
OXFORD
COMPUTER GROUP
Microsoft
IDABUS®
ipg
EXPERTS IN IDENTITY.
ACCESS. GOVERNANCE.
NEXIS

OXFORD COMPUTER GROUP

Cloud-First IAM

James Cowling

September 2024

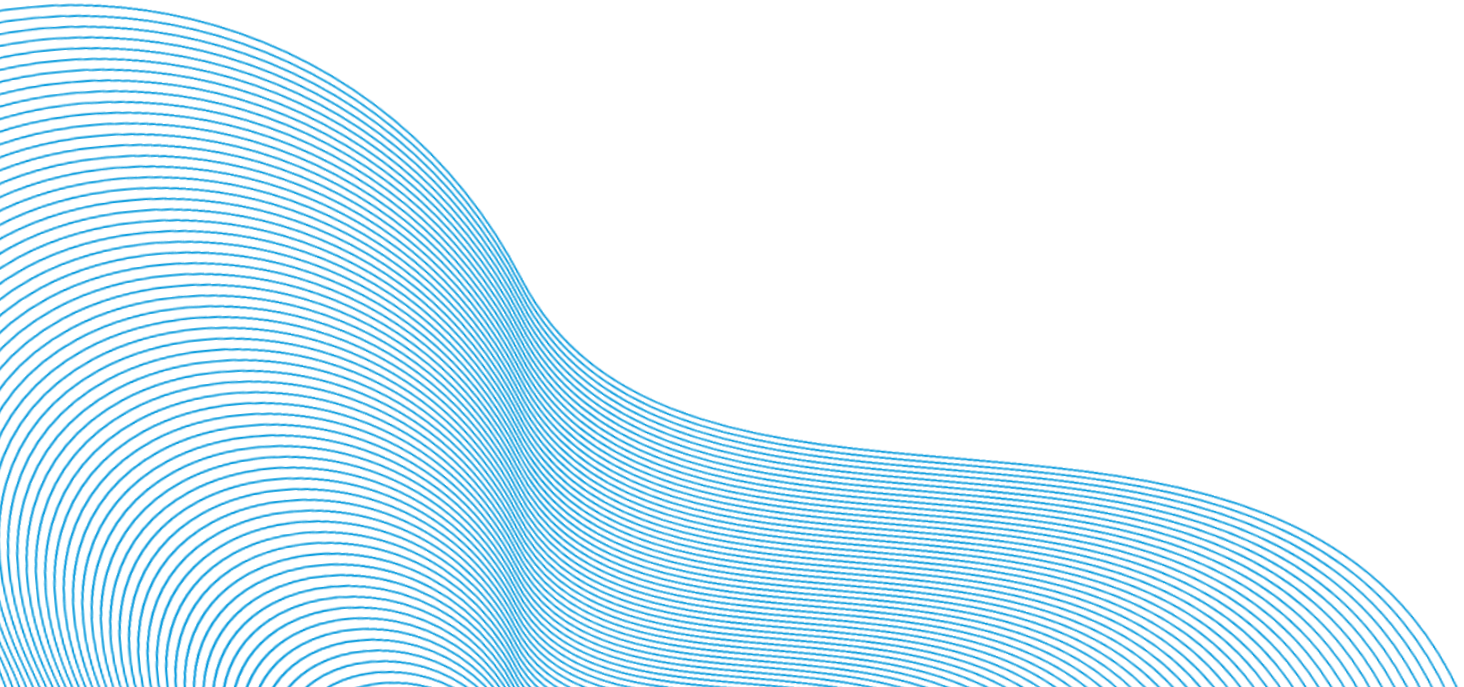
Agenda

Entra IDM – Cloud first identity management

Architectural Scenarios

Tooling

Moving Forward



Microsoft

2024 Partner of the Year

Finalist
Identity Award
Defense and Intelligence Award

OXFORD COMPUTER GROUP

Ziele

- Es sollte eine klare, Cloud-basierte IGA-Zielarchitektur für die nächsten Jahre geben, deren Voraussetzungen und Hindernisse bekannt sind
- Engagement für moderne, sichere Identität mit Standardprotokollen
- Reduzierung der Abhängigkeit von und der Investitionen in Legacy-Plattformen (z. B. MIM und AD)
- Daraus ergibt sich ab sofort ein geordneter Aufgabenkatalog!
- Der Prozess sollte eine Evolution sein, keine Revolution
- Bestehende Investitionen müssen nicht verworfen werden
- Annahme: Entra ID ist Teil jeder Lösung

  http://aka.ms/IdentityGovernanceOverview

OXFORD COMPUTER GROUP

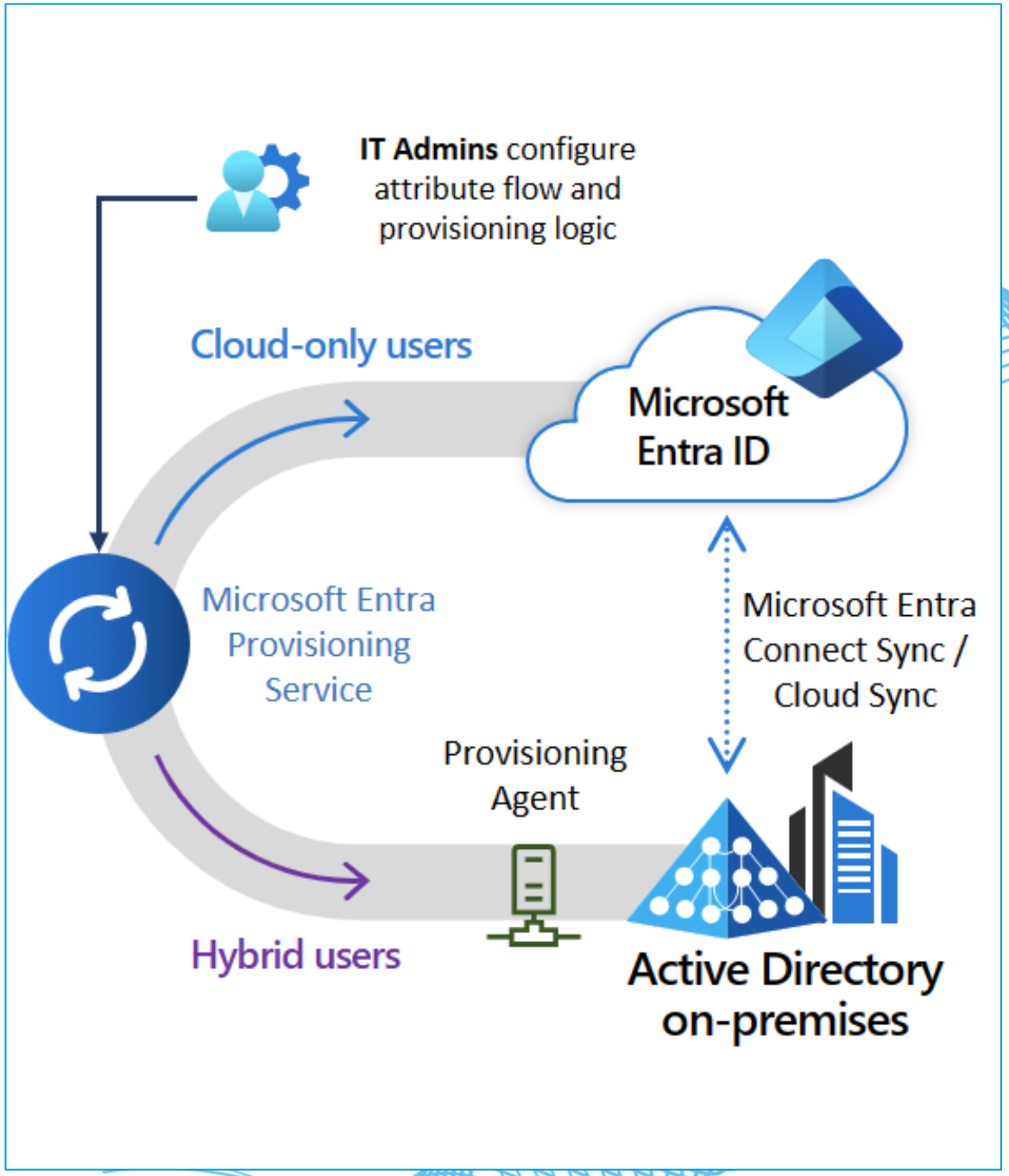
Cloud-First Hybrid Identity

- Traditionelle Hybridszenarien gehen davon aus, dass alle Benutzer lokalen Zugriff haben und einige über Cloud-Konten verfügen
- Cloud-First-Szenarien berücksichtigen die neue Realität – dass alle Benutzer über Cloud-Konten verfügen und nur einige über lokalen Zugriff verfügen, der nach Bedarf hinzugefügt und entfernt werden kann
- Dieser Vortrag konzentriert sich auf Datenflüsse und Managementprozesse – eine vollständige Analyse würde natürlich auch UX, Workflows, Protokollierung und Reporting sowie Themen wie Single-Sign-On und passwortlose Ansätze berücksichtigen
- Cloud-First Identity geht Hand in Hand mit anderen Initiativen wie der reinen Cloud-Geräteverwaltung und der modernen Authentifizierung

OXFORD COMPUTER GROUP

Microsoft Szenarien

- In Microsofts Standarddokumentation geht es um reine Cloud- und Hybridbenutzer
- Hybridbenutzer sind derzeit AD-First
- Allerdings sprechen Kunden zunehmend von Cloud-First-Hybrididentität
- In dieser Präsentation werden Möglichkeiten erörtert, AD als Option und nicht als Voraussetzung zu etablieren

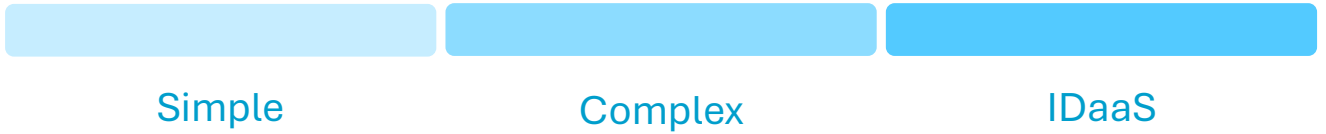


Cloud-First Scenarios

Wir haben 5 Szenarien identifiziert, jedes mit einer Modellquelle und einer Zielarchitektur

Es handelt sich lediglich um Skizzenszenarien: Für einen Discovery-prozess werden immer spezifische Details benötigt

Der Schwerpunkt liegt hier auf dem Datenfluss, aber auch Prozesse und Benutzererfahrung sind bei jeder Analyse wichtig



Private Cloud

Keine Public-Cloud-Funktionalität verfügbar

MIM ist vorhanden, aber keine langfristige Lösung

Planning Only (vorerst)

Komplexe Schemaanforderungen, die die Erweiterbarkeit von Microsoft Entra ID übersteigen

Extrem komplexe Konsolidierungs- und/oder Vorranganforderungen in den vorgelagerten Datenflüssen (d. h. aus mehreren HR-Systemen)

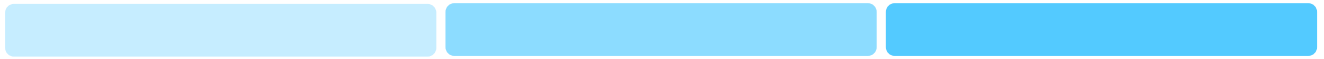
Komplexe Integrationen zwischen MIM und Service Desk, deren Ersetzung zum jetzigen Zeitpunkt kostspielig und komplex wäre

Cloud-First Scenarios

Wir haben 5 Szenarien identifiziert, jedes mit einer Modellquelle und einer Zielarchitektur

Es handelt sich lediglich um Skizzenszenarien: Für einen Discovery-prozess werden immer spezifische Details benötigt

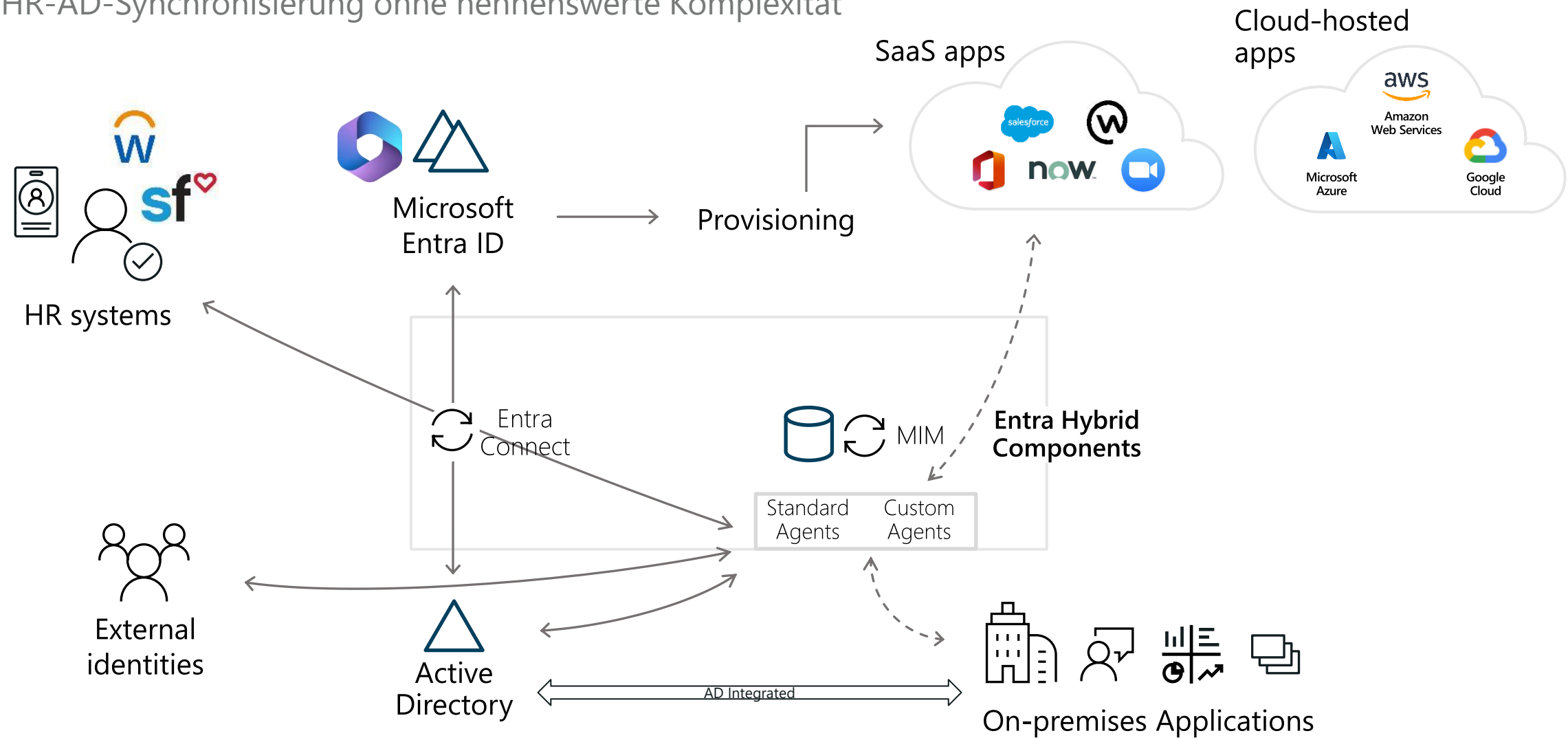
Der Schwerpunkt liegt hier auf dem Datenfluss, aber auch Prozesse und Benutzererfahrung sind bei jeder Analyse wichtig



Simple	Complex	IDaaS
Daten aus einem (einzigen) HR-System, mit möglicher zusätzlicher Quelle für externe Auftragnehmer		
Bereitstellung von Benutzern und Gruppen (möglicherweise mit automatischen Mitgliedschaften) in Active Directory		
Wenige oder keine Funktionen des MIM-Dienstes/Portals werden verwendet		
Keine anspruchsvollen Prozess- oder Logikanforderungen für die Verwaltung nachgelagerter lokaler Systeme		

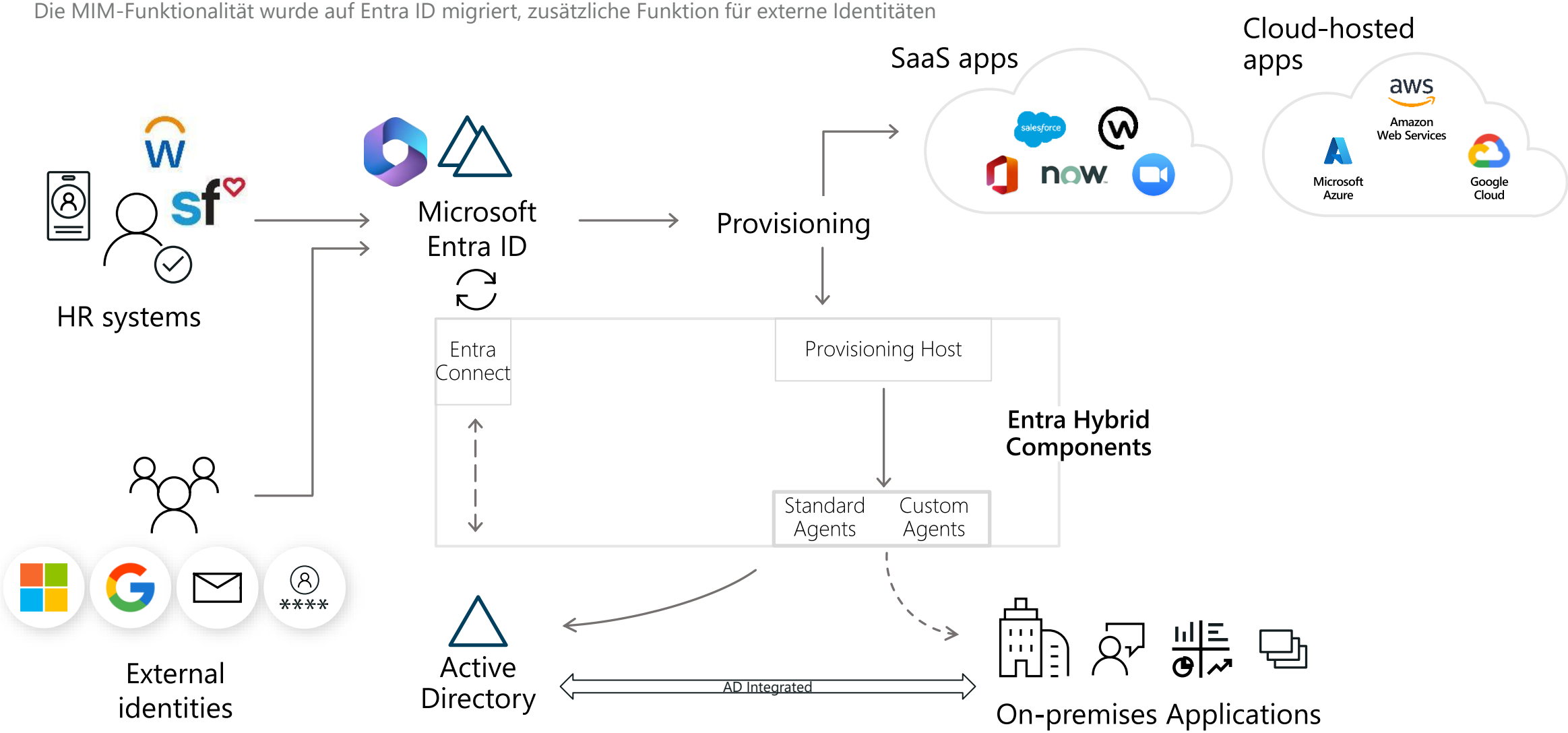
Simple On-Premises-first Identity

HR-AD-Synchronisierung ohne nennenswerte Komplexität



Simple Cloud-first Identity

Die MIM-Funktionalität wurde auf Entra ID migriert, zusätzliche Funktion für externe Identitäten

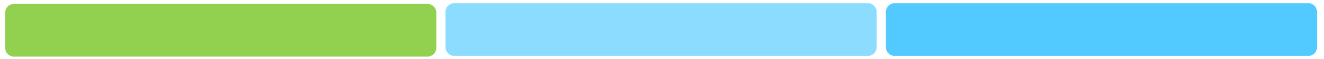


Cloud-First Scenarios

Wir haben 5 Szenarien identifiziert, jedes mit einer Modellquelle und einer Zielarchitektur

Es handelt sich lediglich um Skizzenszenarien: Für einen Discovery-prozess werden immer spezifische Details benötigt

Der Schwerpunkt liegt hier auf dem Datenfluss, aber auch Prozesse und Benutzererfahrung sind bei jeder Analyse wichtig



Simple	Complex	IDaaS
MIM wurde durch Funktionen von Microsoft Entra ID ersetzt: Inbound HR und Outbound Provisioning und Management sowohl für SaaS-Anwendungen als auch für On-Premises-Anwendungen		
Föderierte Integration extern gehosteter digitaler Identitäten ist ein natives Merkmal dieser Architektur und eröffnet eine Vielzahl neuer Möglichkeiten		
Mindestens Microsoft Entra P1-Lizenzen erforderlich		
Möglicherweise ist Microsoft Entra Connect erforderlich (oder auch nicht)		
Um reine Cloud-Szenarien zu unterstützen, benötigen Sie Cloud-verwaltete Geräte (z. B. mit Microsoft Intune).		

Cloud-First Scenarios

Wir haben 5 Szenarien identifiziert, jedes mit einer Modellquelle und einer Zielarchitektur

Es handelt sich lediglich um Skizzenszenarien: Für einen Discovery-prozess werden immer spezifische Details benötigt

Der Schwerpunkt liegt hier auf dem Datenfluss, aber auch Prozesse und Benutzererfahrung sind bei jeder Analyse wichtig

Simple

MIM wurde durch Funktionen von Microsoft Entra ID ersetzt: Inbound HR und Outbound Provisioning und Management sowohl für SaaS-Anwendungen als auch für On-Premises-Anwendungen

Föderierte Integration extern gehosteter digitaler Identitäten ist ein natives Merkmal dieser Architektur und eröffnet eine Vielzahl neuer Möglichkeiten

Mindestens Microsoft Entra P1-Lizenzen erforderlich

Möglicherweise ist Microsoft Entra Connect erforderlich (oder auch nicht)

Um reine Cloud-Szenarien zu unterstützen, benötigen Sie Cloud-verwaltete Geräte (z. B. mit Microsoft Intune)

Complex

Komplexe Logik für Precedence, Transformationen (von Attributen und/oder Schema)

MIM verwaltet Microsoft Entra ID (z. B. Gastkonten, Teams)

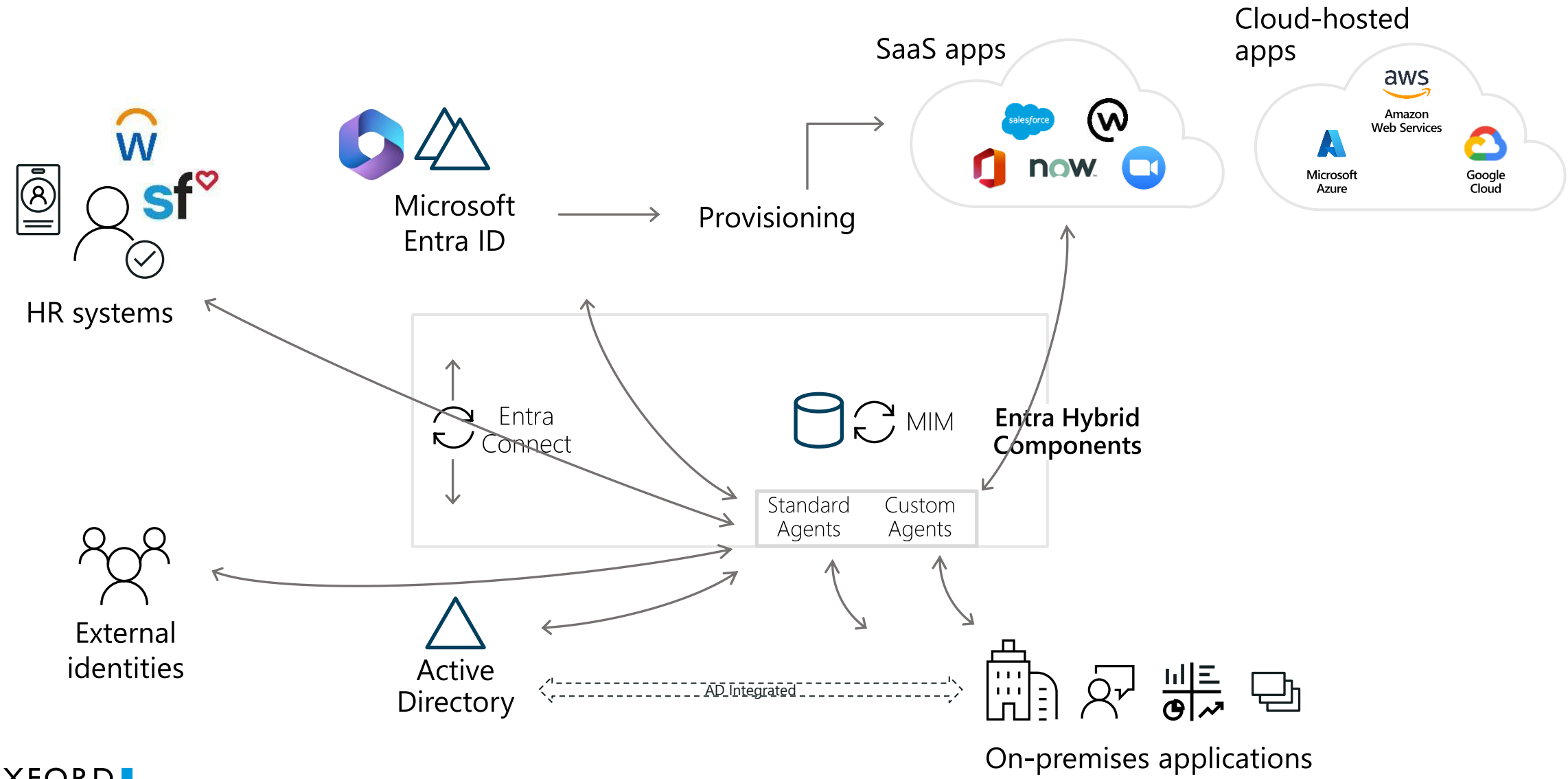
MIM verwaltet andere SaaS-Anwendungen

Eine Kombination aus Geschäftslogik in Microsoft Entra ID und MIM

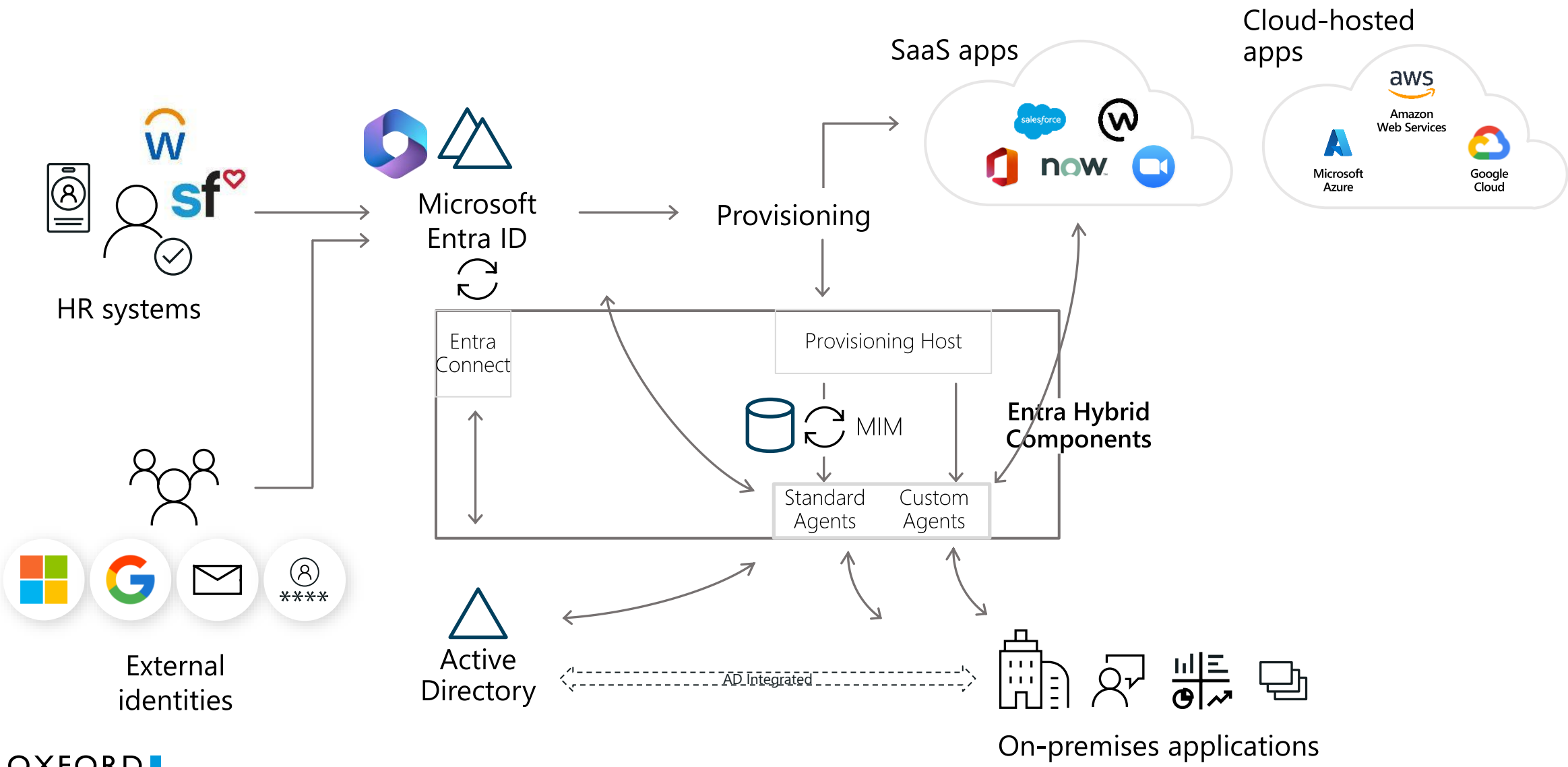
Anforderungen an Identity Governance (Bescheinigung, Funktionstrennung)

IDaaS

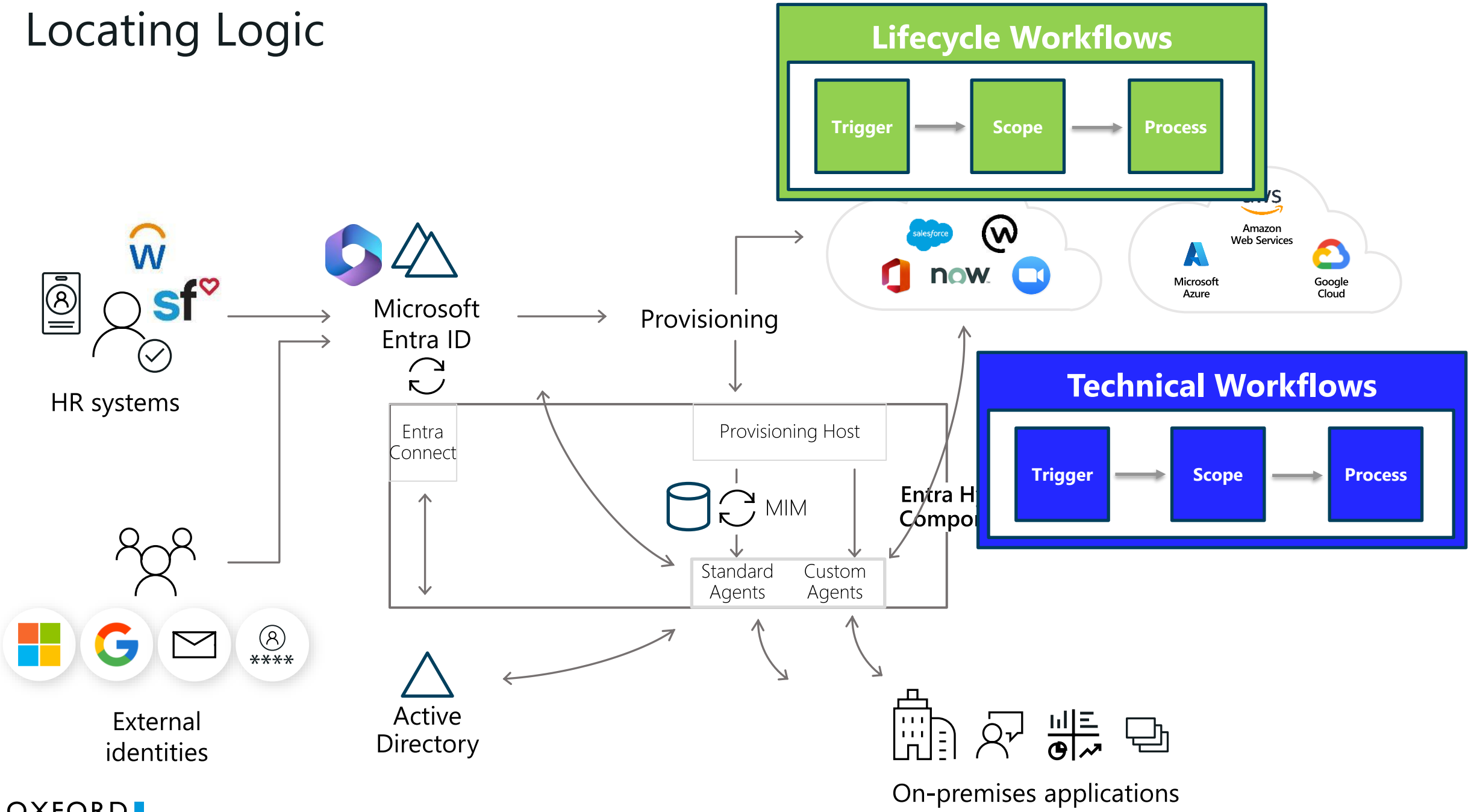
Complex On-Premises-first Identity



Cloud-first Hybrid



Locating Logic



Cloud-First Scenarios

Wir haben 5 Szenarien identifiziert, jedes mit einer Modellquelle und einer Zielarchitektur

Es handelt sich lediglich um Skizzenszenarien: Für einen Discovery-prozess werden immer spezifische Details benötigt

Der Schwerpunkt liegt hier auf dem Datenfluss, aber auch Prozesse und Benutzererfahrung sind bei jeder Analyse wichtig

Simple

MIM wurde durch Funktionen von Microsoft Entra ID ersetzt: Inbound HR und Outbound Provisioning und Management sowohl für SaaS-Anwendungen als auch für On-Premises-Anwendungen

Föderierte Integration extern gehosteter digitaler Identitäten ist ein natives Merkmal dieser Architektur und eröffnet eine Vielzahl neuer Möglichkeiten

Mindestens Microsoft Entra P1-Lizenzen erforderlich

Möglicherweise ist Microsoft Entra Connect erforderlich (oder auch nicht)

Um reine Cloud-Szenarien zu unterstützen, benötigen Sie Cloud-verwaltete Geräte (z. B. mit Microsoft Intune)

Complex

MIM erhält Bereitstellungs-anweisungen und Attribut-änderungen von Microsoft Entra ID

In komplexen Szenarien müssen die Abläufe zwischen HR und Microsoft Entra ID möglicherweise angepasst werden, um eine Konsolidierung vor dem Import zu ermöglichen

Diese Architektur ermöglicht die schrittweise Migration von MIM zu Microsoft Entra ID, ohne die Kosten, das Risiko und den Druck eines Big-Bang-Projekts

Sie benötigen wahrscheinlich Microsoft Entra ID P2-Lizenzen und (je nach Anforderungen) eine Lizenzierung für LifeCycle Workflows mit zusätzlichen Microsoft Entra ID Governance-Lizenzen

IDaaS

Cloud-First Scenarios

Wir haben 5 Szenarien identifiziert, jedes mit einer Modellquelle und einer Zielarchitektur

Es handelt sich lediglich um Skizzenszenarien: Für einen Discovery-prozess werden immer spezifische Details benötigt

Der Schwerpunkt liegt hier auf dem Datenfluss, aber auch Prozesse und Benutzererfahrung sind bei jeder Analyse wichtig

Simple

MIM wurde durch Funktionen von Microsoft Entra ID ersetzt: Inbound HR und Outbound Provisioning und Management sowohl für SaaS-Anwendungen als auch für On-Premises-Anwendungen

Föderierte Integration extern gehosteter digitaler Identitäten ist ein natives Merkmal dieser Architektur und eröffnet eine Vielzahl neuer Möglichkeiten

Mindestens Microsoft Entra P1-Lizenzen erforderlich

Möglicherweise ist Microsoft Entra Connect erforderlich (oder auch nicht)

Um reine Cloud-Szenarien zu unterstützen, benötigen Sie Cloud-verwaltete Geräte (z. B. mit Microsoft Intune)

Complex

MIM erhält Bereitstellungs-anweisungen und Attribut-änderungen von Microsoft Entra ID

In komplexen Szenarien müssen die Abläufe zwischen HR und Microsoft Entra ID möglicherweise angepasst werden, um eine Konsolidierung vor dem Import zu ermöglichen

Diese Architektur ermöglicht die schrittweise Migration von MIM zu Microsoft Entra ID, ohne die Kosten, das Risiko und den Druck eines Big-Bang-Projekts

Sie benötigen wahrscheinlich Microsoft Entra ID P2-Lizenzen und (je nach Anforderungen) eine Lizenzierung für LifeCycle Workflows mit zusätzlichen Microsoft Entra ID Governance-Lizenzen

IDaaS

Eine „zentrale Sicht“ in Ihre IAM-Welt mit benutzerdefinierten Benutzer- und Verwaltungsportalen für die gesamte Lösung

Viele Workflows mit anspruchsvollen Genehmigungs- und Delegationsanforderungen

MIM kann die erforderliche Funktionalität nicht bereitstellen

Die Wartung von MIM zusätzlich zu einer Cloud-Lösung ist nicht machbar (aus finanziellen, betrieblichen oder politischen Gründen)

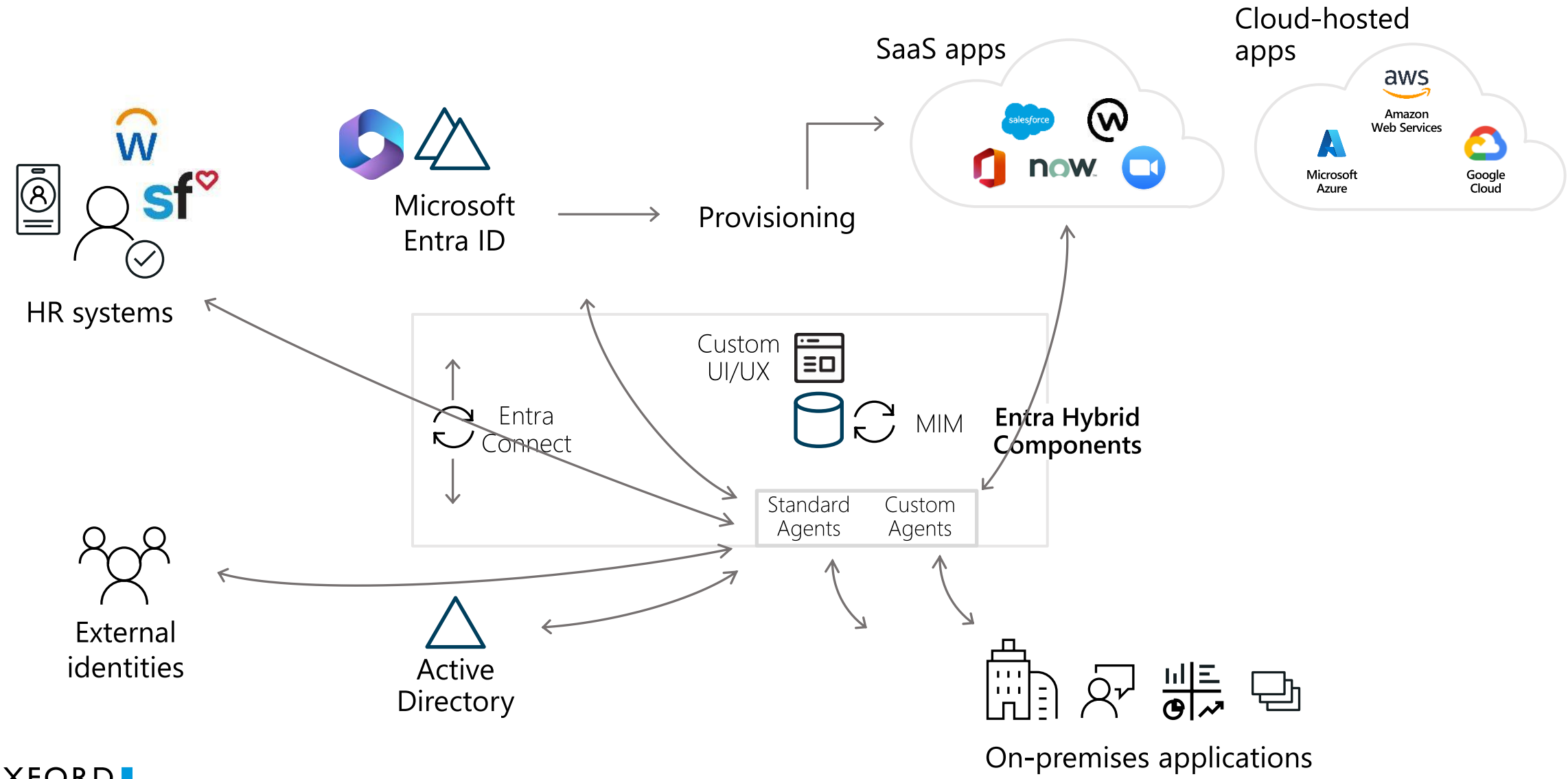
Microsoft Entra ID bleibt der strategische Kern der IDM-Landschaft des Unternehmens, es sind jedoch zusätzliche Funktionen erforderlich

OXFORD COMPUTER GROUP

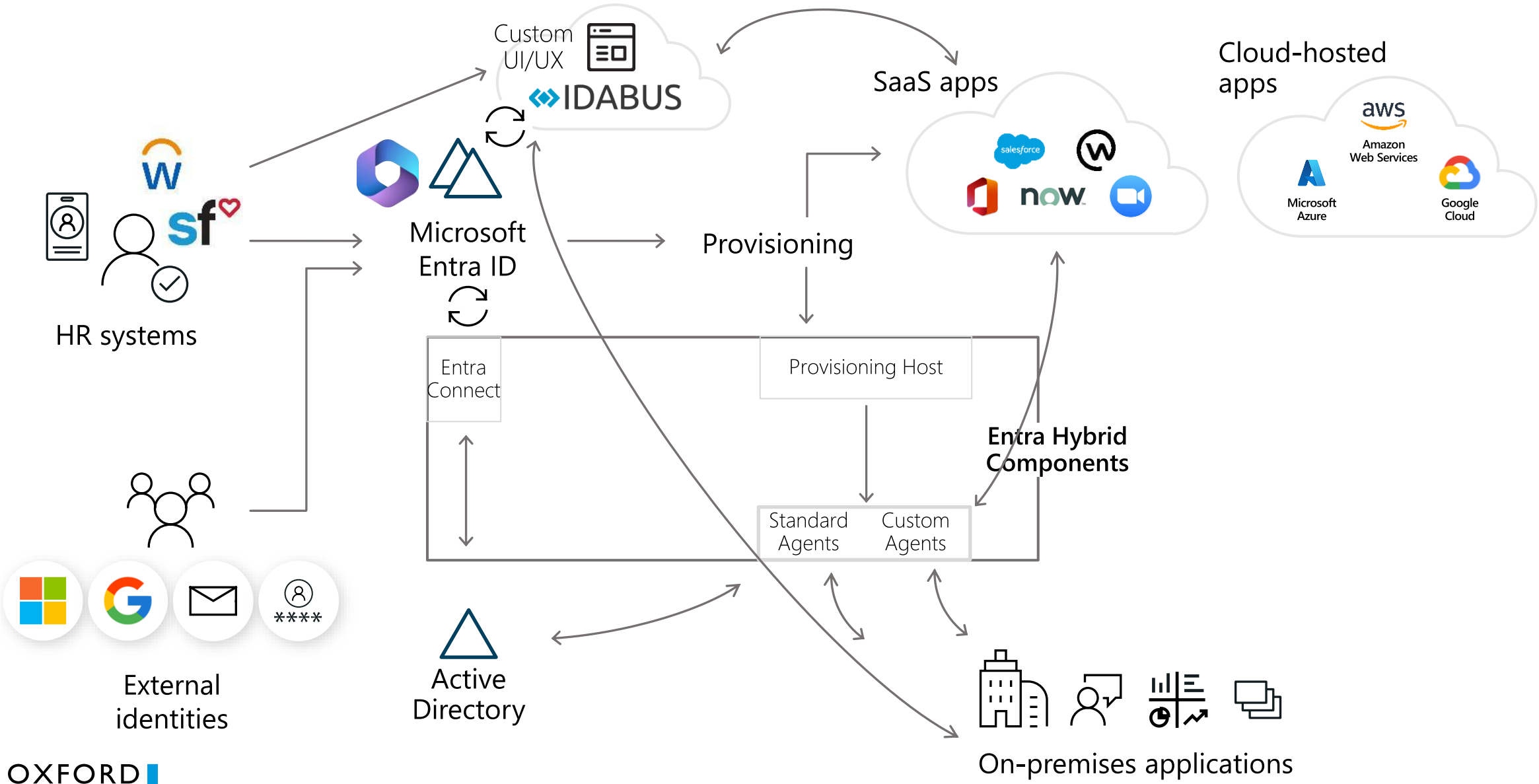
Current Limitations of Entra IDM

- Die benutzerdefinierte SCIM-Bereitstellung ist auf Benutzerobjekte beschränkt
  - Gruppen können mithilfe von Entra Connect Cloud mit AD synchronisiert werden („Group Writeback“)
- Workflows können nicht frei definiert werden
- Fehlende Tools zur Konvertierung in von On-Prem Mastered → Cloud-Mastered Objekte
- Org Strukturen, Vererbung fehlen
- Komplexe Schemaerweiterungen nicht möglich (multi-value…)

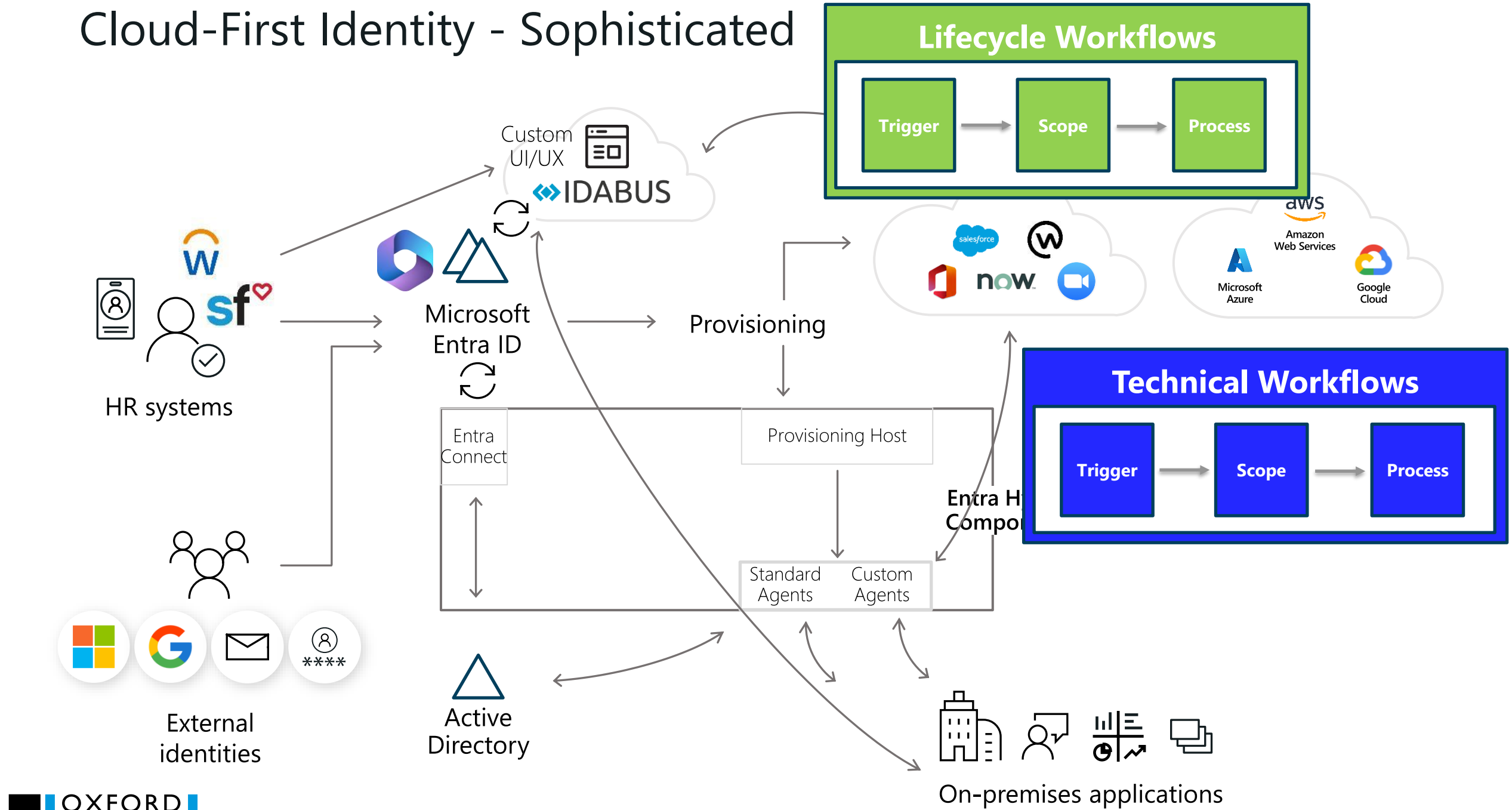
On-Premises-First Hybrid - Sophisticated



Cloud-First Identity - Sophisticated



Cloud-First Identity - Sophisticated



Cloud-First Scenarios

Wir haben 5 Szenarien identifiziert, jedes mit einer Modellquelle und einer Zielarchitektur

Es handelt sich lediglich um Skizzenszenarien: Für einen Discovery-prozess werden immer spezifische Details benötigt

Der Schwerpunkt liegt hier auf dem Datenfluss, aber auch Prozesse und Benutzererfahrung sind bei jeder Analyse wichtig

Simple

MIM wurde durch Funktionen von Microsoft Entra ID ersetzt: Inbound HR und Outbound Provisioning und Management sowohl für SaaS-Anwendungen als auch für On-Premises-Anwendungen

Föderierte Integration extern gehosteter digitaler Identitäten ist ein natives Merkmal dieser Architektur und eröffnet eine Vielzahl neuer Möglichkeiten

Mindestens Microsoft Entra P1-Lizenzen erforderlich

Möglicherweise ist Microsoft Entra Connect erforderlich (oder auch nicht)

Um reine Cloud-Szenarien zu unterstützen, benötigen Sie Cloud-verwaltete Geräte (z. B. mit Microsoft Intune)

Complex

MIM erhält Bereitstellungs-anweisungen und Attribut-änderungen von Microsoft Entra ID

In komplexen Szenarien müssen die Abläufe zwischen HR und Microsoft Entra ID möglicherweise angepasst werden, um eine Konsolidierung vor dem Import zu ermöglichen

Diese Architektur ermöglicht die schrittweise Migration von MIM zu Microsoft Entra ID, ohne die Kosten, das Risiko und den Druck eines Big-Bang-Projekts

Sie benötigen wahrscheinlich Microsoft Entra ID P2-Lizenzen und (je nach Anforderungen) eine Lizenzierung für LifeCycle Workflows mit zusätzlichen Microsoft Entra ID Governance-Lizenzen

IDaaS

Die IDaaS-Lösung ist eng mit Microsoft Entra ID integriert und liefert beispielsweise die Ausgabe (in Form von Gruppenmitgliedschaften oder Zugriffspaketzuweisungen) von rollenbasierten Berechnungen, die sich aus (potenziell mehreren) organisatorischen Zuweisungen und komplexer Aufgabentrennung (SoD) Anforderungen ergeben

Microsoft Entra ID implementiert so viele Bereitstellungsfunktionen wie erforderlich, während IDaaS dies bei Bedarf mit nativen Funktionen unterstützt

OXFORD COMPUTER GROUP

Nächste Schritte

- Etablierung einer Zielarchitektur, um sowohl die Weiterentwicklung planen als auch opportunistisch umsetzen zu können
  - z.B. Cloud HR – kommt eine Migration?

- Ermittlung von Abhängigkeiten und aktuelle Blocker
  - Fortschritte in Richtung Cloud-First-/Cloud-Only-Geräteverwaltung
  - Fortschritte in Richtung passwortlose Identität
  - Abhängigkeit von NTLM/LDAP in Legacysystemen
  - Werkzeuge zur Konvertierung On-prem Objekte → Cloud-Mastered
  - File and Print

OXFORD
COMPUTER GROUP

Connect with us

Email	info@oxfordcomputergroup.global
LinkedIn	@oxford-computer-group-global
Call us	+44 (0)1865 521200
Web	oxfordcomputergroup.global

OXFORD COMPUTER GROUP

Hybrid Security Workshop

James Cowling

July 2024

Hybrid Security Workshop

- Developed with Vattenfall
  - Swedish Energy Company
  - Nuclear plants, nuclear waste reprocessing
  - Somewhat focussed on security
  - Developed with staff from the SOC, Red Teams
- 35,000 Employees
  - 65 people attended this security workshop in 4 deliveries
  - Broad representation from IT: desktop, infra, SOC, Red Teams, Office Apps, Collab, Linux/Unix teams

Workshop Outline

- Module 1: Attacks on IT Infrastructure
- Module 2: Active Directory Security Specifics
- Module 3: Deep-Dive into Kerberos
- Module 4: AD Platform Security
- Module 5: Certificate-based Authentication
- Module 6: Deep-Dive into OAuth2 and OpenID Connect
- Module 7: Hybrid Environments: Single Sign-On and Trust
- Module 8: Password Management and Security
- Module 9: Security with Multi-Tenant and External Users

Slice and Dice

OXFORD COMPUTER GROUP

- Talk about the security of the legacy systems – this should not be neglected
- Customers need to understand what is happening with Hybrid integrations, particularly the influence of device registration on authentication possibilities
- Progress towards Passwordless with Passkeys/FIDO2, Hello for Business Cloud Trust
  - How does all this work, how can we use it to access legacy?
- Take the relevant pieces from the workshop and make a custom session
- Recordings are available

Resources

- Microsoft Entra identity blog
  aka.ms/IdentityBlog
- Microsoft Entra product page
  aka.ms/entra/identitygovernance
- Microsoft Identity solution page
  microsoft.com/Identity
- Microsoft Entra technical documentation
  aka.ms/Entra/IDGovDocs
- Try Microsoft Entra ID Governance free
  aka.ms/EntraIDGovTrial