Webinar:
Azure Readiness - IAM, 4.11.2021.

Herzlich willkommen.

Andreas Gotti
Leiter Business Unit Software Solutions

Bechtle Schweiz AG

Samya Henz
Solution Architekt, Projektleiterin

Bechtle Schweiz AG

Lütfi Civan
Teamleiter Microsoft Team

Bechtle Schweiz AG

Agenda

1. Benutzer- und Rechteverwaltung in Azure
2. Applikationsintegration und -zugriffe in Azure
3. Klassische IAM-Systeme am Beispiel iam amira und Vergleich zu Azure AD
4. Welche Vorteile hat iam amira gegenüber Azure AD
5. Stärken und Vorteile einer möglichen Zielarchitektur mit iam amira und Azure AD
6. Erweiterte Szenarien und Ausblick
7. Wrap-Up
8. Beantwortung von Fragen

Benutzer- und Rechteverwaltung in Azure

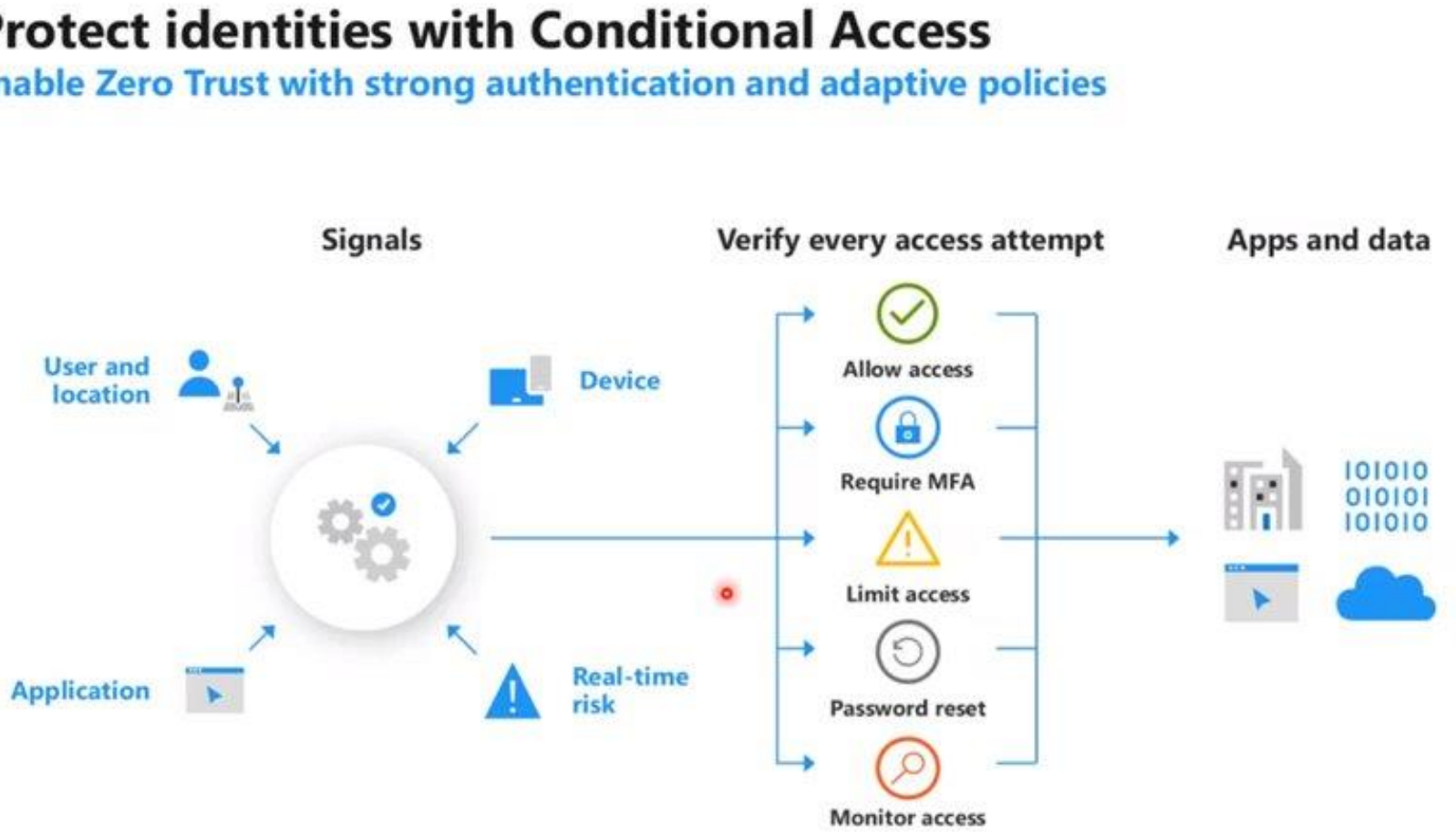
Benutzer- und Rechteverwaltung in Azure

Identity and Access Management critical capabilities

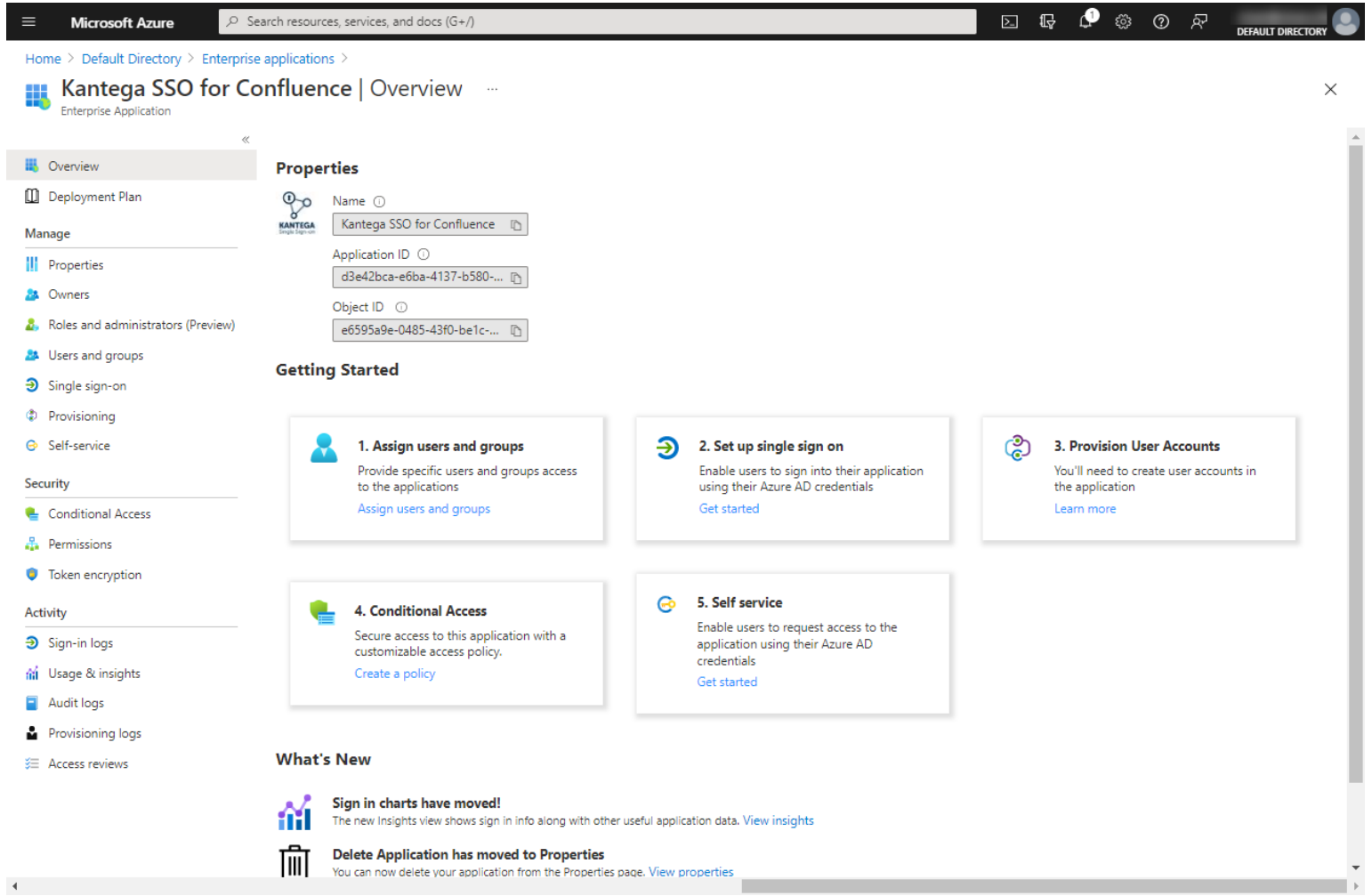
Authentication	Authorization	Administration	Governance	Self-Service Management	Customer IAM	Managing Cloud Infrastructure
✓ User Authentication ✓ MFA ✓ Single Sign on (SSO) ✓ Federation ✓ Passwordless ✓ Certificate/Smartcard based authentication	✓ Machine learning based risk scoring ✓ Adaptive Access ✓ Oauth Authorization ✓ OAuth Token ✓ Attribute mapping ✓ RBAC ✓ Session lifetime management ✓ ABAC	✓ User Management ✓ Group Management ✓ Domain Management ✓ Delegated Administration ✓ Application Management ✓ Password Management	✓ Access certifications ✓ Privileged Access/JIT ✓ Entitlement management ✓ Identity Lifecycle ✓ Access Requests ✓ Workflow ✓ Provisioning ✓ Policy management ✓ Reporting & Analytics ✓ Data Access Policies	✓ Password Reset ✓ Group Management ✓ Credential Registration ✓ Credential Recovery ✓ App Launching ✓ App Catalog ✓ Access Requests ✓ Profile Management	✓ Social Identity Federation ✓ Self-Service Registration ✓ Custom End User Experiences ✓ Customer Data Management ✓ Consent Management ✓ Administer Users & Partners ✓ Privacy Management	✓ Managed Identities ✓ PaaS Identity management ✓ IaaS/VM Identity Management

Applications Access	
Cloud Apps	**Classic Apps**
✓ Pre-integrated SSO and Provisioning ✓ BYO SAML & OATH 2.0 ✓ Custom Provisioning (SCIM)	✓ Web Access Manager (Kerberos, SAML, OATH2, Header-based) ✓ Hosted Directory Services (LDAP, NTLM, Kerberos) ✓ Secure Hybrid Access (Akamai, Arayaka, Citrix, F5, Zscaler) ✓ Windows VDI Integration

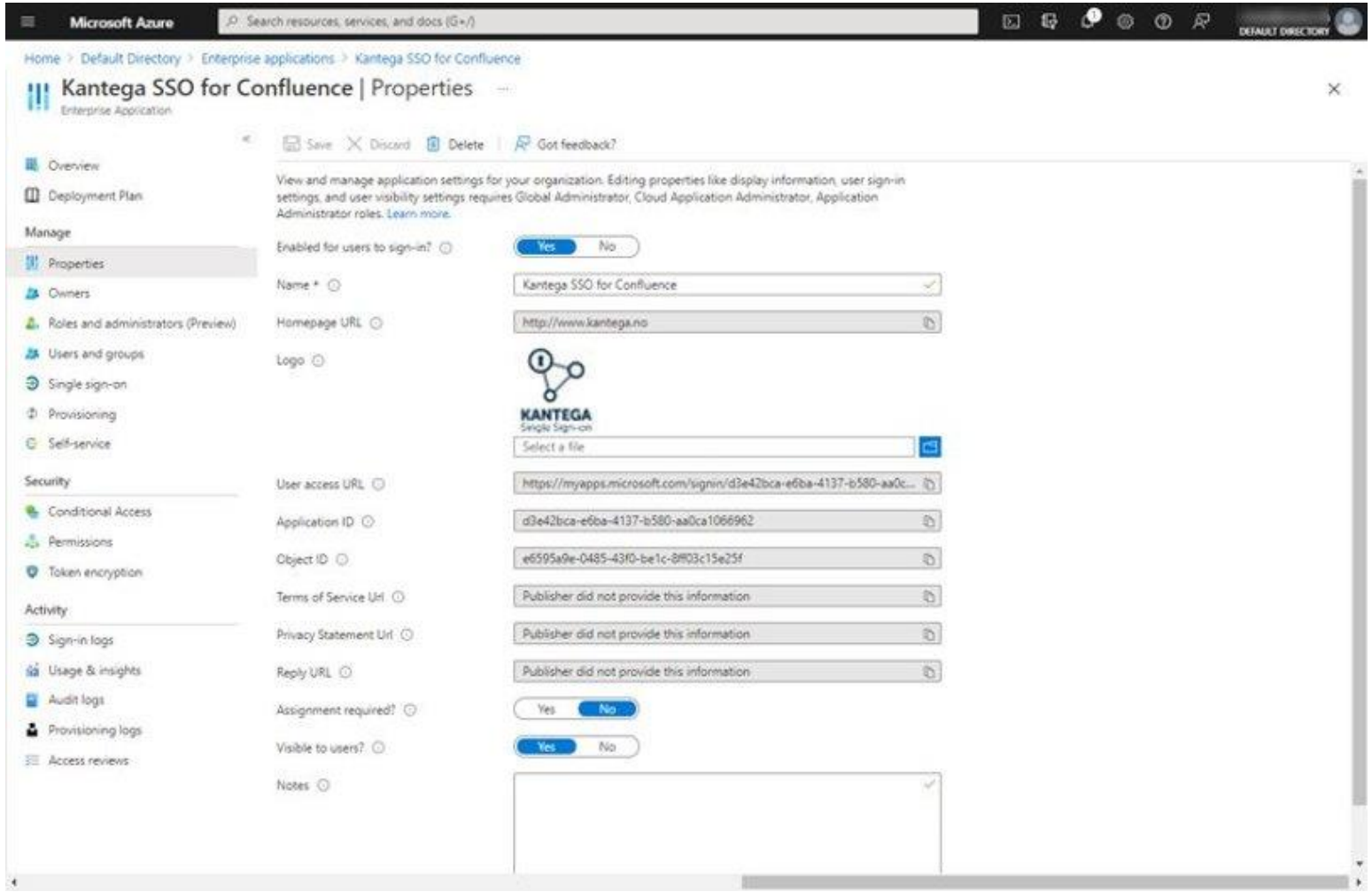
Benutzer- und Rechteverwaltung in Azure



Applikationsintegration und -zugriffe in Azure



Applikationsintegration und -zugriffe in Azure



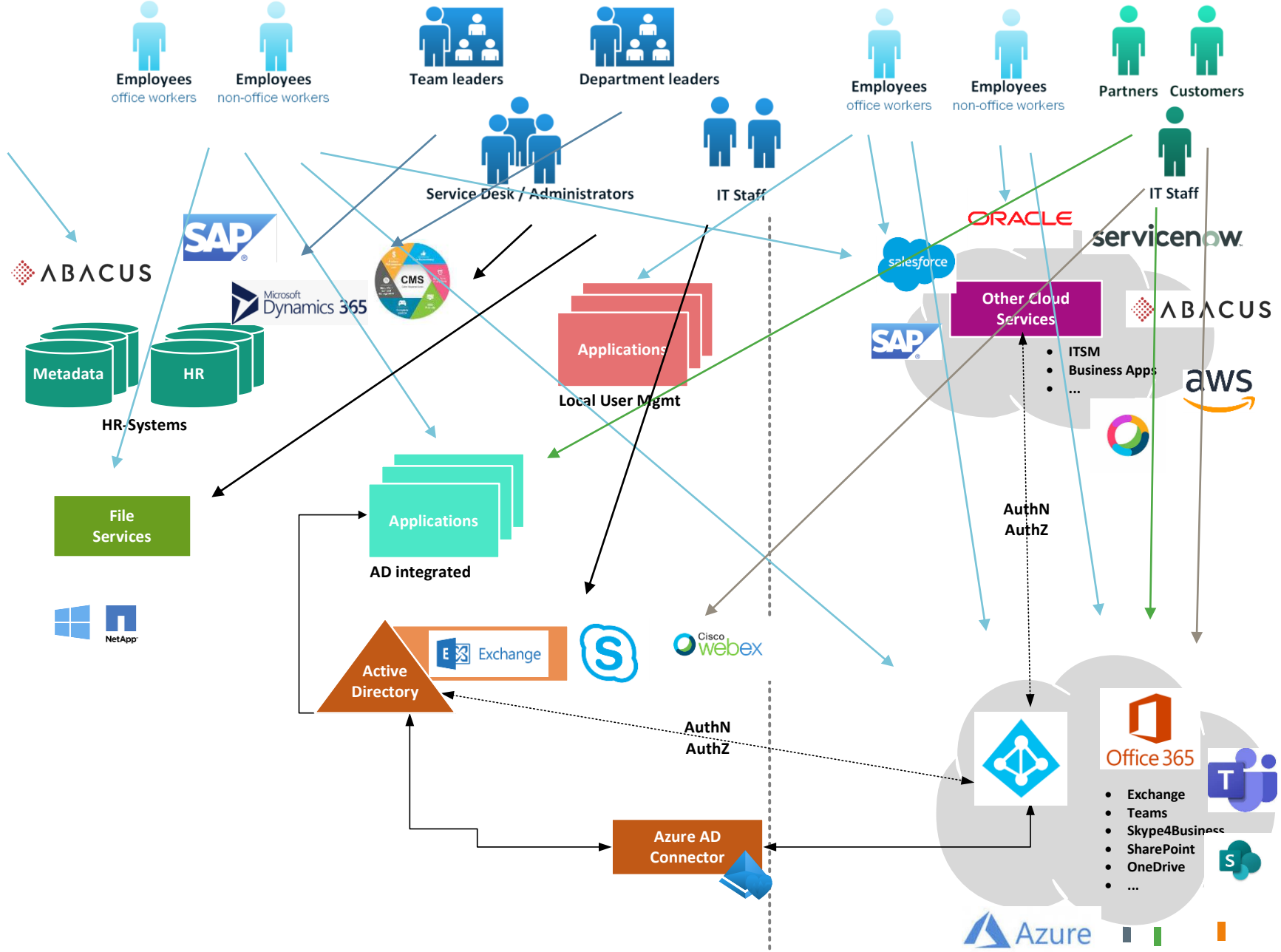
Typi

Users

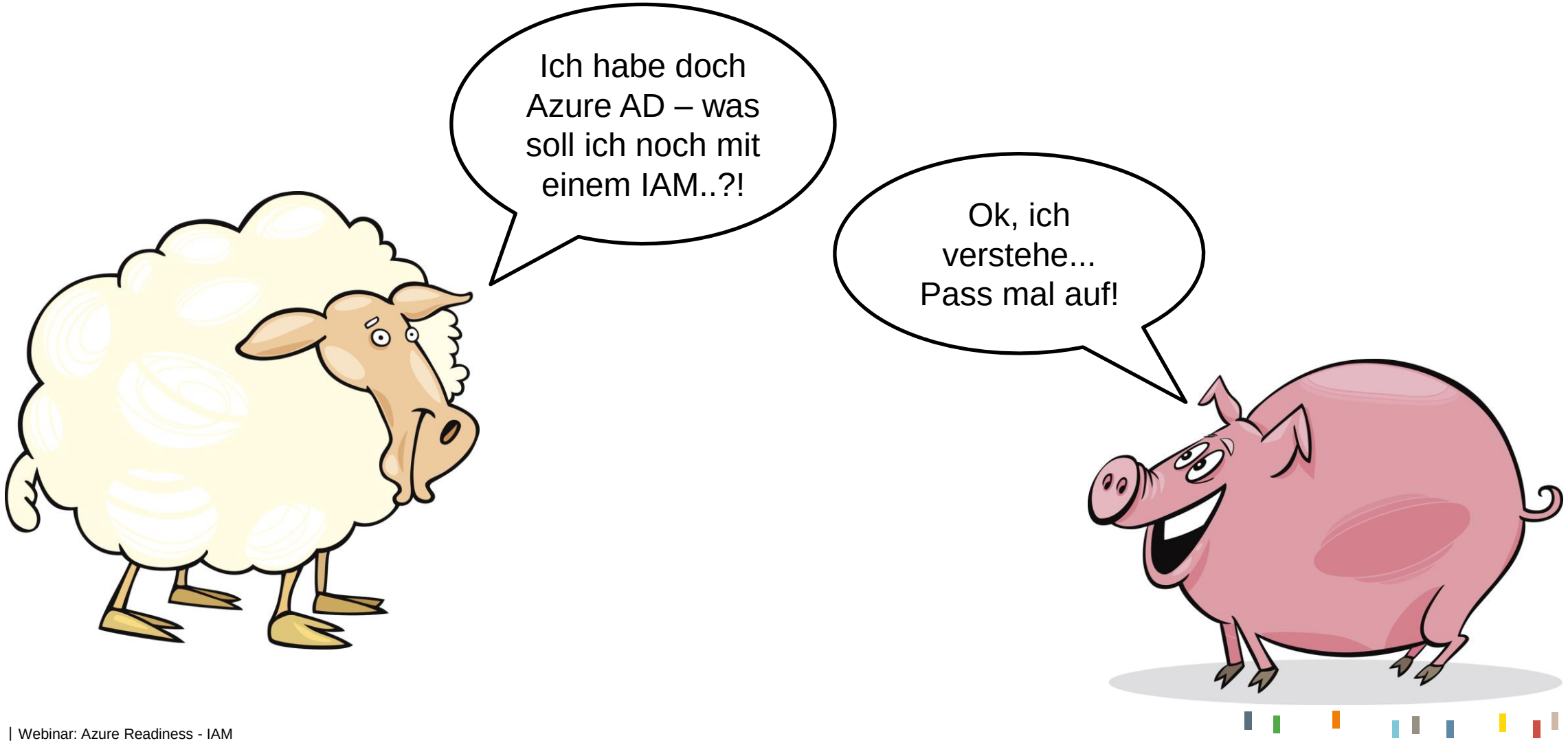
Applications

Appliances

Infrastructure



Was brauche ich – und was habe ich?



Was ist eigentlich Identity & Access Management (IAM)?

"Identity and access management (IAM) is the discipline that enables the **right individuals** to **access** the **right resources** at the **right times** for the **right reasons**. IAM is a crucial undertaking for any enterprise. It is increasingly business-aligned, and it requires **business skills**, not just **technical expertise**."

Quelle: Gartner Glossary

IAM ermöglicht

- … den richtigen Personen,
- … zur richtigen Zeit,
- … den richtigen Zugriff
- … auf die richtigen Ressourcen
- … aus dem richtigen Grund.

Betrifft Technik und Business

Klassische IAM-Systeme und Vergleich zu Azure AD

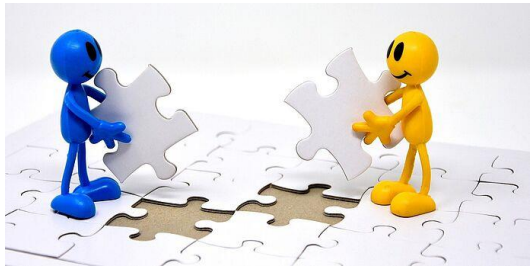
IAM Kernfunktionalitäten

- **Datenmodellierung** – gibt mir den Kontext und die Zusammenhänge
- **Abbildung der Prozesse** – gibt mir die Business-Sicht End-to-End
- **Policies und Automatisierung** – gibt mir die Effizienz und Qualität
- **Audit Trail** – gibt mir die Nachvollzierbarkeit und Transparenz
- **Automatisches (De-)Provisioning** – gibt mir Geschwindigkeit und Sicherheit
- **Plattformunabhängige Orchestrierung** – gibt mir die Unabhängigkeit und übergeordnete Kontrolle
- **Reporting** – gibt mir die Visibilität

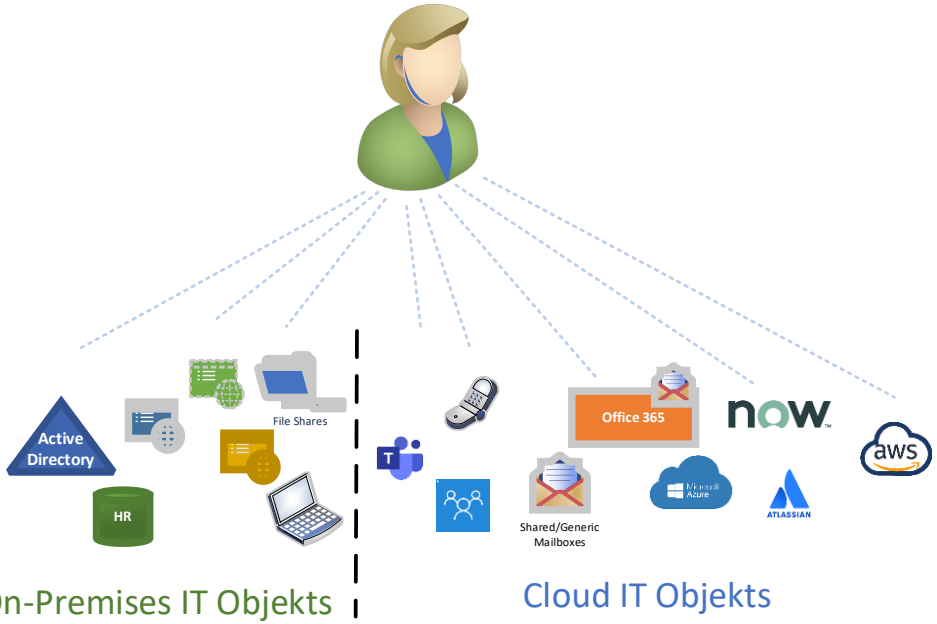
Wo sind die Hauptunterschiede zu Azure AD

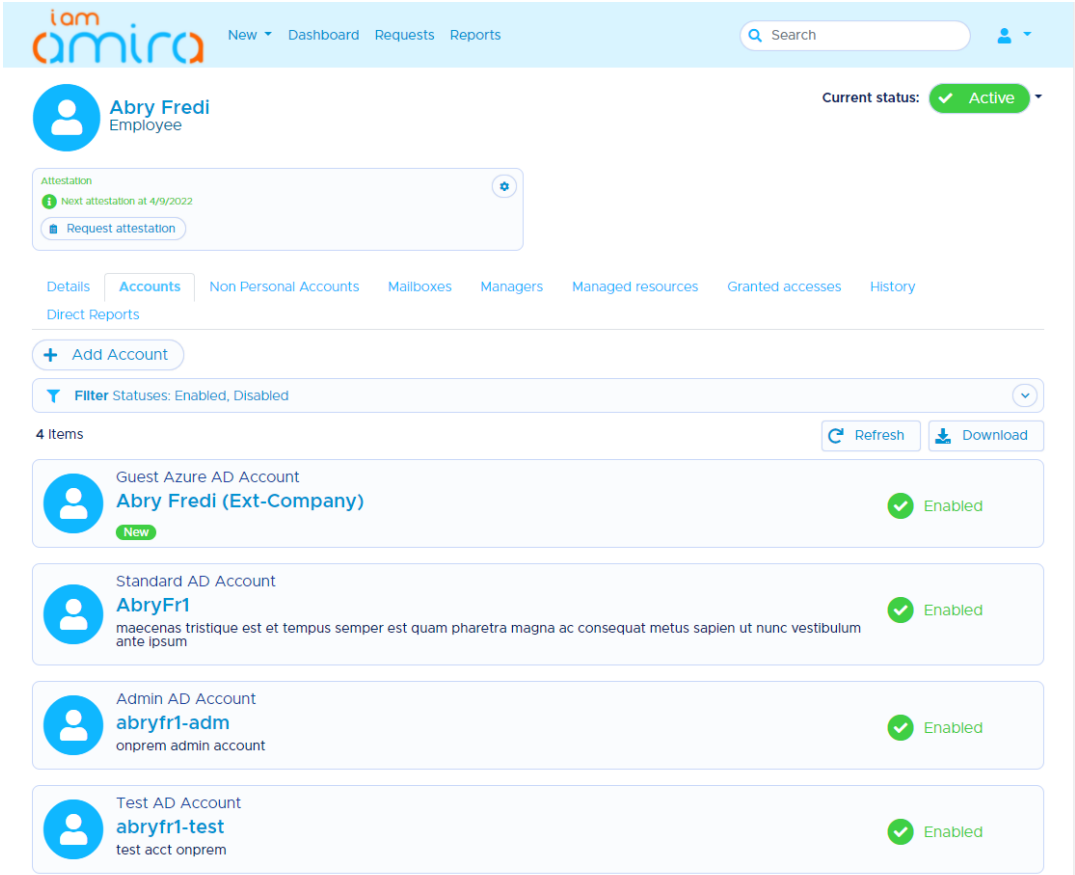
- **Identitäten vs. Accounts** – ist nicht das gleiche
- **Übergeordnete Business- und Prozess-Sicht** – weg von der Technik durch Abstraktion
- **Strikte Typisierung** – nicht alle sind gleich
- **Plattformunabhängigkeit** – nicht alles ist Himmelblau…

Vorteile von iam amira gegenüber Azure AD



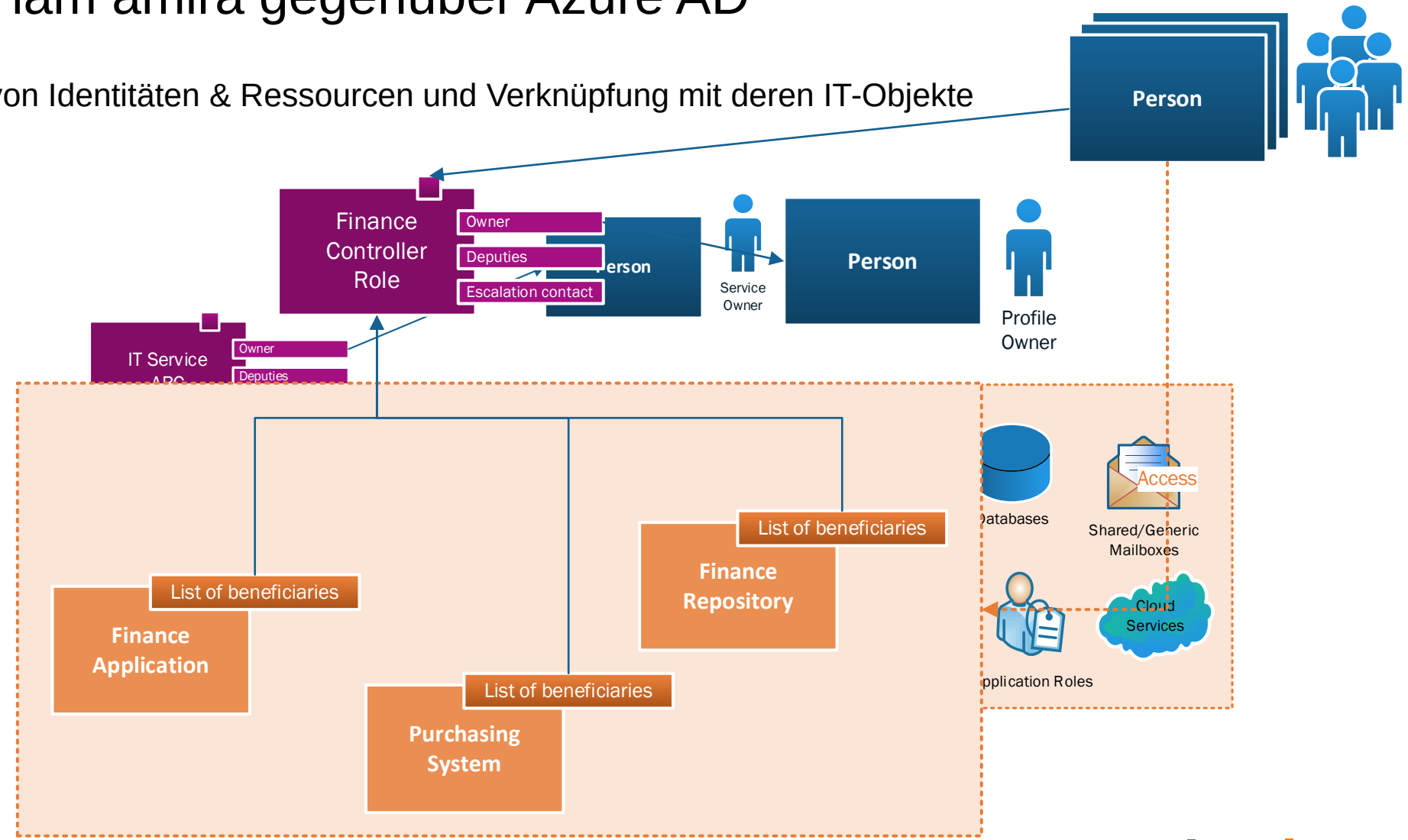
1. Modellierung von Identitäten & Ressourcen und Verknüpfung mit deren IT-Objekte





Vorteile von iam amira gegenüber Azure AD

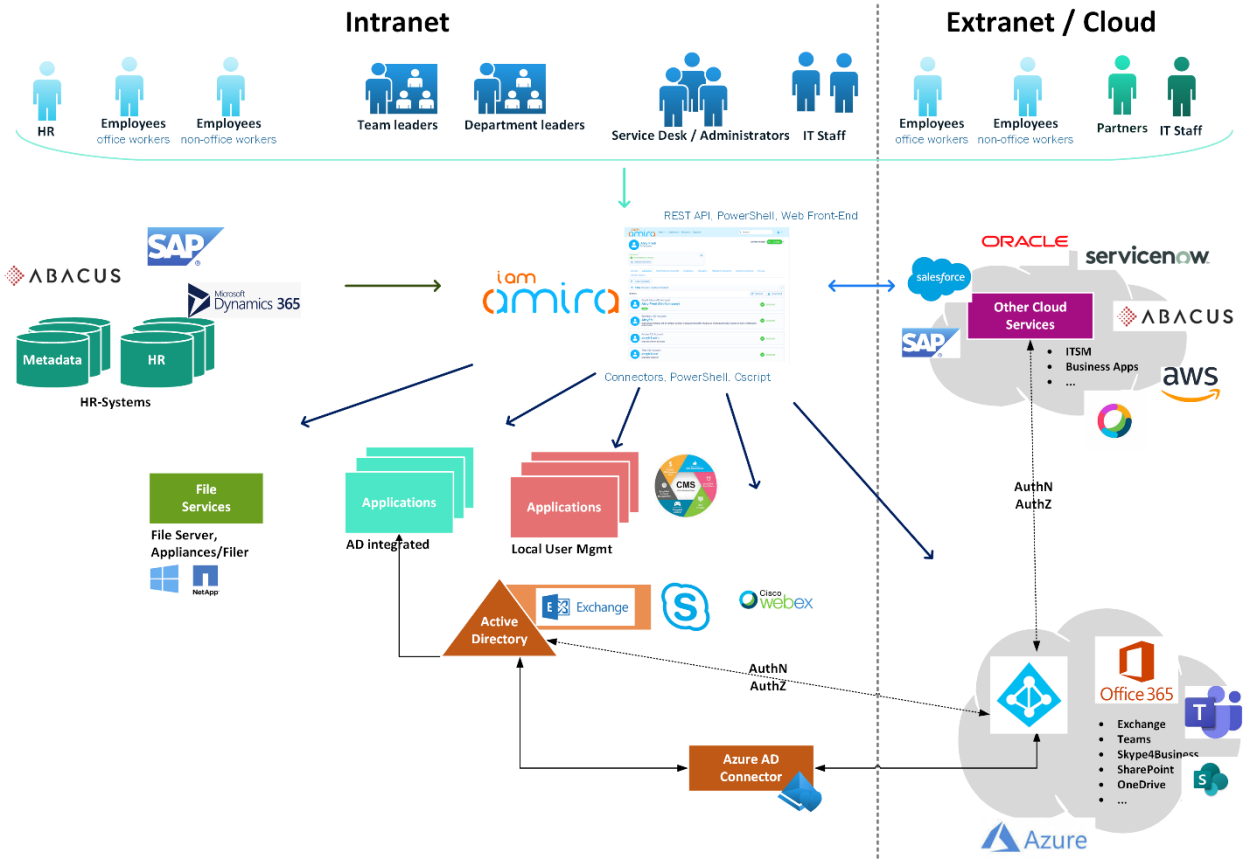
1. Modellierung von Identitäten & Ressourcen und Verknüpfung mit deren IT-Objekte



Vorteile von iam amira gegenüber Azure AD

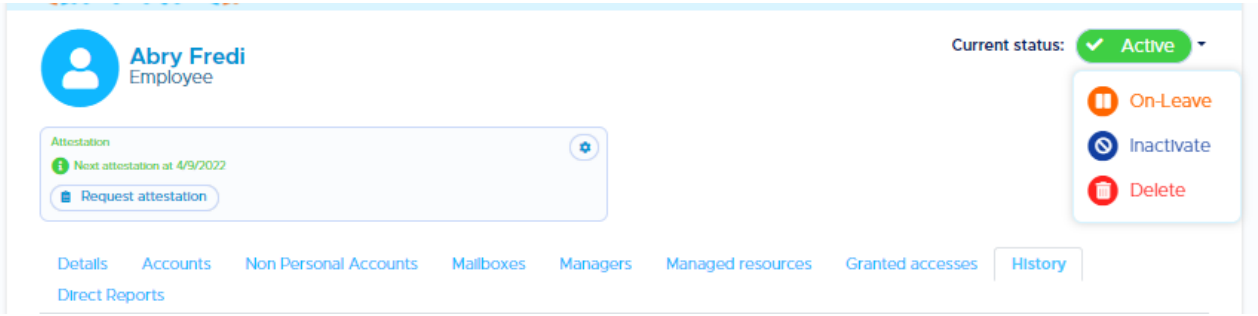
1. Modellierung von Identitäten & Ressourcen und Verknüpfung mit deren IT-Objekte

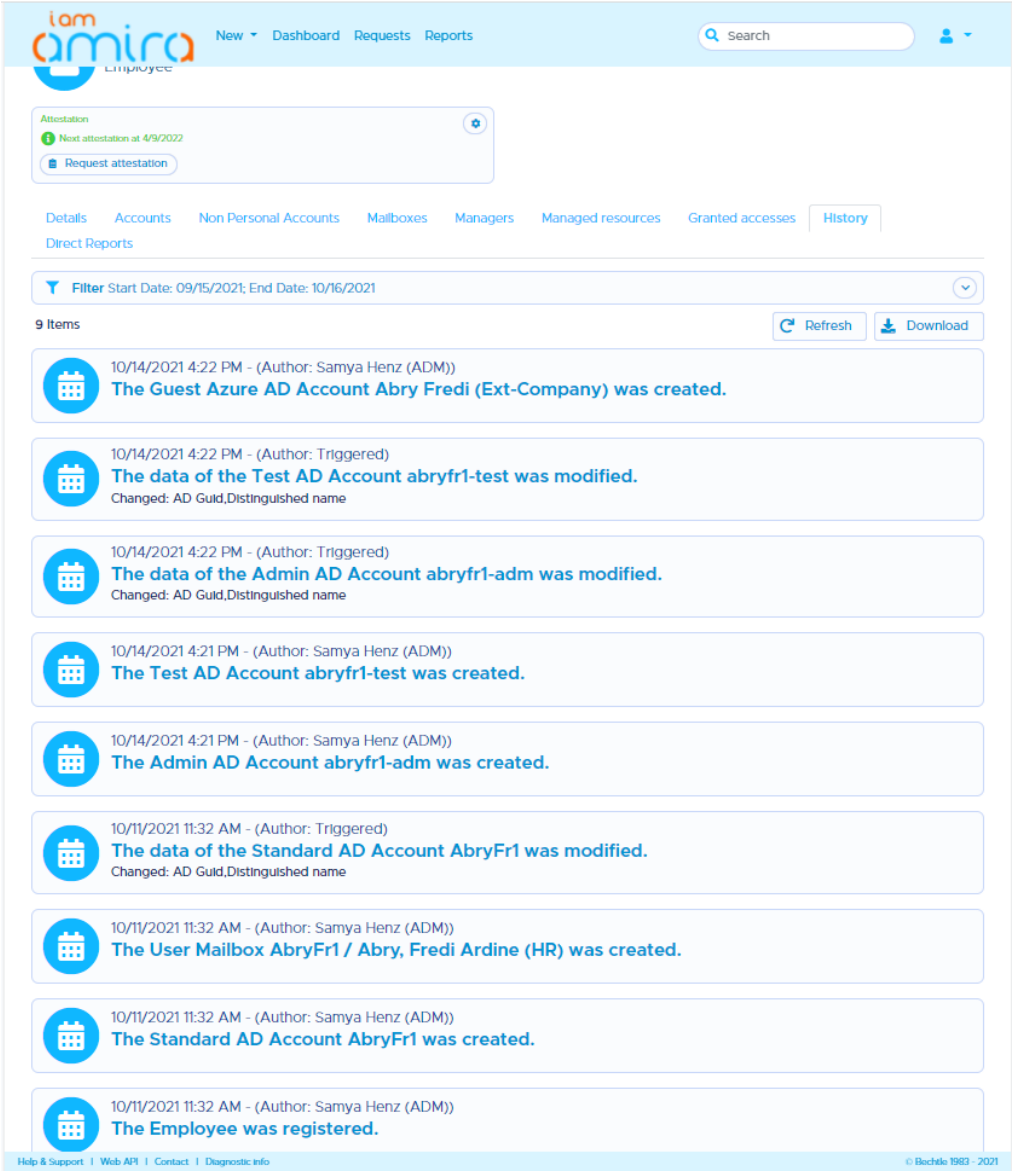
2. Plattformunabhängigkeit – Inbound und Outbound Systeme Anbindungen, On-premises wie in der Cloud



Vorteile von iam amira gegenüber Azure AD

1. Modellierung von Identitäten und Ressourcen Verknüpfung mit deren IT-Objekte
2. Plattformunabhängigkeit – Inbound und Outbound Systeme Anbindungen, On-premises wie auf die C
3. Lifecycle und Audit-Trail, Rollen-basierten Automatisierungen



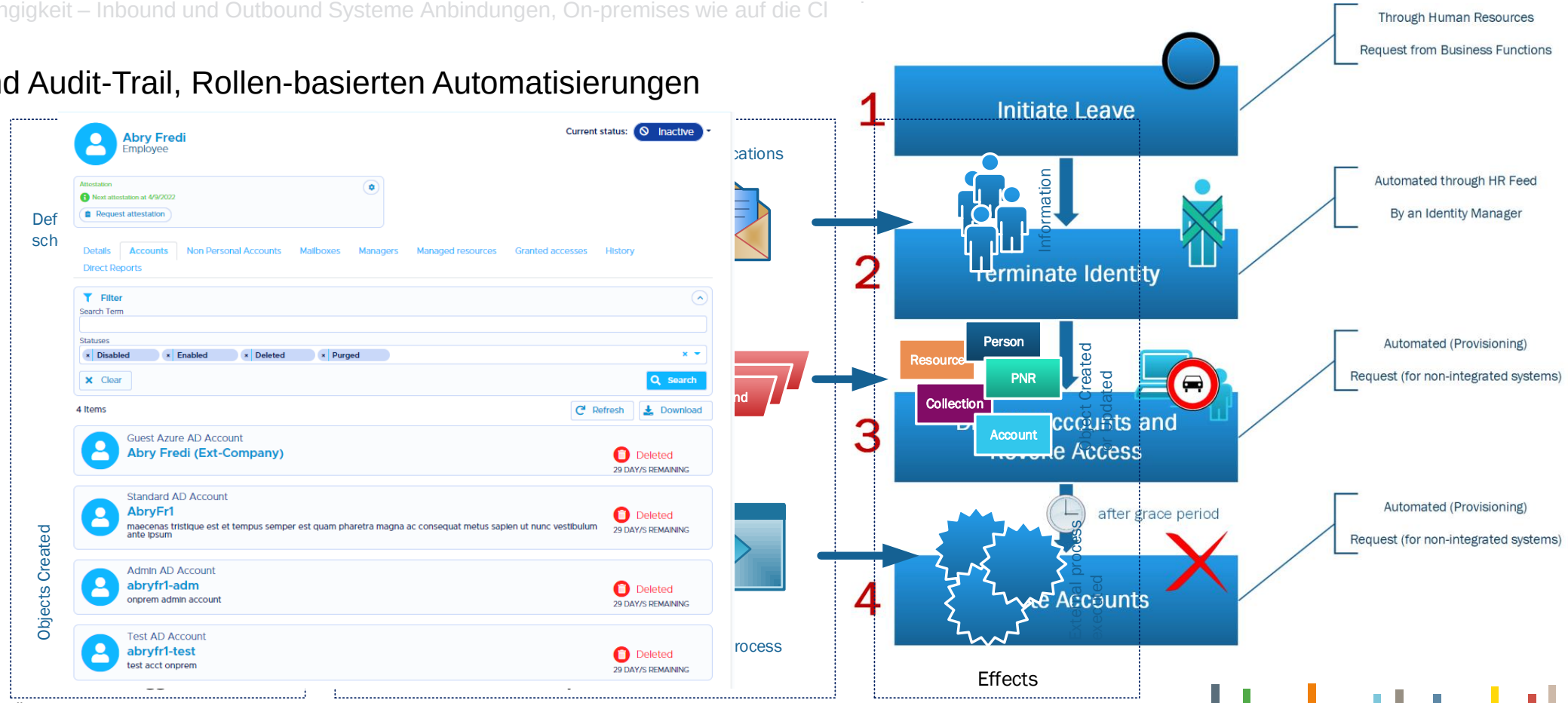


Vorteile von iam amira gegenüber Azure AD

1. Modellierung von Identitäten & Ressourcen und Verknüpfung mit deren IT-Objekte

2. Plattformunabhängigkeit – Inbound und Outbound Systeme Anbindungen, On-premises wie auf die Cl

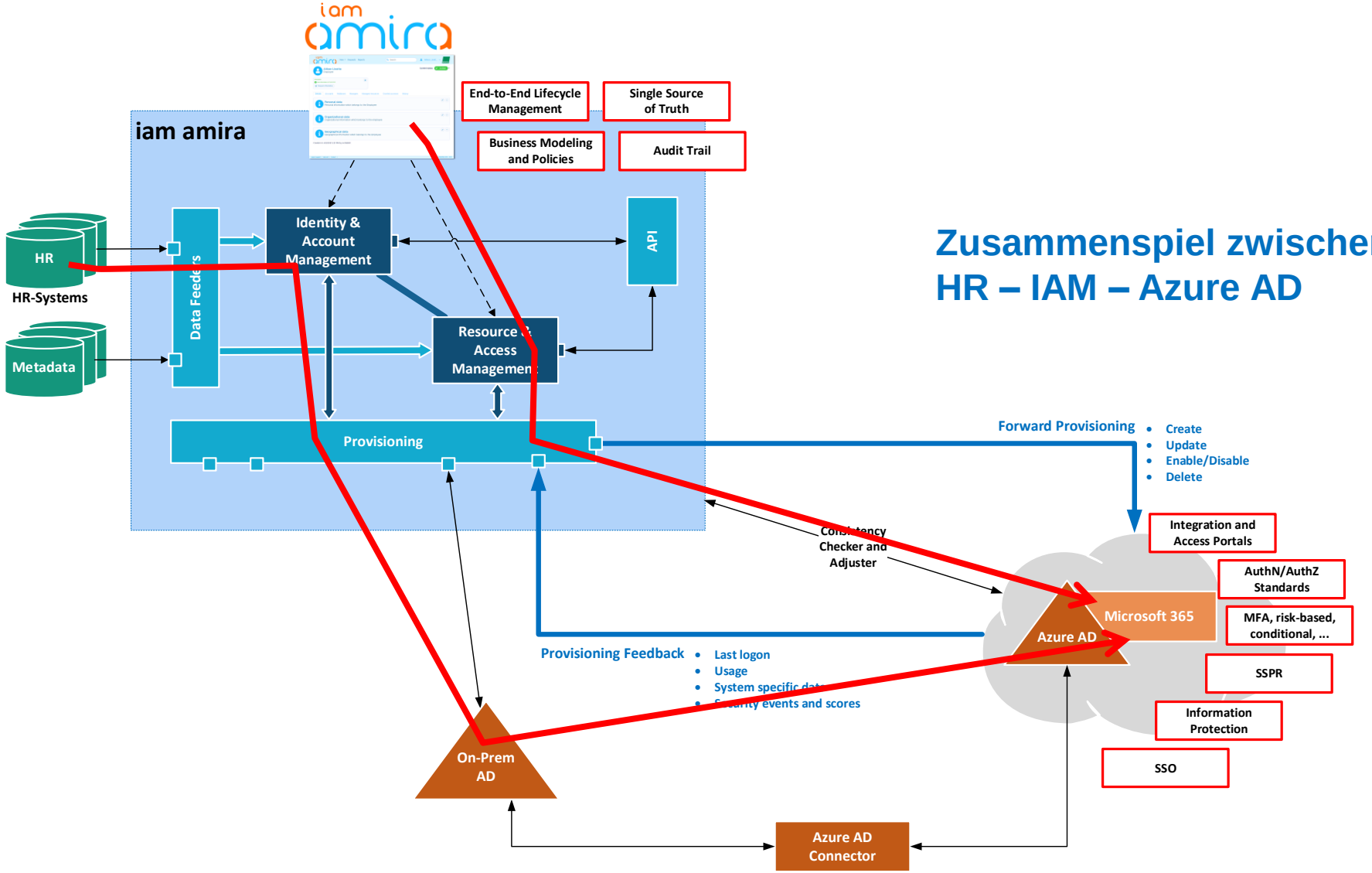
3. Lifecycle und Audit-Trail, Rollen-basierten Automatisierungen



Vorteile von iam amira gegenüber Azure AD

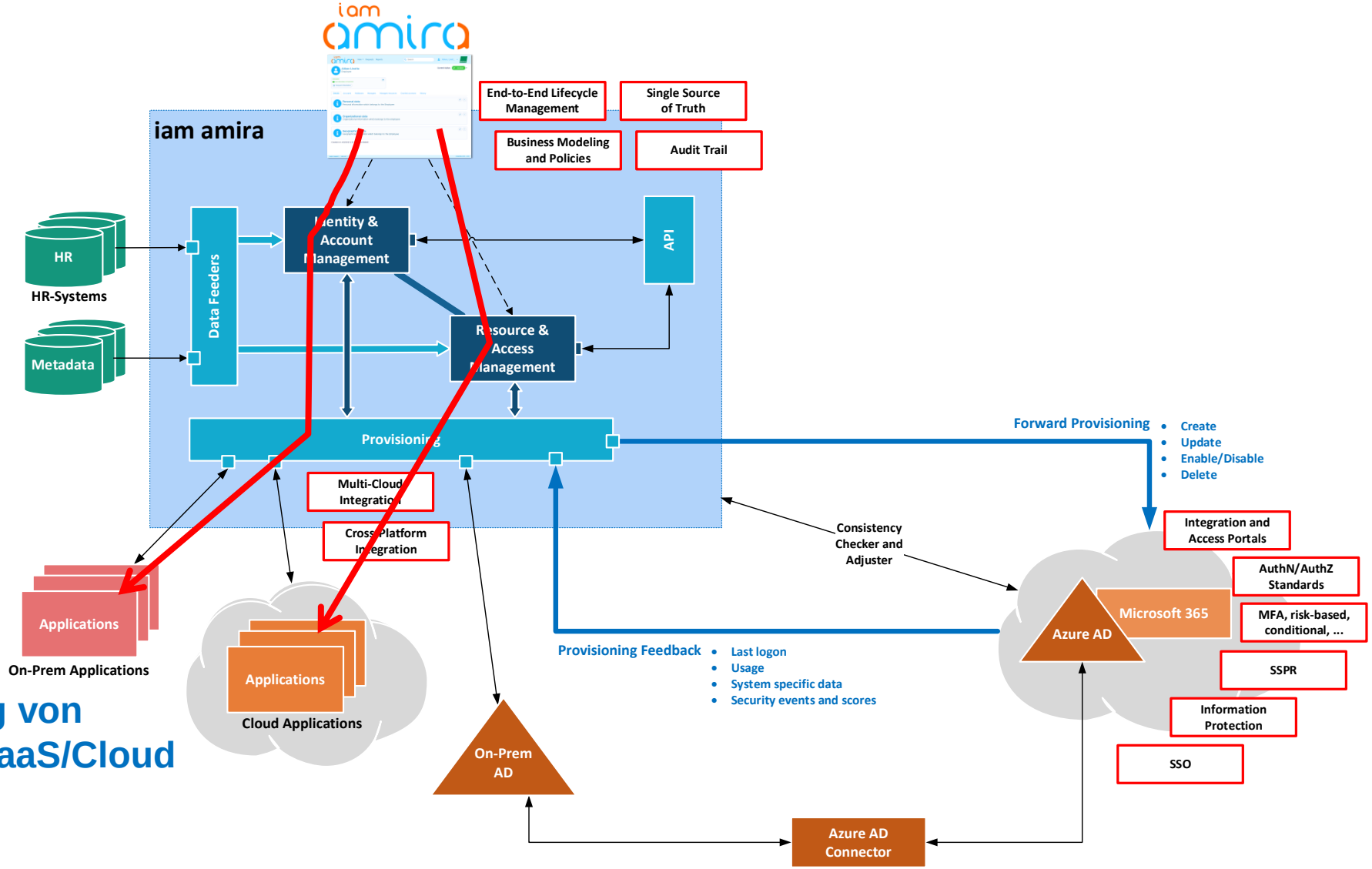
1. Modellierung von Identitäten & Ressourcen und Verknüpfung mit deren IT-Objekte
2. Tool agnostisch – Inbound und Outbound Systeme Anbindungen, On-premises wie
3. Lifecycle und Audit-Trail, Rollen-basierten Automatisierungen
4. Delegierung an den Endbenutzer, Rezertifizierungen

Stärken und Vorteile einer Zielarchitektur mit iam amira und Azure



Zusammenspiel zwischen HR – IAM – Azure AD

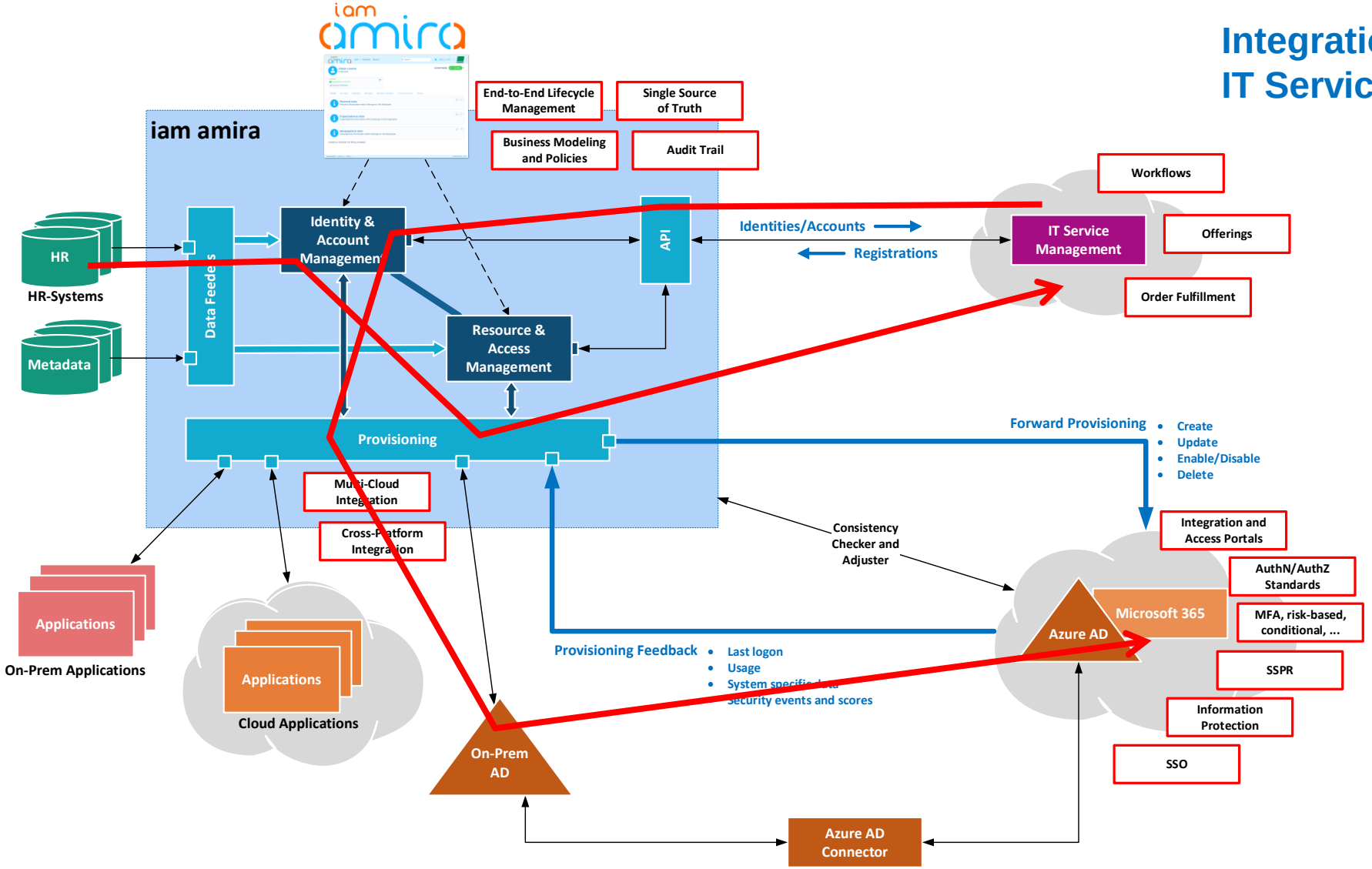
Stärken und Vorteile einer Zielarchitektur mit iam amira und Azure



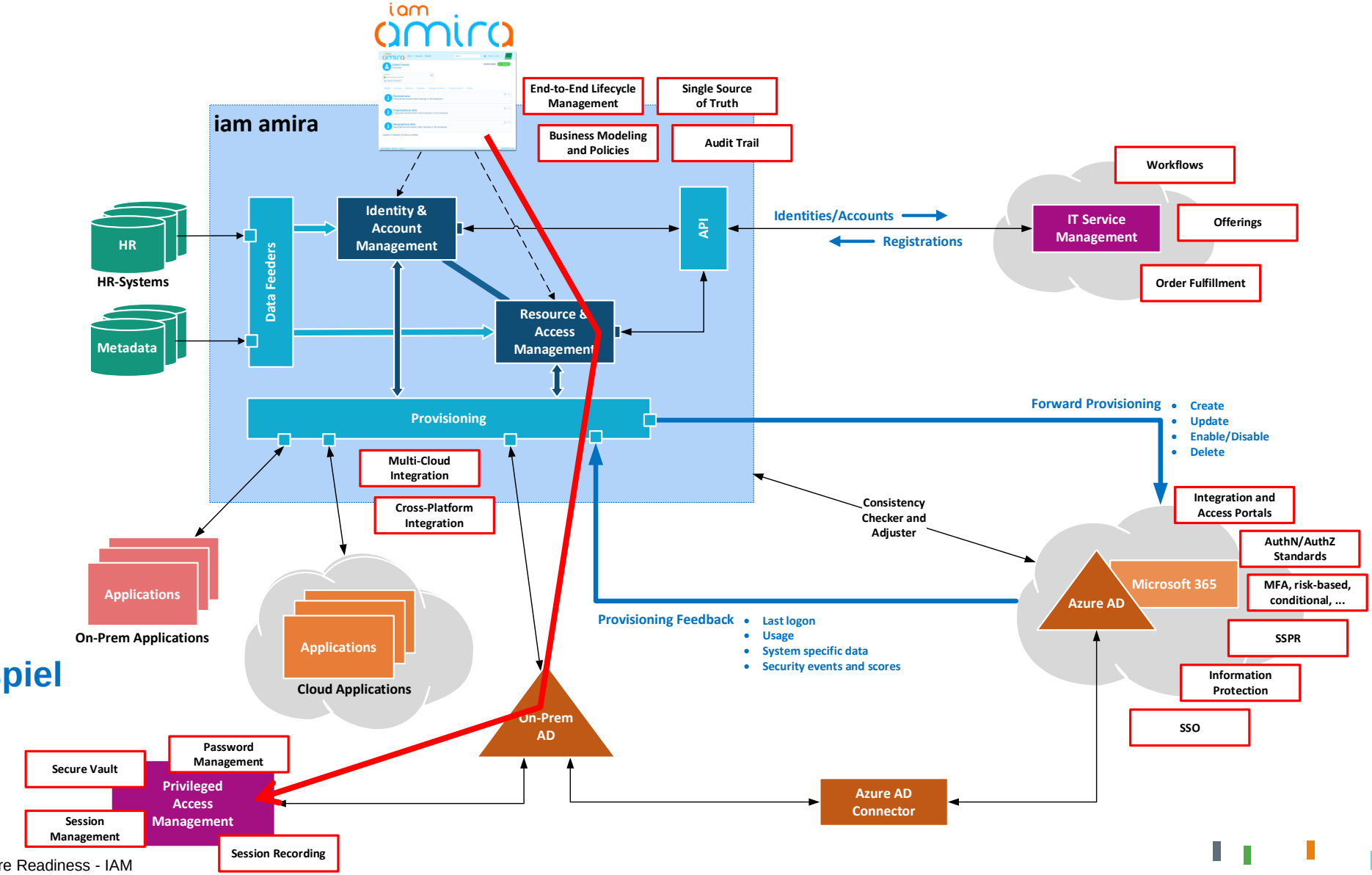
Provisionierung von On-Prem und SaaS/Cloud Applikationen

Stärken und Vorteile einer Zielarchitektur mit iam amira und Azure

Integration mit IT Service Management



Stärken und Vorteile einer Zielarchitektur mit iam amira und Azure



Zusammenspiel IAM – PAM

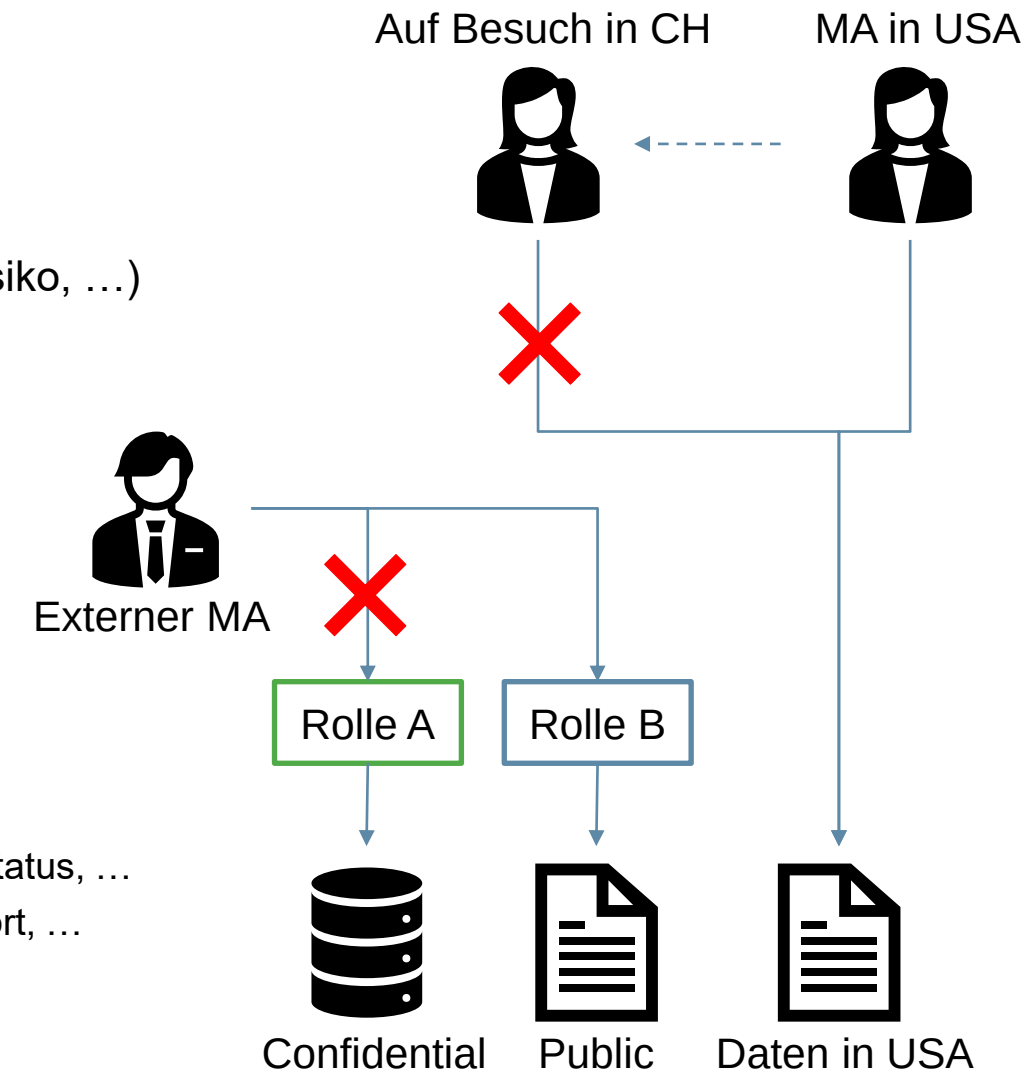
Erweiterte Szenarien und Ausblick

Beispiel – Data Governance

- Klassifizierung der Daten in der Unternehmung
- «Dynamische» Steuerung der Datenzugriffe über den Kontext (Ort, Zeit, Risiko, …)
- Driver hierfür sind gesetzliche Vorgaben und Regulatorien (DSG, DSGVO, Exportrestriktionen, …) oder interne Regeln

Lösungsansatz

- Azure Funktionalitäten
  - Azure Information Protection (AIP)
  - Azure Conditional Access
- iam amira Funktionalitäten
  - Verwaltung und Provisionierung der Meta-Daten
  - Kontext-Information über Benutzer, z.B. Organisation, Standort, Rolle(n), Funktion, Status, …
  - Meta-Daten für Ressourcen, z.B. Klassifizierung, Schutzbedarf, Organisation, Standort, …
  - Durchsetzung von Policies
  - Speicherung von erfolgten Zustimmungen der Benutzer



Nutzen durch den «Better Together» Ansatz

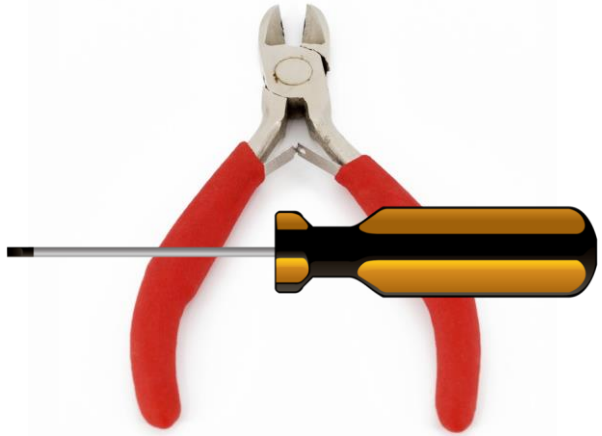
Meine IAM/Azure Checkliste

- ✓ Governance
- ✓ Lifecycle Management End-2-End
- ✓ Plattformunabhängigkeit
- ✓ Services statt Silos
- ✓ Integrativer Ansatz
- ✓ Übergeordnete Sicht durch Kontext
- ✓ Single Source of Truth
- ✓ Transparenz
- ✓ Nachvollziehbarkeit

Wrap-Up

Erkenntnisse

- Azure AD bietet eine Fülle von wertvollen Funktionalitäten rund um das Thema IAM
- Aber Azure AD ist und kann nicht alles…
- … und Azure AD ist auch kein IAM System in klassischen Sinn
- Deshalb die Komplementierung und Integration mit einer «echten» IAM Lösung wie iam amira



Wie wird IAM zum Erfolg

- IAM ist ein Unternehmensprojekt – ich muss meine Key Player und Stakeholder im Boot haben
- Bei IAM geht es in erster Linie um Prozesse, Daten und Services
- Stellen Sie Ihre Benutzer in den Mittelpunkt – um die geht es
- Ich muss meine Anforderungen genau kennen und priorisieren – «must/need/nice»… und «not»
- Ich brauche eine langfristige Strategie und Vision, die ich in Phasen umsetzen kann
- IAM braucht Zeit, aber Quick-Wins sind wichtig

Besten Dank! Stellen Sie uns Ihre Fragen.

Vorschau.

09.11.2021	Webinar: Azure Readiness - Azure Virtual Desktop - Teil 2
18.11.2021	Webinar: IoT - Temperaturüberwachung
23.11.2021	Webinar: Adobe Sign im HR
25.11.2021	Webinar: Cisco Meraki Enterprise Network
30.11.2021	Webinar: Apple im Unternehmen mit Bechtle

Mehr Infos unter bechtle.com/ch/ueber-bechtle/events

Handeln Sie jetzt. Kontaktieren Sie uns.

Bechtle Schweiz AG
Tel. +41 56 418 33 33
bechtle.ch/kontakt

Andreas Gotti
Leiter Business Unit Software, Bechtle Schweiz AG
andreas.gotti@bechtle.com