



Azure Active Directory

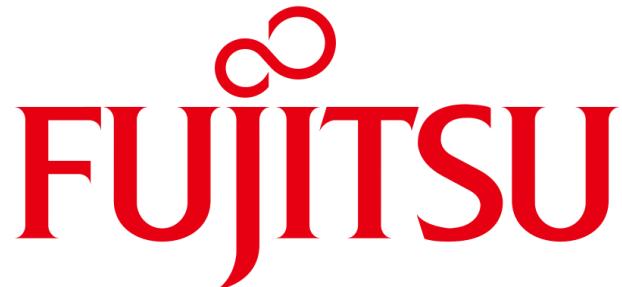
Effektive Maßnahmen für mehr Sicherheit

Thomas Naunheim
Microsoft MVP, Cloud Security Architect
@glueckkanja-gab AG



Vielen Dank an unsere Sponsoren!

Platinum



Gold





Thomas Naunheim

Cloud Security Architect
@glueckkanja-gab AG

Koblenz, Germany

 @Thomas_Live

 cloud-architekt.net





IDENTITY SECURITY
POSTURE



CONDITIONAL ACCESS
UND TOKEN SICHERHEIT



PRIVILEGED IDENTITY
AND ACCESS



WORKLOAD IDENTITIES
UND APP INTEGRATION



IDENTITY SECURITY POSTURE



Angriffe auf "Modern Identity"

The cybersecurity bell curve:

Basic security hygiene still protects against 98% of attacks



Source: Microsoft ("Identity is the new battle ground")



Security Defaults für alle Azure AD Tenants

Home > EntraLab

EntraLab | Properties

Azure Active Directory

Identity Governance
Application proxy
Custom security attributes (Preview)
Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
User settings
Properties Properties
Security
Monitoring
Sign-in logs
Audit logs
Provisioning logs
Log Analytics
Diagnostic settings
Workbooks
Usage & insights
Bulk operation results (Preview)

Save Discard Got feedback?

Tenant properties

Name * ✓

Country or region
United States

Location
United States datacenters

Notification language
English

Tenant ID
043bf1ec-de95-4a87-8daa-c0b3f2aa6f80

Technical contact
thomas@cloud-architekt.net

Global privacy contact

Privacy statement URL

Access management for Azure resources

Thomas@entralab.onmicrosoft.com (Thomas@entralab.onmicrosoft.com) can manage access to all Azure subscriptions and management groups in this tenant. [Learn more](#)

[Manage security defaults](#) Manage security defaults

Enable security defaults

Security defaults are basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity-related attacks.

[Learn more](#)

Enable security defaults

Yes No



Security Defaults für alle Azure AD Tenants

- Frühere “Baseline” policies in Conditional Access

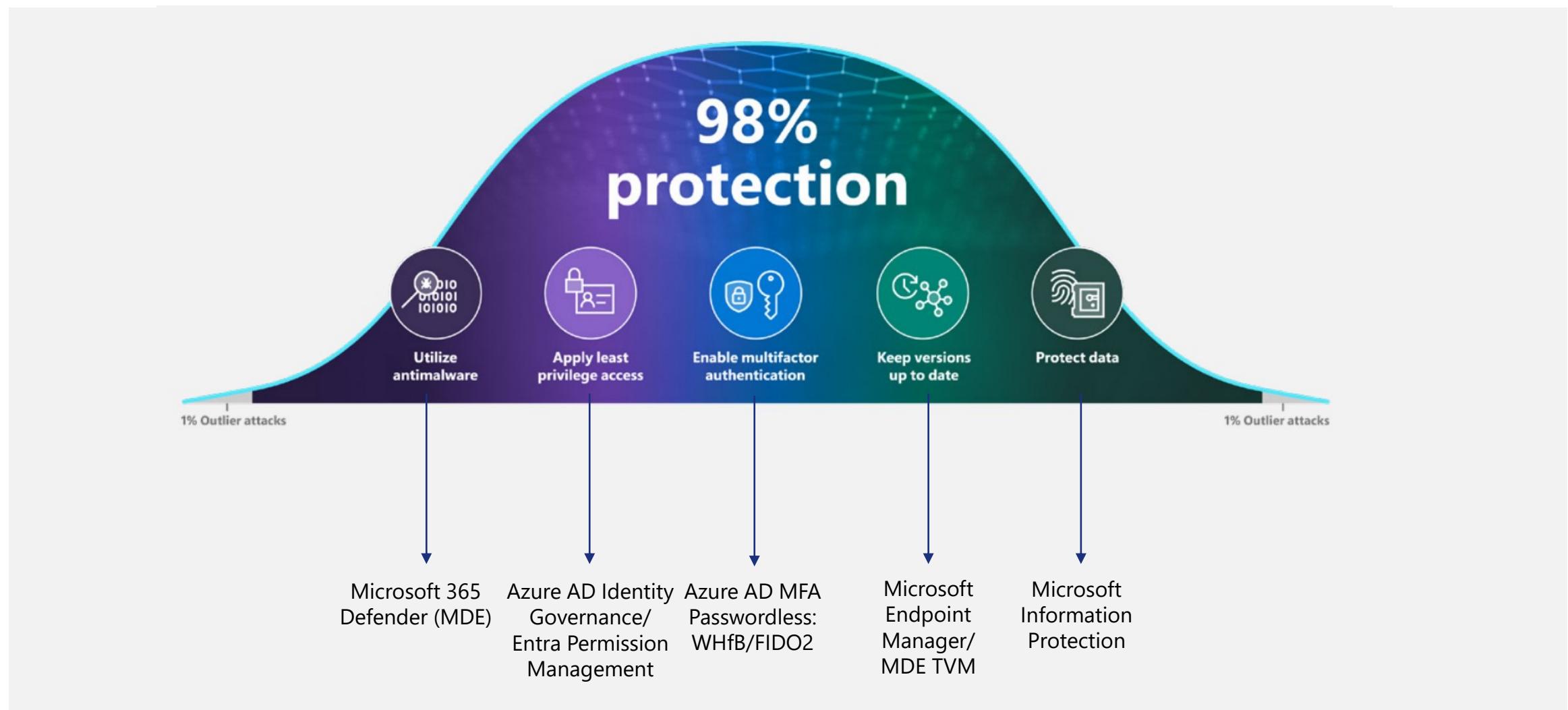
POLICY NAME	ENABLED
Baseline policy: Require MFA for admins	✓
Baseline policy: End user protection (Preview)	...
Baseline policy: Block legacy authentication (Preview)	...
Baseline policy: Require MFA for Service Management (Preview)	...

- Keine zusätzlichen Kosten oder Azure AD Lizenzen notwendig (verfügbar für alle, standardmäßig aktiviert bei neuen Azure AD Tenants)
- *“Security defaults provide secure default settings that (Microsoft) manages on behalf of organizations to keep customers safe **until they are ready to manage their own identity security story.**”*

Quelle: [Introducing security defaults - Microsoft Tech Community](#)



Schutz der "Modern Identity"



Source: Microsoft ("Identity is the new battle ground")



Microsoft Secure Score

Microsoft Secure Score

Overview Recommended actions **Recommended actions** History Metrics & trends

Export

Rank	Recommended action	Score
8	Block abuse of exploited vulnerable signed drivers	+0.9%
9	Block Win32 API calls from Office macros	+0.9%
10	Update Microsoft Defender Antivirus definitions	+0.9%
11	Block execution of potentially obfuscated scripts	+0.9%
12	Block Adobe Reader from creating child processes	+0.9%
13	Block all Office applications from creating child processes	+0.9%
14	Block credential stealing from the Windows local security aut...	+0.9%
15	Block executable files from running unless they meet a preval...	+0.9%
16	Block untrusted and unsigned processes that run from USB	+0.9%

Block credential stealing from the Windows local security authority subsystem (lsass.exe)

To address

[Go to threat and vulnerability management to take action](#) Manage tags

General	Exposed entities	Implementation
Description <p>Attack Surface Reduction (ASR) rules are the most effective method for blocking the most common attack techniques being used in cyber attacks and malicious software. This ASR rule locks down LSASS.</p> <p>This security control is only applicable for machines with Windows 10, version 1803 or later. Attackers can use tools like Mimikatz to scrape cleartext passwords and NTLM hashes from LSASS.</p>		Details <p>Points achieved 0/9</p> <p>History 0 events</p> <p>Category Device</p> <p>Product Defender for Endpoint</p>



Microsoft Identity Secure Score

Microsoft Secure Score

Overview Recommended actions History Metrics & trends

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Applied filters: Category: Identity [X](#)

Your secure score Include [▼](#)

Filtered score: 84.63%

103.25/122 points achieved

100%
80%
60%

25/05 31/05 06/06 12/06 18/06 24/06 30/06 06/07 12/07 18/07 24/07 30/07 05/08 11/08 17/08 22/08

Breakdown points by: Category [▼](#)

Category	Score
Identity	84.63%
Points achieved	84.63%
Opportunity	0

Actions to review

Action Status	Count
Regressed	0
To address	7
Planned	0
Risk accepted	0
Recently added	0
Recently updated	0

Top recommended actions

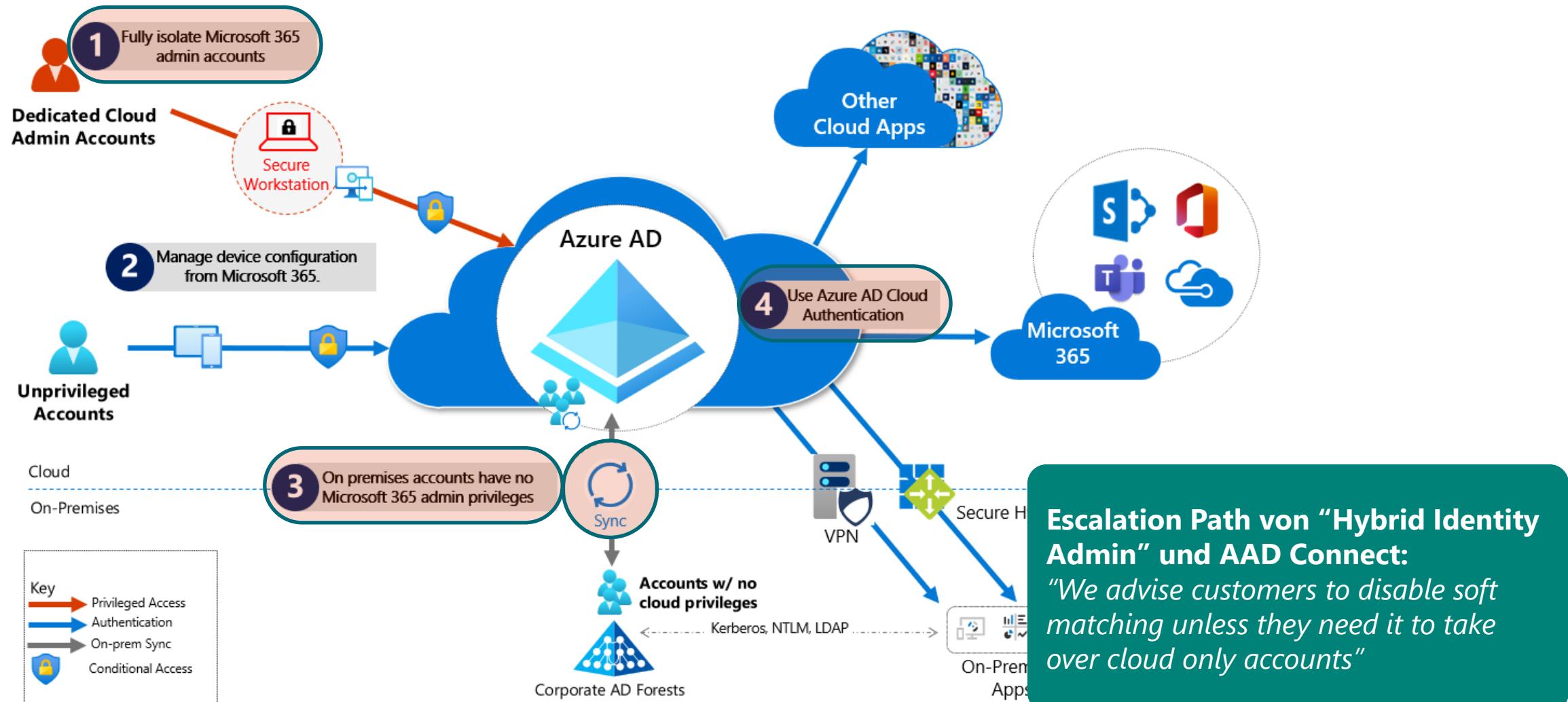
Recommended action	Score impact	Status	Category
Require multifactor authentication for administrative roles	+8.2%	<input type="radio"/> To address	Identity
Resolve unsecure domain configurations	+4.1%	<input type="radio"/> To address	Identity
Ensure all users can complete multifactor authentication	+7.38%	<input type="radio"/> To address	Identity
Set a honeypot account	+0.82%	<input type="radio"/> To address	Identity
Configure VPN integration	+0.82%	<input type="radio"/> To address	Identity



DEMO

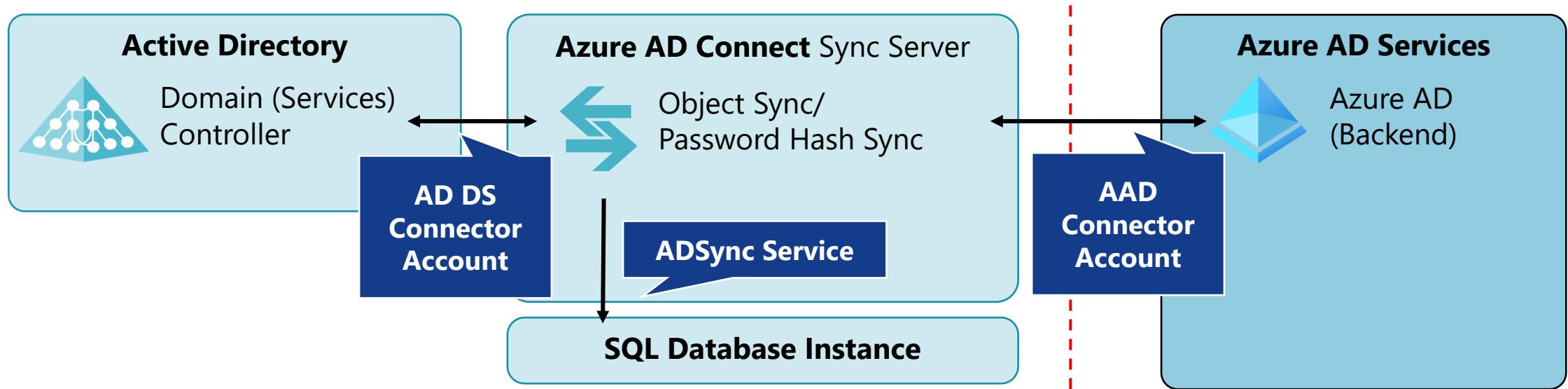
Default Tenant Security
& Strong Authentication

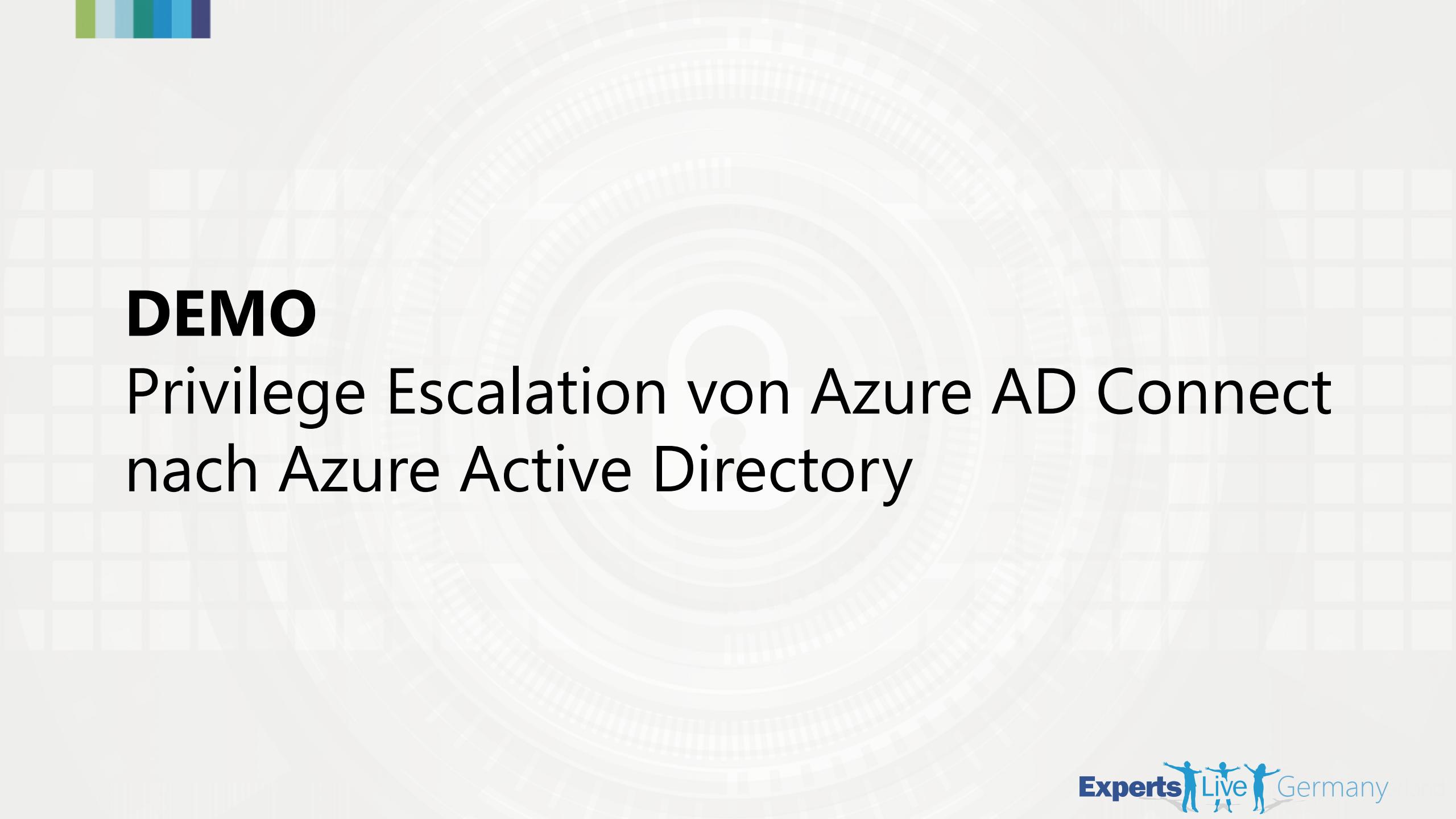
Angriffsfläche und -pfade bei Hybrid Identity





Azure AD Connect: Dienstkonten und -zugriffe





DEMO

Privilege Escalation von Azure AD Connect
nach Azure Active Directory



CONDITIONAL ACCESS UND TOKEN SICHERHEIT



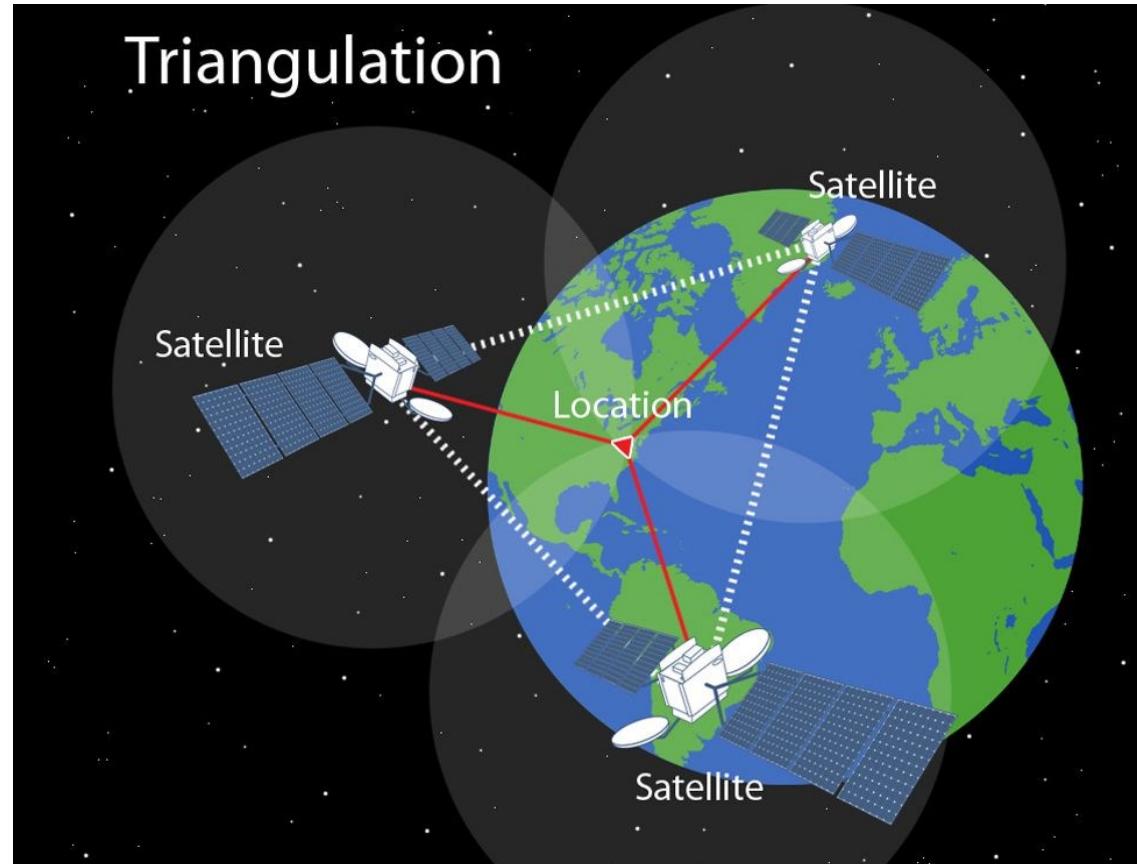
Design von Conditional Access Policies



Schütze jeden Benutzer und jede App durch ein einfaches aber effektives
Conditional Access Design!



Effektive “Conditions” und “Controls”



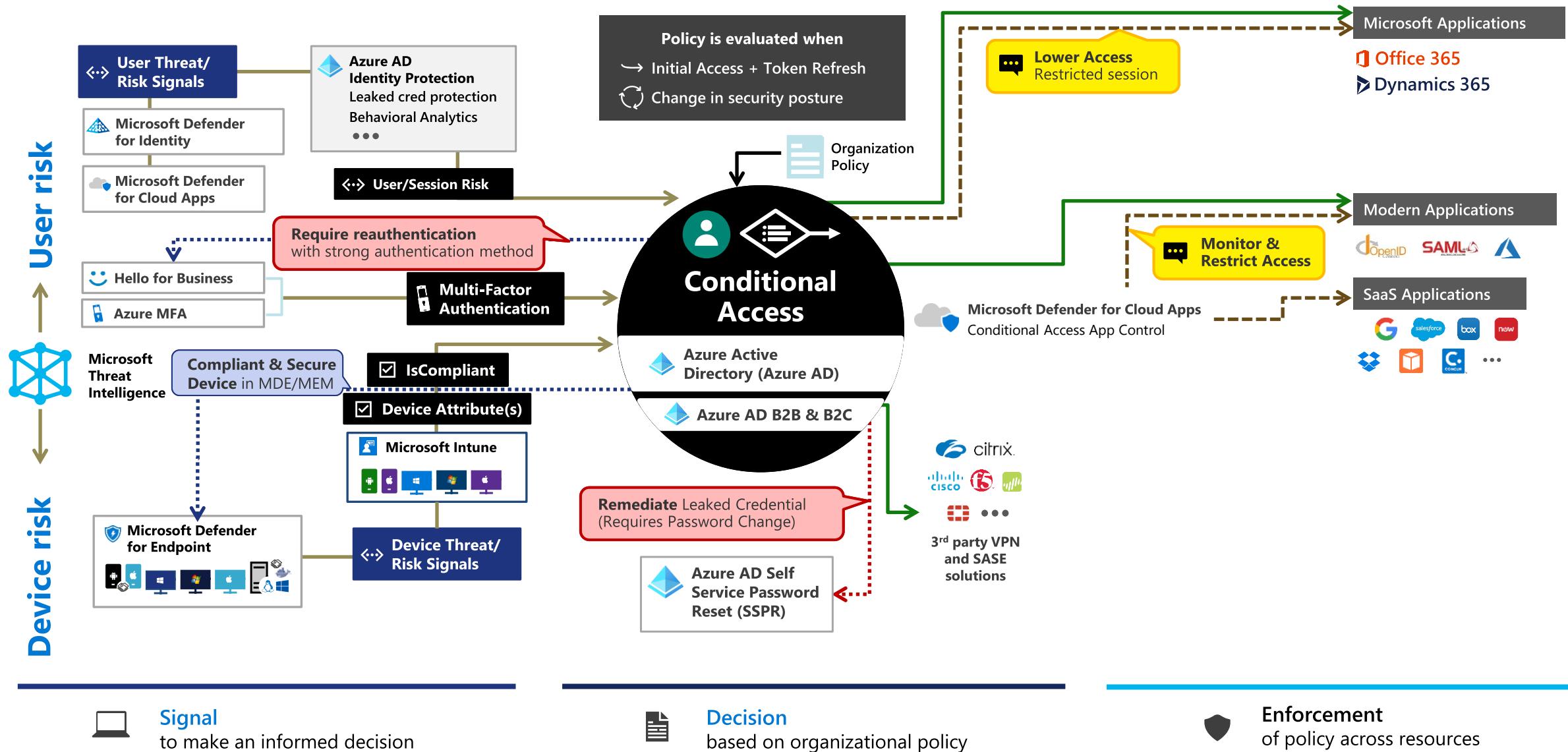


Never trust, always verify

Image Source: Microsoft ("Zero Trust Definition and Models")

Legend

- Full access
- Limited access
- Risk Mitigation
- Remediation Path





DEMO

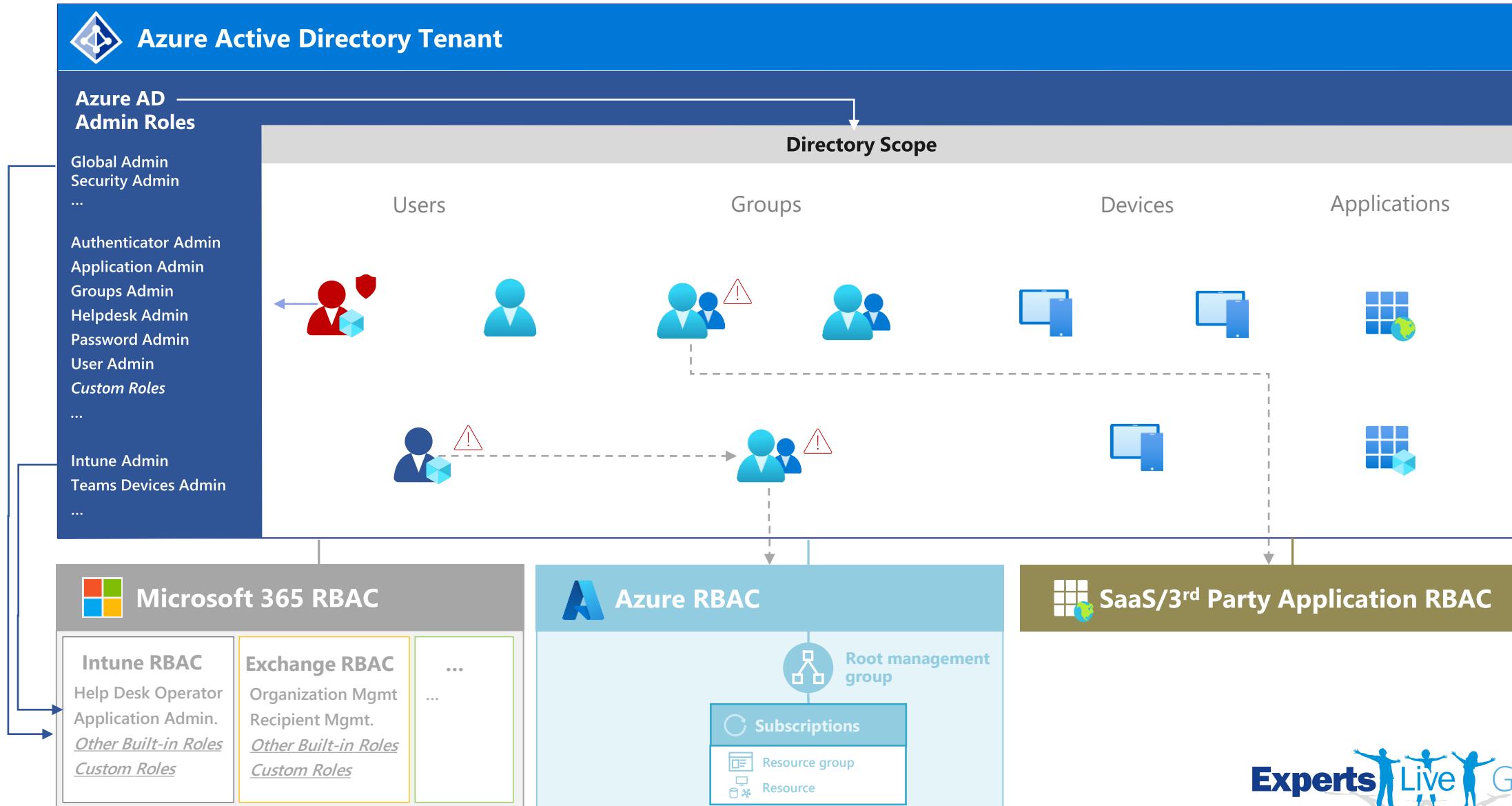
Templates von Conditional Access,
Token und Cloud Session Security



PRIVILEGED IDENTITY AND ACCESS

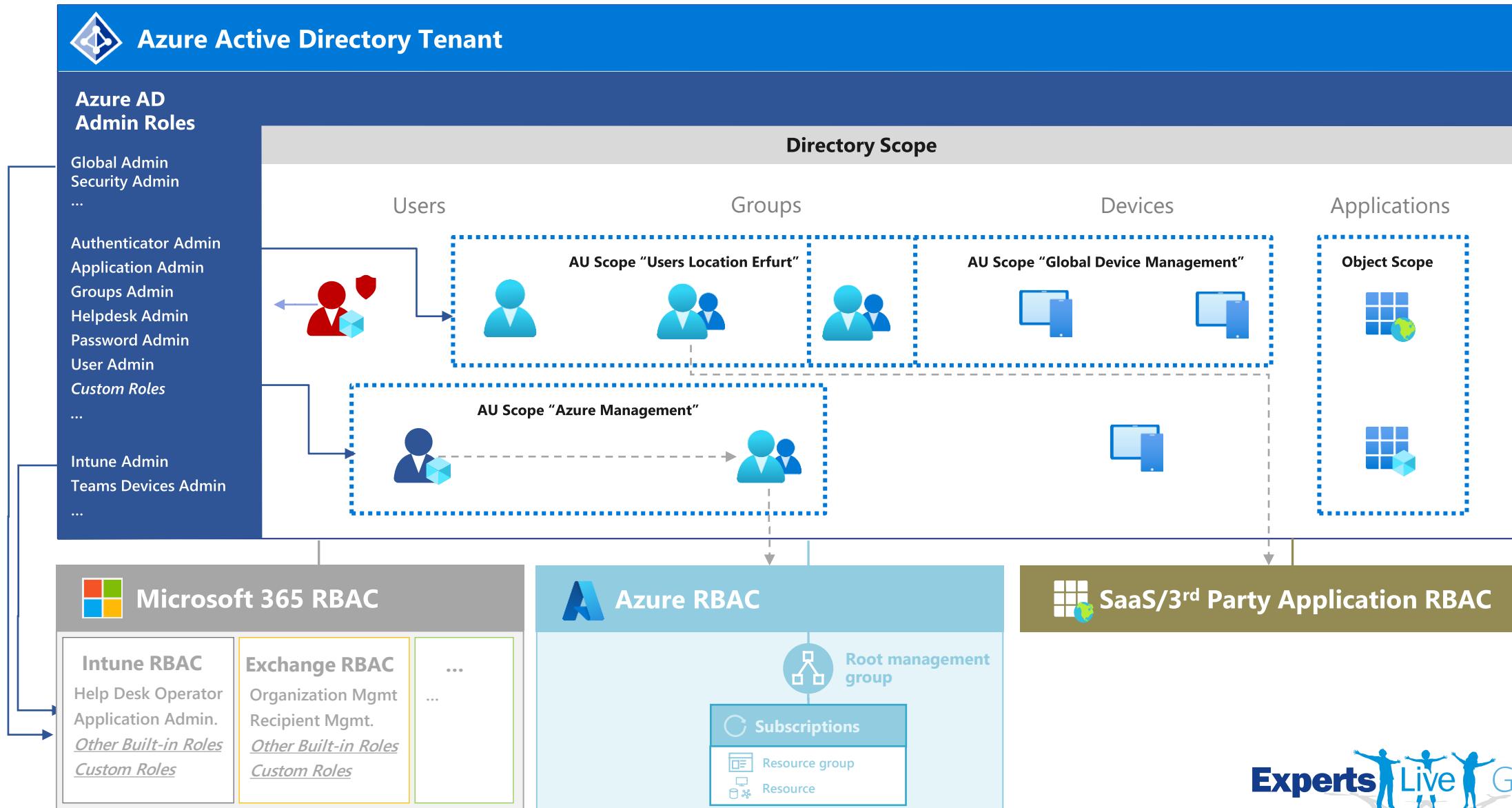


Delegierung mit Azure AD RBAC





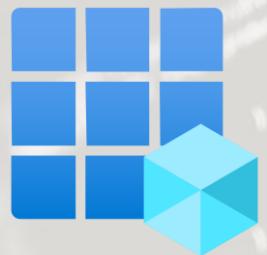
Delegierung mit Azure AD RBAC





DEMO

Sensitive Azure AD RBAC roles
und Delegierung von Admin. Tasks



APP INTEGRATION UND WORKLOAD IDENTITIES

Kritische Berechtigungen für Azure AD Apps

- Eingeschränkte Zugriff auf Enterprise App bei sensitive Delegated Permissions

The screenshot shows the 'Graph explorer (official site) | Properties' section of the Azure Graph Explorer. A red box highlights the 'Assignment required?' switch, which is set to 'No'. An arrow points from this switch to a green box containing the 'dug_AAD.PrivilegedAccounts' app role assignment.

Graph explorer (official site) | Properties

Enterprise Application

Assignment required? ⓘ Yes No

Assign users and groups to app-roles for your application here. App-roles are made available by the developer of the application by using the application registration.

DU dug_AAD.PrivilegedAccounts Group Default Access

- Standardmäßige Berechtigung zur Registrierung von Enterprise Apps (Service Principals)

The screenshot shows the 'App registrations' section of the Azure App registrations page. A red box highlights the 'Users can register applications' switch, which is set to 'Yes'. An arrow points from this switch to a green box containing information about the 'Application developer' role.

App registrations

Users can register applications ⓘ Yes No

Application developer

Description: Users in this role will continue to be able to register app registrations even if the Global Admin has turned off the tenant level switch for "Users can register apps".

Kritische Berechtigungen für Azure AD Apps

- Berechtigung auf "Application" und "Service Principal" Objekte und Credentials

The screenshot illustrates two key administrative roles for an Azure AD application:

BusinessApp-Auth-WebAPI | Owners (Left Panel):

- Manage** section includes: Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, and **Owners**.
- Owners** list: Thomas Naunheim (selected).

Cloud application administrator | Assignments (Right Panel):

- Eligible assignments** tab is selected.
- Assignment details: Thomas Naunheim (thomas@cloud-architel) assigned to Cloud Application Administrator role in BusinessApp-Auth-WebAPI (Application).

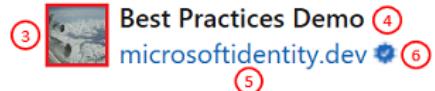


User Consent und Phishing Angriffe



① testuser@fourthcoffeetest.onmicrosoft.com

② Permissions requested



This application is not published by Microsoft or your organization. ⑦

This app would like to:

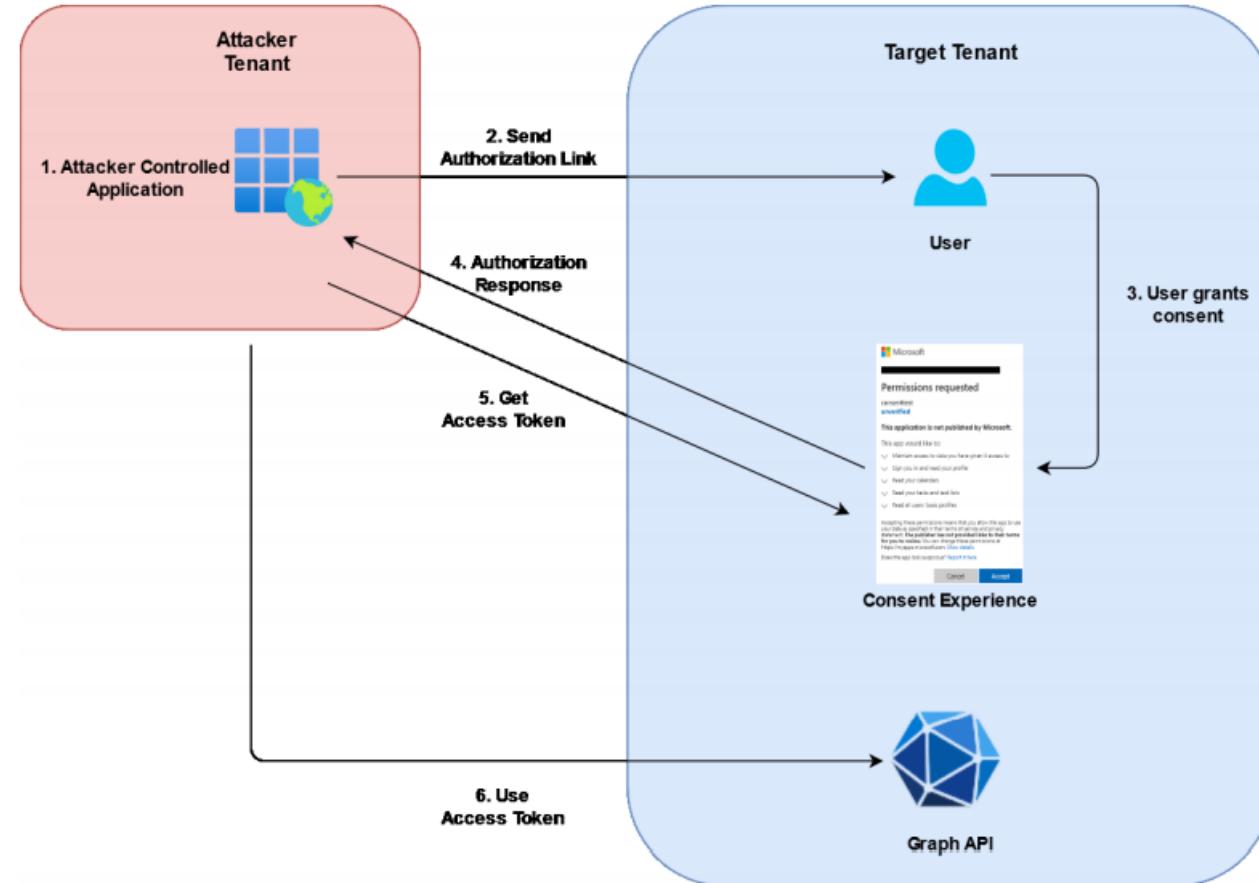
- ✓ Maintain access to data you have given it access to
 - ✗ Sign you in and read your profile
 - ✗ Allows you to sign in to the app with your organizational account and let the app read your profile. It also allows the app to read basic company information.
- ⑨ This is a permission requested to access your data in Fourth Coffee. ⑧

Accepting these permissions means that you allow this app to use your data as specified in their [terms of service](#) and [privacy statement](#). You can change these permissions at <https://myapps.microsoft.com>. ⑩ ⑪

Only accept if you trust the publisher and if you selected this app from a store or website you trust. Ask your admin if you're not sure. Microsoft is not involved in licensing this app to you. [Hide details](#)

Does this app look suspicious? [Report it here](#) ⑫

[Cancel](#) [Accept](#)



DEMO

Illicit Consent Grant Attacks und Consent (Framework) Permission



Azure AD Security | Zusammenfassung



Implementierung eines "Identity Security Posture" Management und Überprüfung der Standardkonfigurationen
Nutzung von cloud-basierten und Phishing-resistenten Authentifizierungsmethoden (PHS + FIDO2/WHfB)
Absicherung und Schutz von Azure AD Connect Komponenten als Tier0 inklusive Monitoring und MDE



Nutzen von eindeutigen und aussagekräftigen Signalen als "Conditions" in Conditional Access
Überwachung der Abdeckung und Anwendung von den konfigurierten Policies
Starke "Conditions" und "Controls" für Benutzerzugriff (Device-Compliance und MFA oder Eingeschr. Session)



Privilegierte Zugriffe auf "autorisierte" Zugriffswege einschränken (z.B. Device Filter für SAW/PAW)
Vermeidung von Azure AD Rollen auf Directory-Ebene und ähnlichen Rollen aus anderen RBAC systemen
Etablierung eines least-privileged RBAC designs (Tiered Admin Model) mit Identity Governance-Prozessen



Deaktivierung oder Einschränkung des "User Consent" und implementierung von "Admin approval" workflow
Ersetzen von "Owner" durch Azure AD Rollen, Einschränkung von
Implementierung eines Lifecycle und Inventarisierung sowie Security Monitorings für Workload Identities



Azure AD Attack & Defense Playbook



<https://github.com/Cloud-Architekt/AzureAD-Attack-Defense>

written by Sami Lamppu, Joosua Santasalo and Thomas Naunheim



Bitte gebt uns euer Feedback

Feedbackbogen abgeben und Geschenk mitnehmen

Vielen Dank!



@Thomas_Live



Cloud-Architekt.net