# SailPoint

## Identity Security für dynamische IT-Umgebungen

Moderne IT-Landschaften sind zunehmend komplex und dynamisch. Unternehmen müssen nicht nur interne Mitarbeiter verwalten, sondern eine Vielzahl von weiteren Identitäten - von externen Partnern über Service Accounts bis zu KI-Agenten – über Cloud- und On-Premise-Systeme hinweg steuern. Die Herausforderung besteht darin, sicherzustellen, dass nur die richtigen Personen zur richtigen Zeit Zugriff auf die richtigen Ressourcen haben. Manuelle Prozesse und isolierte Lösungen können mit dieser Dynamik nicht Schritt halten und führen zu Sicherheitsrisiken, übermäßigen Berechtigungen und Compliance-Verstößen.

### SailPoint Identity Security Cloud – KI-gestützte Plattform auf Atlas

Die SailPoint Identity Security Cloud ist eine skalierbare, KI-gesteuerte SaaS-Lösung, die auf der SailPoint Atlas-Plattform aufbaut. Sie wurde entwickelt, um Identitäten, Zugriffe und Berechtigungen in Echtzeit zu verwalten und zu schützen. Die Lösung automatisiert Zugriffsentscheidungen durch künstliche Intelligenz, bietet Echtzeit-Transparenz zur Risikominderung und ermöglicht kontinuierliche interne Compliance. Durch Automatisierung und maschinelles Lernen stellt ISC sicher, dass Zugriffsprozesse beschleunigt werden, während gleichzeitig die Sicherheit gestärkt wird.

## Vier Kernlösungsbereiche der Identity Security Cloud

Die Identity Security Cloud umfasst vier zentrale Lösungsbereiche, die als integrierte Suite zur Verfügung stehen:

### Lifecycle Management

Automatisierung der gesamten Identitätslebenszyklen Joiner, Mover und Leaver. Durch Automatisierung werden manuelle Aufgaben reduziert, Provisioning und Deprovisioning beschleunigt und Access Creep minimiert. Dies ermöglicht schnelleres Onboarding, nahtlose interne Wechsel und sicheres Offboarding unter Wahrung der Compliance.

### Access Modeling

KI-gestützte Definition, Visualisierung und Verfeinerung von Zugriffsrechten. Durch maschinelles Lernen liefert Access Modeling automatisierte Vorschläge zur Rollenerstellung, reduziert Überberechtigungen und optimiert die Zugriffshygiene. Dies verringert Audit-Aufwand und erhöht die operative Effizienz.

### Compliance Management

Automatische Durchsetzung von Zugriffsrichtlinien, Optimierung von Zertifizierungen und Prüfung des Benutzerzugriffs über die gesamte Identitätslandschaft hinweg. Auditoren erhalten vollständige Transparenz darüber, wer Zugriff auf was hat und warum. Dies reduziert Audit-Belastung, vermeidet kostspielige Verstöße und gewährleistet kontinuierliche Compliance mit weniger manuellem Aufwand.

### Identity Analytics

Bereitstellung handlungsrelevanter Identitätsinformationen durch Analyse von Benutzerverhalten, Zugriffstrends und Richtlinienverstößen. Klare Einblicke in Zugriffsrisiken, Anomalie-Erkennung und datengestützte Entscheidungen verbessern die Sicherheitslage. Intelligente Dashboards und Reporting ermöglichen proaktives Bedrohungsmanagement und effektivere Sicherheitsstrategien.

## IdentityAI® – Maschinelles Lernen für smarte Zugriffsentscheidungen

Die Plattform wird durch IdentityAI® angetrieben – SailPoints proprietäre KI-Engine, die vertrauenswürdige Datenintelligenz nutzt, um Identity Governance zu optimieren. IdentityAI® bietet konkrete Funktionen:

- Access Modeling: Empfiehlt optimale Rollen durch Analyse von Zugriffsmustern über die gesamte Organisation hinweg.
- Access Recommendations: Nutzt Peer-Group-Vergleiche, um Genehmigungen zu leiten und Entscheidungsmüdigkeit zu reduzieren.
- Identity Outliers: Erkennt abnormales Zugriffsverhalten durch maschinelles Lernen und hebt es zur Überprüfung hervor. Der Outlier Risk Score liefert einen konsistenten Rahmen zur Behebung von Zugriffs-Anomalien in Echtzeit.
- Role Insights & Mining: Beschleunigt die Rollenerstellung und -verfeinerung durch intelligentes Clustering.
- Certification & Request Suggestions: Optimiert Governance, indem empfohlene Aktionen während Reviews angezeigt werden.
- SailPoint Harbor Pilot: Ein KI-Agent, der hilft, Identitätsdaten abzufragen, Workflows zu erstellen und Erkenntnisse in natürlicher Sprache zu gewinnen.

Diese KI-gestützten Funktionen ermöglichen es Unternehmen, Least-Privilege-Zugriff durchzusetzen, Risiken zu reduzieren und Identity Governance mit Zuversicht zu automatisieren.

## Technische Merkmale & Sicherheitsmodelle

## Architektur & Bereitstellung:

- Cloud-Native SaaS: Keine Backend-Infrastruktur erforderlich, automatische Updates, hohe Skalierbarkeit
- Atlas-Plattform: Einheitliche, intelligente Basis, die neue Identity-Security-Herausforderungen bewältigt, ohne Neuarchitektur erforderlich zu sein
- Extensibility Framework: Ermöglicht tiefe Konfiguration über gesamte Sicherheitssysteme hinweg zur Durchsetzung von Least-Privilege-Zugriff

## Integration & Konnektivität:

- Umfassender Connector-Katalog: SailPoints extensiver Connector- und Integrationskatalog ermöglicht Identity Security für Hunderte von Anwendungen – von Cloud-Diensten (AWS, Microsoft 365, Salesforce) über On-Premise-Systeme (SAP, Active Directory) bis zu Legacy-Applikationen
- Zero Trust Support: Die Plattform unterstützt die Implementierung von Zero Trust Security Models durch durchgehende Least-Privilege-Durchsetzung

## Erweiterbare Module (Advanced Capabilities):

- Machine Identity Security (für Service Accounts, Bots, RPAs)
- Non-Employee Risk Management
- Data Access Security (für unstrukturierte Daten)
- Cloud Infrastructure Entitlement Management
- Access Risk Management
- Password Management
- Agent Identity Security
- Observability & Insights