Teil 3 der Artikelserie fokussiert sich auf den Markt für Cloud-basierten IGA-Lösungen (Identity Governance & Administration), dem neuen Modebegriff für das Verwalten von Identitäten und Berechtigungen (IAM). Dieser ist derart dicht besiedelt, dass eine abschließende Betrachtung aller Optionen im Detail geradezu unmöglich ist. Es gibt hochspezialisierte Analysten wie KuppingerCole oder Gartner, die zweifelsohne umfassendere und detailliertere Einschätzungen bzgl. dem Markt von IAM-Lösungen abgeben können. Unser Blickwinkel ist in dieser Artikelserie jedoch speziell. Wir richten uns explizit an SAP IDM-Kunden und zeigen Ihnen mögliche Optionen, die wir als unabhängiger Dienstleisters mit jahrzehnte-langer Erfahrung in SAP-Kundenprojekten sehen.

Cloud Services haben in der Praxis alle dasselbe Problem: Es handelt sich nicht mehr, wie man es von SAP IDM gewohnt ist, um hochflexible Individualsoftware, sondern Standard-Software, die meistens weniger bis garnicht anpassbar ist. Die Buchung bzw. Implementierung eines Cloud-Service muss daher unbedingt vorab auf eventuelle Showstopper geprüft werden. Sollten keine Showstopper vorhanden sein, oder Ihr Unternehmen flexibel genug durch Prozess-Standardisierung auf diese reagieren können (siehe dazu auch Teil 1 dieser Serie), bieten Cloud-Services Vorteile, die nicht ignoriert werden können. Den Vertriebs-Spruch „Sie kümmern sich um Ihr Geschäft und wir kümmern uns um den Rest“ haben Sie sicher schon einmal gehört. Mit schlanken Prozessen und dem entsprechenden Cloud-Services ist dies tatsächlich denkbar.

Bitte beachten Sie, dass diese Einschätzungen **keineswegs als abschließend betrachtet werden können** und **keine individuelle Beratung** ersetzen.

- Teil 1: Das Ende einer Ära: Die Zukunft nach SAP IDM
- Teil 2: SAP – Cloud Identity Services, GRC edition for SAP HANA
- **Teil 3: Cloud Services**
- Teil 4: On-Premise Lösungen: z.B. One Identity

Die vorgestellten Optionen in diesem Artikel sind:

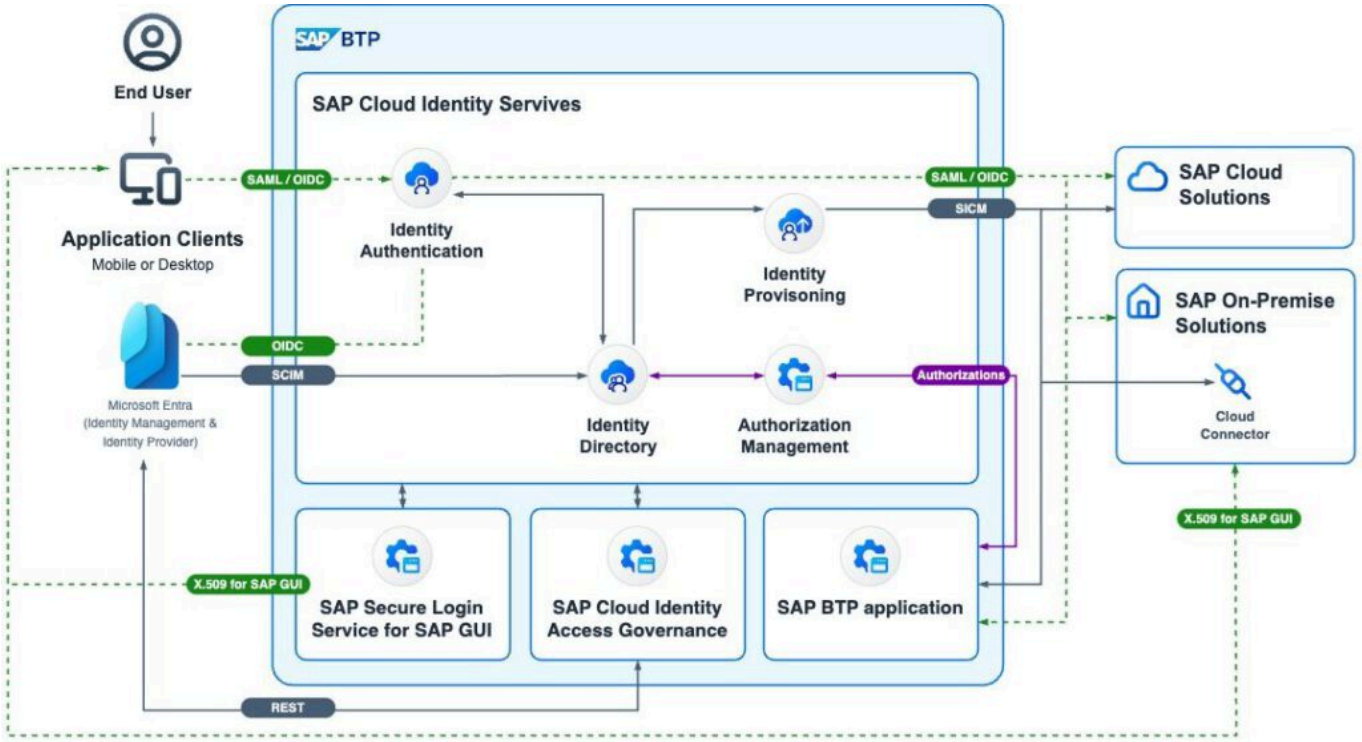
- Option A: Microsoft Entra
- Option B: Omada Identity Cloud
- Option C: Okta
- Option D: IBM Security Verify

Option A: Microsoft Entra

Die DSAG-Technologietage 2024 in Hamburg standen am 06.02. gerade in den Startlöchern, als das Gespann Jürgen Müller (CTO SAP) und Sebastian Westphal (DSAG-Fachvorstand) die wahrscheinlich wichtigste Meldung des Jahres für den Bereich Identity- und Access Management bekannt geben. Was bei Insidern bekannt und in der Gerüchteküche schon längst spekuliert wurde, manifestierte sich mit einer Folie, die Microsoft Entra als „offiziellen“ Nachfolger von SAP IDM deklariert.

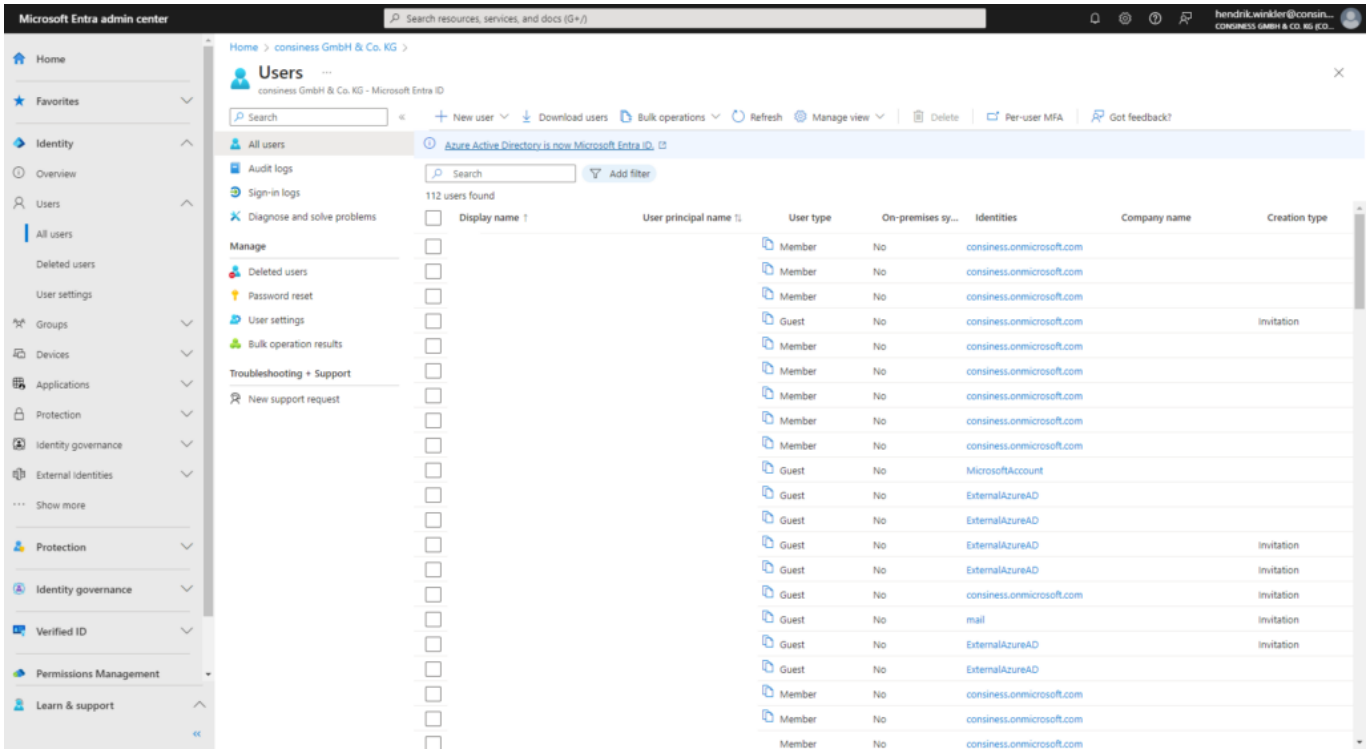
Doch was ist eigentlich Microsoft Entra? Früher bekannt als Azure Active Directory oder Azure AD, ist Entra ID eine cloudbasierte Identitäts- und Zugriffsverwaltungslösung. Es bietet Authentifizierungs- und Autorisierungsdienste für verschiedene Microsoft-Dienste wie Microsoft 365, Dynamics 365 und Microsoft Azure. Am 11. Juli 2023 kündigte Microsoft die Umbenennung von Azure AD in Microsoft Entra (-ID) an, um die Konsistenz mit anderen Microsoft Cloud-Produkten zu verbessern.

Der On-Premise Vorgänger von Entra ist das altbekannte Microsoft Active Directory (AD), ein Verzeichnisdienst, der 1999 eingeführt wurde und der de-facto Standard für die Verwaltung von Windows-Benutzerkonten, Applikationsberechtigungen sowie E-Mail-Konten. Durch die Monopol-artige Stellung von Microsoft-Produkten im Business-Umfeld wird das Active Directory wahrscheinlich allen SAP-Kunden in der einen oder anderen Form genutzt. Nicht selten befinden sich alle Identitäten, die Organisationsstruktur und Informationen über den Zugriff zu zahlreichen Applikationen innerhalb der sogenannten AD-Struktur. Aus diesem Grund ist bei vielen SAP-IDM Implementierungen das erste non-SAP-System, welches in die IAM-Infrastruktur als Identitäts-Provider und/oder Zielsystem eingebunden wird.



Die neue Referenzarchitektur von SAP!? (Quelle: https://community.sap.com/t5/technology-blogs-by-sap/preparing-for-sap-identity-management-s-end-of-maintenance-in-2027/ba-p/13596101)

Folgend der DSAG-Ankündigung legt SAP in einem Blog-Post nach und präsentiert eine Architektur, die höchstwahrscheinlich als Referenz für die folgenden Jahre gesehen werden kann. Die Abbildung zeigt Entra als zentralen Identity Provider und Identity Management-Lösung, welche über Schnittstellen mit den SAP Cloud Identity Services und Cloud IAG integriert wird. Der IPS (Identity Provisioning Service) ist über den Cloud-Connector dafür zuständig, das Tor zwischen Cloud und On-Premise Lösungen zu öffnen. Auch wenn diese Architektur auf den ersten Blick kompliziert aussieht, hat sie den großen Vorteil, dass SAP-lastige Unternehmen in der Cloud sowieso schon Entra (bzw. Azure AD), SAP IAS und IPS im Einsatz haben.

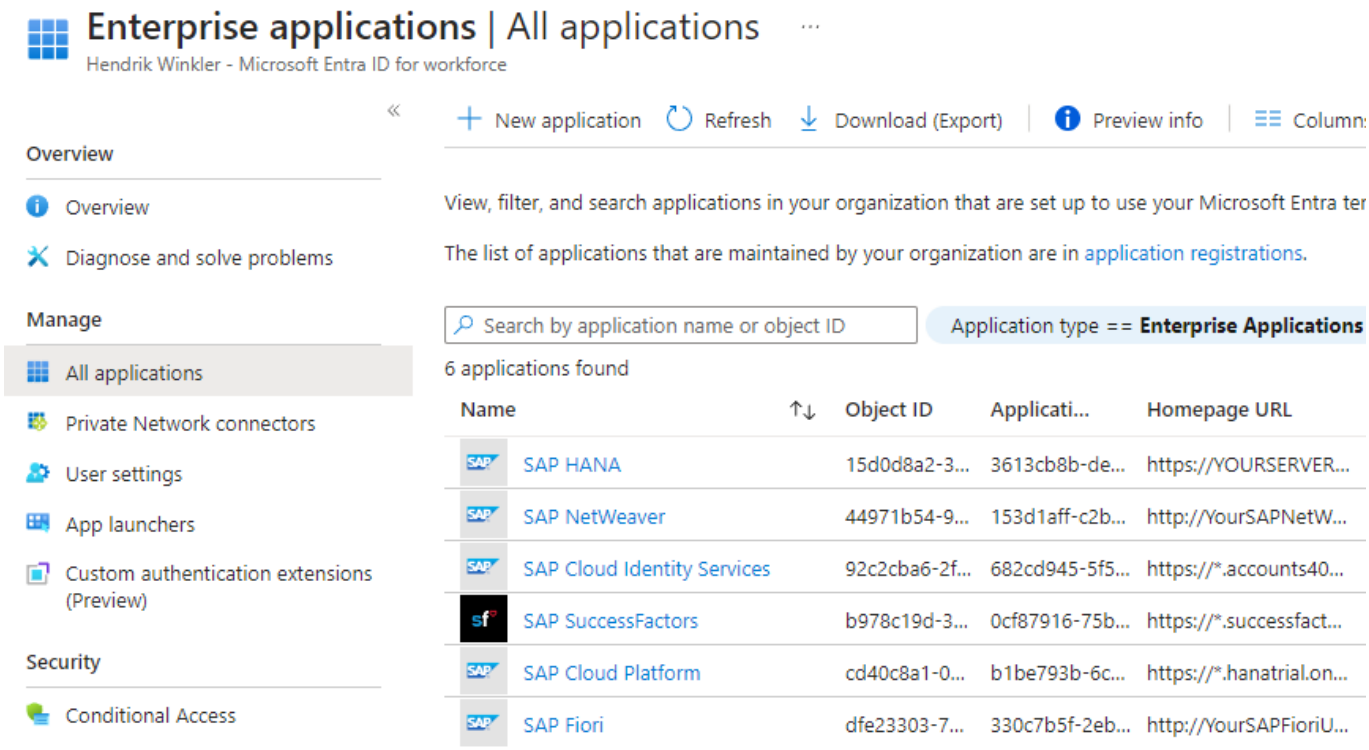


Auch consiness verwendet für interne Zwecke Entra

Sofern Sie oder ihr Unternehmen mit Office 365 und/oder Azure-Awendungen arbeiten, ist es extrem wahrscheinlich, dass Sie bereits eine eigene Instanz von Entra im Einsatz haben. Entra selbst begrüßt den Anwender bzw. Administrator mit einer aufgeräumten Oberfläche. Bereits das Menü verrät dem geschulten Blick den groben Umfang der Applikation:

- Nutzer und Gruppen (Verzeichnisdienst, wie aus dem Active Directory bekannt)
- Applikationen und Geräte (Konnektoren / Konfigurationsmanagement)
- Schutz (Authentifizierung, Passwort-Management)
- Externe Identitäten (Kollaboration mit Identitäten außerhalb der Organisation)
- Governance (Identity-Lifecycle, PAM)

Für die Provisionierung in externe Systeme kommt der Azure AD Provisioning Service zum Einsatz, welcher eine Reihe von Applikationen zum Vorschein bringt. Auch SAP Konnektoren können, wenn auch mit etwas Aufwand, eingerichtet werden. Das Provisioning wird hierbei über das SCIM Protokoll bereitgestellt, liefert nach unseren Kenntnisstand jedoch kaum Möglichkeiten, über die Standard-Funktionen hinauszugehen.



SAP Integration über Enterprise Application-Provisioning

Ein weiterer positiver Aspekt von Entra ist die Transparenz in der Preisgestaltung. Während bei SAP-Produkten selbst die Kunden oft nicht genau wissen, was sie für Ihre Applikationen eigentlich zahlen müssen, besticht Entra mit einer Preispolitik, die man mit etwas Kreativität auch auf einen Bierdeckel drucken könnte. Es ist jedoch zu beachten, dass die designierte Infrastruktur mit SAP auch Kosten für die jeweiligen SAP-Produkte beinhalten würde.

Vorbildlich transparente Preispolitik

Vorteile

- Service, auch unabhängig von der IAM-Architektur, meistens schon vorhanden
- schlanke Architektur ohne zusätzliche Drittsysteme
- Partnerschaft mit SAP
- Moderne Applikation
- Hervorragende Dokumentation

Nachteile

- Zusätzlicher lock-in-Effekt auf Microsoft-Produkte
- Preissteigerungen für Abonnements sind Kunden unausweichlich ausgesetzt
- Keine Unterstützung von verteilten Domänen
- On-Premise Infrastruktur (z.B. Windows Domänencontroller) benötigt weiterhin klassisches Active Directory
- Umfang der SAP-Partnerschaft und somit Unterstützung bzw. Anpassbarkeit auf erweiterte SAP-Integrationsszenarien bleibt abzuwarten

Einschätzung

Quizfrage: Was ist der uneinholbar große Vorteil von Entra? Netzwerkeffekte! Dass Microsoft ein Quasi-Monopol für Anwendungssoftware in der Business-Welt hat ist

nicht nur ein Anlage-Tipp am Aktienmarkt, sondern auch eine valide Entscheidungsgrundlage für ihre nächste IAM-Landschaft.

Wie bei anderen Cloud-Lösungen auch, dürfte trotz Partnerschaft mit SAP die Achillesferse in der Flexibilität bzgl. kundeneigener Anforderungen liegen. Ob die Standard-Infrastruktur, bestehend aus Entra, IAS/IPS und IAG jemals in der Lage sein wird, ihre Besonderheiten wie eigenentwickelte Tabellen und Felder in ABAP zu provisionieren, bleibt zu bezweifeln. Wir lassen uns gern positiv überraschen!

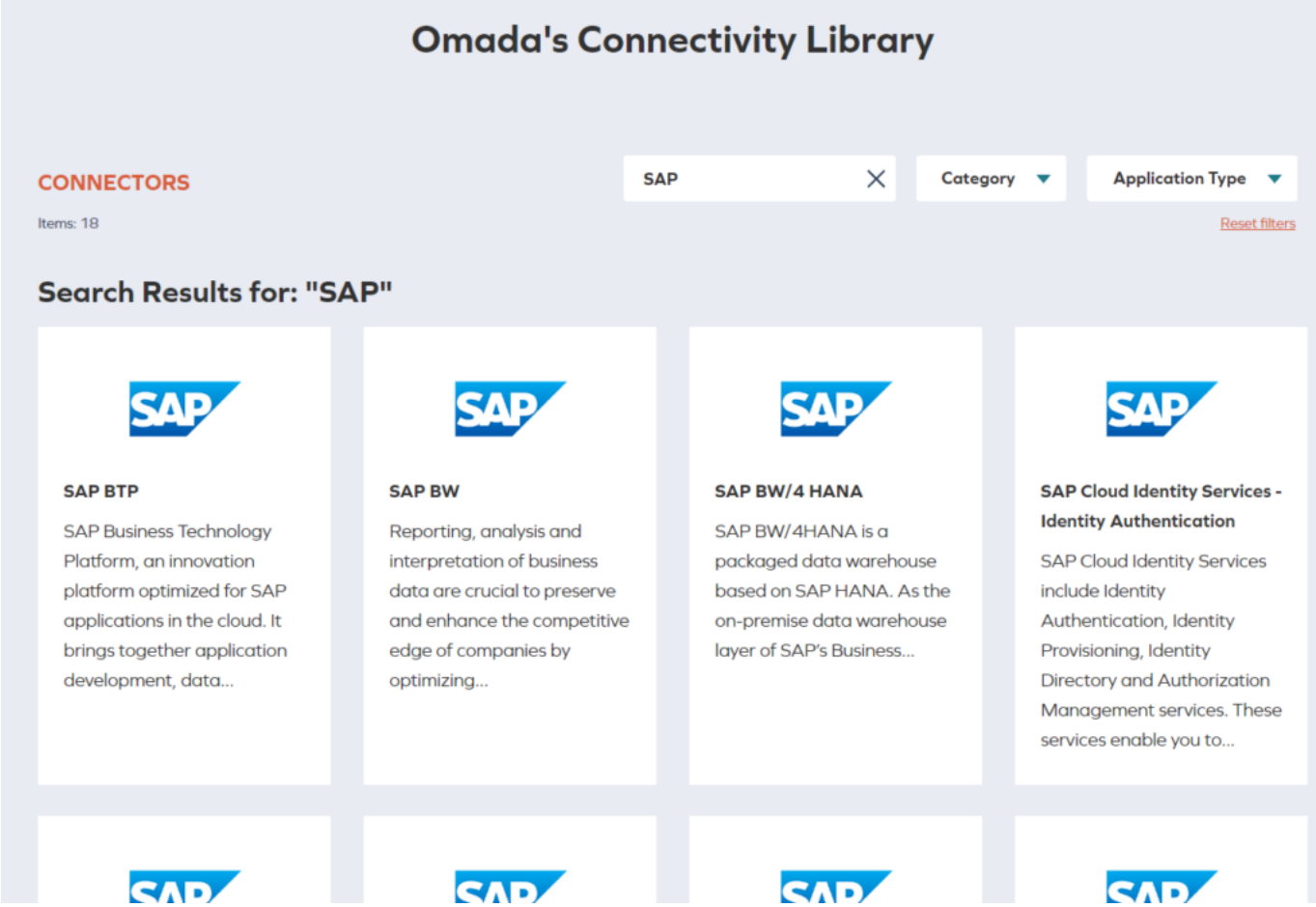
Option B: Omada Identity Cloud

Alle unter einem Dach! Omada Identity Cloud ist der modernisierte Cloud-Ableger des Omada Identity Managers. Die Identity Cloud bietet alle wesentlichen Funktionen zur sicheren, konformen und effizienten Verwaltung aller Benutzerzugriffe auf Systeme, Daten und Anwendungen in hybriden, Cloud- und Multi-Cloud-Umgebungen.

Das Fundament von Omada ist eine moderne, Cloud-nativen Microservice-Architektur aufgebaut und bietet Geschwindigkeit, intelligente Entscheidungsunterstützung, Konnektivität und eine höhere Performance als Vorgängerprodukte.

Die Lösung selbst basiert auf über 20 Jahren Erfahrung und ist fokussiert auf schnelle und zuverlässige Ergebnisse für Unternehmen. Sie umfasst konzeptionell das Best-Practice-Framework für Identity-Governance-Prozesse (IdentityPROCESS+), eine Bereitstellungs- und Betriebsmethodik (IdentityPROJECT+) und garantierten Mehrwert für Kunden durch Schulungen, Support und Dienstleistungen (Identity Success).

Die Möglichkeiten bzgl. der Integration von Anwendungen sind in in der Omada Connectivity Library hervorragend dokumentiert. Bei keinem anderen Produkt fällt es uns leichter, eine bestehende Infrastruktur auf die Kompatibilität mit den Konnektoren der IAM-Lösung zu prüfen.



Omada Connectivity Library

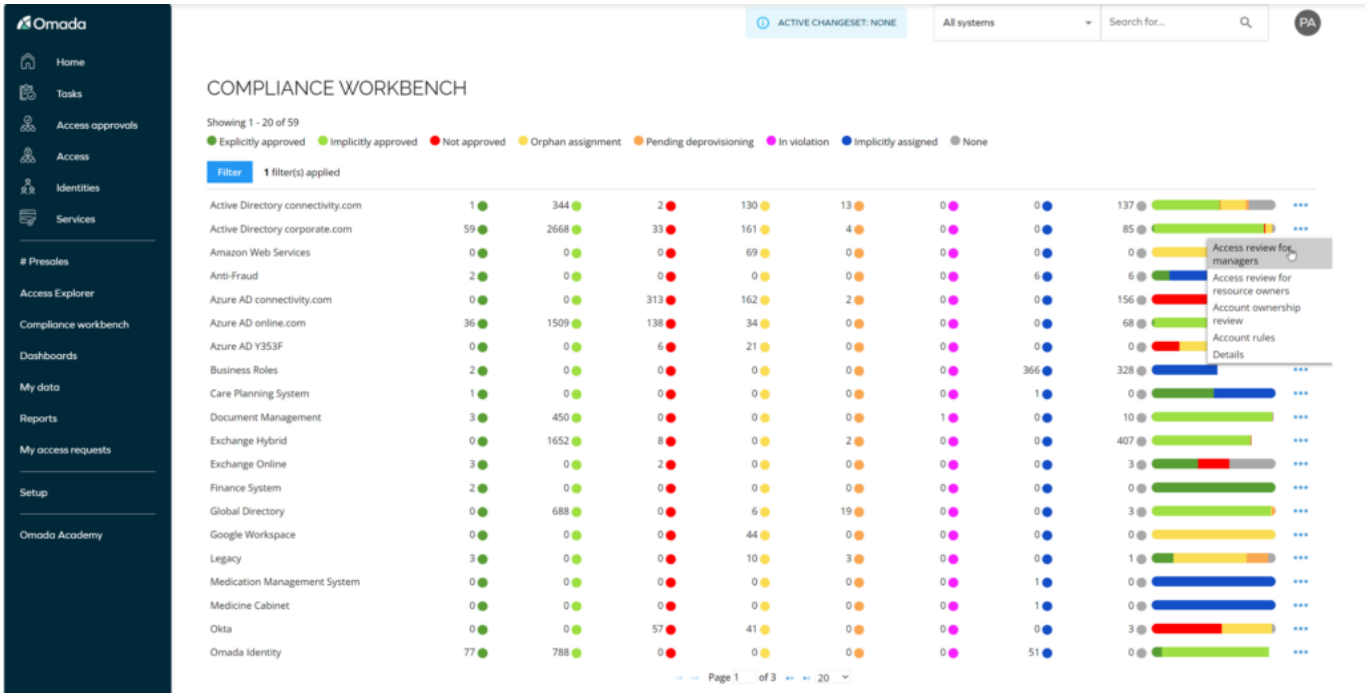
Am Beispiel einer angestrebten SAP-Integration konnten wir alle gängigen Konnektoren vorfinden. Die unterstützten Objekte und Operationen sind jeweils aufgeführt. Das Team von Omada hat uns signalisiert, dass auf Rückfrage auch kundeneigene „Sonderwünsche“ implementiert werden können, sollte der Standard-Umfang nicht ausreichen.

Supported Objects and Operations

LDAP Objects	Omada Identity Data Model	Operations
Users	Account	Create, Read, Update, Delete
Groups	Resource	Read
Group Memberships	Resource Assignment	Create, Read, Update, Delete

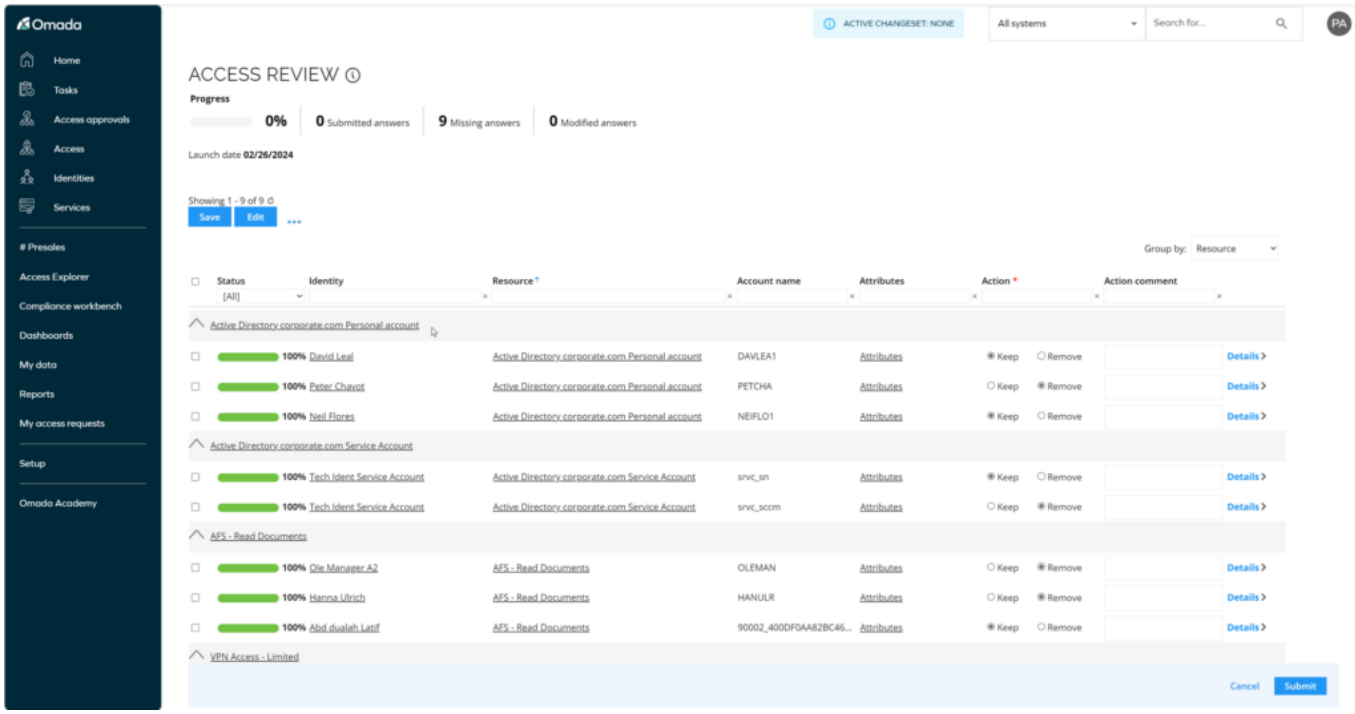
Unterstützte Objekte und Operationen am Beispiel des SAP IPS Konnektors

Weiterhin hervorzuheben ist das offensiv vermarktete Versprechen einer schnellen und effizienten Einführung. Über das Accelerator Package wird ein standardisiertes Projekt- und Vorgehensmodell für die Implementierung der Software und Prozesse geboten. Eine (auch von uns) avisierte Projektdauer von 12+ Monaten für eine IAM-Einführung soll in vielen Fällen auf nur 4 Wochen reduziert werden. Ein Prozess, der nur mit einer hoch standardisierten und voll ausgebauten Software-Lösung möglich ist.



Alles auf einem Blick – Compliance Workbench

Um diesen Punkt zu verdeutlichen sollen an dieser Stelle die Compliance-Workbench und das Access Review exemplarisch gezeigt werden. Die Compliance-Workbench gibt eine standardisierte Übersicht aller integrierten Systeme und wertet Zuweisungen je nach Status aus. Eine einfache Möglichkeit um größere Lücken in den Prozessen der gesamten Systemlandschaft zu identifizieren. Das Access Review Feature ist eine vorgefertige Lösung für die möglichst-bequeme Durchführung von Attestations (bzw. Rezertifizierungen).



Geführter Attestation-Prozess

Vorteile

- Hersteller, der seit >20 Jahren spezialisiert auf IAM-Software ist
- Großer Umfang von Standard-Funktionen
- Schnelle und unkomplizierte Einführung
- Starkes, deutschsprachiges Team und Präsenz mit direktem Draht zum Hersteller

Nachteile

- Keine Online-Trial-Funktion wie bei der Konkurrenz (Demos können jedoch angefordert werden)
- Vergleichsweise geringe Anpassbarkeit für hochspezialisierte Szenarien

Einschätzung

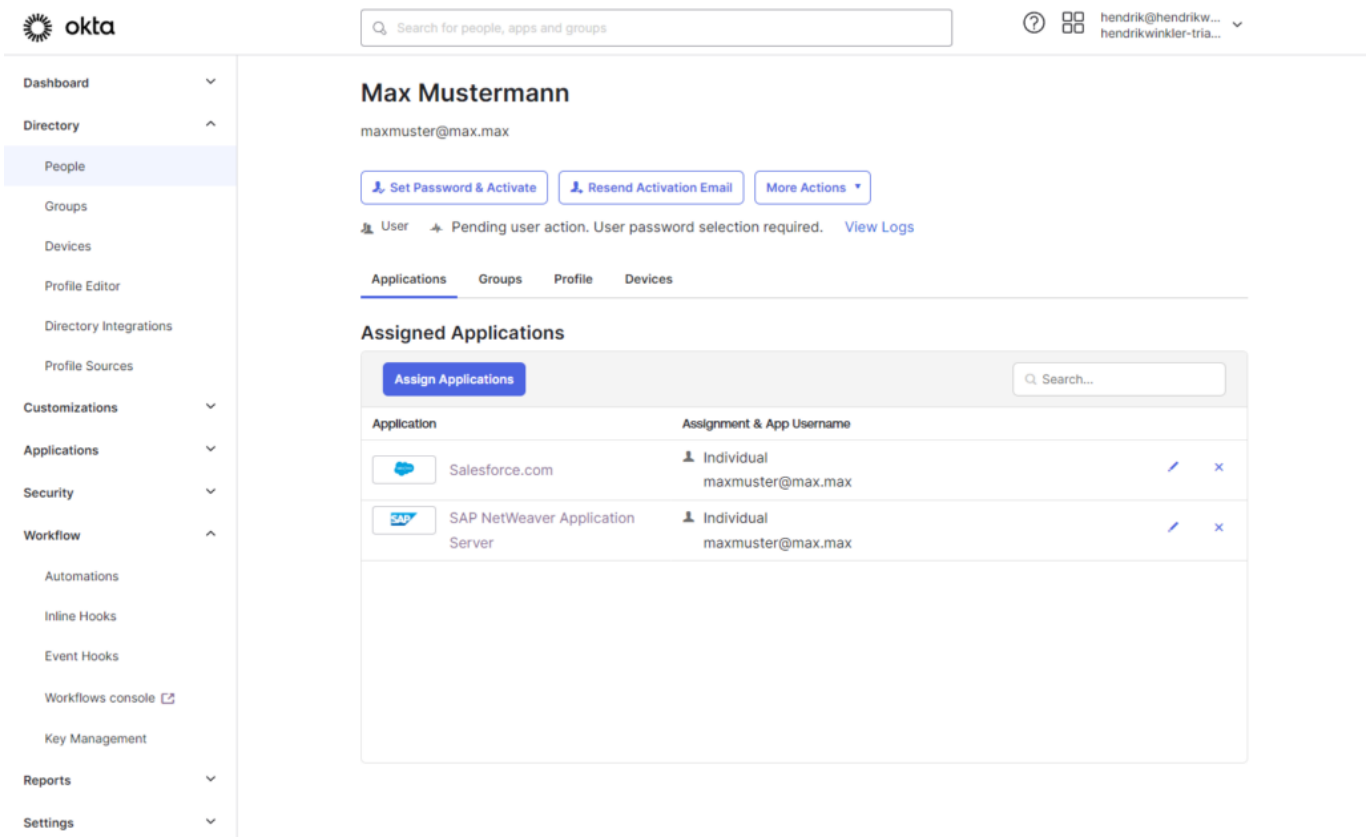
Die Stärke der Omada Identity Cloud ist zweifelsohne eine Lösung anzubieten, die wir neu-Deutsch als „Feature-Rich“ bezeichnen würden. Wer den Omada Identity Manager bucht erhält Software einer hochspezialisierten Firma mit zahlreichen Funktionen, die bei anderen Lösungen fehlen oder aufwendig mit

Eigenentwicklungen dazugebaut werden müssen.

Auch wenn die Software ihren Ursprung in Dänemark hat können sich Kunden auf ein sehr engagiertes und fähiges deutschsprachiges Team freuen und dort Ihre Wünsche und Anforderungen einbringen. Eine Nähe zum Hersteller, die man bei Schwergewichten Microsoft und SAP vermissen wird. Wenn Sie auf eine Lösung setzen wollen, die „einfach funktioniert“ und auf hochspezialisierte SAP-Integrationszenarien verzichten können, gehört die Omada Identity Cloud aus unserer Sicht zu der engeren Auswahl.

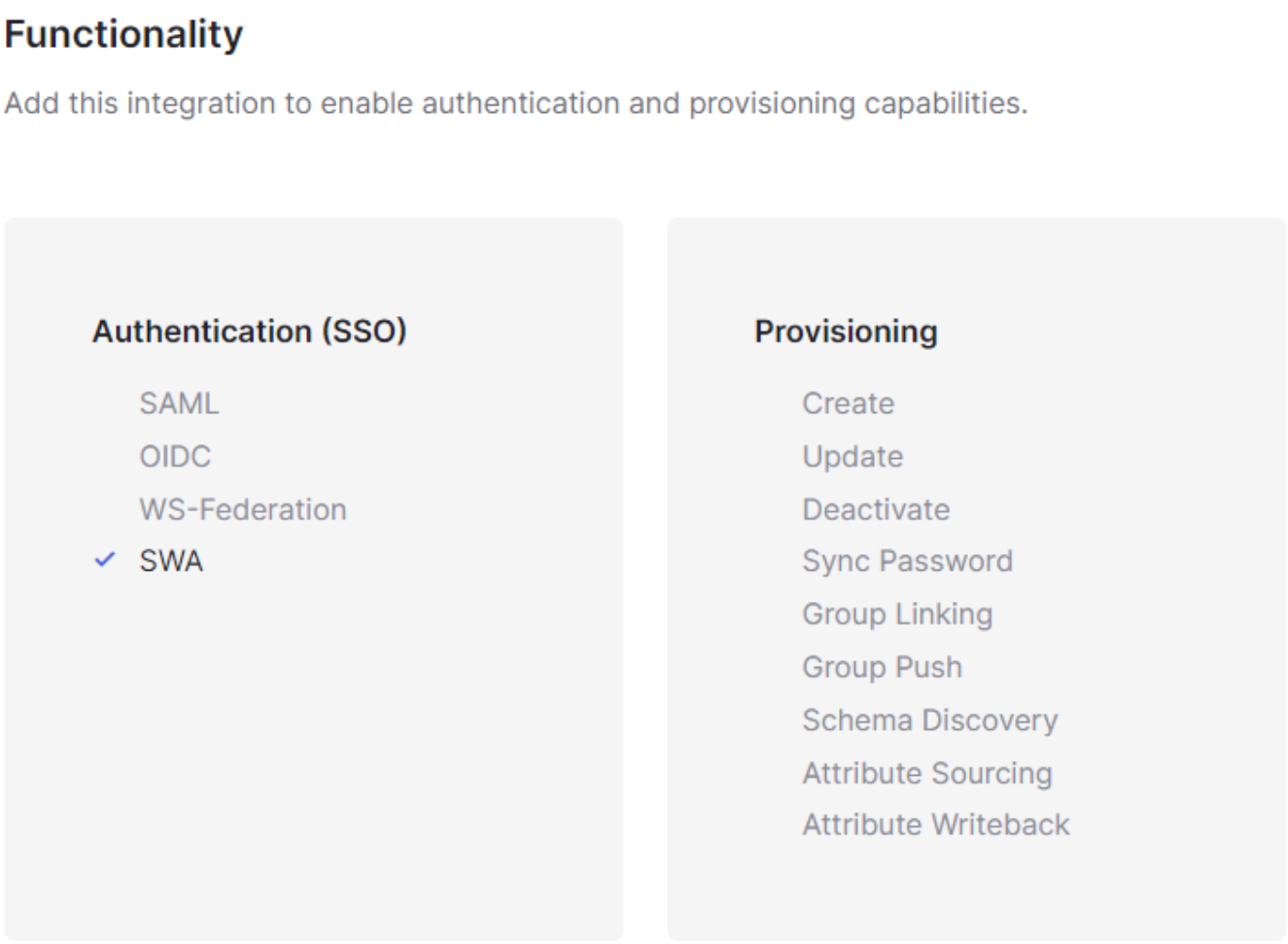
Option C: Okta

Okta ist ein unabhängiger Anbieter, der sich auf Identitäts- und Zugriffsmanagement spezialisiert hat. Die Plattform ist bekannt für ihre Flexibilität und Benutzerfreundlichkeit, wobei sie eine breite Palette von Funktionen zur Identitätsverwaltung bietet, einschließlich Single Sign-On (SSO), Multi-Faktor-Authentifizierung (MFA) und Lebenszyklusmanagement für Identitäten. Okta legt großen Wert auf die Integration mit einer Vielzahl von Anwendungen und Plattformen, was es zu einer beliebten Wahl für Unternehmen macht, die eine heterogene IT-Landschaft haben und eine nahtlose Benutzererfahrung über verschiedene Anwendungen hinweg wünschen.



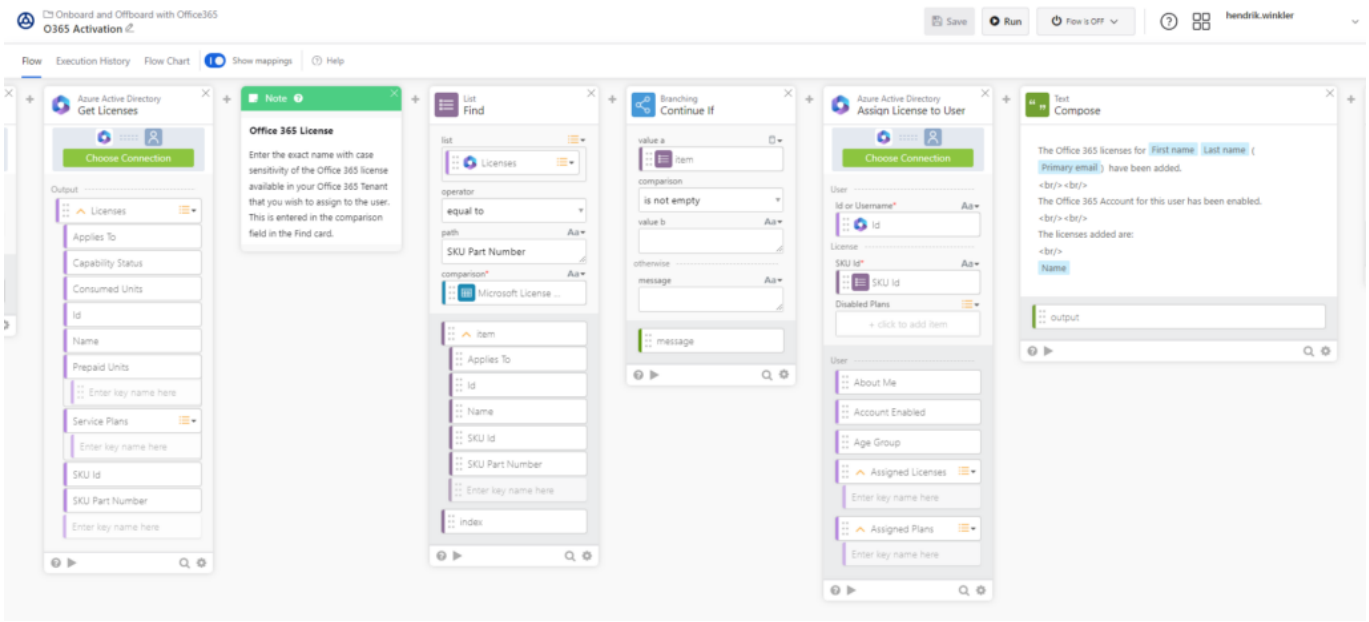
People, Groups, Devices – Ein moderner Verzeichnisdienst in Aktion

Technisch und konzeptionell betrachtet stellt Okta ein sogenanntes Directory-as-a-Service (DaaS) dar. Dies bedeutet, dass es sich im Kern um einen Verzeichnisdienst handelt, welcher in der Cloud als Service angeboten wird. Verzeichnisdienste unterscheiden sich von einer Identity-Management Lösung in sofern, dass sie die Daten über Personen und Objekte (z.B. Netzwerkinfrastruktur) vorhalten und für Drittapplikationen bereitstellen, ohne in diesen Nutzerkonten und Berechtigungen direkt zu verwalten. Mit diesem Ansatz steht Okta in direkter Konkurrenz zu dem Microsoft Active Directory bzw. Entra.



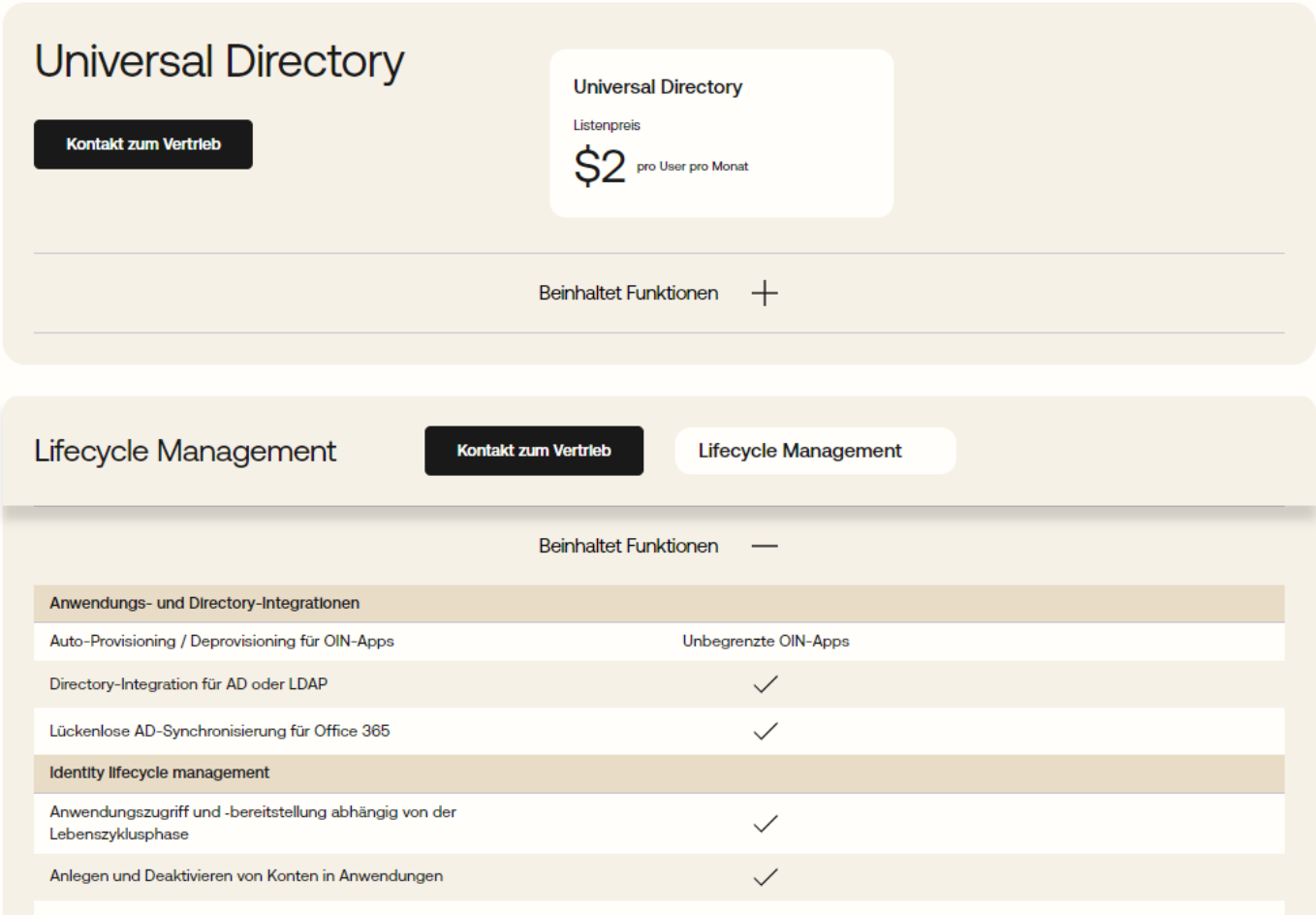
Funktionalität des SAP NetWeaver-Connector

Genau wie bei Microsoft Entra sind hier jedoch die Übergänge von einer DaaS-Lösung zum Identity-Management fließend und es können auch Provisionierungsszenarien konfiguriert werden. Okta besticht dabei durch eine, zumindest von uns wahrgenommene, höhere Flexibilität als bei Konkurrenzprodukten. Dies wird vor allem bei der Workflow-Funktionalität deutlich.



Die grafische Okta Workflow-Engine wird mit Templates angeboten

Die Preisgestaltung von Okta ist sehr individuell und wirkt somit fair. Sie basiert auf den spezifischen Produkten, die ein Kunde wählt, und der Anzahl der Benutzer, die diese Produkte nutzen werden. Zu den Produkten gehören Single Sign-On, Multi-Faktor-Authentifizierung, Universal Directory, Lifecycle Management, API Access Management und mehr.



Okta Pricing – Transparent und individuell anpassbar

Jedes dieser Produkte hat seinen eigenen Preis pro Benutzer pro Monat. Darüber hinaus gibt es einen Mindestjahresvertrag. Für Enterprise-Kunden mit einer großen Anzahl von Benutzern sind Volumenrabatte verfügbar. Es ist wichtig zu beachten, dass die tatsächlichen Preise variieren können und es am besten ist, sich direkt an Okta zu wenden, um die genauesten und aktuellsten Informationen zu erhalten.

Vorteile

- Hohe Anpassbarkeit für eine Cloud-Lösung
- Starke weltweite Verbreitung
- Gilt als nutzerfreundlich und leicht und schnell zu implementieren
- Sehr individuelles Preismodell

Nachteile

- On-Premise Infrastruktur (z.B. Windows Domänencontroller) benötigt weiterhin klassisches Active Directory
- Grundkonstrukt von Okta sind, wie in Verzeichnisdiensten üblich, Gruppen. Keine Unterscheidung zu Rollen.
- Kein Hauptfokus auf den SAP-lastigen DACH-Markt und demzufolge auch kaum erweiterte SAP-Integrationsszenarien

Einschätzung

Von Gartner wird Okta vermutlich nicht ohne Grund als „Leader“ für Identity und Access Management-Lösungen eingestuft. Mit den laut eigenen Angaben über 18.000 Kunden dürfte Okta nach unseren Recherchen die am weitesten verbreitete Lösung hinter dem von Microsoft dominierten Markt sein.

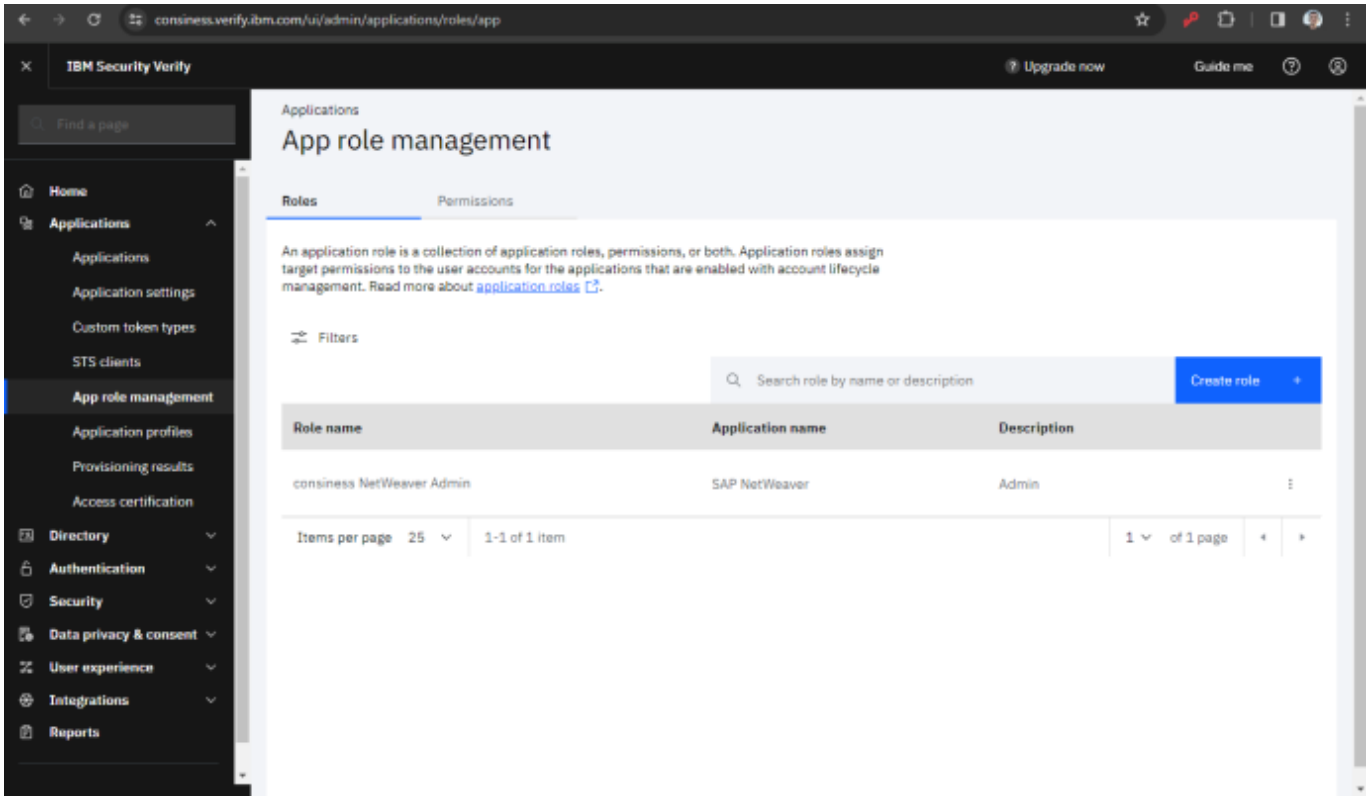
SAP-Integrations-Szenarien sollten sich auf bei dem Einsatz von Okta auf den Standard begrenzen. Auch die Verfügbarkeit von Okta-Experten im deutschsprachigen Raum fällt tendenziell geringer ist als der der Konkurrenz. Darüber hinaus ist zu beachten, dass sie Ihre Microsoft-basierte On-Premise Infrastruktur weiterhin über ein klassisches Active Directory steuern müssen.

Sollte Ihr Unternehmen dennoch gewillt sein, sich von der Monopol-artigen Marktmacht von Microsoft unabhängiger zu machen, ist Okta die richtige Wahl. Der Vorteil liegt vor allem darin, dass es sich um eine vergleichsweise gut anpassbare, leicht zu implementierende und auf die Branche spezialisierte Lösung handelt, mit der sich nahezu ihre gesamte Infrastruktur einbinden lässt.

Option D: IBM Security Verify

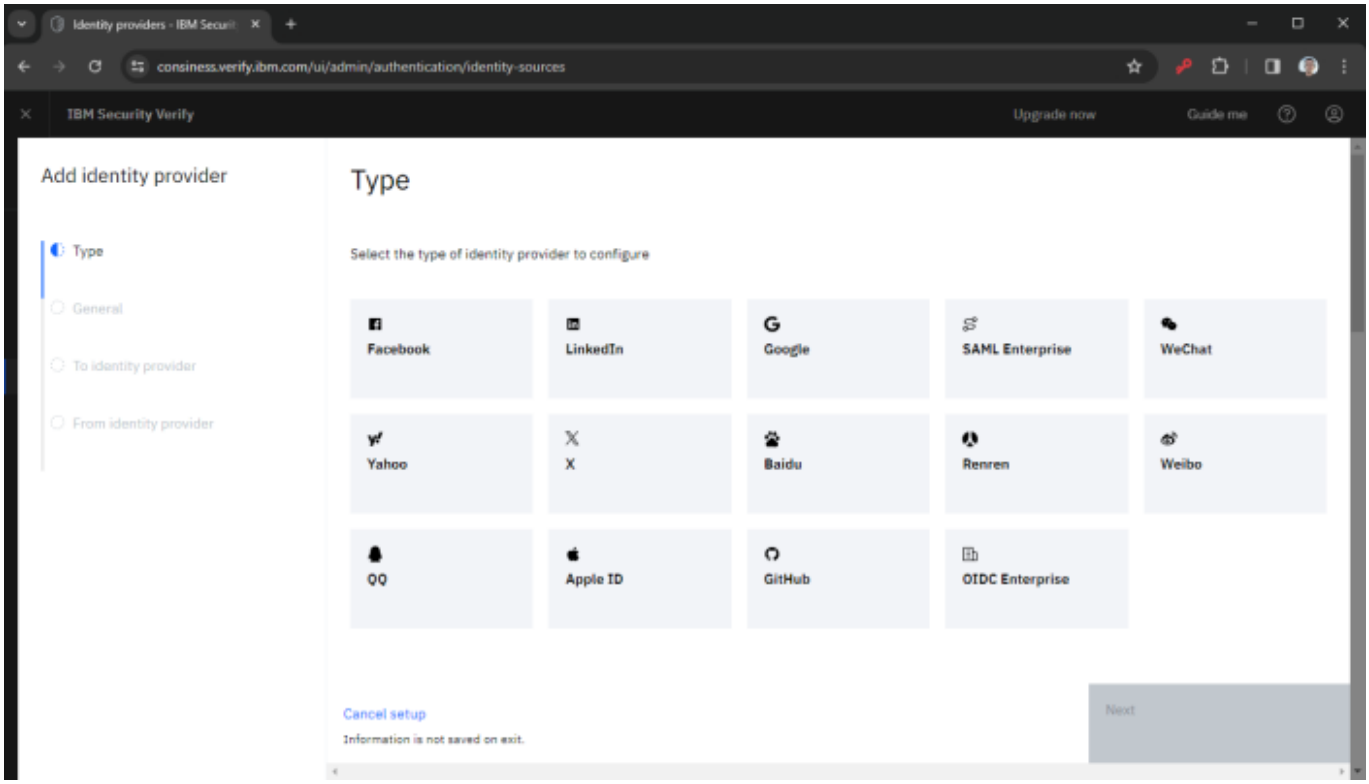
Als vierte Option reiht sich die Lösung des Software-Giganten IBM nahtlos in die Welt der Cloud-basierten IAM-Lösungen ein. Da wir mit diesem Produkt weniger Berührungspunkte haben, fällt dieser Absatz etwas kürzer aus.

IBM Security Verify ist das Ergebnis einer kontinuierlichen Weiterentwicklung und Verbesserung der Sicherheitslösungen von IBM. Vor der Einführung von IBM Security Verify war das Produkt als IBM Cloud Identity bekannt. Vielen Branchen-Kennern ist noch der IBM Tivoli Identity Manager bekannt, welcher unserer Einschätzung nach historisch gesehen dem SAP IDM technisch überlegen war.



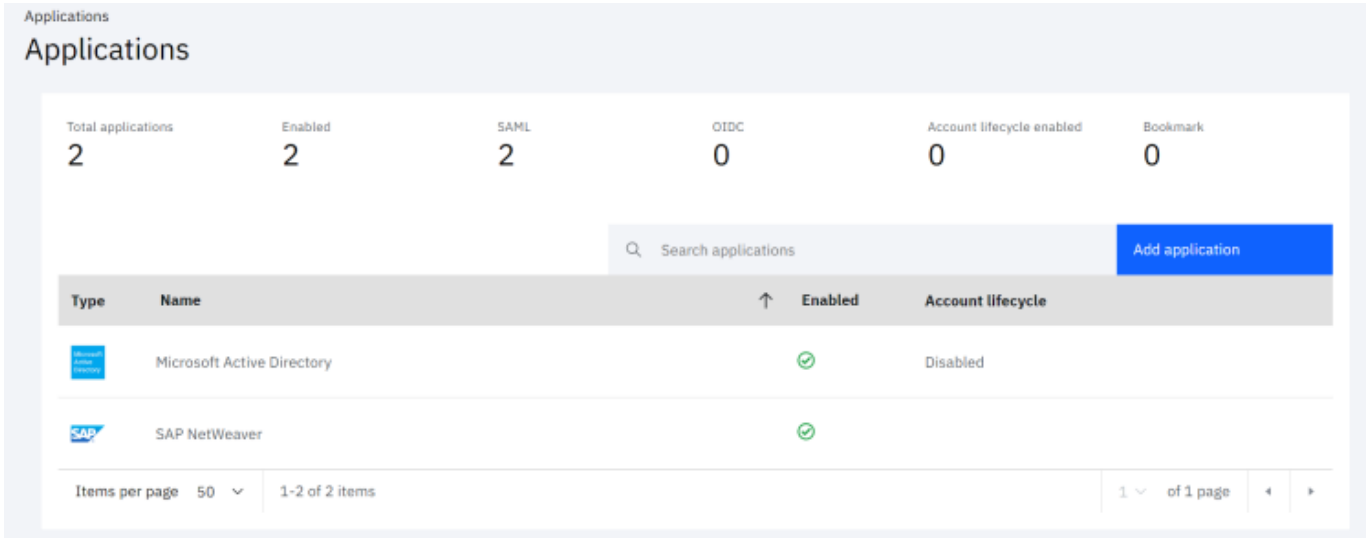
Sieht so aus, wie man sich eine IAM-Lösung vorstellt: IBM Security Verify

In der Cloud-Ära werden jedoch die Karten neu gemischt und IBM präsentiert eine Lösung, welche schon auf den ersten Blick äußerst intuitiv und vertraut wirkt. Zu den Features gehören unter Anderem ein ein SAML- und OIDC-basiertes Single Sign-On, ein sogenannter „digitaler Arbeitsplatz“, welcher (ähnlich wie ein Citrix Launcher) den Zugriff auf alle berechtigten Applikationen erleichtert, eine adaptive Zugriffskontrolle mit künstlicher Intelligenz und branchenübliche Identity Governance-Funktionen.



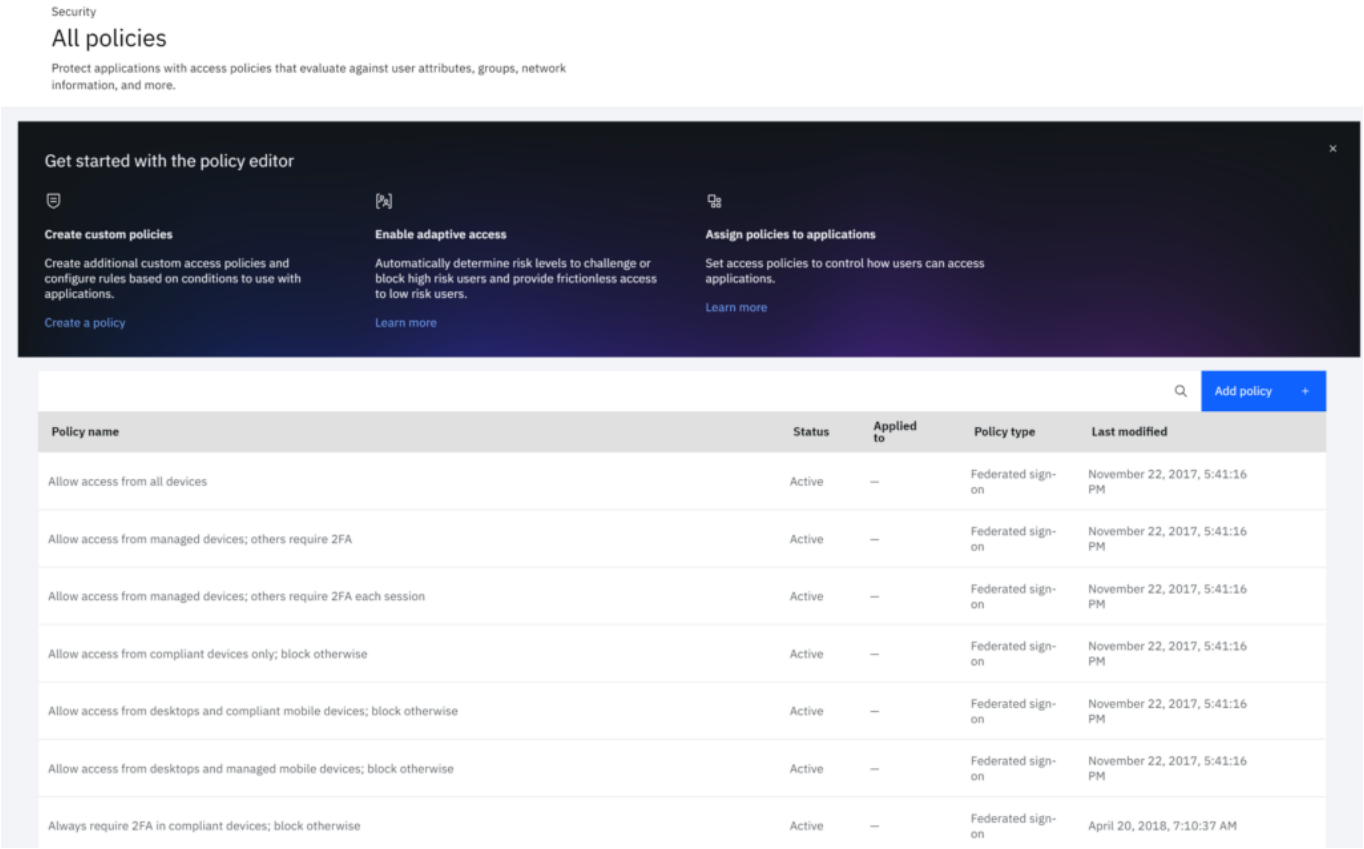
Out-of-the-box Identity Provider: Fokus auf B2C

Ein Blick in die Identity Provider zeigt, dass mit IBM Security Verify alle gängigen B2C Authentifizierungs-Szenarien abgedeckt werden können. Ein LinkedIn-basierter Login für ihre Applikation ist hier mit einem Wizard in wenigen Klicks umgesetzt. Auf der Gegenseite konnten wir, als SAP-zentrische „Tester“ der Lösung, nur ein vorgefertigtes Integrationspaket für den klassischen SAP NetWeaver vorfinden.



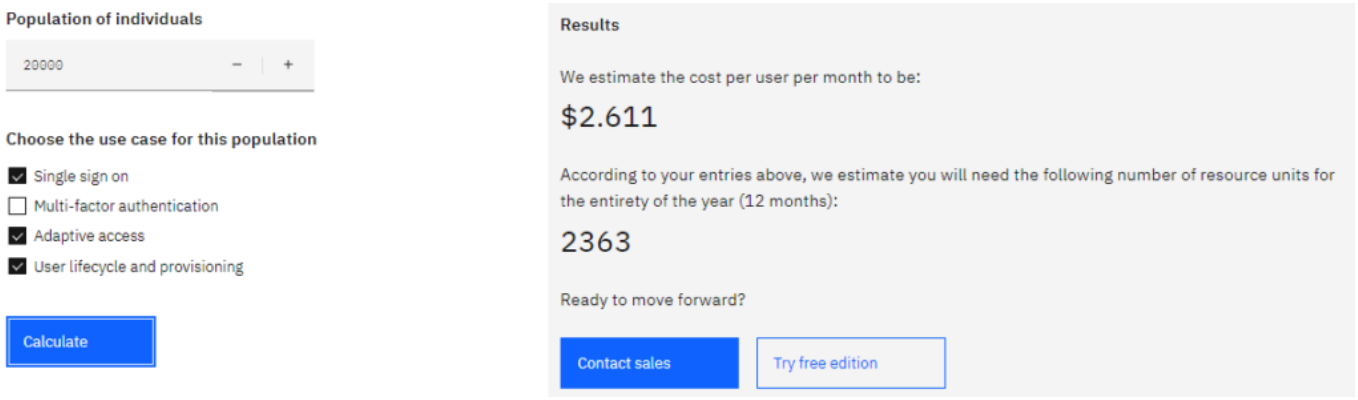
Begrenzte Auswahl von SAP-typischen Applikationen/Konnektoren

Sehr gelungen und gut aufgeräumt bewerten wir den Policy Editor. An dieser Stelle können für Gruppen von Applikationen einfach und übersichtlich Sicherheitseinstellungen vorgenommen und auditiert werden.



Policy Editor – Schlank und übersichtlich

Die Preisgestaltung kann auf der Webseite von IBM Security Verify eingesehen und exemplarisch berechnet werden. Wie in anderen Cloud-Lösungen auch, hängt die Preisgestaltung primär davon ab, welche Features und wieviele Identitäten letztendlich verwaltet werden sollen.



IBM Pricing Calculator

Einschätzung

Grundsätzlich haben wir nach einer ersten Demonstration den Eindruck, dass es sich um eine weitere, sehr gut strukturierte DaaS-Lösung mit üblichen IAM-Features handelt. Ob die Erweiterbarkeit der Lösung ähnlich flexibel ist, wie z.B. bei IBM Tivoli der Fall war, können wir an dieser Stelle nicht einschätzen. Aufgrund der relativ hohen Bekanntheit der Vorgängerlösungen im deutschsprachigen Raum, soll ein Hinweis auf IBM Security Verify jedoch nicht fehlen.

Zusammenfassung

Cloud-Computing ist in aller Munde und die Konkurrenz am Markt wächst stetig. Selbst Schwergewichte im On-Premise Markt wie Quest (mehr zu One Identity in Teil 4) positionieren sich mittlerweile mit eigenen Cloud-Ablegern ihrer erfolgreichen Produkte. Dementsprechend ist eine abschließende Betrachtung aller Optionen nahezu unmöglich und die Entscheidung für ein Produkt nicht selten davon abhängig, wie erfolgreich das Produkt im Markt positioniert bzw. beworben wird.

Für SAP-Kunden dürfte unserer Einschätzung nach die Zusammenarbeit von Microsoft und SAP das Geschäft dominieren. Als Ergebnis erhalten Kunden eine Infrastruktur aus Produkten, die sie auch bei dem Einsatz einer Drittlösung ohnehin im Einsatz hätten. Dies verschlankt die Architektur und verschafft somit strategische Vorteile. Ob diese Lösung allerdings mit demselben Fokus und derselben Qualität angeboten wird, wie es ein Spezialist wie Omada kann, bleibt abzuwarten. Der mangelnde Support von SAP IDM innerhalb der letzten Jahre könnte nicht wenigen Kunden noch als negativer Nachgeschmack in Erinnerung bleiben und sie dazu bringen, sich anderweitig am Markt umzusehen.

Weiter zum Teil 4: On-Premise Lösungen: z.B. One Identity

Über den Autor

Hendrik Winkler ist Partner der consiness und Lead Architekt für Identity und Access Management Lösungen. Er kann auf umfangreiche Expertise in SAP ABAP, GRC, Cloud-Technologien und SAP Identity Management zurückgreifen. Mit über zehn Jahren in der IT-Branche hat er sich auf die Entwicklung und Implementierung von komplexen IAM-Systemen spezialisiert, wobei er stets ein Auge auf Sicherheit, Benutzerfreundlichkeit und Compliance hat.

Der Artikel ist auch bei Linkedin erschienen:

https://www.linkedin.com/pulse/das-ende-einer-%2525C3%2525A4ra-teil-34-cloud-services-hendrik-winkler-yojve/?trackingId=glRrkQNpQ4GFMJ7ENa53qQ%3D%3D