

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

Microsoft Security technology

			
<p>Identity and access management</p> <p>Secure access for a connected world</p>	<p>Threat protection</p> <p>Stop attacks with integrated, automated SIEM and XDR</p>	<p>Information protection</p> <p>Protect sensitive data and manage insider risks with intelligence</p>	<p>Cloud security</p> <p>Safeguard your multi-cloud resources</p>

Benutzer- und Rechteverwaltung in Azure

Identity and Access Management critical capabilities

Authentication	Authorization	Administration	Governance	Self-Service Management	Customer IAM	Managing Cloud Infrastructure
<ul style="list-style-type: none"> ✓ User Authentication ✓ MFA ✓ Single Sign on (SSO) ✓ Federation ✓ Passwordless ✓ Certificate/Smartcard based authentication 	<ul style="list-style-type: none"> ✓ Machine learning based risk scoring ✓ Adaptive Access ✓ OAuth Authorization ✓ OAuth Token ✓ Attribute mapping ✓ RBAC ✓ Session lifetime management ✓ ABAC 	<ul style="list-style-type: none"> ✓ User Management ✓ Group Management ✓ Domain Management ✓ Delegated Administration ✓ Application Management ✓ Password Management 	<ul style="list-style-type: none"> ✓ Access certifications ✓ Privileged Access/JIT ✓ Entitlement management ✓ Identity Lifecycle ✓ Access Requests ✓ Workflow ✓ Provisioning ✓ Policy management ✓ Reporting & Analytics ✓ Data Access Policies 	<ul style="list-style-type: none"> ✓ Password Reset ✓ Group Management ✓ Credential Registration ✓ Credential Recovery ✓ App Launching ✓ App Catalog ✓ Access Requests ✓ Profile Management 	<ul style="list-style-type: none"> ✓ Social Identity Federation ✓ Self-Service Registration ✓ Custom End User Experiences ✓ Customer Data Management ✓ Consent Management ✓ Administer Users & Partners ✓ Privacy Management 	<ul style="list-style-type: none"> ✓ Managed Identities ✓ PaaS Identity management ✓ IaaS/VM Identity Management
Applications Access						
Cloud Apps			Classic Apps			
<ul style="list-style-type: none"> ✓ Pre-integrated SSO and Provisioning ✓ BYO SAML & OATH 2.0 ✓ Custom Provisioning (SCIM) 			<ul style="list-style-type: none"> ✓ 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

Protect identities with Conditional Access

Enable Zero Trust with strong authentication and adaptive policies



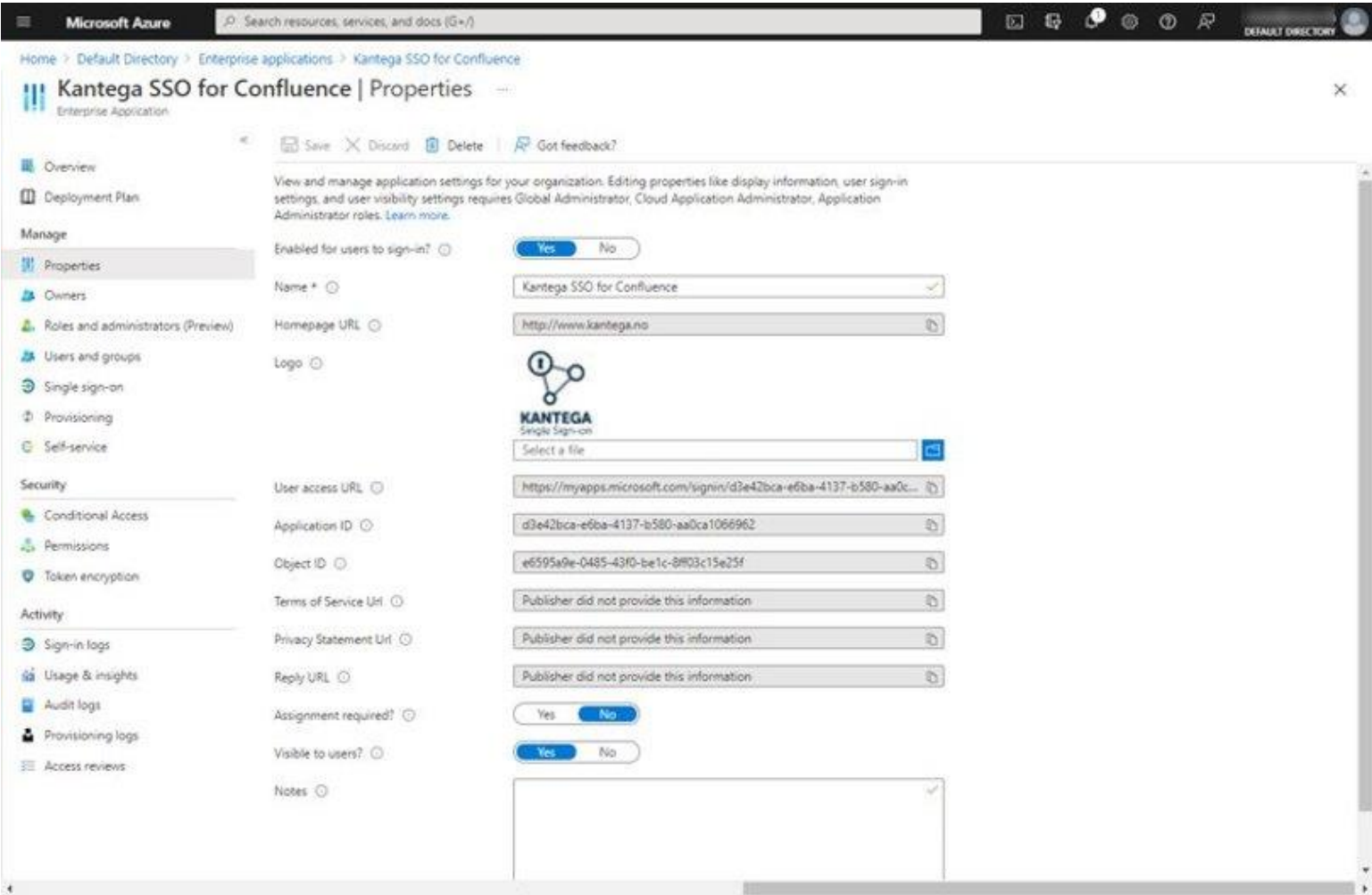
Applikationsintegration und -zugriffe in Azure

The screenshot displays the Microsoft Azure portal interface for an Enterprise Application named 'Kantega SSO for Confluence'. The top navigation bar includes the Microsoft Azure logo, a search bar, and user profile information. The breadcrumb trail shows 'Home > Default Directory > Enterprise applications > Kantega SSO for Confluence | Overview'. A left-hand navigation pane lists various management options such as Overview, Deployment Plan, Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Provisioning, Self-service, Security (Conditional Access, Permissions, Token encryption), and Activity (Sign-in logs, Usage & insights, Audit logs, Provisioning logs, Access reviews).

The main content area is divided into several sections:

- Properties:** Displays key identifiers for the application:
 - Name: Kantega SSO for Confluence
 - Application ID: d3e42bca-e6ba-4137-b580-...
 - Object ID: e6595a9e-0485-43f0-be1c-...
- Getting Started:** A series of five numbered steps to configure the application:
 - 1. Assign users and groups:** Provide specific users and groups access to the applications. [Assign users and groups](#)
 - 2. Set up single sign on:** Enable users to sign into their application using their Azure AD credentials. [Get started](#)
 - 3. Provision User Accounts:** You'll need to create user accounts in the application. [Learn more](#)
 - 4. Conditional Access:** Secure access to this application with a customizable access policy. [Create a policy](#)
 - 5. Self service:** Enable users to request access to the application using their Azure AD credentials. [Get started](#)
- What's New:**
 - Sign in charts have moved!** The new Insights view shows sign in info along with other useful application data. [View insights](#)
 - Delete Application has moved to Properties** You can now delete your application from the Properties page. [View properties](#)

Applikationsintegration und -zugriffe in Azure



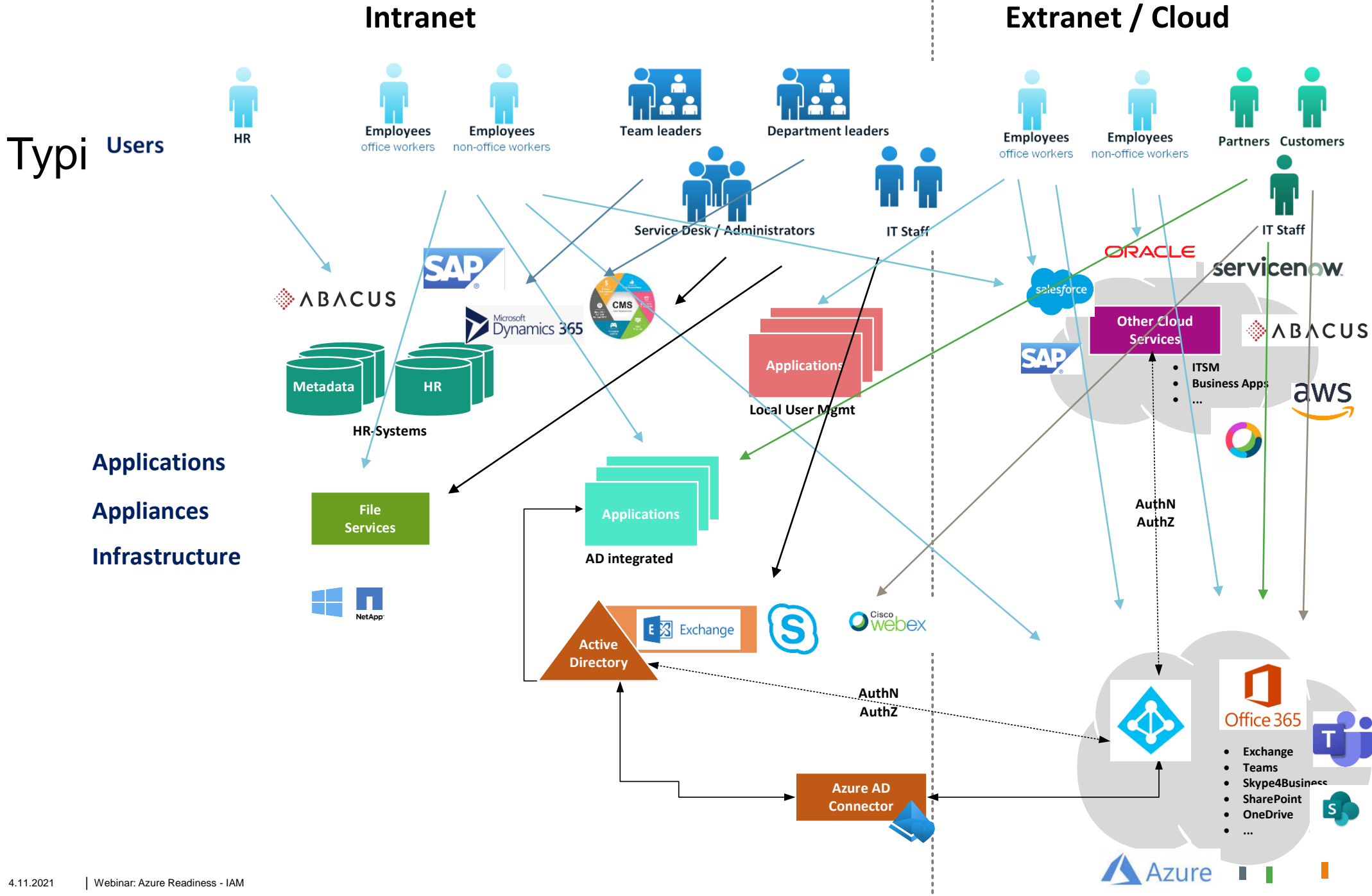
The screenshot displays the 'Properties' page for an enterprise application in the Microsoft Azure portal. The breadcrumb navigation shows the path: Home > Default Directory > Enterprise applications > Kantega SSO for Confluence. The page title is 'Kantega SSO for Confluence | Properties'.

The left-hand navigation pane includes sections for Overview, Deployment Plan, Manage, Security, and Activity. Under 'Manage', the 'Properties' option is selected. Other options include Owners, Roles and administrators (Preview), Users and groups, Single sign-on, Provisioning, and Self-service. Under 'Security', there are options for Conditional Access, Permissions, and Token encryption. Under 'Activity', there are options for Sign-in logs, Usage & insights, Audit logs, Provisioning logs, and Access reviews.

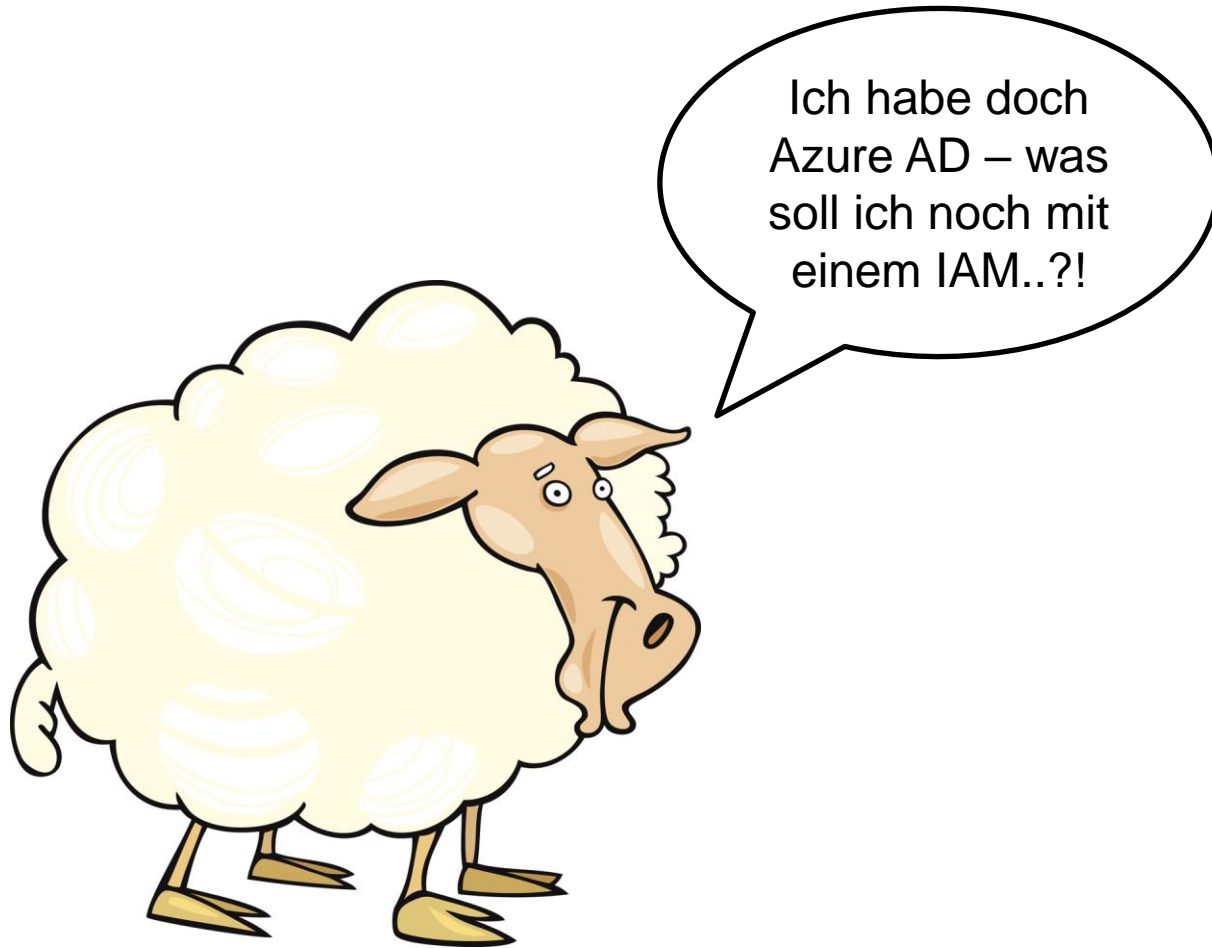
The main content area shows the application's configuration details:

- Enabled for users to sign-in?**: Radio buttons for 'Yes' (selected) and 'No'.
- Name**: Text field containing 'Kantega SSO for Confluence'.
- Homepage URL**: Text field containing 'http://www.kantega.no'.
- Logo**: Image upload area showing the 'KANTEGA Single Sign-on' logo.
- User access URL**: Text field containing 'https://myapps.microsoft.com/signin/d3e42bca-e6ba-4137-b580-aa0c...'.
- Application ID**: Text field containing 'd3e42bca-e6ba-4137-b580-aa0ca1066962'.
- Object ID**: Text field containing 'e6595a9e-0485-43f0-be1c-8f03c15e25f'.
- Terms of Service URL**: Text field containing 'Publisher did not provide this information'.
- Privacy Statement URL**: Text field containing 'Publisher did not provide this information'.
- Reply URL**: Text field containing 'Publisher did not provide this information'.
- Assignment required?**: Radio buttons for 'Yes' and 'No' (selected).
- Visible to users?**: Radio buttons for 'Yes' (selected) and 'No'.
- Notes**: A large text area for additional information.

At the top of the main content area, there are action buttons: Save, Discard, Delete, and Got feedback? Below these buttons is a warning message: 'View and manage application settings for your organization. Editing properties like display information, user sign-in settings, and user visibility settings requires Global Administrator, Cloud Application Administrator, Application Administrator roles. Learn more.'



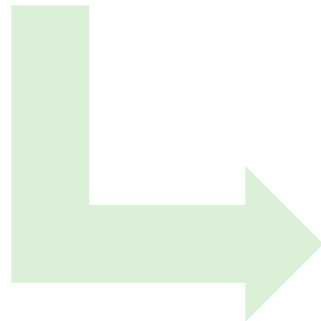
Was brauche ich – und was habe ich?



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

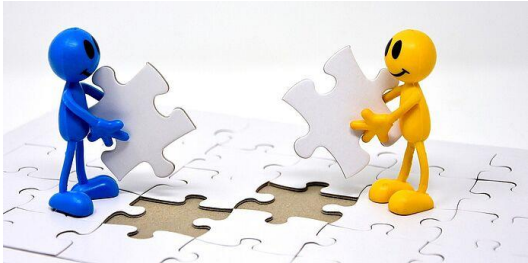
IAM Kernfunktionalitäten

- **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 Nachvollziehbarkeit und Transparenz
- **Automatisches (De-)Provisioning** – gibt mir Geschwindigkeit und Sicherheit
- **Plattformunabhängige Orchestrierung** – gibt mir die Unabhängigkeit und übergeordnete Kontrolle
- **Reporting** – gibt mir die Visibilität

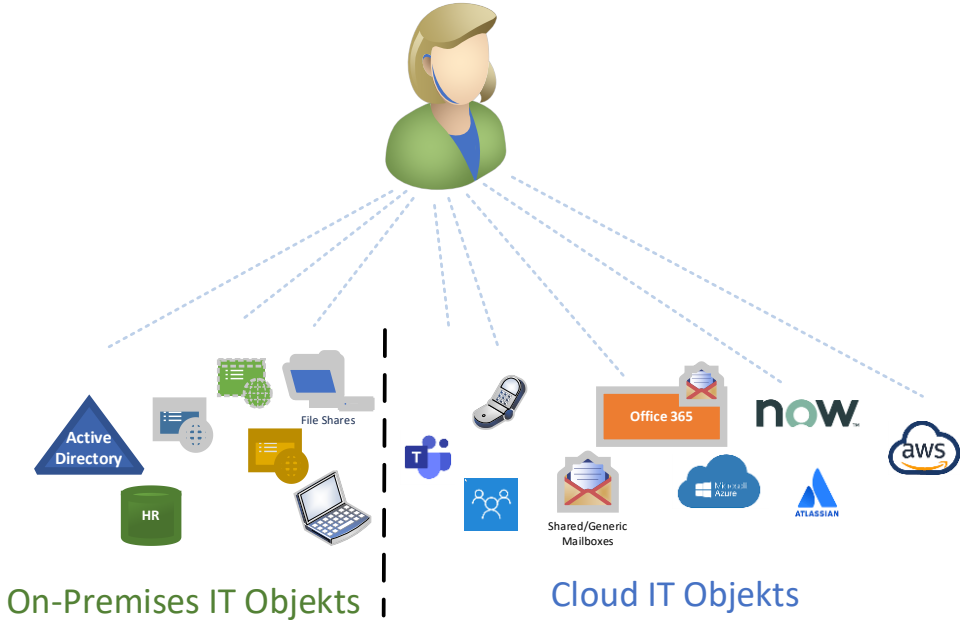
Wo sind die Hauptunterschiede zu Azure AD

- **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

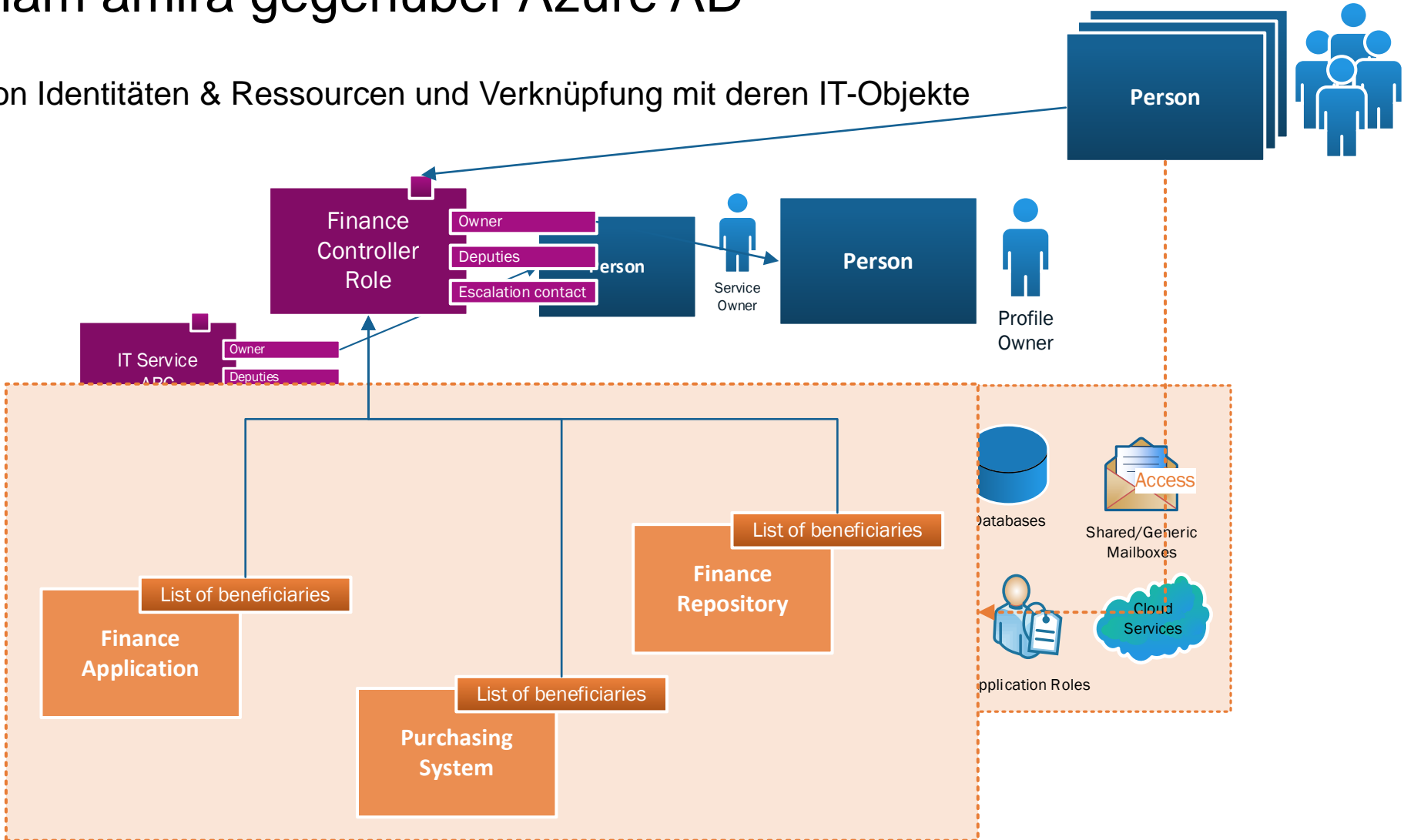


The screenshot shows the iam amira dashboard for user 'Abry Fredi' (Employee). The current status is 'Active'. It displays an attestation section with a 'Next attestation at 4/9/2022' and a 'Request attestation' button. Below this are tabs for 'Details', 'Accounts', 'Non Personal Accounts', 'Mailboxes', 'Managers', 'Managed resources', 'Granted accesses', and 'History'. The 'Accounts' tab is selected, showing a list of 4 items:

Account Name	Status
Guest Azure AD Account Abry Fredi (Ext-Company)	Enabled
Standard AD Account AbryFr1 maecenas tristique est et tempus semper est quam pharetra magna ac consequat metus sapien ut nunc vestibulum ante ipsum	Enabled
Admin AD Account abryfr1-adm onprem admin account	Enabled
Test AD Account abryfr1-test test acct onprem	Enabled

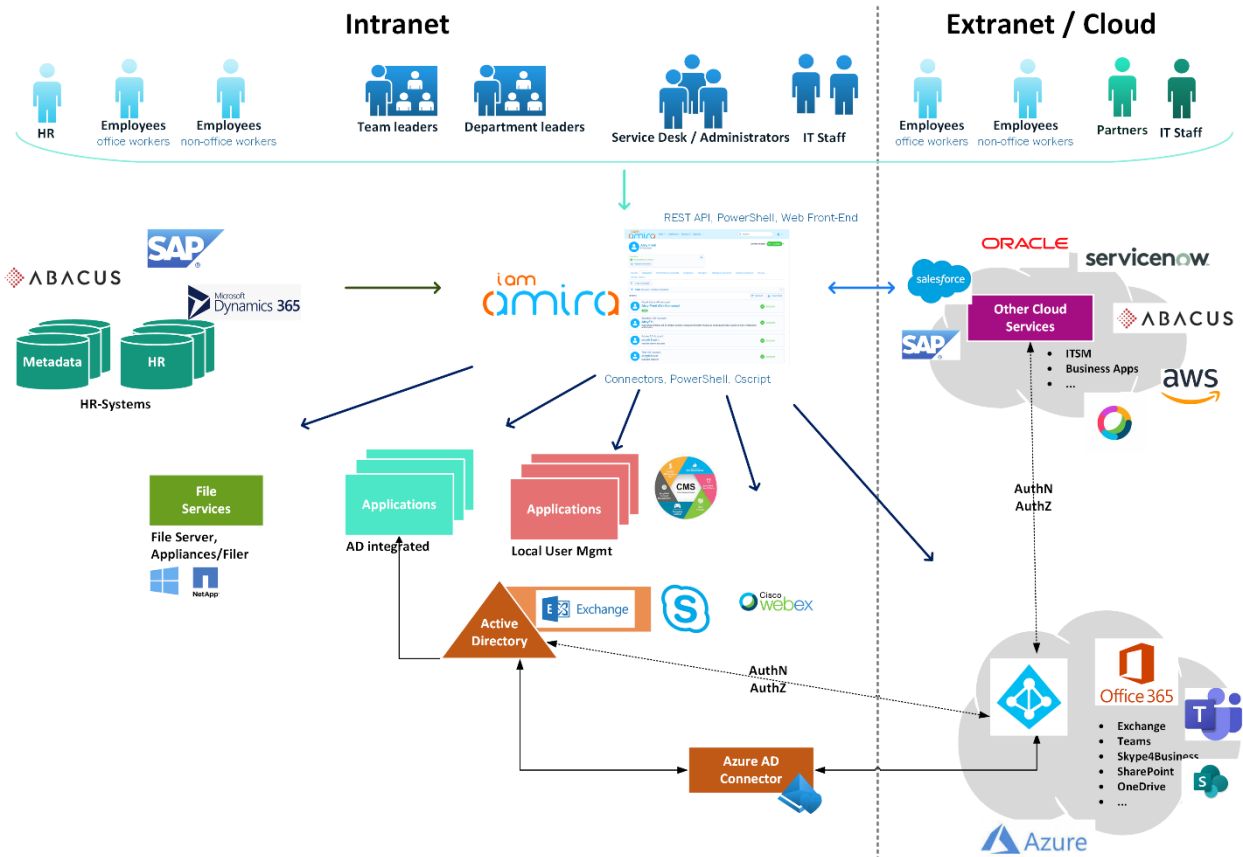
Vorteile von iam amira gegenüber Azure AD

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



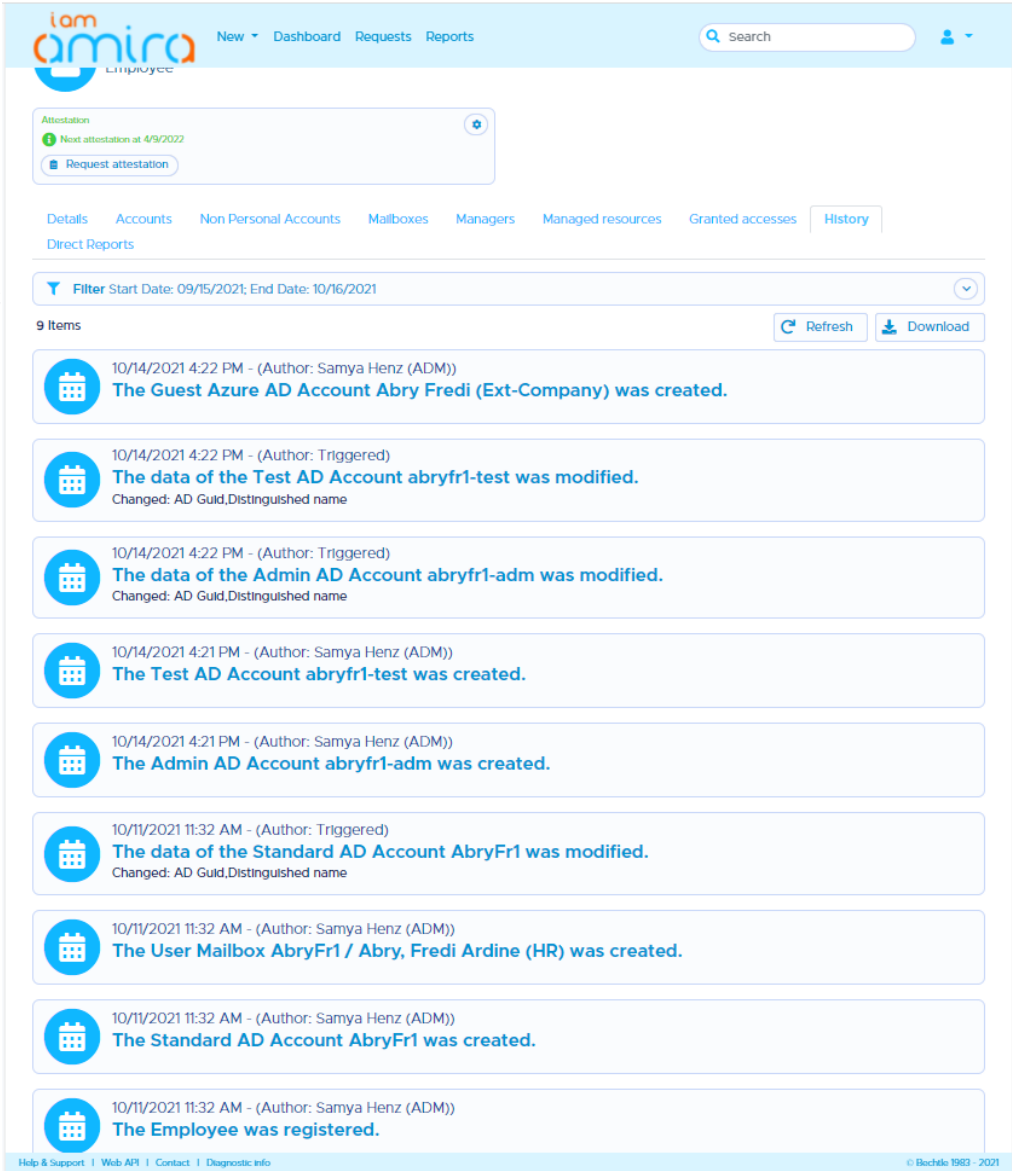
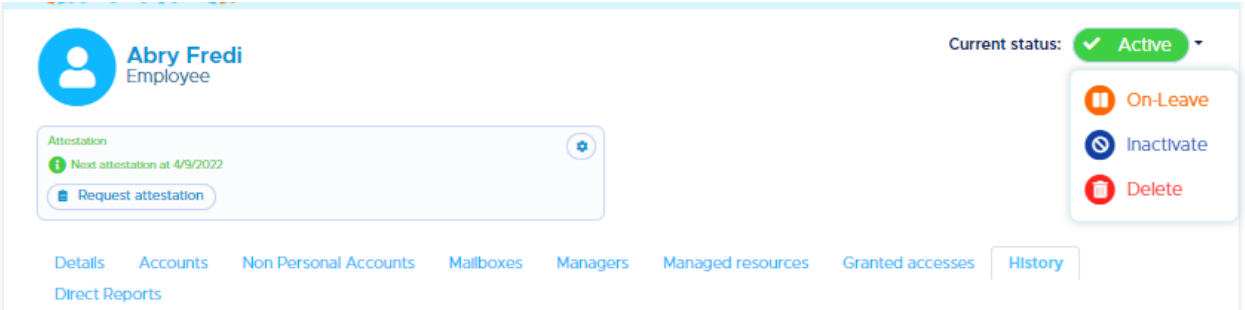
Vorteile von iam amira gegenüber Azure AD

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

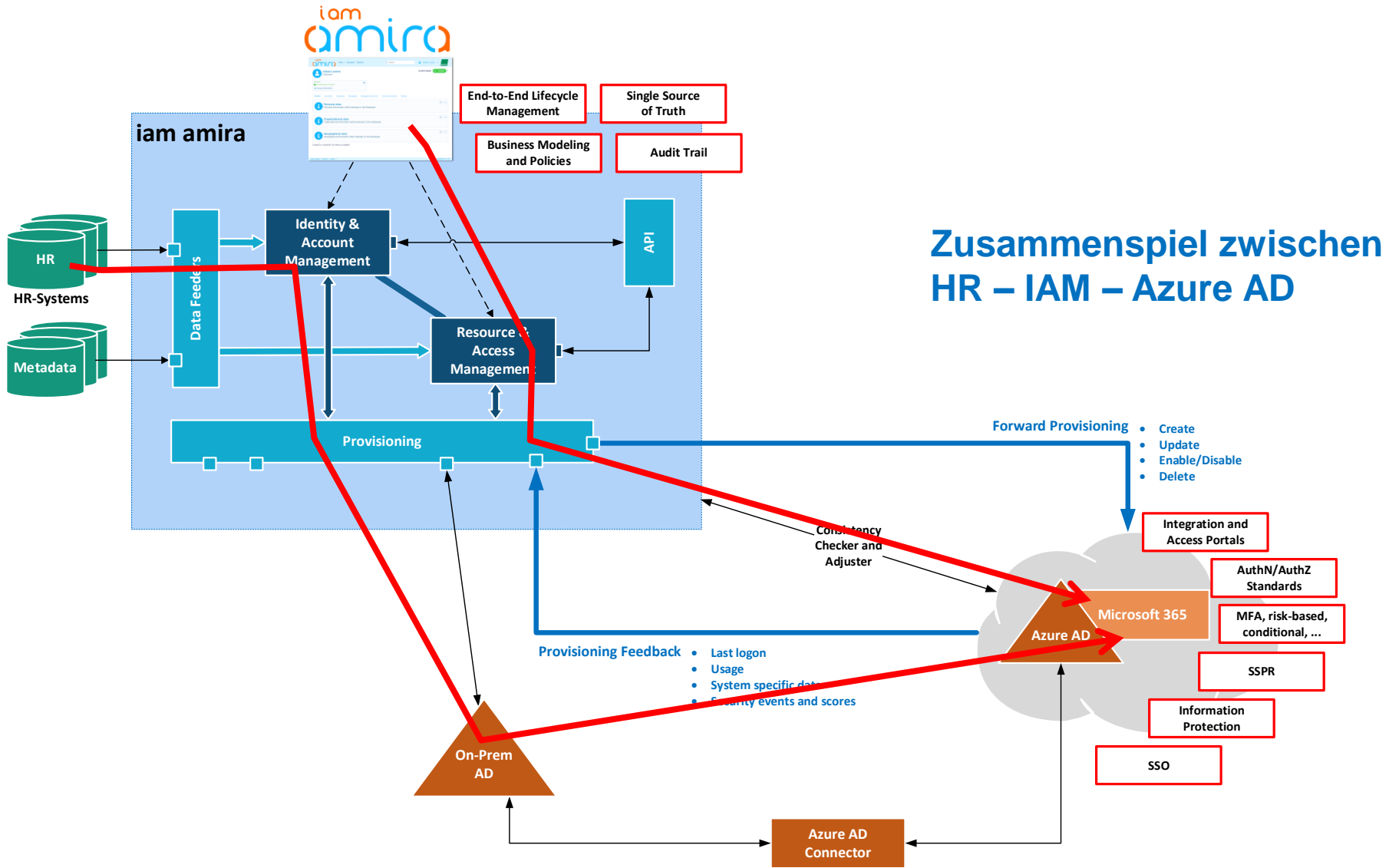


Vorteile von iam amira gegenüber Azure AD

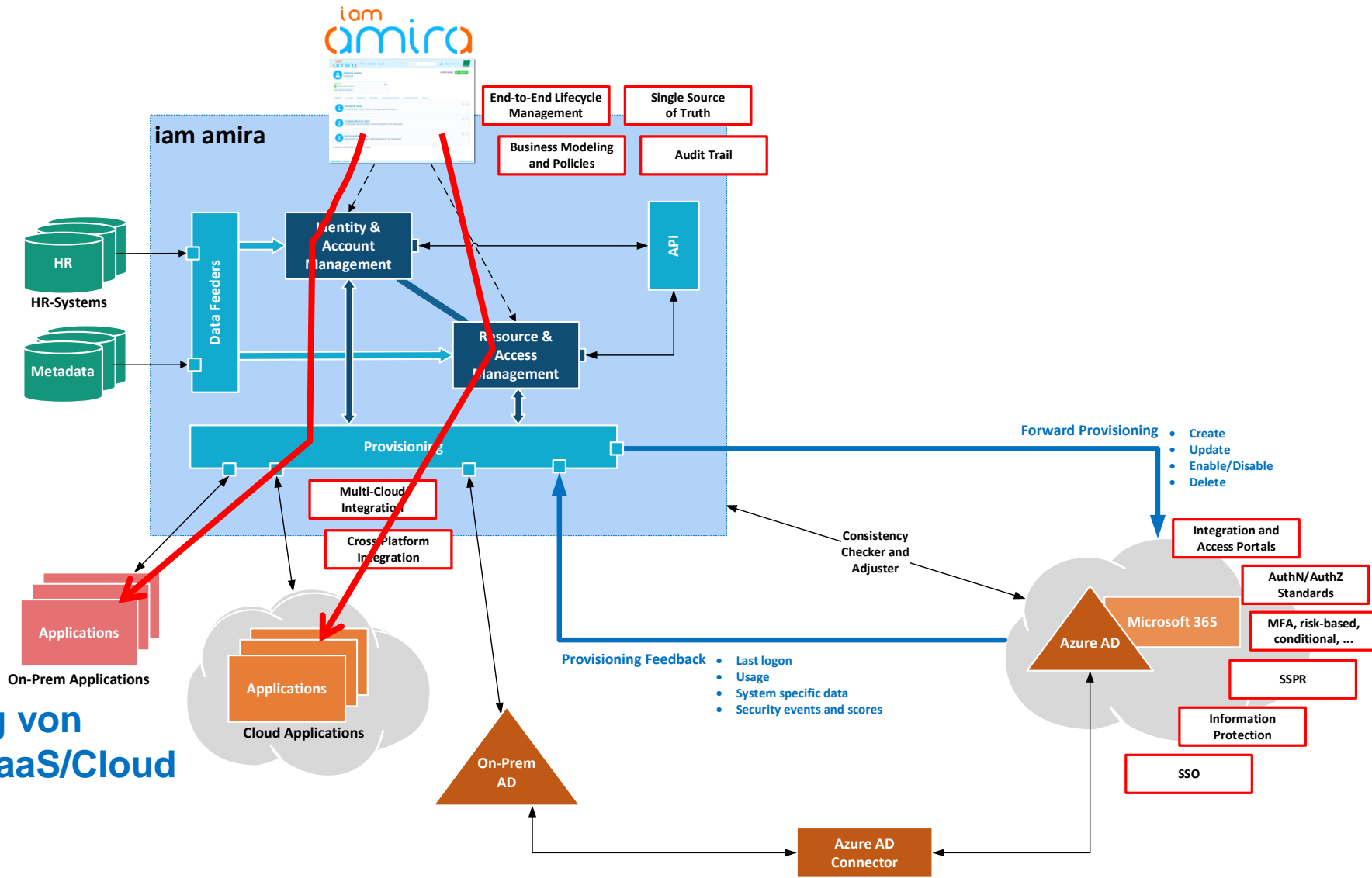
1. Modellierung von Identitäten & Ressourcen und Verknüpfung mit deren IT-Objekten
2. Tool agnostisch – Inbound und Outbound Systeme Anbindungen, On-premises wie
3. Lifecycle und Audit-Trail, Rollen-basierten Automatisierungen
4. Delegation an den Endbenutzer, Rezertifizierungen

The screenshot shows the iam amira web interface. At the top, there's a navigation bar with 'New', 'Dashboard', 'Requests', and 'Reports'. A search bar is on the right. Below the navigation, there's a 'My requests' section with a user profile icon and a 'Requests' icon. A blue arrow points from the user profile to a clipboard icon with a checklist, which in turn points to a 'Request' card. The 'Request' card shows details like 'Request', 'Status', 'Start Date', and 'End Date'. Below the card, there's a list of 242 items. The first item is 'New Office 365 Team (Unrestricted): T_LAB01_Market' (REQ-00000242) with a status of 'Approved'. The second item is 'New Office 365 Team (Unrestricted): T_LAB01_...' (REQ-00000241) with a status of 'Approved' and a 'Gruppe ABC' label. The third item is 'New Office 365 Team (Unrestricted): T_LAB01_Emergency_Team' (REQ-00000240) with a status of 'Approved'. The fourth item is 'New Shared Folder: Share 001 > Tid...' (REQ-00000239) with a status of 'Approved' and labels for 'Marketing' and 'Finanzen'. A green double-headed arrow connects the 'Request' card to the 'Gruppe ABC' label. An orange arrow points from the 'Request' card to the 'Marketing' and 'Finanzen' labels. A blue double-headed arrow connects the 'Request' card to the 'New Office 365 Team (Unrestricted): T_LAB01_...' item. A green double-headed arrow connects the 'Request' card to the 'New Office 365 Team (Unrestricted): T_LAB01_Emergency_Team' item. A blue double-headed arrow connects the 'Request' card to the 'New Shared Folder: Share 001 > Tid...' item. A green double-headed arrow connects the 'Marketing' and 'Finanzen' labels to the 'New Office 365 Team (Unrestricted): T_LAB01_Emergency_Team' item.

Stärken und Vorteile einer Zielarchitektur mit iam amira und Azure



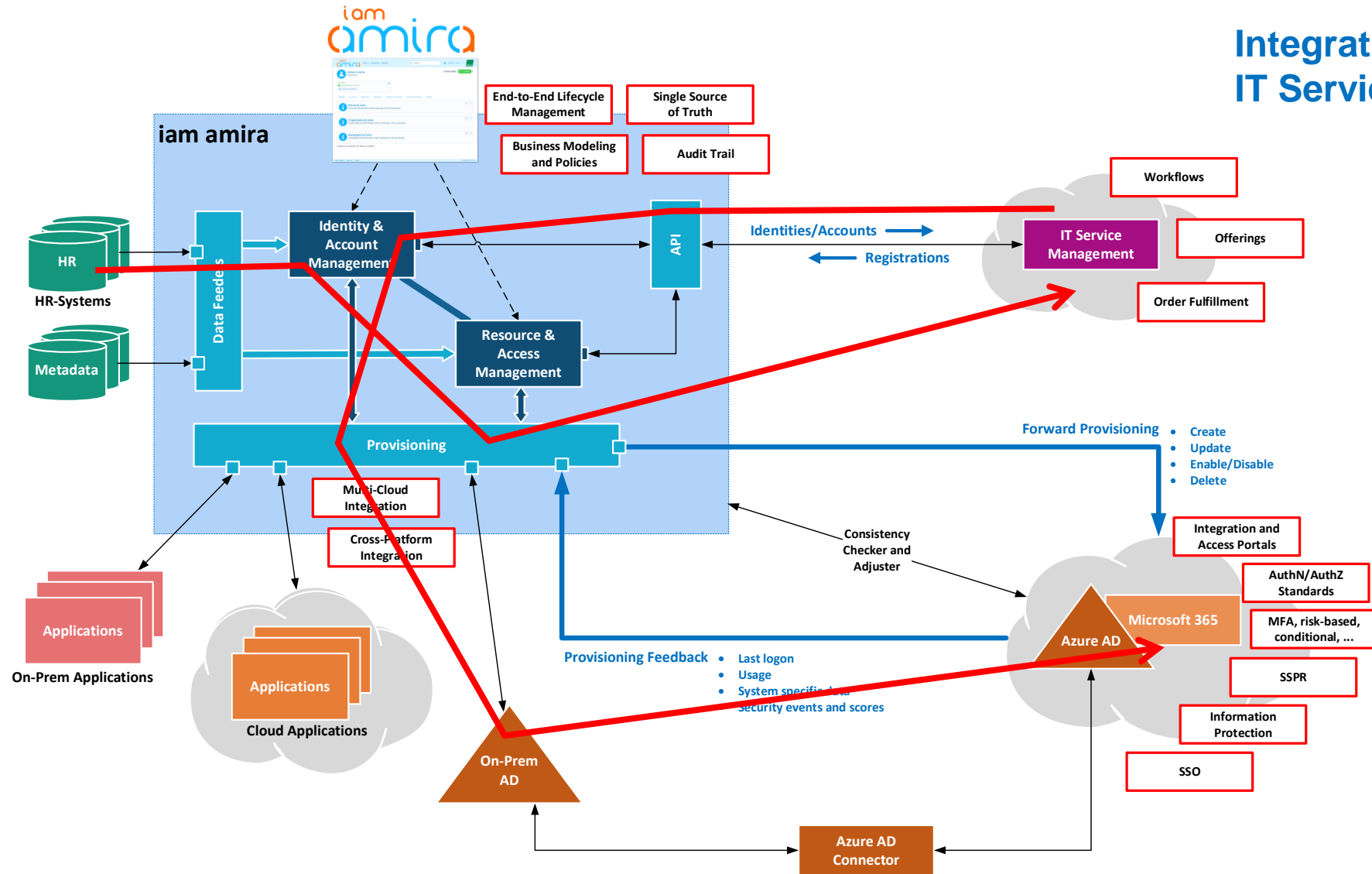
Stärken und Vorteile einer Zielarchitektur mit iam amira und Azure



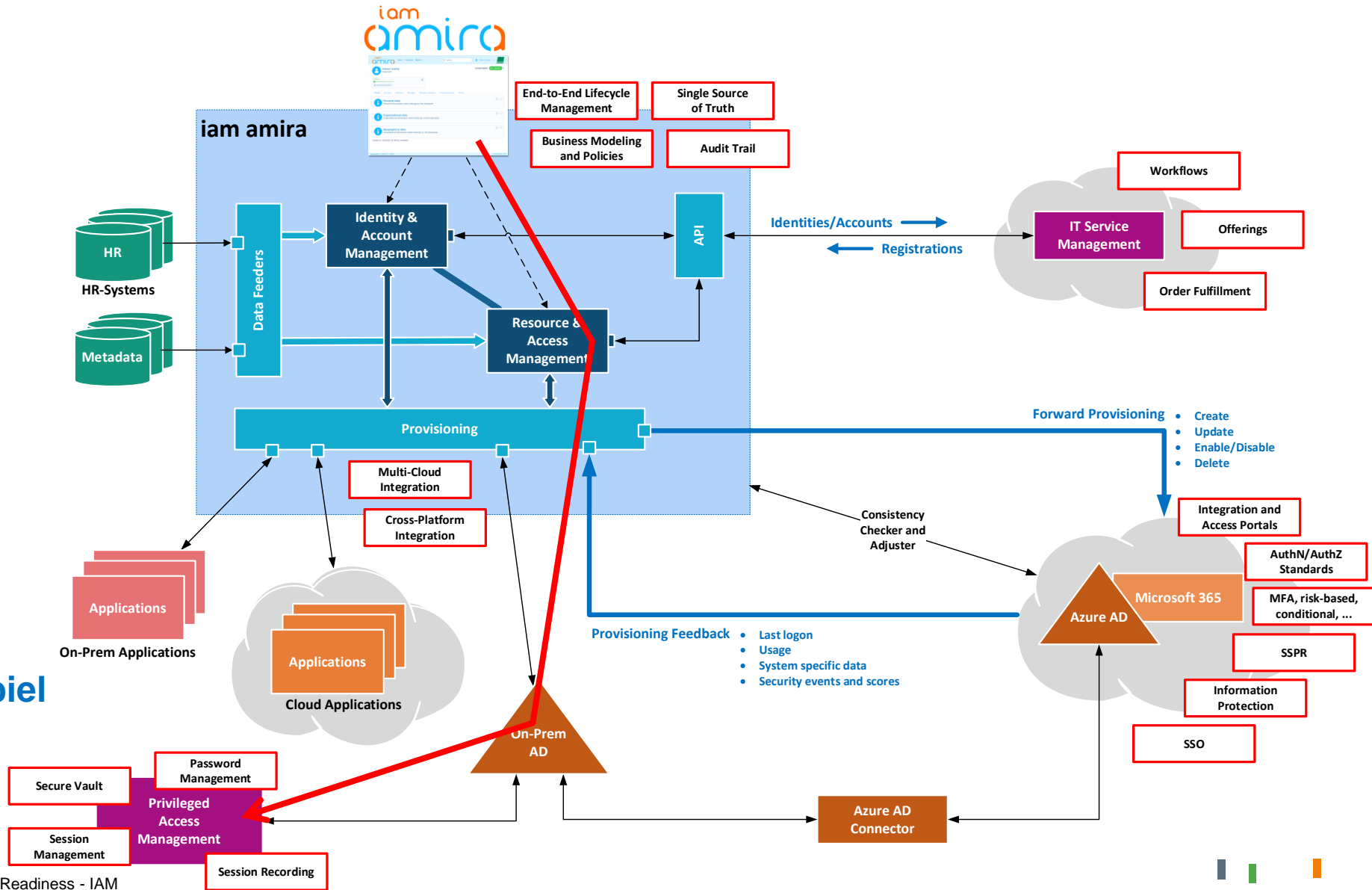
Provisionierung von On-Prem und SaaS/Cloud Applikationen

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

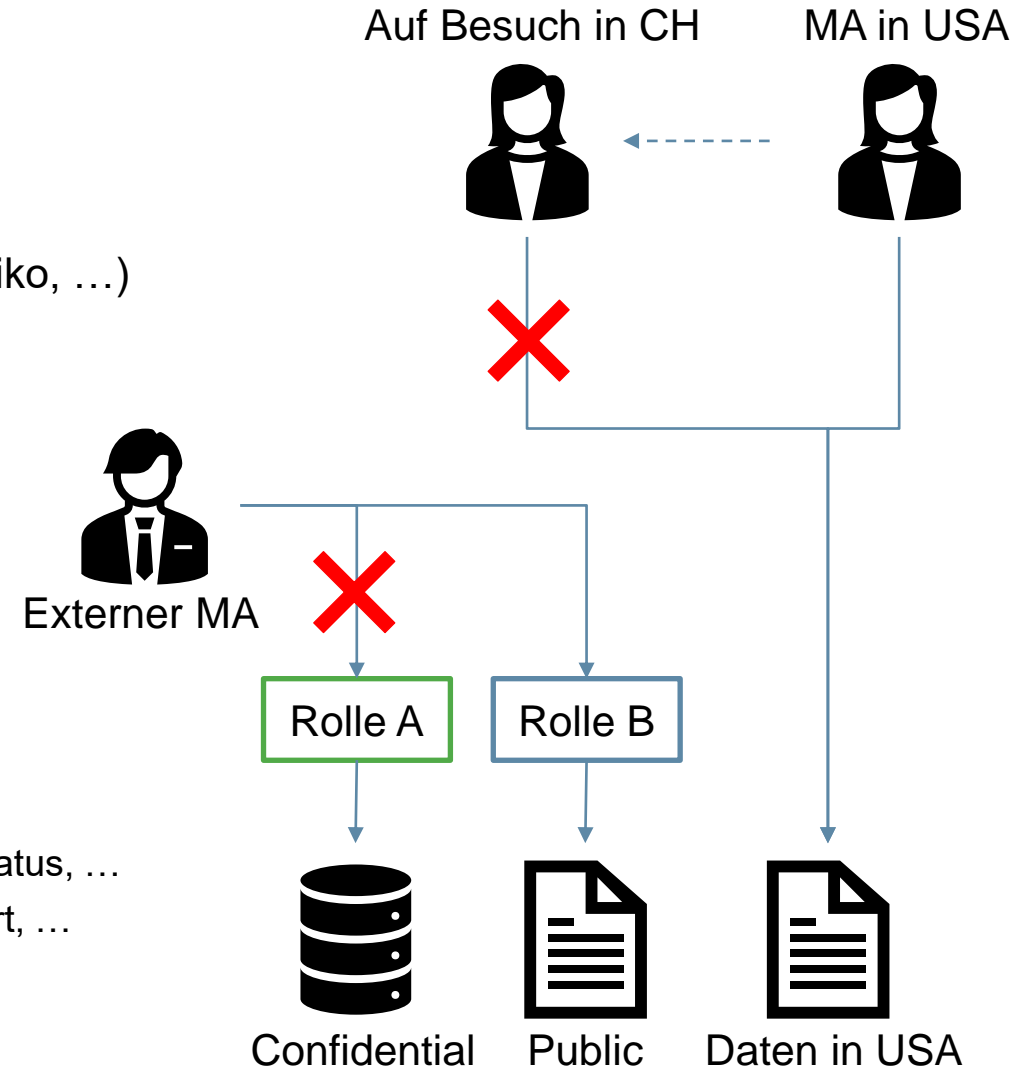
Erweiterte Szenarien und Ausblick

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*



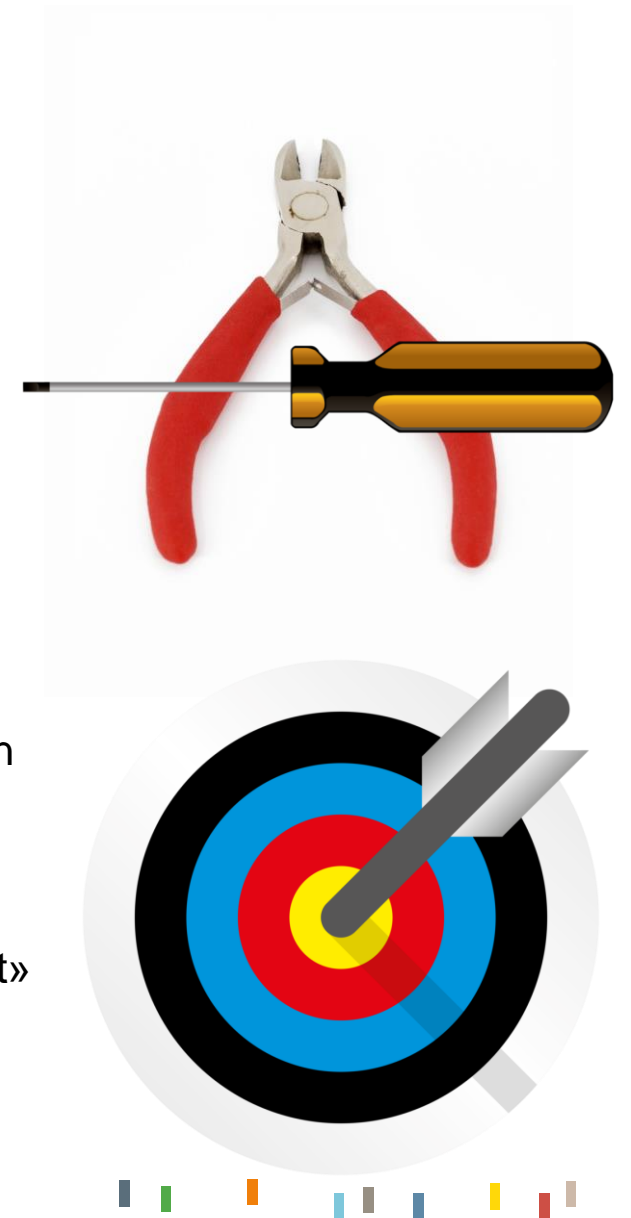
Wrap-Up

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.



Weitere Infos:
bechtle.com/ch

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