Azure Active Directory Effektive Maßnahmen für mehr Sicherheit

Thomas Naunheim

Microsoft MVP, Cloud Security Architect

@glueckkanja-gab AG

Experts Live Germany

Vielen Dank an unsere Sponsoren!

Platinum

FUJITSU

THOMAS KRENN®

bluechip
CREATING COMPUTERS.

Lenovo™

Gold

EXPERTS INSIDE

EasyLife 365

SVA

NiCE
IT Management Solutions

Experts Live Germany

Thomas Naunheim

Cloud Security Architect
@glueckkanja-gab AG

Koblenz, Germany

@Thomas_Live

cloud-architekt.net

Microsoft® Most Valuable Professional

Azure Meetup BONN

CLOUD IDENTITY SUMMIT '22

Cloud Inspires Podcast

Stories and people behind "Cloud Transformation"

Experts Live Germany

IDENTITY SECURITY POSTURE

CONDITIONAL ACCESS UND TOKEN SICHERHEIT

PRIVILEGED IDENTITY AND ACCESS

WORKLOAD IDENTITIES UND APP INTEGRATION

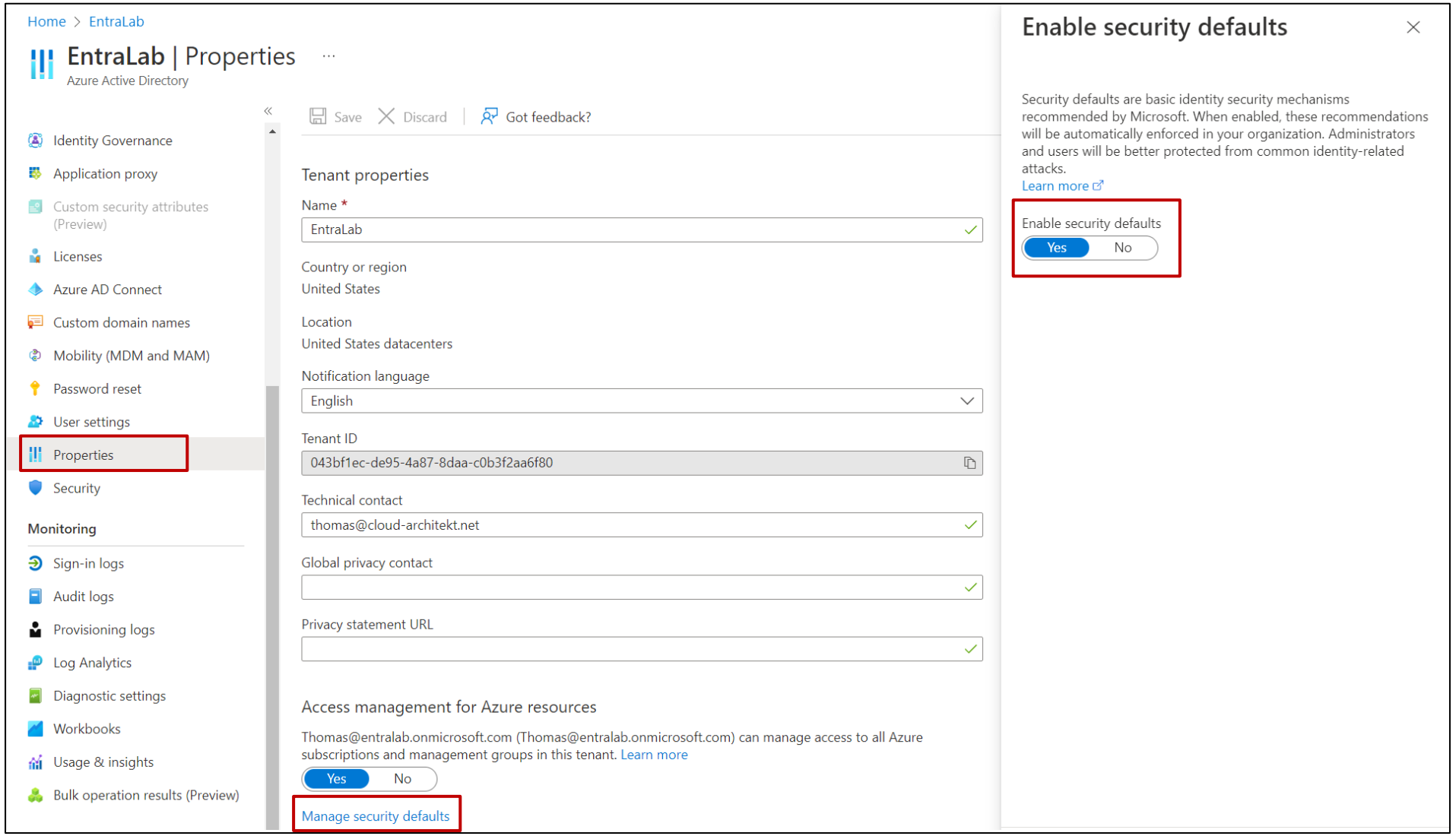
IDENTITY SECURITY POSTURE

Angriffe auf “Modern Identity”

The cybersecurity bell curve:
Basic security hygiene still protects against 98% of attacks

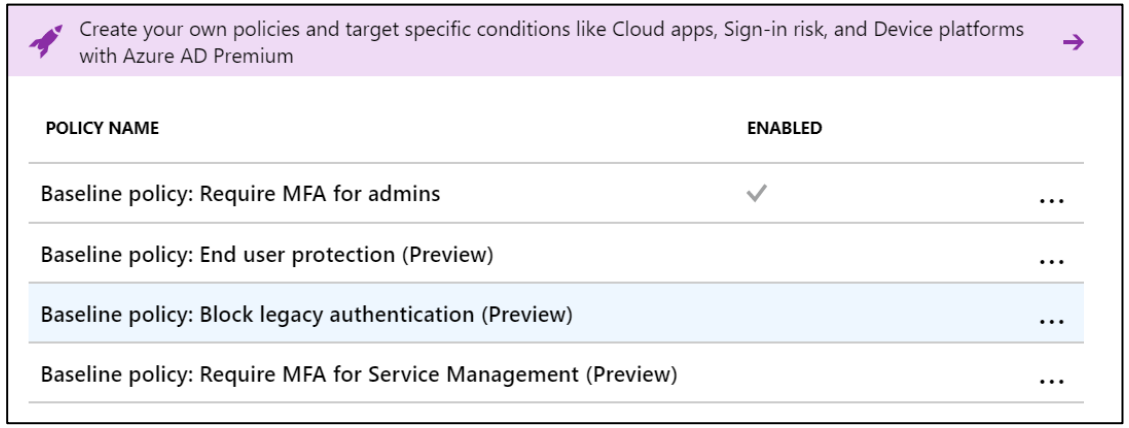
Source: Microsoft (“Identity is the new battle ground”)

Security Defaults für alle Azure AD Tenants



Security Defaults für alle Azure AD Tenants

- Frühere “Baseline” policies in Conditional Access

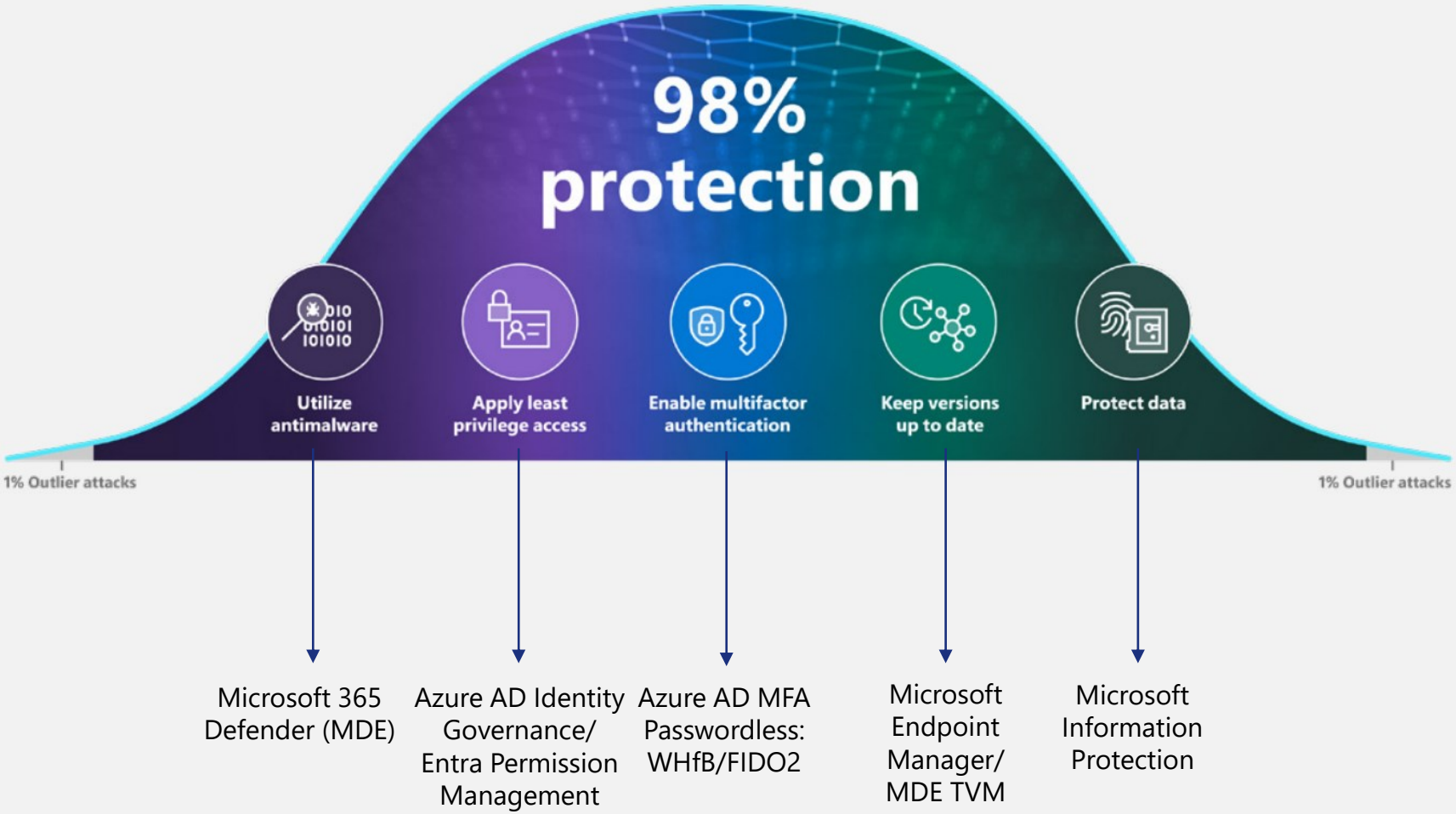


- Keine zusätzlichen Kosten oder Azure AD Lizenzen notwendig
  (verfügbar für alle, standardmäßig aktiviert bei neuen Azure AD Tenants)

- *“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.****”*

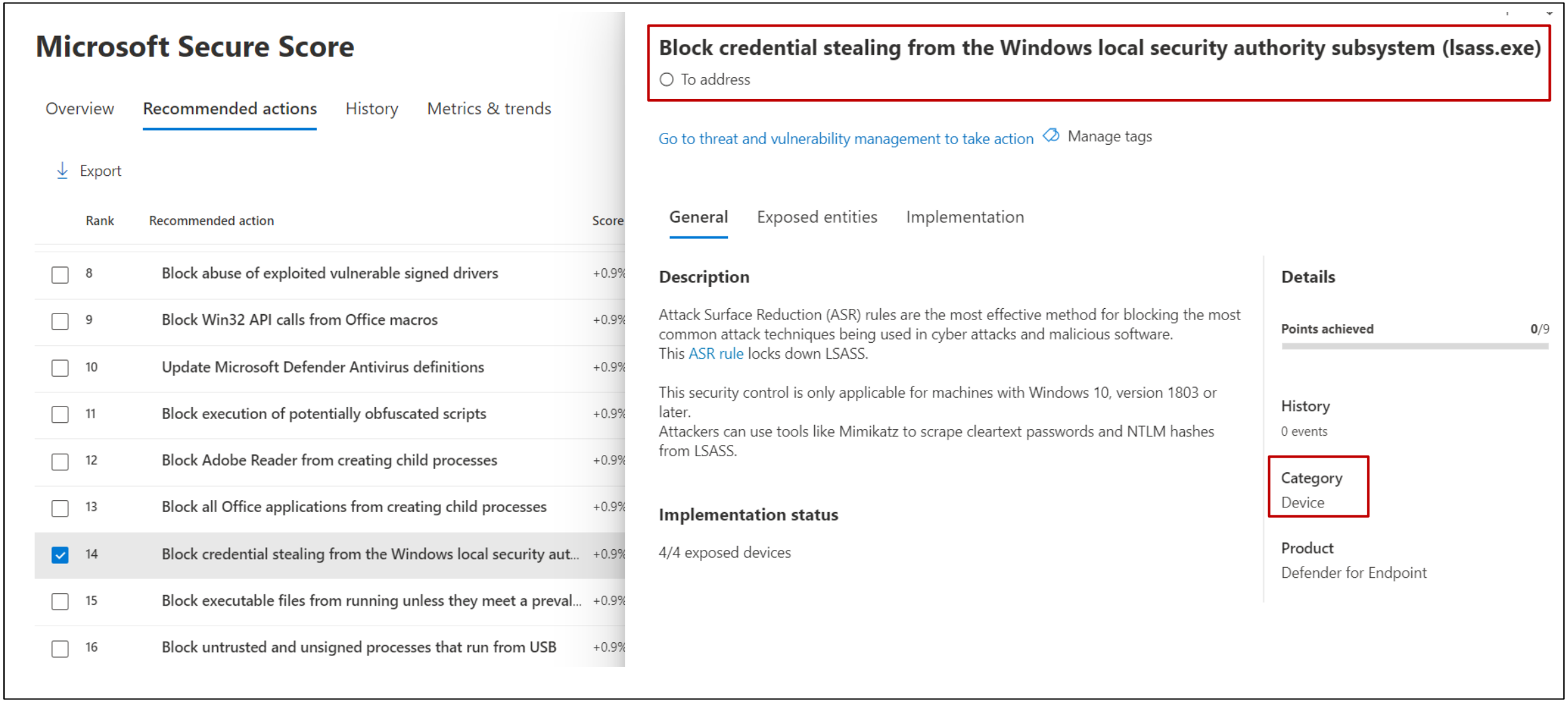
  Quelle: Introducing security defaults - Microsoft Tech Community

Schutz der “Modern Identity”

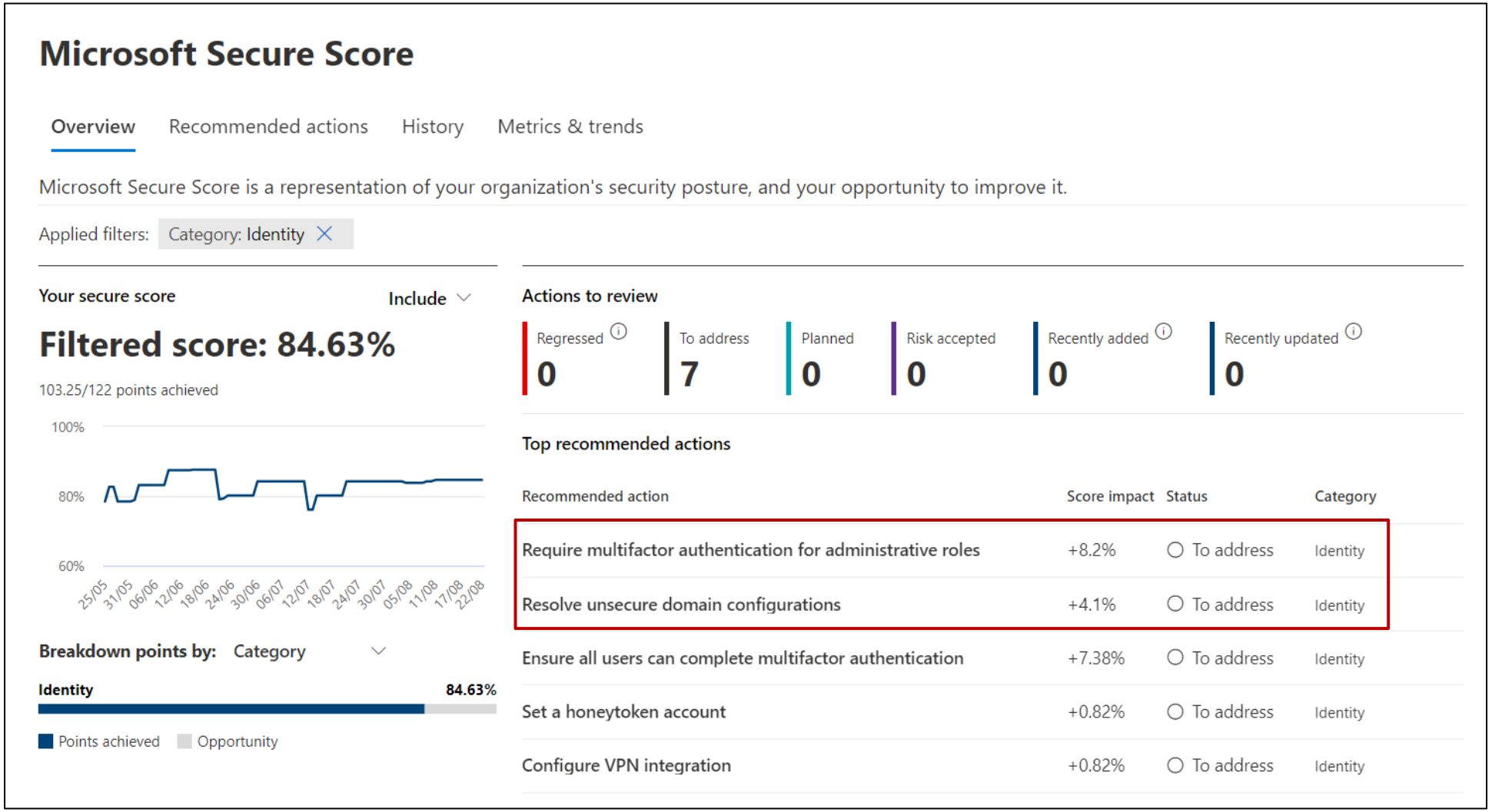


Source: Microsoft (“Identity is the new battle ground”)

Microsoft Secure Score



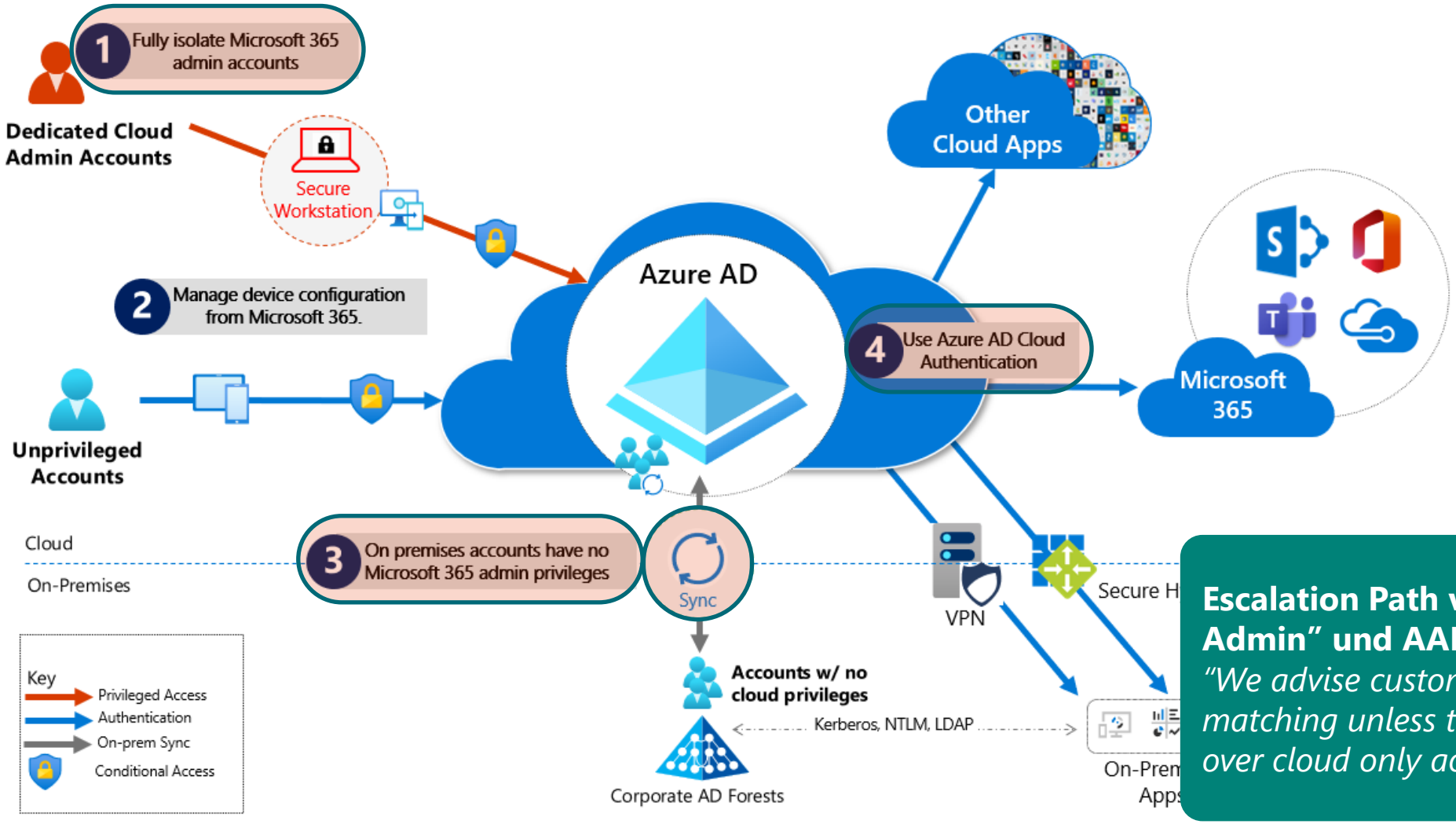
Microsoft Identity Secure Score



DEMO

Default Tenant Security
& Strong Authentication

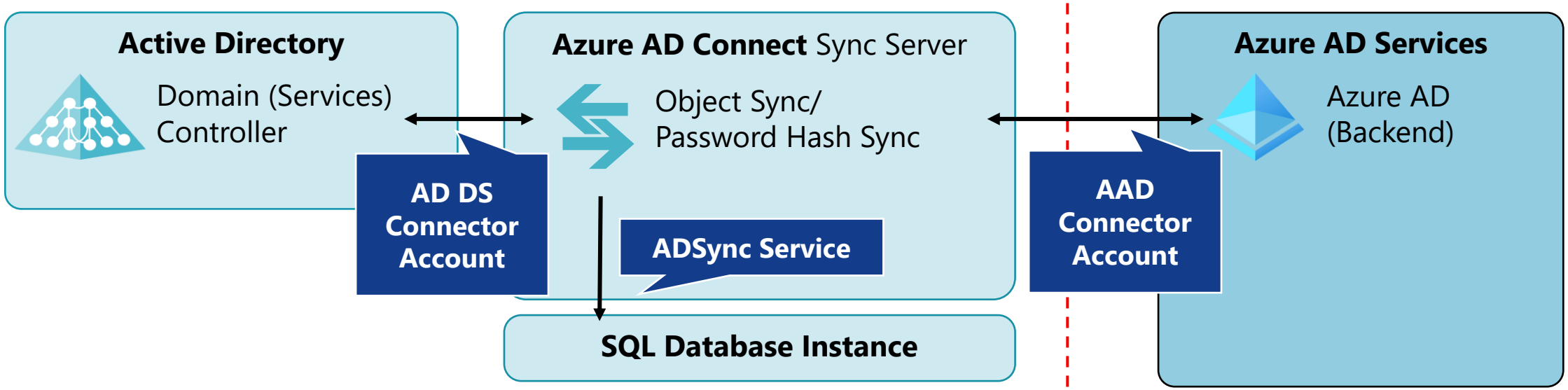
Angriffsfläche und -pfade bei Hybrid Identity



Escalation Path von "Hybrid Identity Admin" und AAD Connect:
"We advise customers to disable soft matching unless they need it to take over cloud only accounts"

Source: Microsoft ("Protecting Microsoft 365 from on-premises attacks")

Azure AD Connect: Dienstkonten und -zugriffe



DEMO

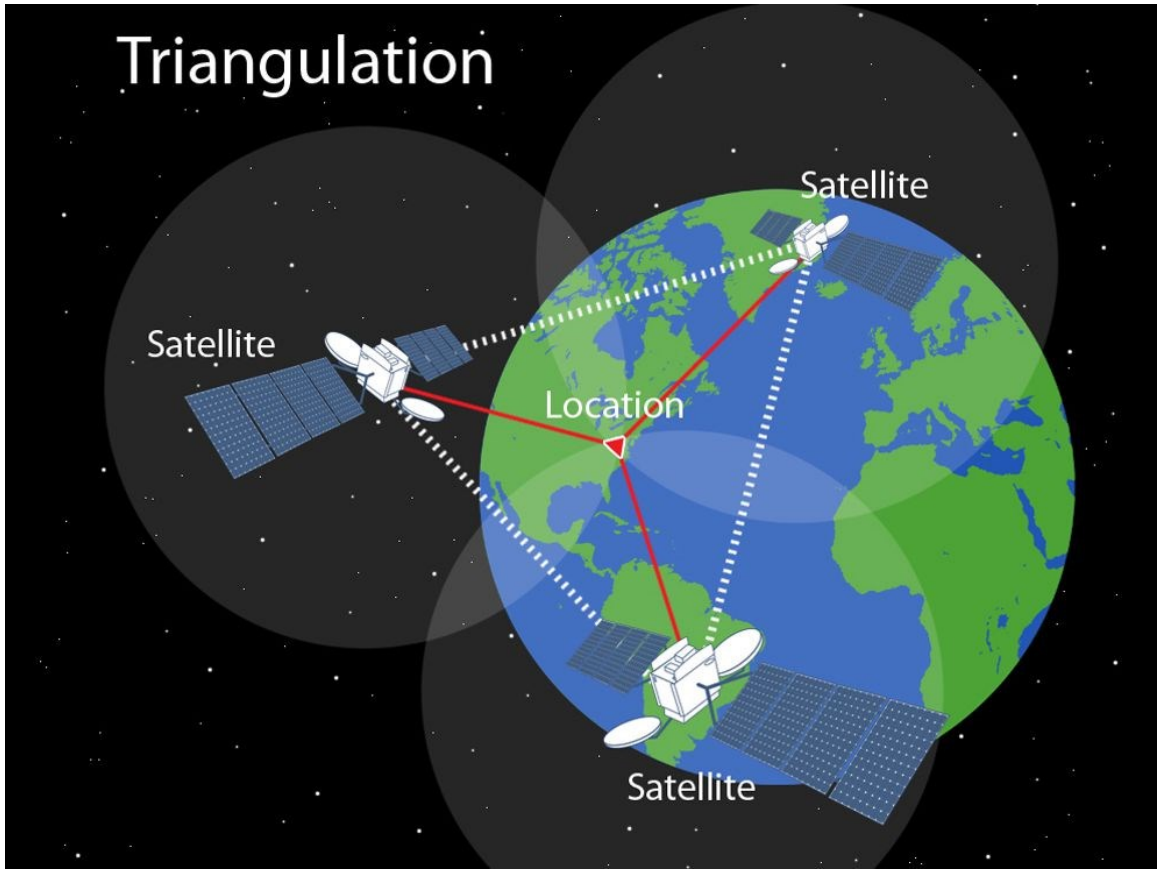
Privilege Escalation von Azure AD Connect nach Azure Active Directory

CONDITIONAL ACCESS UND TOKEN SICHERHEIT

Design von Conditional Access Policies

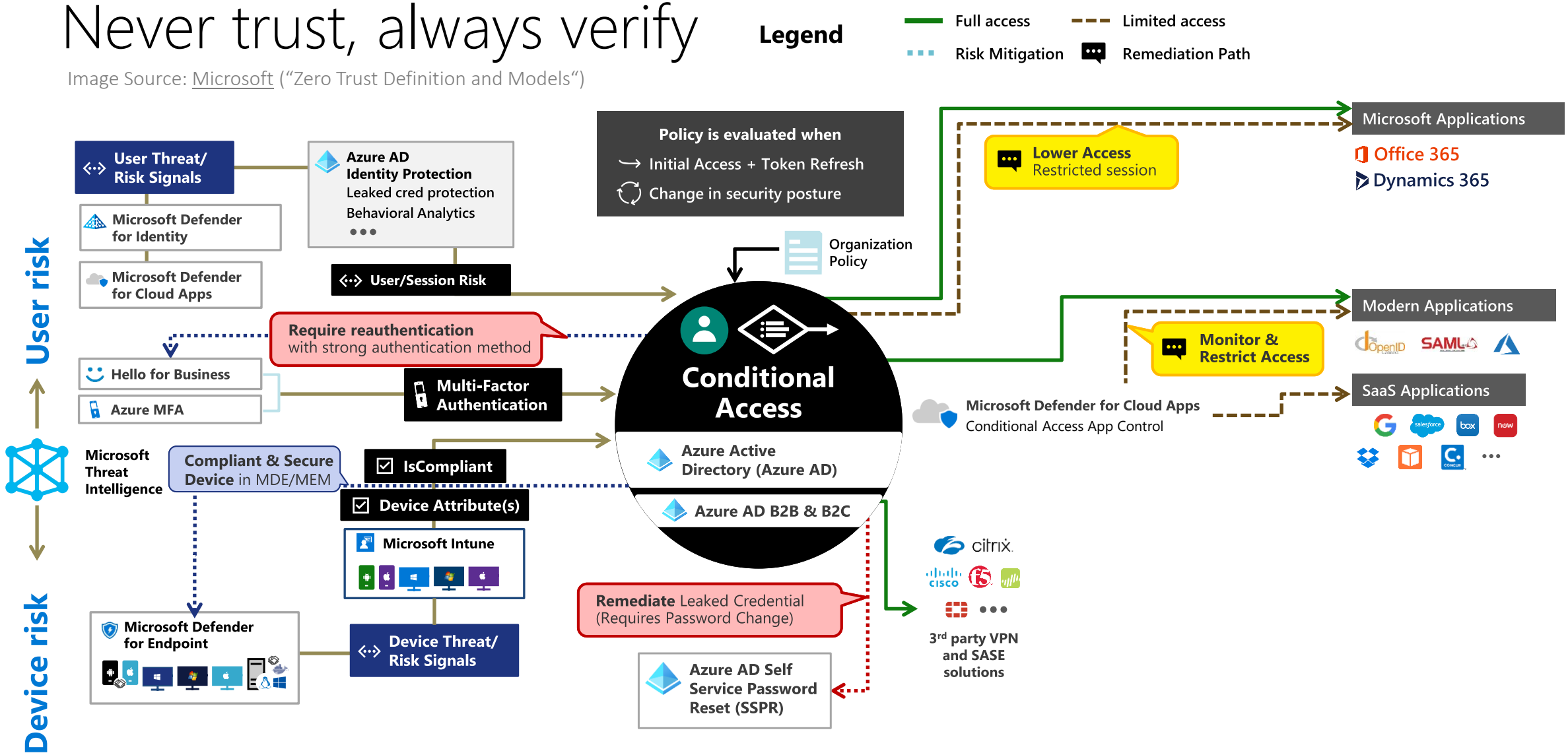
Schütze jeden Benutzer und jede App durch ein einfaches aber effektives Conditional Access Design!

Effektive “Conditions” und “Controls”



Never trust, always verify

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



Signal
to make an informed decision

Decision
based on organizational policy

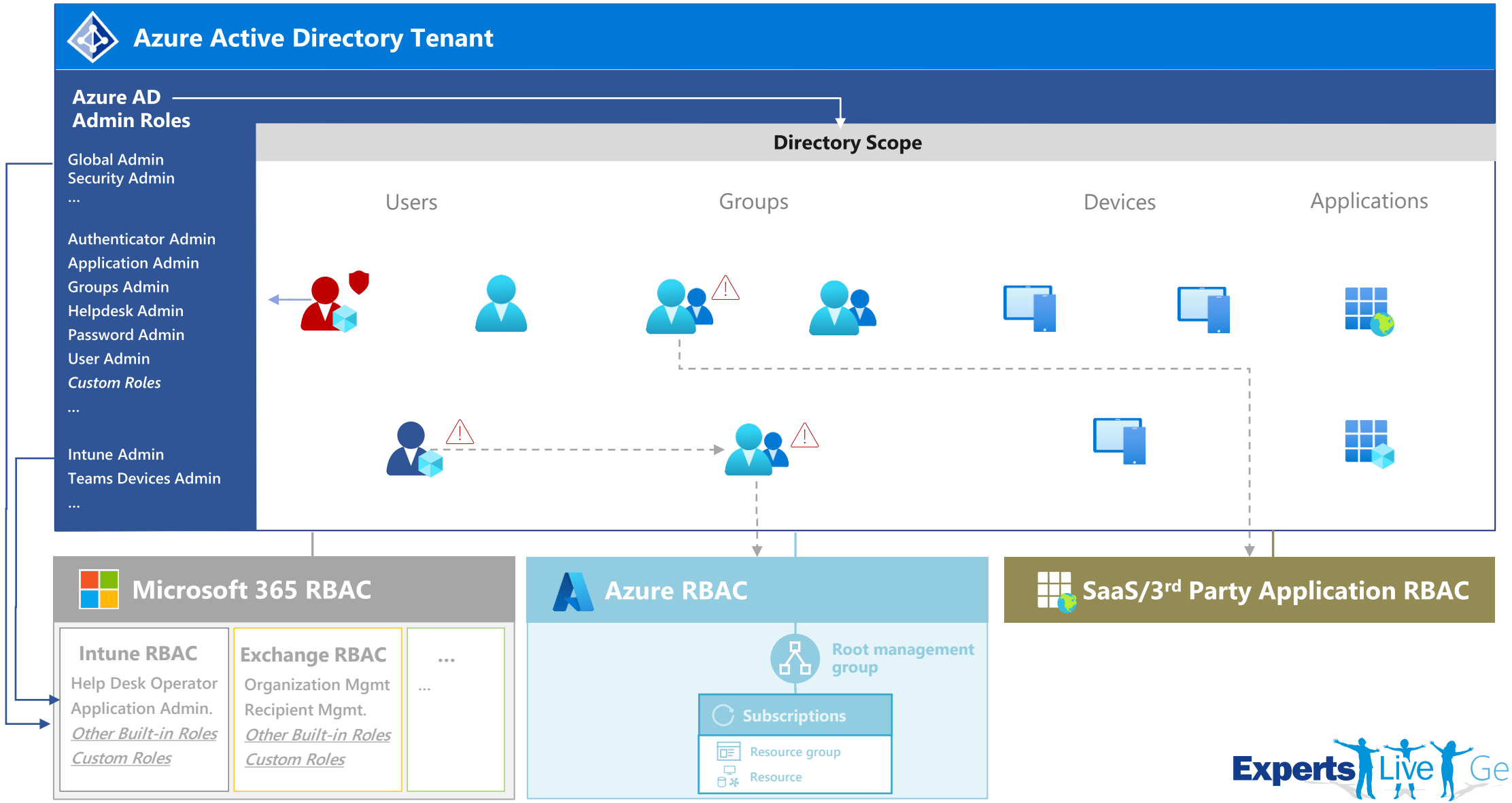
Enforcement
of policy across resources

DEMO

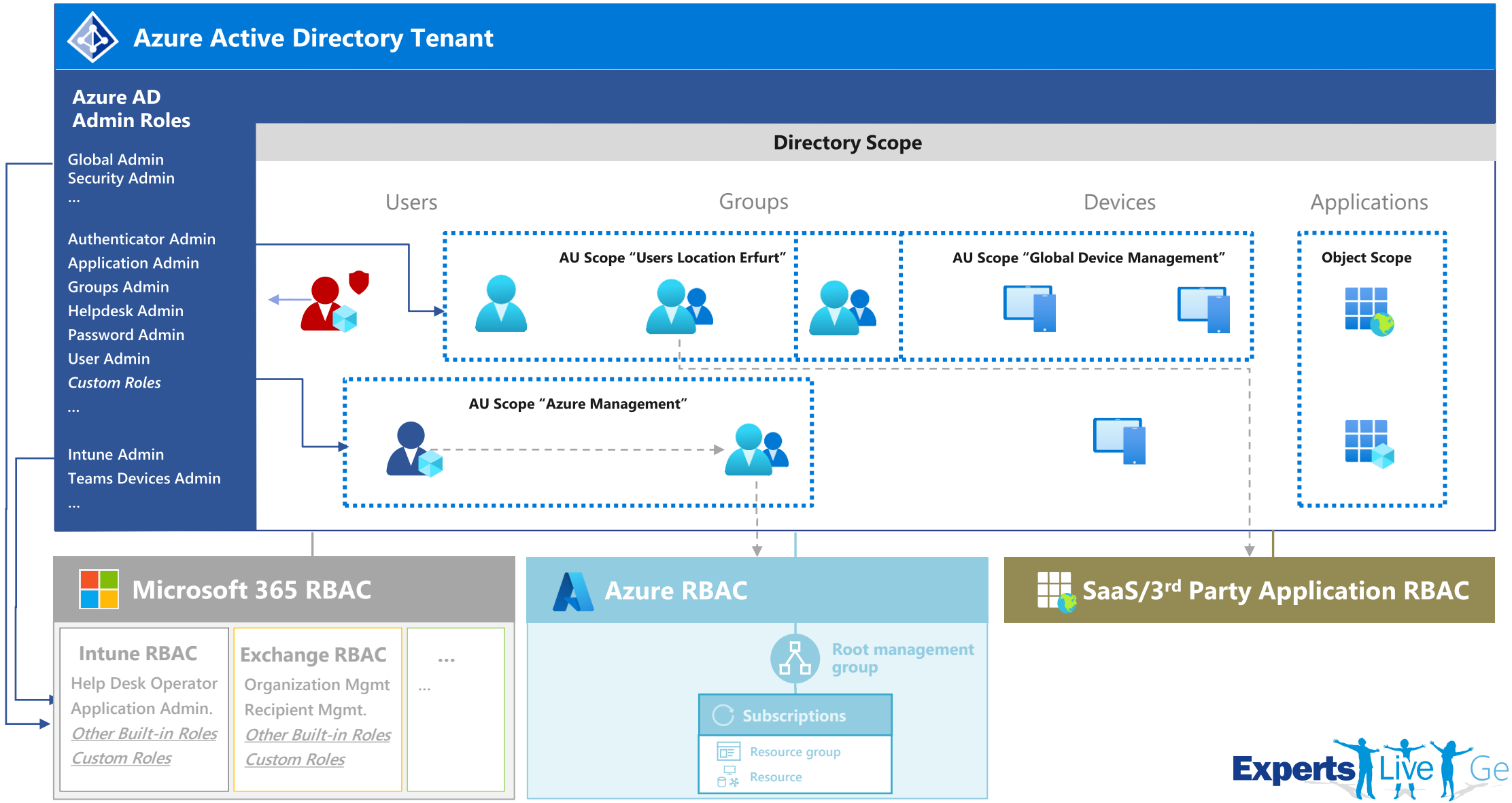
Templates von Conditional Access, Token und Cloud Session Security

PRIVILEGED IDENTITY AND ACCESS

Delegierung mit Azure AD RBAC



Delegierung mit Azure AD RBAC



DEMO

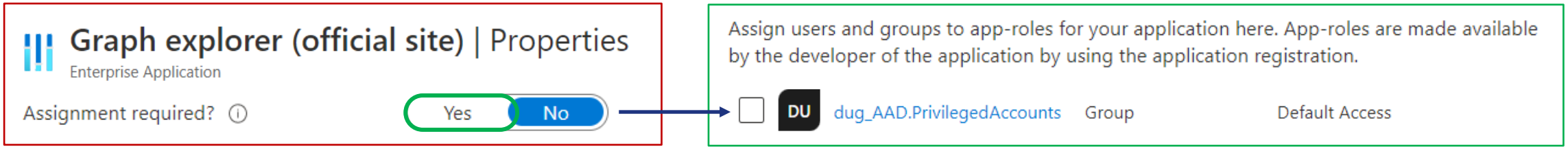
Sensitive Azure AD RBAC roles
und Delegierung von Admin. Tasks

APP INTEGRATION UND WORKLOAD IDENTITIES

Experts Live Germany

Kritische Berechtigungen für Azure AD Apps

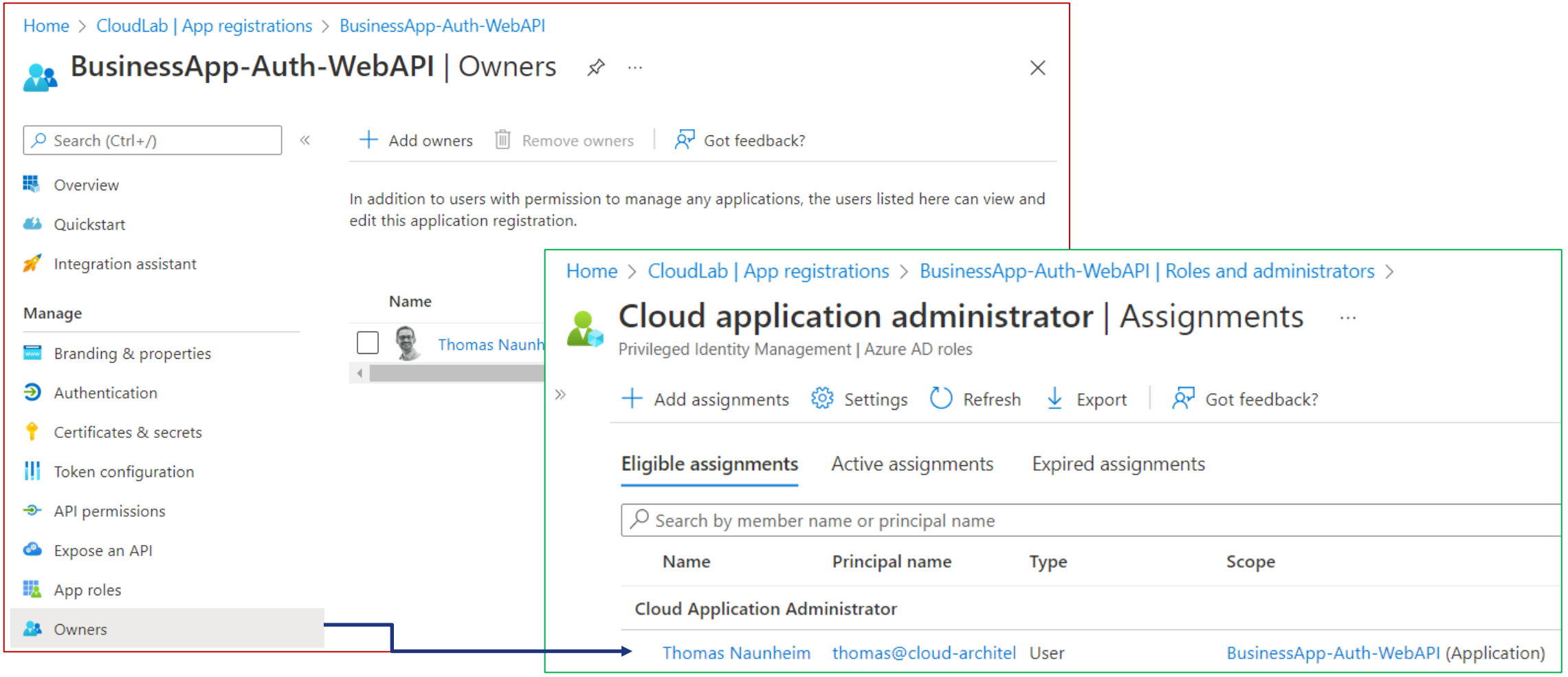
- Eingeschränkte Zugriff auf Enterprise App bei sensitive Delegated Permissions



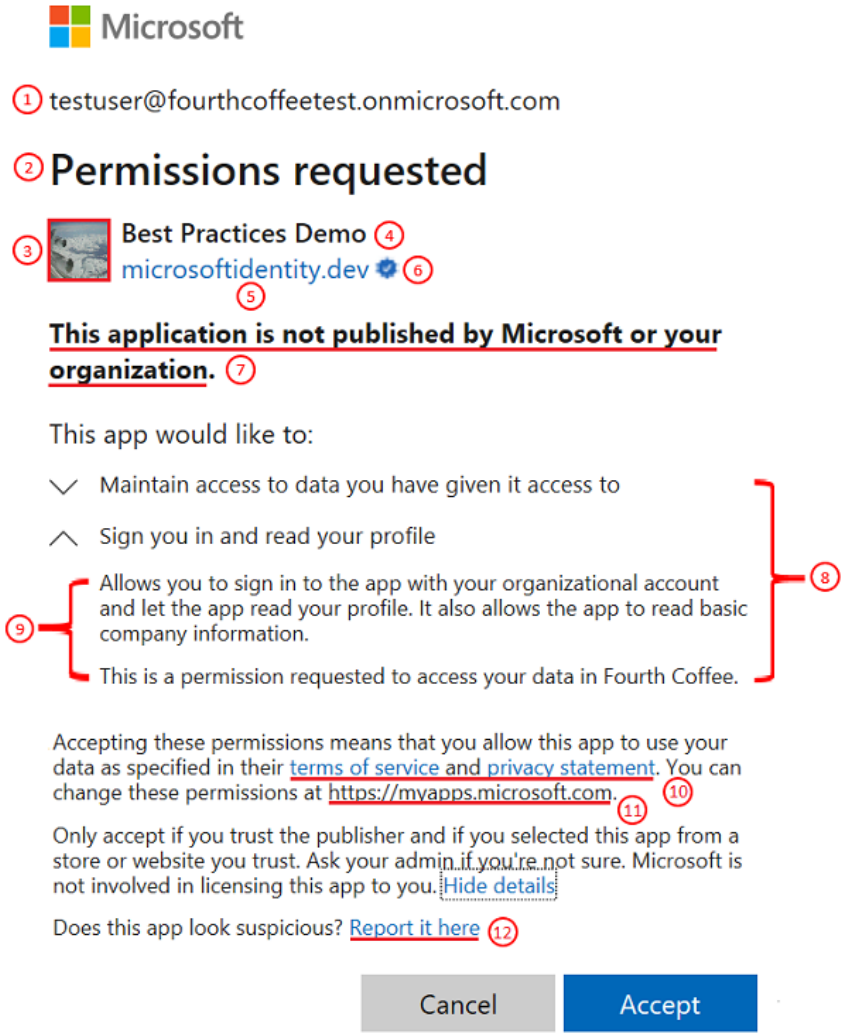
- Standardmäßige Berechtigung zur Registrierung von Enterprise Apps (Service Principals)

Kritische Berechtigungen für Azure AD Apps

- Berechtigung auf “Application” und “Service Principal” Objekte und Credentials



User Consent und Phishing Angriffe



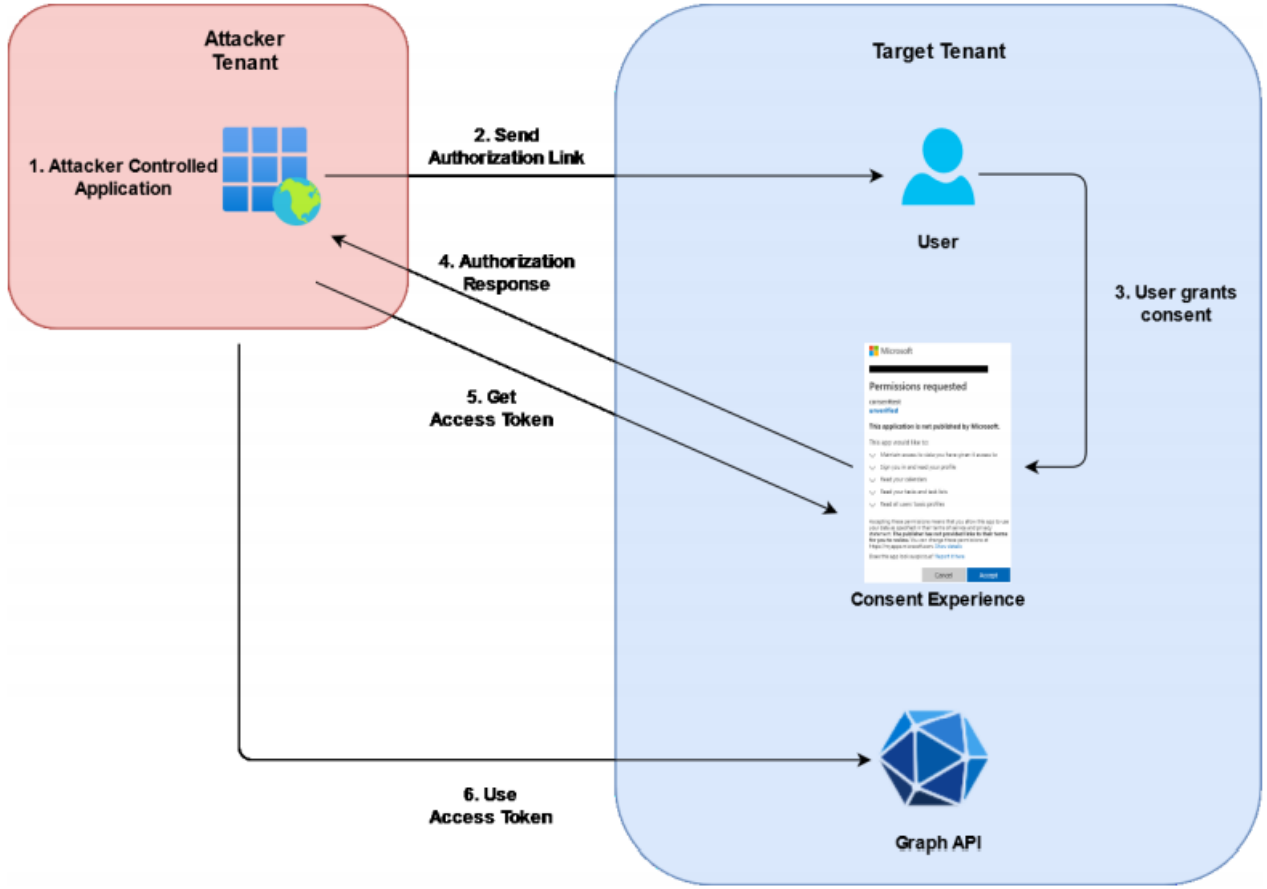


Image source: Introduction To 365-Stealer by Altered Security

DEMO

Illicit Consent Grant Attacks und Consent (Framework) Permission

Azure AD Security | Zusammenfassung

Implementierung eines “Identity Security Posture” Management und Übeprüfung 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

Experts Live Germany

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

Experts Live Germany