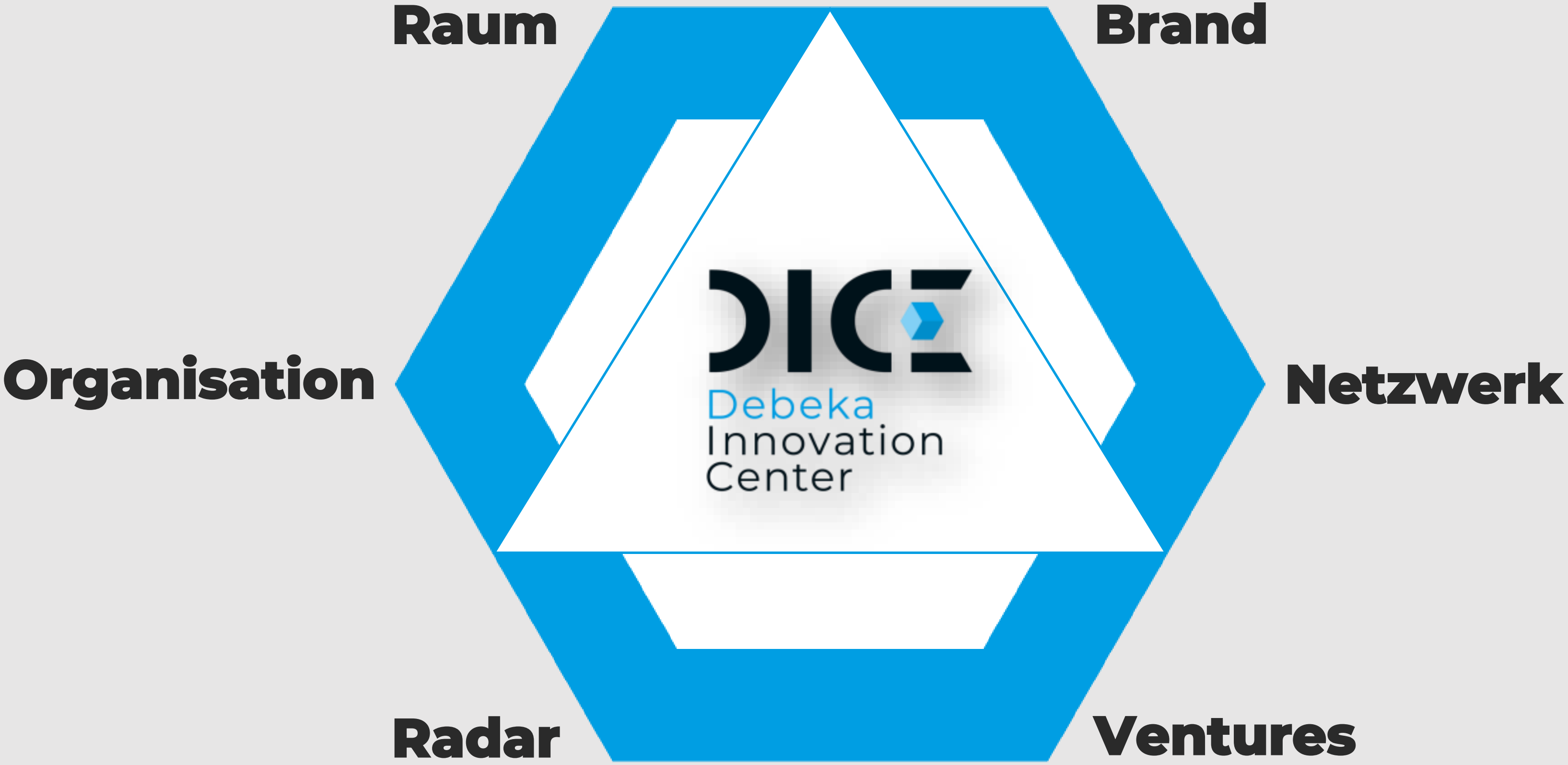
#NeverStop Learning

„Thomas erprobt und entwickelt cloudbasierte IT–Lösungen und unterstützt hierbei agile Projekte.“

@Thomas_Live

Mit Talenten über agile Projekte zur Innovation!

Warum?



Raum

Brand

Organisation

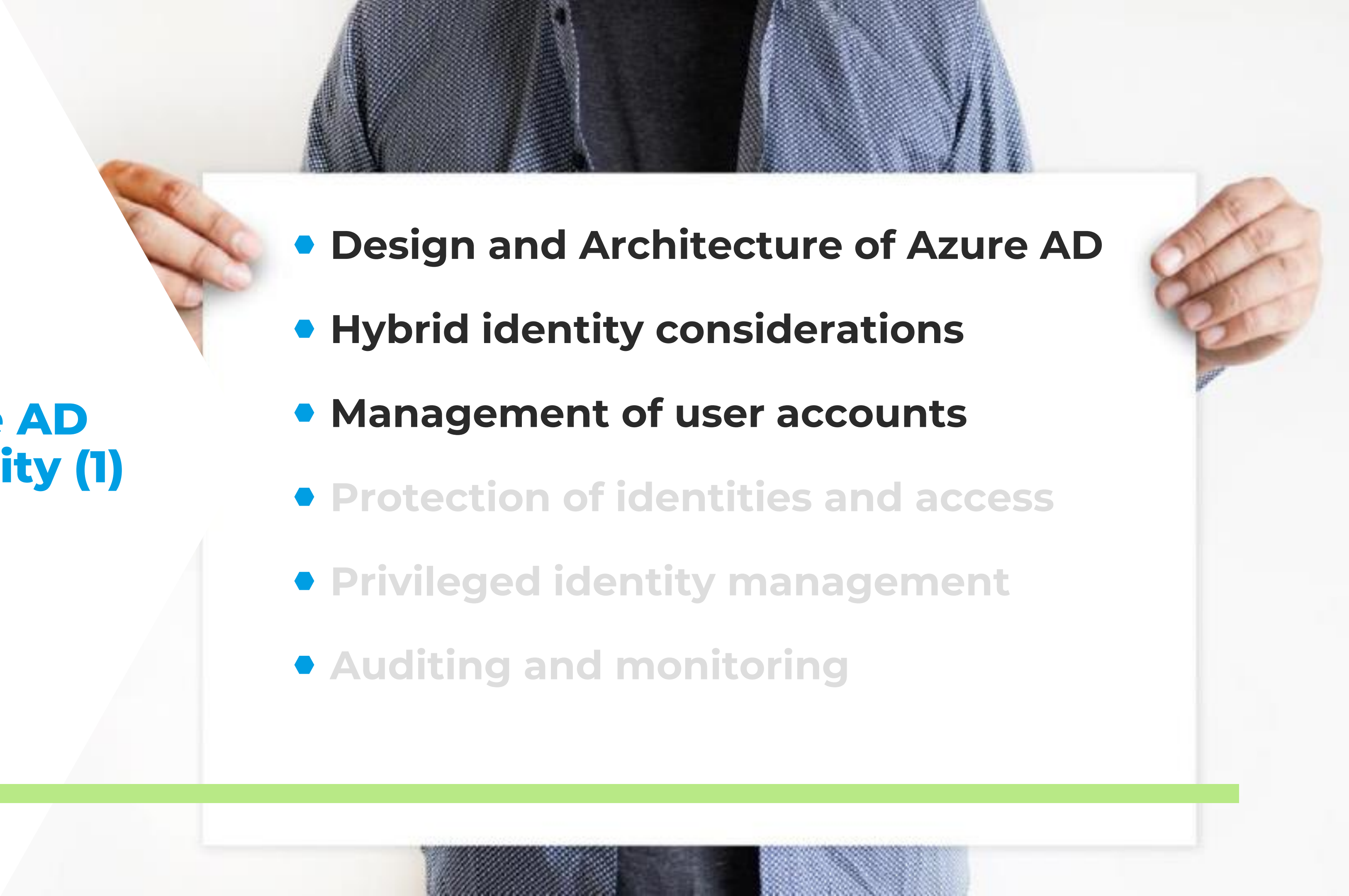
Netzwerk

Radar

Ventures

DICE
Debeka
Innovation
Center

Warum?



Azure AD Security (1)

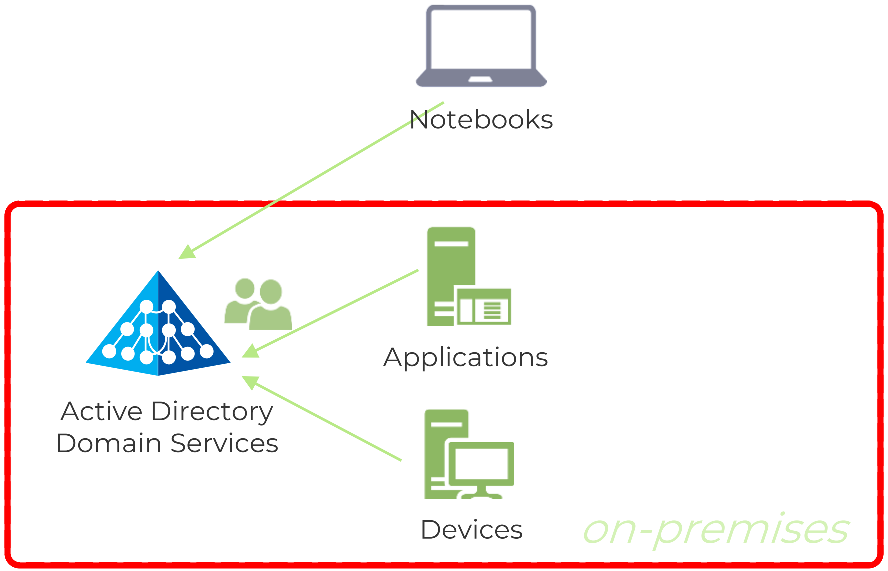
- Design and Architecture of Azure AD
- Hybrid identity considerations
- Management of user accounts
- Protection of identities and access
- Privileged identity management
- Auditing and monitoring

Welche Erfahrung habt Ihr bereits mit Azure AD?

Design and Architecture of Azure Active Directory

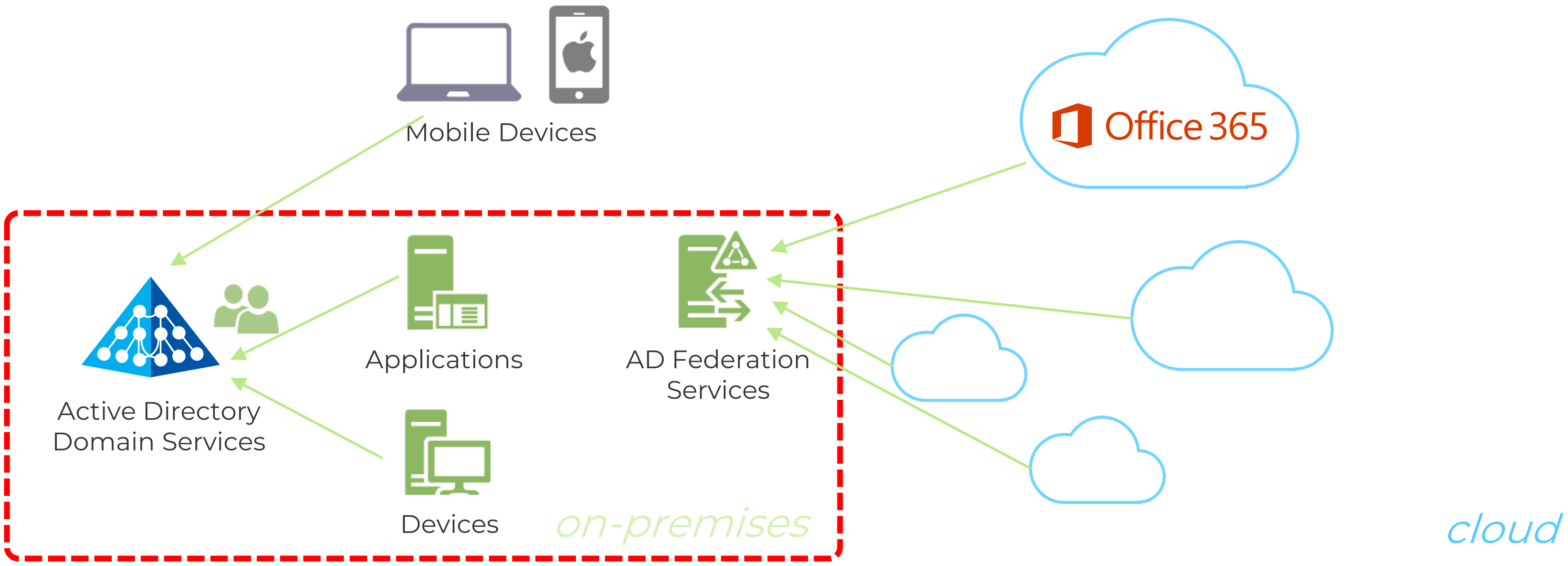
Design and Architecture of Azure AD

Transformation of identity and security perimeter



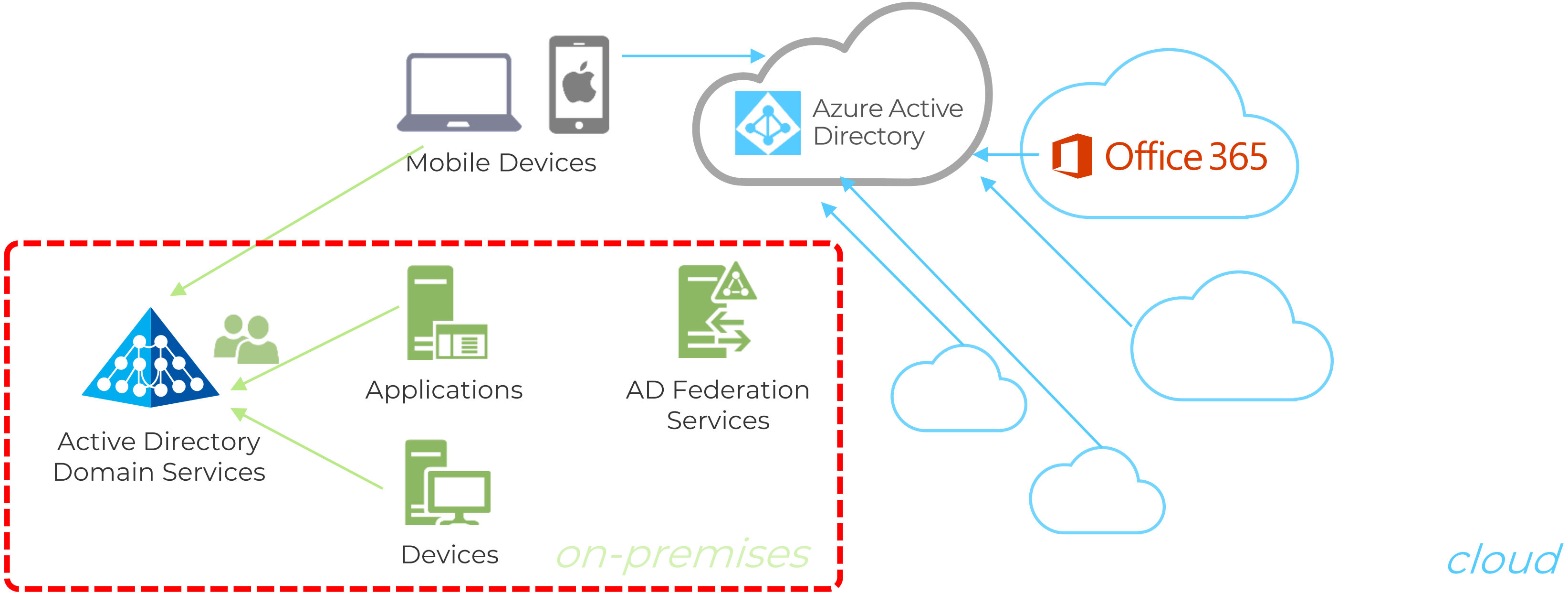
Design and Architecture of Azure AD

Transformation of identity and security perimeter



Design and Architecture of Azure AD

Transformation of identity and security perimeter



Design and Architecture of Azure AD

Legacy and Modern Management, Protocols and APIs

(Windows Server)		(Azure)
AD Domain	**AD Federation Services**	**Azure Active Directory**
Forest/Domain	ADFS Farm	Tenant
LDAP / ADSI		Graph API (Rest-APIs)
NTLMv2, Kerberos	SAML, WS*, OAuth, OIDC	SAML, WS*, OAuth, OIDC
Domain Membership	Workplace Join	Domain Join, Device Registered
Group Policy Management		- (Intune Device policies)
Organizational Units		Flat (excl. Administrative Units)
Internal corporate network	External network (WAP)	Cloud-Services/Web-Focused
IT-Driven Management		User-Driven / SSPR-Features

Design and Architecture of Azure AD

Legacy and Modern Management, Protocols and APIs

(Windows Server) **AD Domain Services**	(Azure) **Azure Active Directory**
Forest/Domain	Tenant
LDAP / ADSI	Graph API (Rest-APIs)
NTLMv2, Kerberos	SAML, WS*, OAuth, OIDC
Domain Membership	Domain Join, Device Registered
Group Policy Management	- (Intune Device policies)
Organizational Units	Flat (excl. Administrative Units)
Internal corporate network	Cloud-Services/Web-Focused
IT-Driven Management	User-Driven / SSPR-Features

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

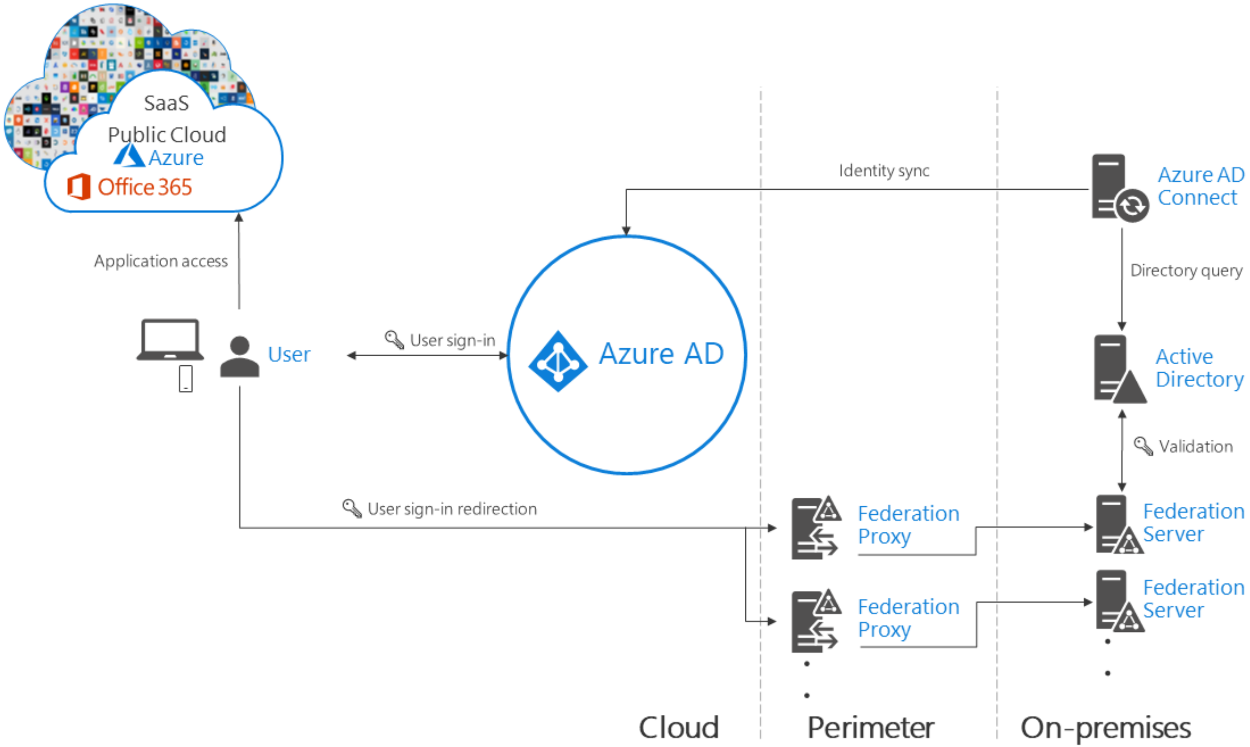
Design and Architecture of Azure AD

Cloud Identity models

- **Cloud Identity**
  - Independent identity, no synchronization with on-premises IAM
  - Separated user lifecycle in Azure Active Directory
- **Federated Identity**
  - Hybrid identity, authentication redirected to AD Federation Services
  - SSO with high-flexibility, security and operational workloads on-premises
- **Synchronized Identity**
  - Hybrid identity, password (hashes) are synced and handled by Azure AD
  - Enabling SSO with Hybrid WHfB or Seamless SSO

Design and Architecture of Azure AD

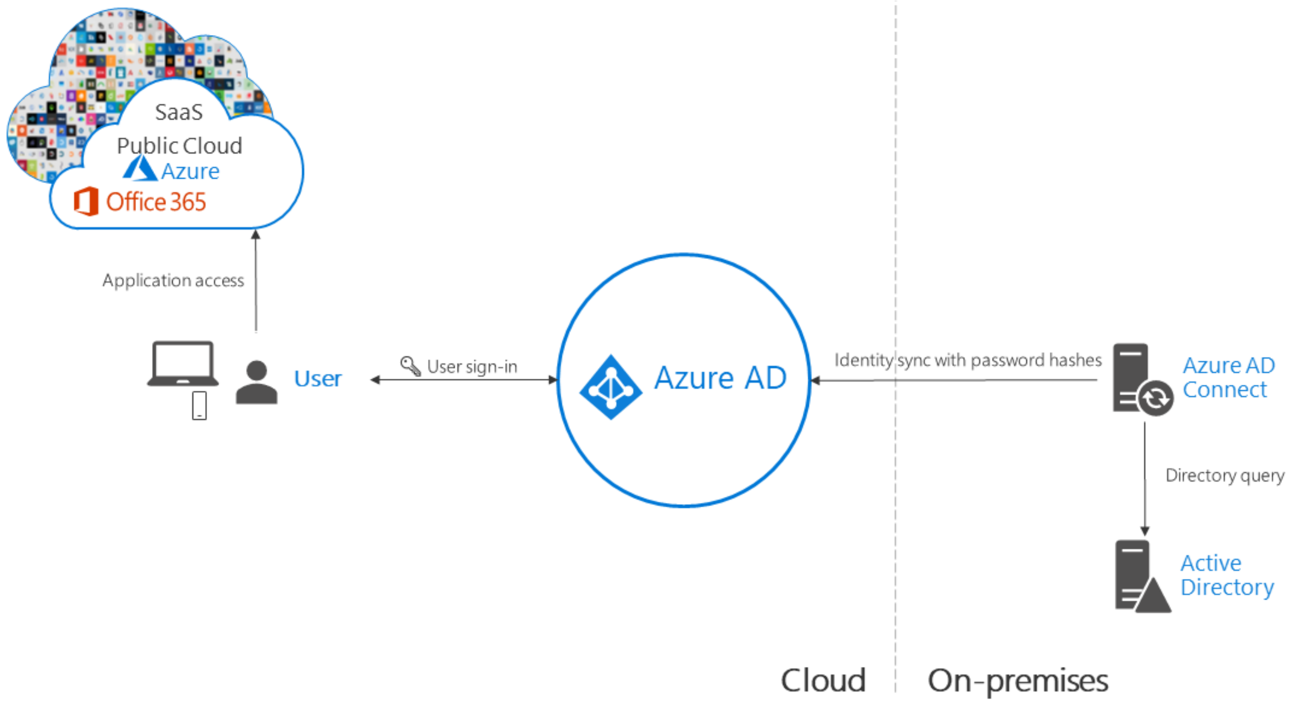
Hybrid Authentication with Federation Services (AD FS)



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

Design and Architecture of Azure AD

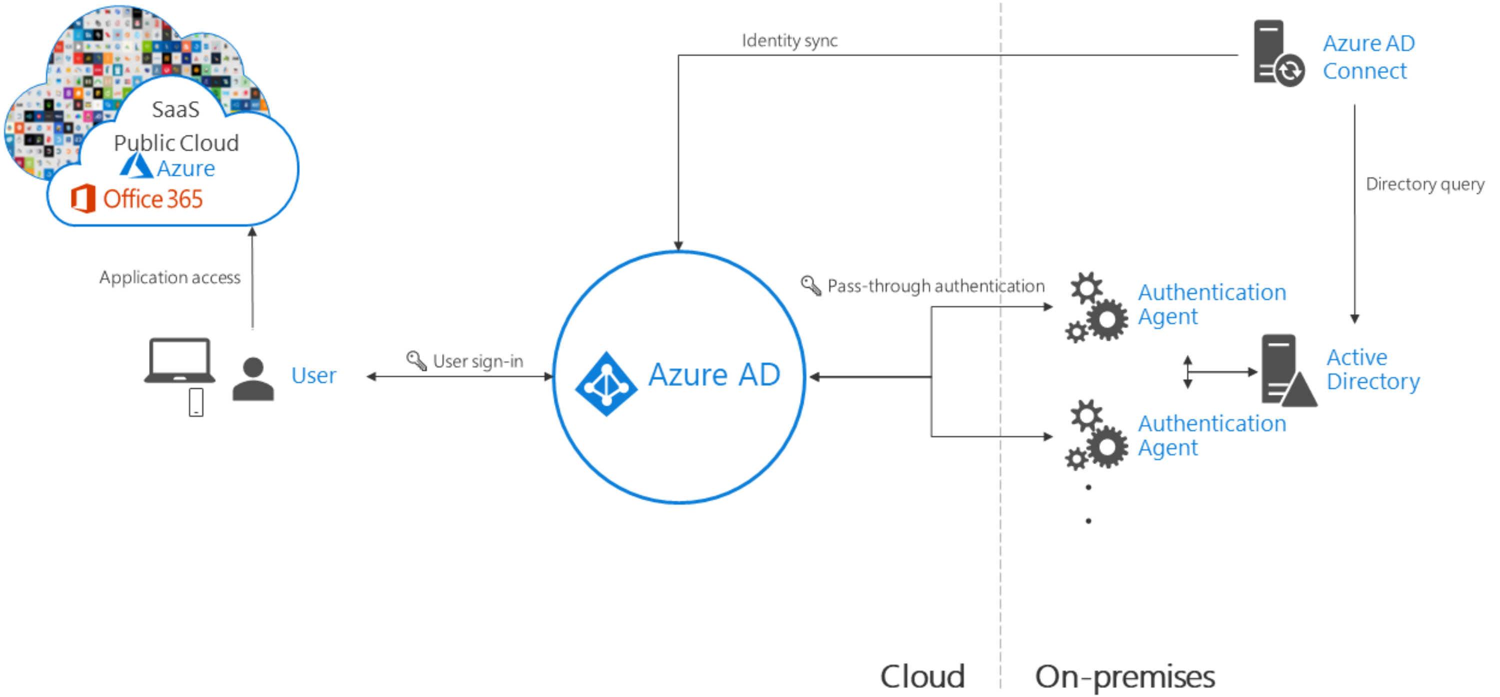
Hybrid Authentication with Password hash sync (PHS)



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

Design and Architecture of Azure AD

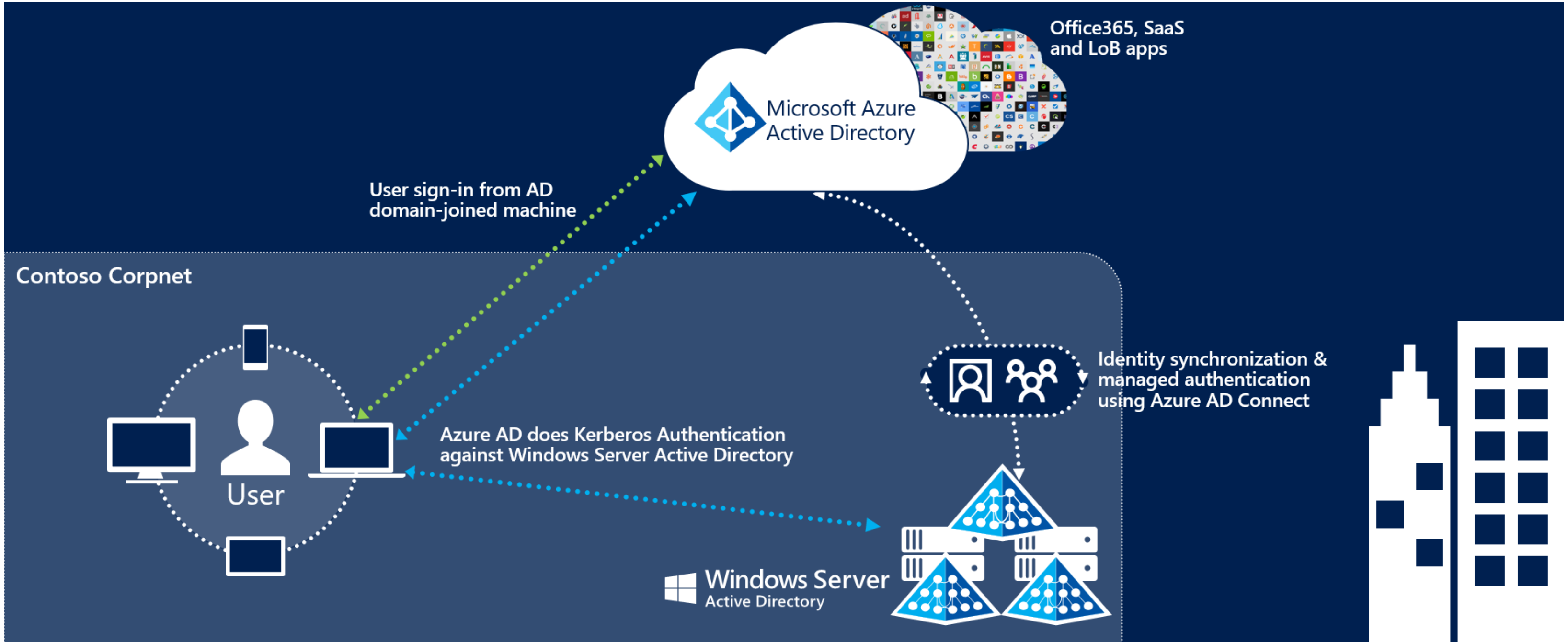
Hybrid Authentication with Pass-Trough Authentication (PTA)



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

Design and Architecture of Azure AD

Hybrid Authentication with Seamless Single-Sign On (sSSO)


Office365, SaaS and LoB apps
Microsoft Azure Active Directory
User sign-in from AD domain-joined machine
Contoso Corpnet
Identity synchronization & managed authentication using Azure AD Connect
User
Azure AD does Kerberos Authentication against Windows Server Active Directory
Windows Server Active Directory

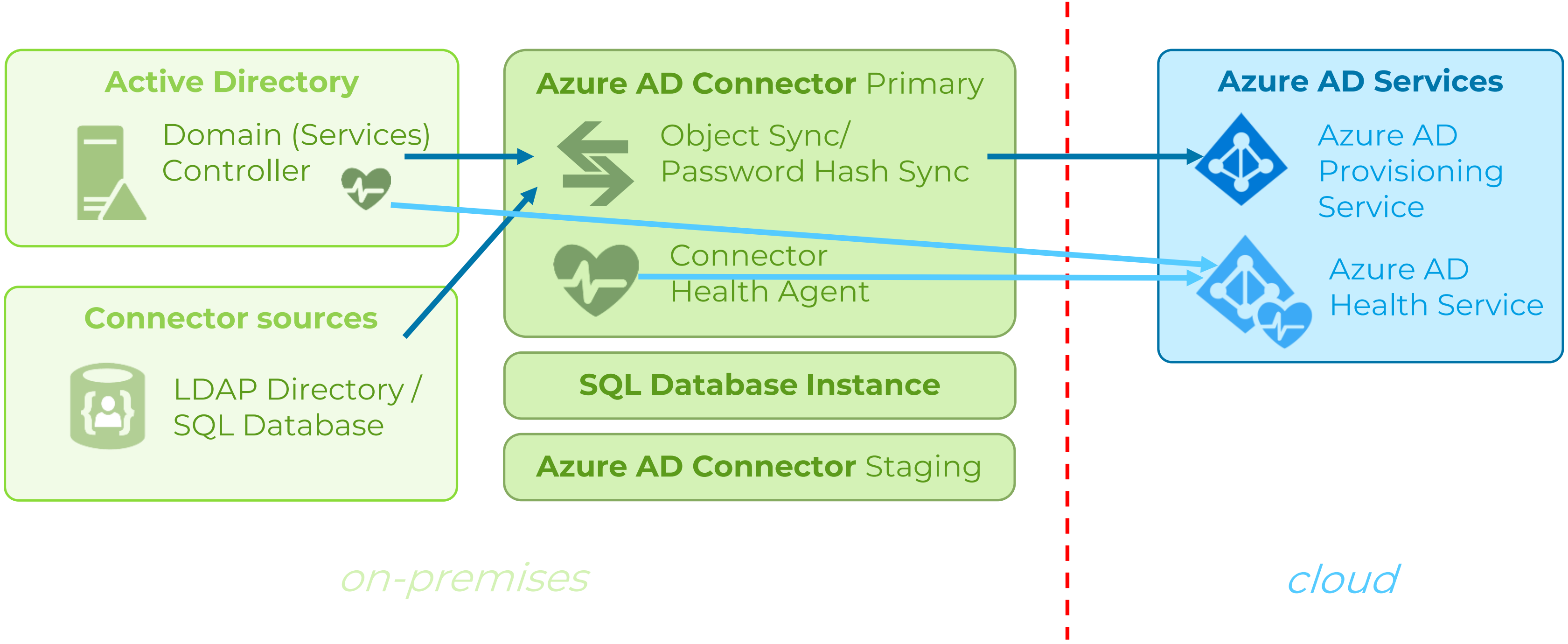
Source: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso

Design and Architecture of Azure AD
How to choose the hybrid authentication model?

- **Comparing technical methods**
  - Understanding / Deep dive on PTA Authentication Agents
- **Aware of effort and business requirement**
- **Early review with Governance and IT compliance to consider company IT security and data policies**

Design and Architecture of Azure AD

Synchronization identities from on-prem to cloud



Active Directory

Domain (Services) Controller

Connector sources

LDAP Directory / SQL Database

Azure AD Connector Primary

Object Sync/ Password Hash Sync

Connector Health Agent

SQL Database Instance

Azure AD Connector Staging

Azure AD Services

Azure AD Provisioning Service

Azure AD Health Service

on-premises

cloud

Design and Architecture of Azure AD

Synchronization identities from on-prem to cloud

- **Azure AD Connect as identity bridge**
  - Connect on-premises identity infrastructure to Azure AD
  - Writeback of password, devices and groups
  - PTA, sSSO, Configuration Wizards and AAD Health Connect
- **Supported topologies (multi-forest-support)**
- **Inbound provisioning solutions via HR → e.g. Workday**

Design and Architecture of Azure AD

One tenant to rule them all?

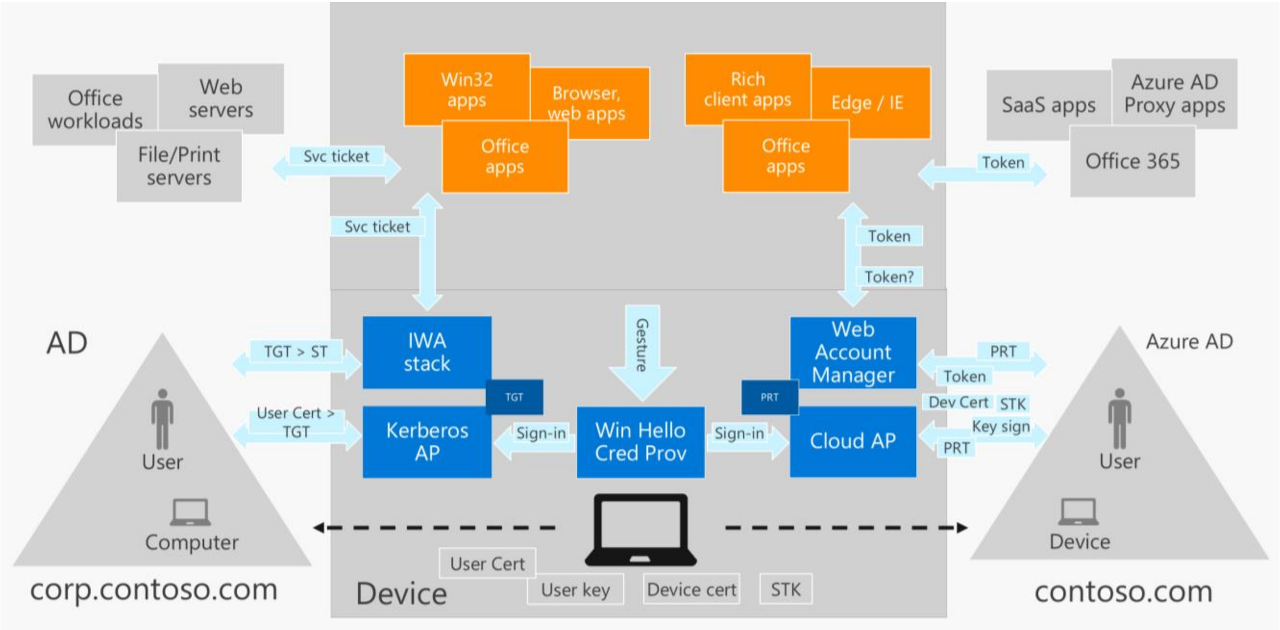
- **Tenant isolation (security boundary)**
  - Staging environments, (geopolitical) region or B2C (local) accounts
  - Granulator control over admin. privileges → Administrative Units
- **Tenant friending**
- **Location of identity data storage and security considerations**
  - MFA information outside of the EU*
  - Data privacy regulation (GDPR, workers' council) e.g. in Germany
  - Where is my data located? How Microsoft secure my data in Azure AD?

* Detailed information: https://docs.microsoft.com/bs-latn-ba/azure/active-directory/fundamentals/active-directory-data-storage-eu

Hands-on: Hardening of tenant default settings

Design and Architecture of Azure AD

Authentication with Hello for Business (WHfB) on Windows 10



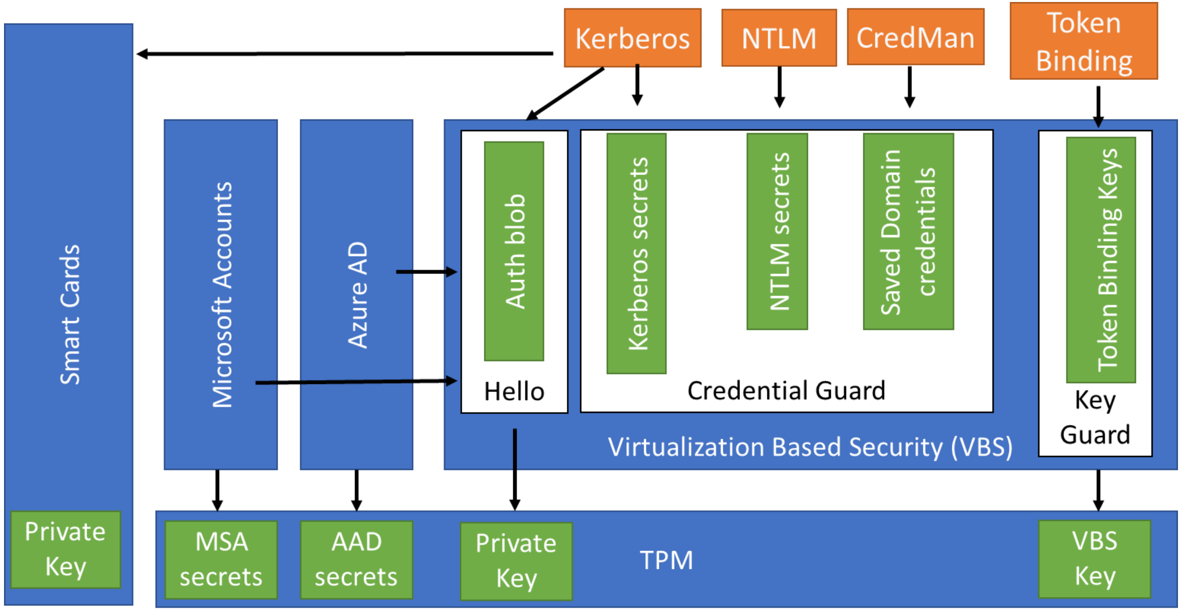
Deep Dive of Azure AD Authentication → https://jairocadena.com/

Source: https://jairocadena.com/2018/04/02/windows-hello-for-business-registration-and-authentication-with-azuread/

Design and Architecture of Azure AD

Guards of different credential types

- **Ignite 2017 Session:** Credential protection of Windows



Source: https://channel9.msdn.com/Events/Ignite/Microsoft-Ignite-Orlando-2017/BRK2077

Hybrid identity considerations

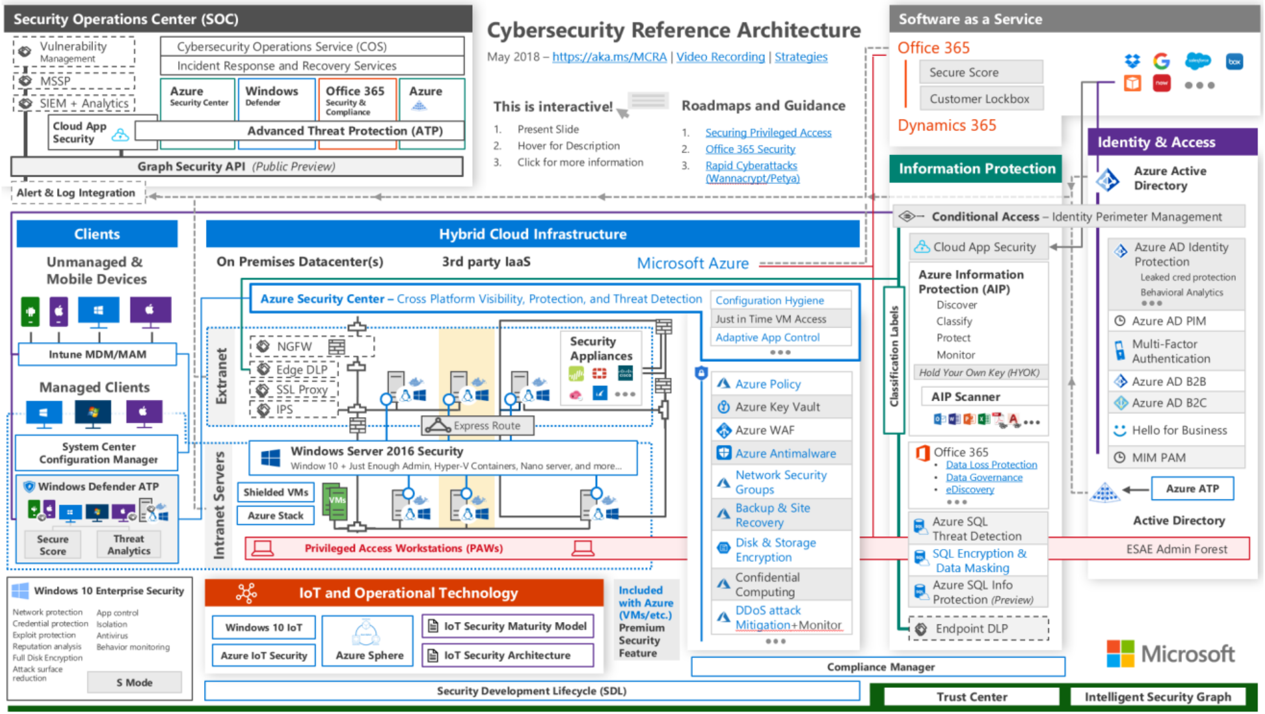
Hybrid identity considerations

Things to Do Before you install Azure AD Connect

- **Mind shift in (identity) strategy and level of transformation**
  - Standardized, Modernized, Transformed
- **Customize or develop an deployment plan**
- **IDFix to prepare and check directory objects and attributes**
  - Synchronization of nested groups and user accounts (expiration)
- **Identity lifecycle use cases that needs to be validated**
- **Assignment of Azure AD Licenses**

Hybrid identity considerations

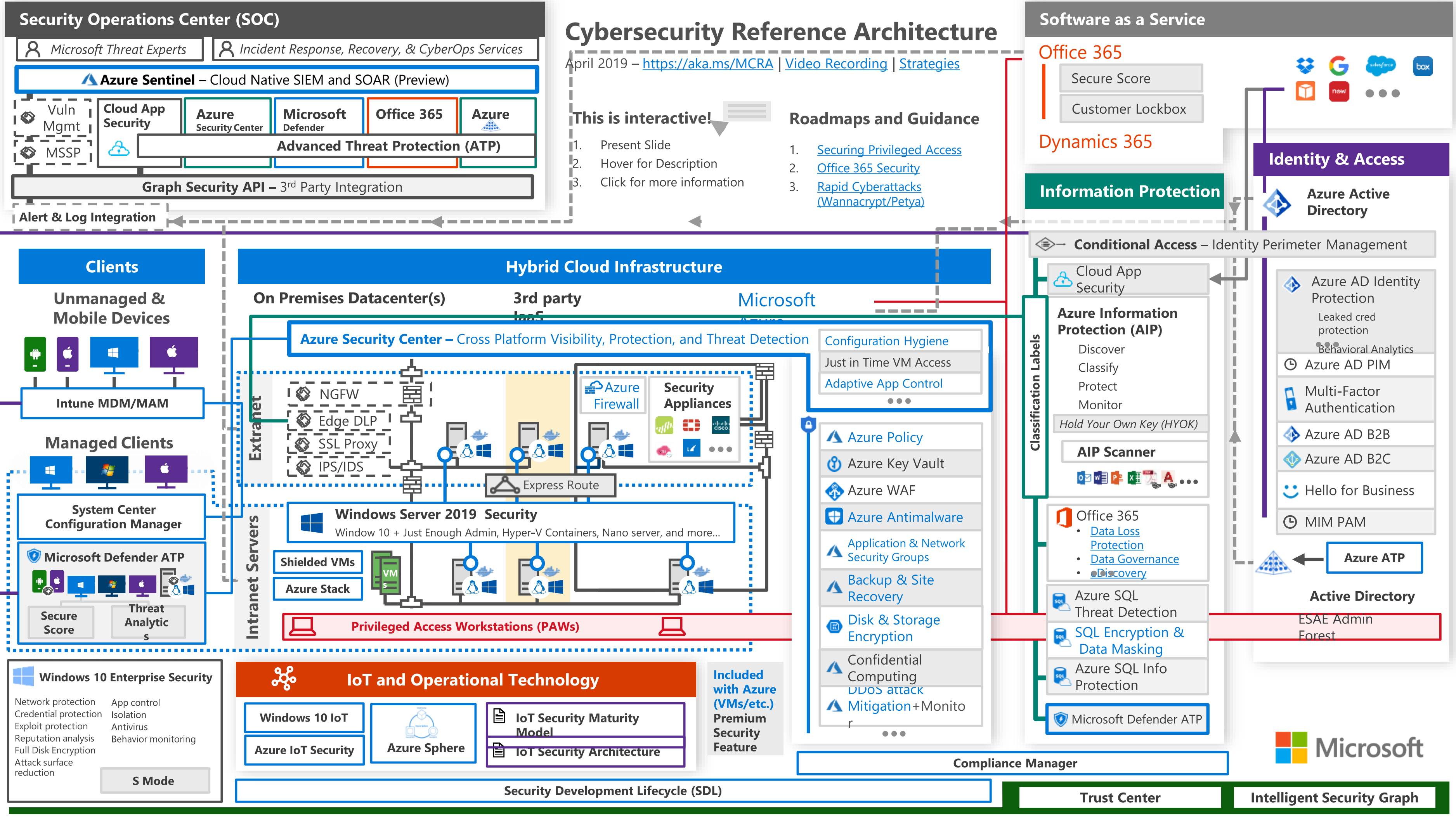
Reference Architecture: Security for a Hybrid Enterprise



Source: https://gallery.technet.microsoft.com/Cybersecurity-Reference-883fb54c

Cybersecurity Reference Architecture

April 2019 – https://aka.ms/MCRA | Video Recording | Strategies



This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks (Wannacrypt/Petya)

Security Operations Center (SOC)

Microsoft Threat Experts

Incident Response, Recovery, & CyberOps Services

Azure Sentinel – Cloud Native SIEM and SOAR (Preview)

Vuln Mgmt

MSSP

Cloud App Security

Azure Security Center

Microsoft Defender

Office 365

Azure

Advanced Threat Protection (ATP)

Graph Security API – 3rd Party Integration

Alert & Log Integration

Software as a Service

Office 365

Secure Score

Customer Lockbox

Dynamics 365

Identity & Access

Azure Active Directory

Conditional Access – Identity Perimeter Management

Azure AD Identity Protection

Leaked cred protection

Behavioral Analytics

Azure AD PIM

Multi-Factor Authentication

Azure AD B2B

Azure AD B2C

Hello for Business

MIM PAM

Azure ATP

Active Directory

ESAE Admin Forest

Information Protection

Cloud App Security

Classification Labels

Azure Information Protection (AIP)

Discover

Classify

Protect

Monitor

Hold Your Own Key (HYOK)

AIP Scanner

Office 365

- Data Loss Protection
- Data Governance
- eDiscovery

Azure SQL Threat Detection

SQL Encryption & Data Masking

Azure SQL Info Protection

Microsoft Defender ATP

Clients

Unmanaged & Mobile Devices

Intune MDM/MAM

Managed Clients

System Center Configuration Manager

Microsoft Defender ATP

Secure Score

Threat Analytics

Windows 10 Enterprise Security

Network protection

Credential protection

Exploit protection

Reputation analysis

Full Disk Encryption

Attack surface reduction

App control

Isolation

Antivirus

Behavior monitoring

S Mode

Hybrid Cloud Infrastructure

On Premises Datacenter(s)

3rd party IaaS

Microsoft Azure

Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

Configuration Hygiene

Just in Time VM Access

Adaptive App Control

Extranet

NGFW

Edge DLP

SSL Proxy

IPS/IDS

Azure Firewall

Security Appliances

Express Route

Intranet Servers

Windows Server 2019 Security

Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more…

Shielded VMs

Azure Stack

VMs

Privileged Access Workstations (PAWs)

Azure Policy

Azure Key Vault

Azure WAF

Azure Antimalware

Application & Network Security Groups

Backup & Site Recovery

Disk & Storage Encryption

Confidential Computing

DDoS attack Mitigation+Monitor

IoT and Operational Technology

Windows 10 IoT

Azure IoT Security

Azure Sphere

IoT Security Maturity Model

IoT Security Architecture

Included with Azure (VMs/etc.)

Premium Security Feature

Compliance Manager

Security Development Lifecycle (SDL)

Trust Center

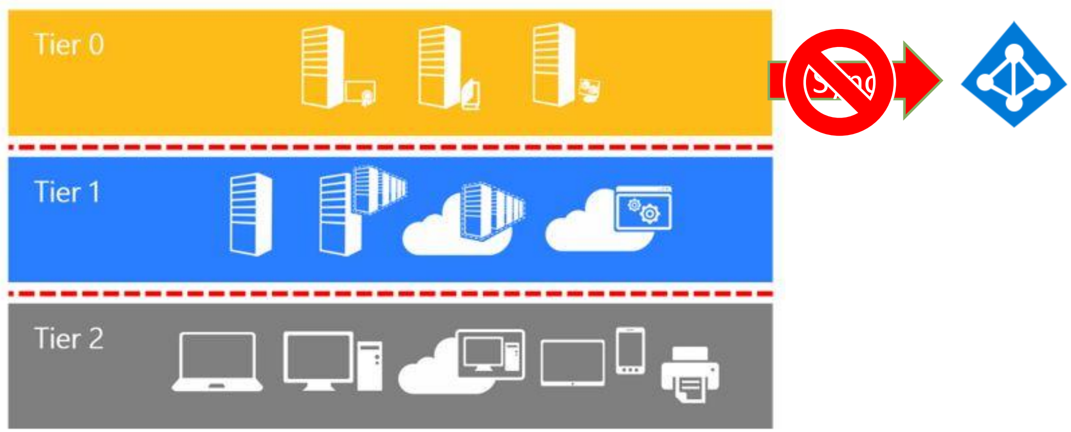
Intelligent Security Graph

Microsoft

Hybrid identity considerations

ESAE model and Azure Active Directory

- Implement concepts of securing privileged access
- Adapting of tiering model for hybrid identity components
  - AAD Connect-related components (incl. database), PTA agent = Tier0



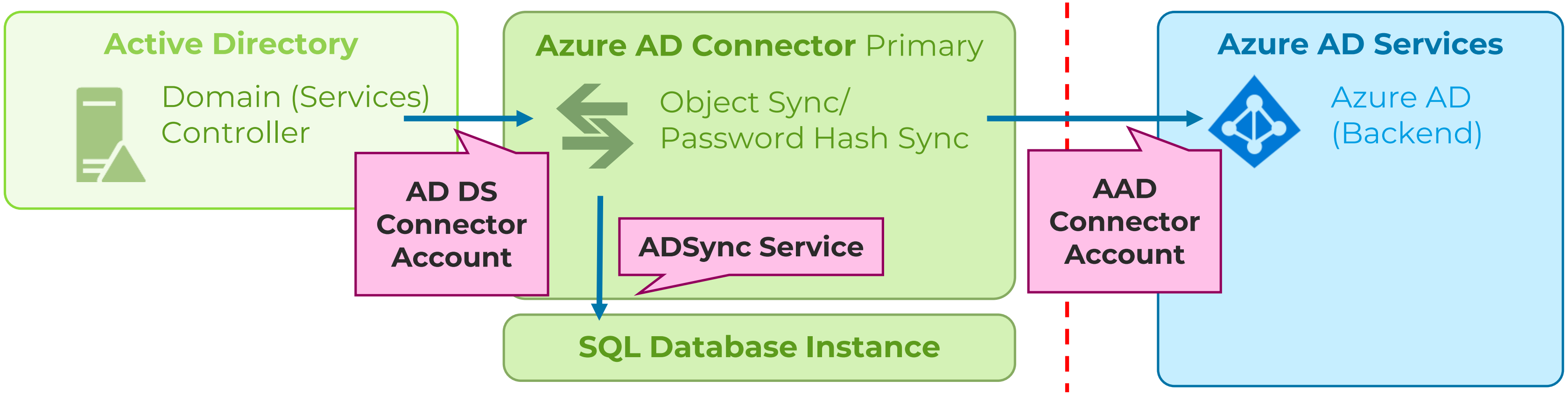
Source: ehttps://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

Hybrid identity considerations
Design decisions of Azure AD Connect

- **Placing of Azure AD connect, PTAs servers and databases**
  - PTA Agents can be installed on Windows Server Core
- **Required internet connectivity (direct / proxy)**
  - Running tests with „AADConnect-CommunicationsTest.ps1“
- **Review the synced attributes, filtering and write-back options with IT security and data privacy**
- **Hybrid identity monitoring solution (Azure ATP/Microsoft ATA)**

Hybrid identity considerations

Design decisions of Azure AD Connect



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

Hybrid identity considerations

Attack scenarios of hybrid identity

- **Non MFA-enabled accounts**
  → Attack surface reduction and alerting

- **Password Spraying (e.g. Mailsniper)**

  → Recommendation of Microsoft for defending

- **Phishing attacks**

  → Attack simulator in Office 365

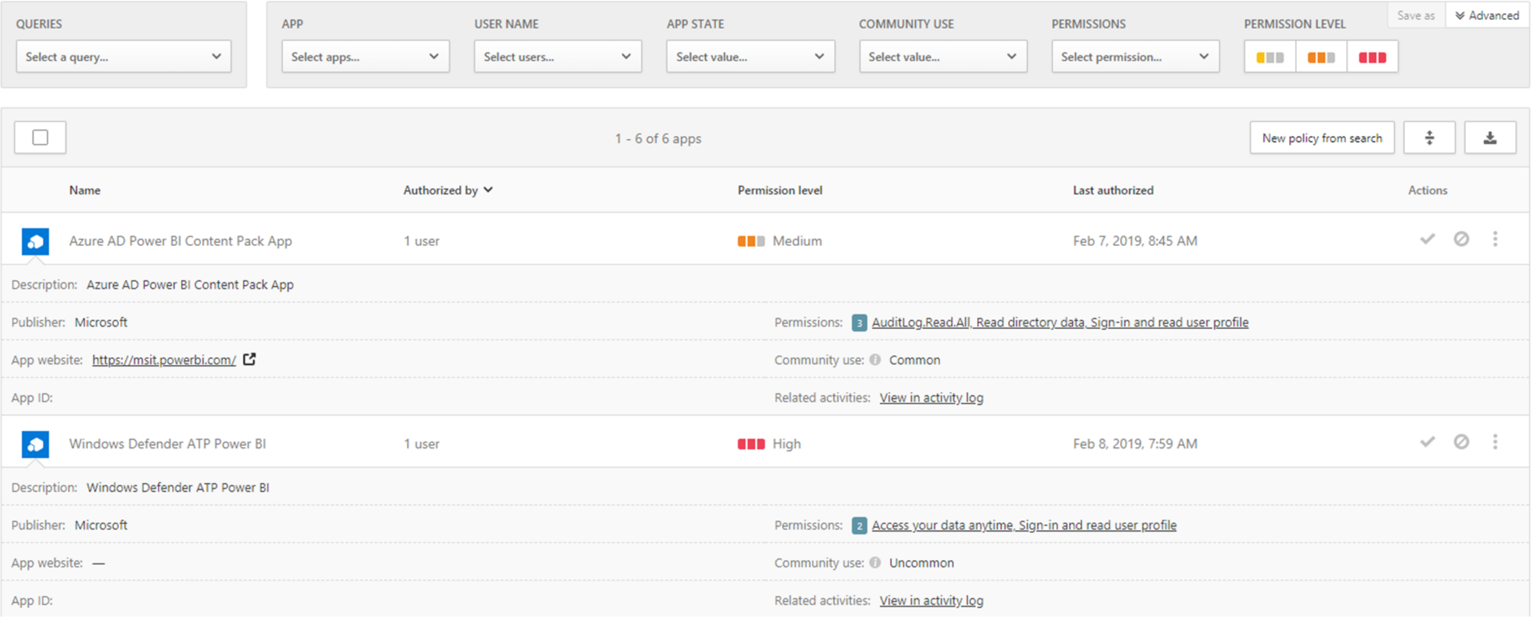
- **Illicit (App) Consent Grant**

  → Inventory of apps, disable grant consent to unmanaged apps

Hybrid identity considerations

Defending attack scenarios of hybrid identity

- **Microsoft Cloud App Security + Azure ATP + Azure Sentinel**



QUERIES: Select a query...

APP: Select apps...

USER NAME: Select users...

APP STATE: Select value...

COMMUNITY USE: Select value...

PERMISSIONS: Select permission...

PERMISSION LEVEL

Save as | Advanced

□ 1 - 6 of 6 apps | New policy from search

Name	Authorized by	Permission level	Last authorized	Actions
Azure AD Power BI Content Pack App	1 user	Medium	Feb 7, 2019, 8:45 AM	✓ ⊘ ⋮

Description: Azure AD Power BI Content Pack App

Publisher: Microsoft

Permissions: 3 AuditLog.Read.All, Read directory data, Sign-in and read user profile

App website: https://msit.powerbi.com/

Community use: Common

App ID:

Related activities: View in activity log

Name	Authorized by	Permission level	Last authorized	Actions
Windows Defender ATP Power BI	1 user	High	Feb 8, 2019, 7:59 AM	✓ ⊘ ⋮

Description: Windows Defender ATP Power BI

Publisher: Microsoft

Permissions: 2 Access your data anytime, Sign-in and read user profile

App website: —

Community use: Uncommon

App ID:

Related activities: View in activity log

Hybrid identity considerations
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)
- **Alternate: Windows Hello for Business (Hybrid)**

Management of user accounts

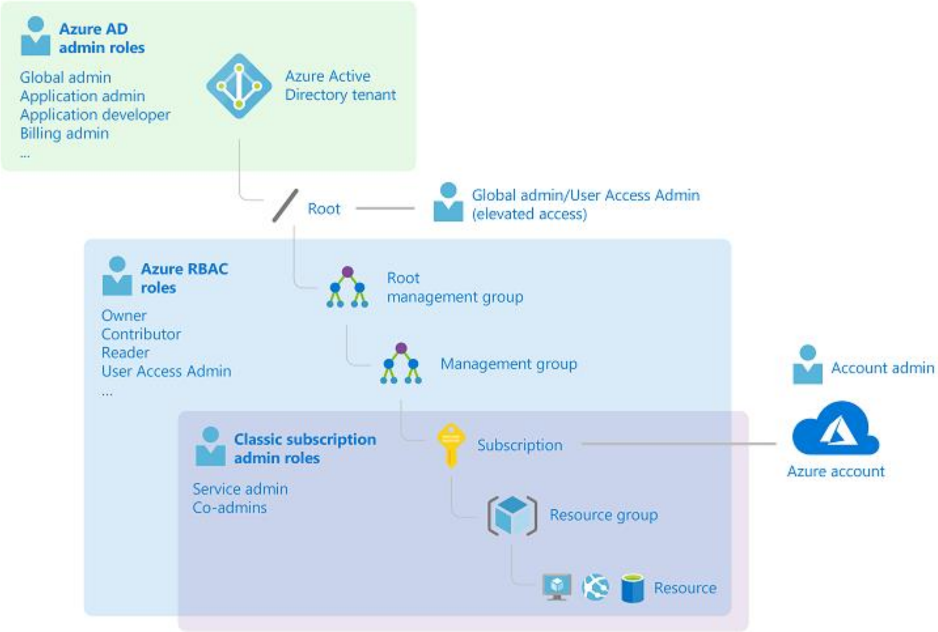
Management of user accounts
Different user types and roles

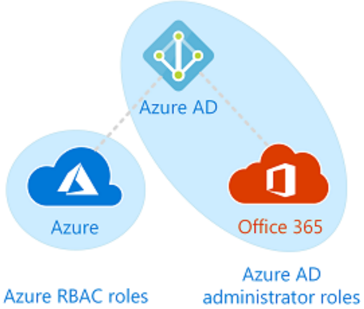
- **Cloud-Only, Synced (Hybrid), Guest**
- **Privileged accounts**
  - Don’t mix on-premises and cloud privileged accounts
  - Cloud-only or synced/managed identities from on-Premises?
  - Built role-based security groups based on your RBAC concept
- **Break glass accounts**
  - Must be covered by naming convention (no specific user type)
  - Guidelines for managing emergency access accounts (“break glass”)

Management of user accounts

Azure RBAC roles and Azure AD administrators

- **Relation between Azure, Azure AD and Azure**



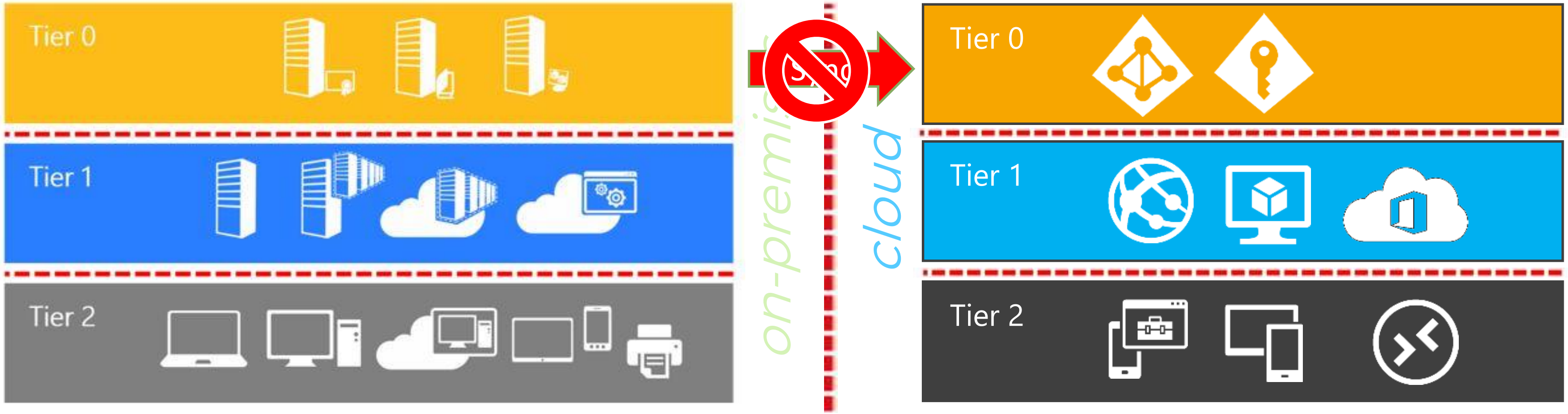


Source: https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles

Management of user accounts

Adopting ESAE tier model in Azure (Active Directory)

- **Adapting of securing privileges for hybrid and cloud identity**
  - Tiering model and separated privileged accounts in Azure?

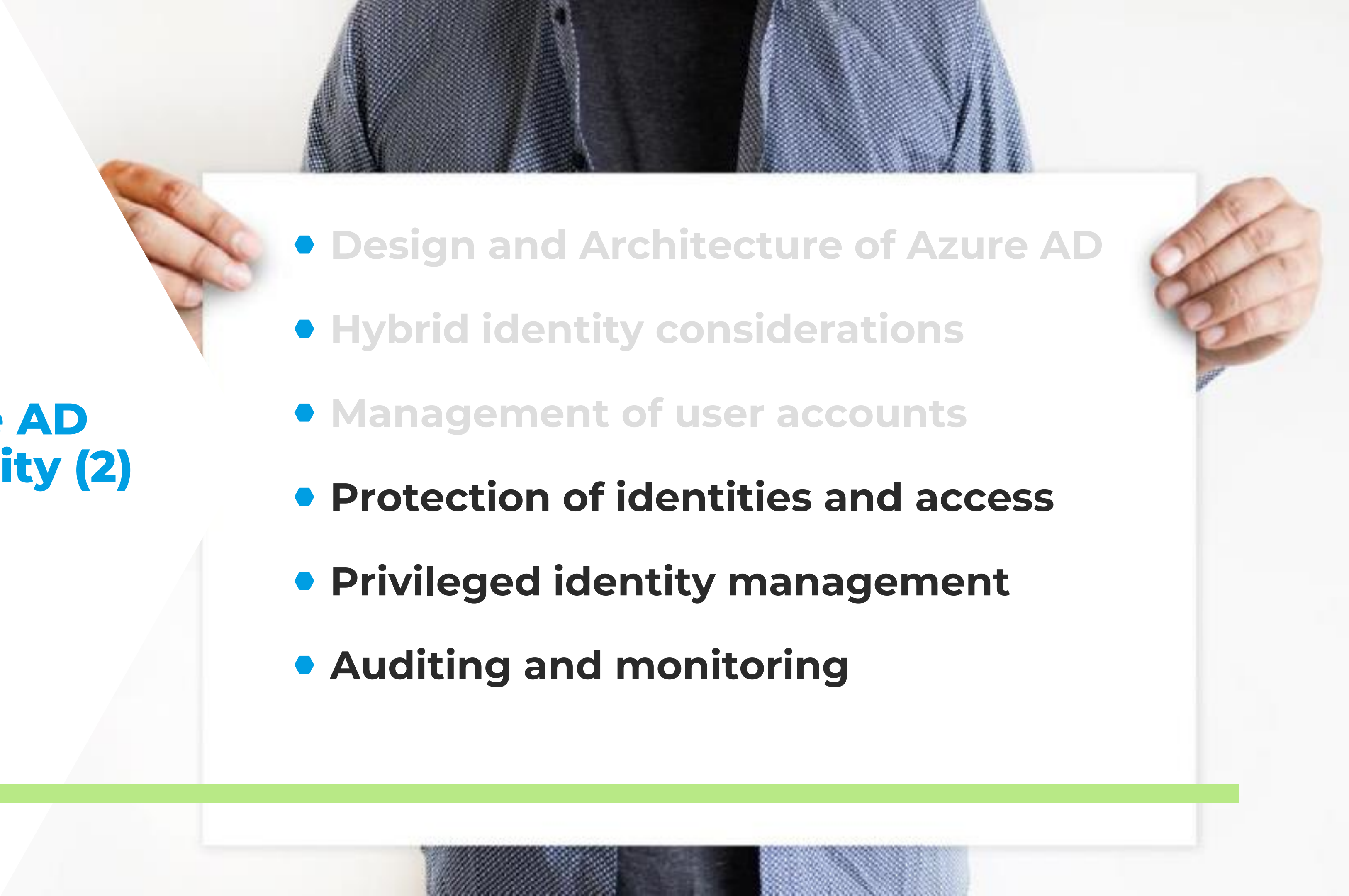


Source: https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

Hands-on: Privileged and Break-Glass Accounts

Debeka
Innovation
Center

Azure AD Security (2)



- Design and Architecture of Azure AD
- Hybrid identity considerations
- Management of user accounts
- Protection of identities and access
- Privileged identity management
- Auditing and monitoring

DICE
Debeka
Innovation
Center

Thank you!

DICE - Debeka Innovation Center
dice@debeka.de
Universitätsstraße 4-6
56070 Koblenz