one identity

Category: Online-Marketing
geschrieben von Tobias Hager | 29. Januar 2026



One Identity: Sicherheit und Kontrolle neu definiert

Du glaubst, Identitätsmanagement ist nur was für paranoide Admins mit zu viel Freizeit? Dann willkommen in der Realität von 2025, in der ein einziger kompromittierter Account dein ganzes Unternehmen lahmlegen kann. One Identity ist nicht einfach nur ein weiteres Tool im Security-Regal – es ist der Gamechanger, der Zugriff, Berechtigungen und Risiken in einer smarten, zentralisierten Plattform orchestriert. Und ja, es ist Zeit, dass du aufwachst.

- Was One Identity ist – und warum herkömmliches IAM (Identity and Access Management) nicht mehr reicht
- Warum Identitäts- und Zugriffsmanagement der neue Dreh- und Angelpunkt der IT-Security ist

- Wie One Identity Sicherheit, Kontrolle und Compliance in einem Framework vereint
- Die technischen Komponenten: Identity Governance, Privileged Access Management, Provisioning & mehr
- Warum herkömmliche Active Directory-Setups ein Sicherheitsrisiko sind
- Wie du mit One Identity komplexe Berechtigungsstrukturen automatisierst und auditierbar machst
- Die Integration in hybride und Multi-Cloud-Umgebungen – ohne Chaos
- API-first: Warum One Identity für DevOps, SecOps und ITSM ein Geschenk ist
- Eine Schritt-für-Schritt-Anleitung zum Einstieg in One Identity
- Fazit: Warum ein fehlendes IAM-Konzept heute nicht mehr naiv, sondern gefährlich ist

One Identity: Was steckt wirklich hinter dem Begriff?

One Identity ist keine fancy Marketingphrase, sondern eine vollwertige Identity-Security-Plattform, die das Chaos aus Benutzerkonten, Zugriffskontrollen, Rollenmodellen und Audit-Protokollen herauszieht – und in ein zentrales, automatisiertes Framework gießt. Die Plattform besteht aus mehreren Komponenten, die nahtlos ineinandergreifen, um Identitäten zu verwalten, Berechtigungen zu kontrollieren und Sicherheitslücken zu schließen, bevor sie jemand anderes findet.

Im Kern geht es um Identity Governance and Administration (IGA), Privileged Access Management (PAM), Access Management (AM) und User Lifecycle Management. Diese Funktionen sind nicht neu – aber One Identity liefert sie in einer konsolidierten, API-fähigen Plattform, die sich sowohl in Legacy-Systeme als auch in moderne Cloud-Stacks integrieren lässt. Und das bedeutet: Kontrolle. Sichtbarkeit. Skalierbarkeit.

Vergiss das Flickwerk aus AD, LDAP, Azure AD, OpenLDAP, SAP-Berechtigungen und lokalen Admin-Konten. One Identity bringt Ordnung ins Chaos – und zwar auf Enterprise-Niveau. Die Plattform ist skalierbar, mandantenfähig, auditierbar und bereit für regulatorische Anforderungen wie DSGVO, ISO 27001, NIS2 oder SOX. Wer heute noch glaubt, ein Excel-Sheet reiche zur Rollenzuweisung, sollte sich auf eine unangenehme Überraschung vorbereiten.

Die zentrale Idee: Jede Identität bekommt genau die Berechtigungen, die sie braucht – nicht mehr, nicht weniger. Und das bitte automatisch, nachvollziehbar und widerrufbar. Willkommen in der Welt von One Identity.

Warum klassisches

Identitätsmanagement 2025 ein Sicherheitsrisiko ist

Wenn du denkst, ein Active Directory mit ein paar Gruppenrichtlinien sei ein sicheres IAM-Setup, dann hast du das Memo nicht gelesen. Klassische Ansätze wie manuelle Provisionierung, lokale Admin-Konten, statische Rollen oder fehlende Audit-Trails sind heute nicht nur ineffizient – sie sind gefährlich. Ransomware-Gruppen, Insider Threats und Supply-Chain-Angriffe nutzen genau diese Schwachstellen aus, um sich Zugang zu kritischen Systemen zu verschaffen.

Identitäten sind der neue Perimeter. Firewalls und VPNs sind nett, aber wenn ein kompromittierter Benutzer sich intern mit Admin-Rechten bewegen kann, hast du verloren. Genau hier setzt One Identity an: mit granularen Zugriffskontrollen, Just-in-Time-Berechtigungen, automatischer Rezertifizierung von Rechten und vollständiger Nachvollziehbarkeit jeder Aktion.

Ein weiterer Schwachpunkt: Schatten-IT. Benutzer registrieren sich bei SaaS-Tools, autorisieren OAuth-Zugriffe und umgehen zentrale IT-Prozesse. Ohne ein zentrales IAM-System hast du null Überblick – und genau das kostet Unternehmen Millionen. One Identity bringt diese Wildwuchs-APIs zurück unter Kontrolle – mit Identity Federation, SSO, MFA und zentralem Policy-Management.

Die Realität: In 2025 ist klassisches IAM nicht nur veraltet – es ist fahrlässig. Und das wissen auch Regulierungsbehörden. Wer kein tragfähiges IAM-Konzept hat, riskiert nicht nur Datenverluste, sondern auch Bußgelder und Reputationsschäden. Und genau deshalb ist One Identity keine Option – sondern Pflicht.

Die technische Architektur von One Identity: Module, APIs, Infrastruktur

One Identity ist modular aufgebaut – aber nicht fragmentiert. Die Plattform besteht aus mehreren Produkten, die sich nahtlos integrieren lassen, darunter:

- Identity Manager: Zentrale Plattform für IGA mit Rollenmanagement, automatisierter Provisionierung und Audit-Logging
- Safeguard: Privileged Access Management mit Session Recording, Just-in-Time Access, Passwort-Vaulting und Approval Workflows
- OneLogin: Cloud-native Access Management mit SSO, MFA, Adaptive Authentication und Integration in über 6.000 SaaS-Anwendungen

- Starling Connect: API-basiertes Provisioning für Cloud-Apps mit Connector-Framework und Echtzeit-Synchronisierung

Die technische Basis ist API-first. Das bedeutet: One Identity lässt sich nicht nur als GUI bedienen, sondern vollständig über RESTful APIs steuern. Für DevOps und SecOps bedeutet das: Endlich lassen sich Benutzer, Gruppen und Zugriffsrechte über CI/CD-Pipelines verwalten. Für ITSM-Teams: Automatisierung von Joiner-Mover-Leaver-Prozessen über ITIL-konforme Workflows.

Die Plattform unterstützt hybride Szenarien: On-Prem, Cloud, Multi-Cloud, SaaS – egal. Die Architektur ist mandantenfähig, HA-ready und skalierbar auf mehrere Millionen Identitäten. Besonders wichtig: Die Logging- und Audit-Funktionen sind manipulationssicher, revisionskonform und mit externen SIEM-Systemen integrierbar – z. B. Splunk, QRadar oder Azure Sentinel.

One Identity ist kein Tool. Es ist ein Framework. Und wer es richtig implementiert, erschafft eine Sicherheitsarchitektur, die nicht nur schützt, sondern beschleunigt.

Use Cases aus der Praxis: Automatisierung, Sicherheit, Compliance

Du willst wissen, was One Identity in der Praxis kann? Hier ein paar realistische Szenarien, die täglich in Unternehmen ablaufen – und ohne IAM zur tickenden Zeitbombe werden:

- Joiner-Prozess: Ein neuer Mitarbeiter wird eingestellt. One Identity provisioniert automatisch Benutzerkonten in AD, Azure AD, Office 365, Salesforce und SAP – basierend auf der Rolle und Abteilung.
- Rollenbasierte Zugriffskontrolle: Mitarbeiterwechsel? Kein Problem. Die Rollenlogik sorgt dafür, dass Zugriffsrechte automatisch angepasst oder entzogen werden. Kein manuelles Nachpflegen mehr. Kein Wildwuchs.
- Privileged Session Management: Ein externer Dienstleister braucht Admin-Zugriff auf ein System? Safeguard generiert einen temporären Zugriff mit Session Recording, Approval und automatischem Ablauf – keine dauerhaften Konten, kein Risiko.
- Rezertifizierung & Audit: Alle Rechte werden in regelmäßigen Intervallen automatisch überprüft. Manager bestätigen oder widerrufen Zugriffe. Das System erstellt revisionssichere Reports – fertig für ISO-Audits.

Und das Beste: Diese Prozesse sind nicht nur sicherer, sondern auch schneller. Keine Tickets mehr, keine manuellen Freigaben, kein Excel-Chaos. Stattdessen: Automatisierung, Transparenz, Kontrolle.

Schritt-für-Schritt: So startest du mit One Identity

Der Einstieg in One Identity ist kein Quick-Win – aber absolut machbar. Hier ein bewährter Fahrplan für den Start:

1. Ist-Analyse & Zieldefinition: Welche Systeme existieren? Welche Identitäten? Welche Risiken? Ziel: ein vollständiger Überblick über Benutzer, Rollen, Systeme, Risiken.
2. Use Case definieren: Starte mit einem klaren Anwendungsfall – z. B. Provisionierung und Rezertifizierung von AD-Usern. Klein starten, groß skalieren.
3. Systemintegration: Verbinde AD, Azure AD, HR-Systeme, SaaS-Apps. Nutze die vorhandenen Konnektoren von One Identity oder baue eigene via API.
4. Rollenmodell entwickeln: Definiere Rollen, Berechtigungen, Policies. Starte mit wenigen Rollen und erweitere iterativ.
5. Workflows konfigurieren: Automatisiere Joiner-Mover-Leaver-Prozesse, Genehmigungsworkflows, Rezertifizierungen.
6. Audit & Logging aktivieren: Stelle sicher, dass alle Aktionen protokolliert werden. Binde dein SIEM an.
7. Pilot testen & skalieren: Teste mit einer Abteilung. Sammle Feedback. Dann ausrollen.

One Identity ist kein Plug-and-Play – aber es ist ein Sicherheits-Booster, der sich bezahlt macht. Und zwar schnell.

Fazit: IAM ist kein Luxus, sondern Überlebensstrategie

Willkommen in der Ära, in der Identitäten das neue Einfallstor für Angriffe sind – und in der du dir keine Fehlkonfiguration mehr leisten kannst. One Identity definiert Sicherheit und Kontrolle neu: nicht als Barriere, sondern als Enabler für Geschwindigkeit, Compliance und Skalierbarkeit. Wer 2025 noch ohne strukturiertes IAM unterwegs ist, fliegt nicht nur unter dem Radar – er fliegt raus.

Die gute Nachricht? Du kannst heute damit anfangen, dein Identitätsmanagement auf ein neues Level zu heben. Mit One Identity. Mit Automatisierung. Mit Transparenz. Und mit einem Mindset, das endlich versteht: Kontrolle ist kein Feind der Agilität – sie ist ihre Voraussetzung.