AIRLOCK®
SECURE ACCESS HUB

FACTSHEET

Zugriff für alle Benutzer. Reibungslos.

Airlock IAM

www.airlock.com

Im Airlock Secure Access Hub wird Airlock IAM meist in Kombination mit Airlock Gateway, einer Komponente zum Schutz von Web-Applikationen und APIs (WAAP), eingesetzt. Die Aufgabe von Airlock IAM ist es, Benutzer zu verwalten, zu authentifizieren und die entsprechenden Identitätsinformationen in der passenden Form an die gewünschte Applikation zu übermitteln.

Customer IAM (cIAM)

Airlock IAM verwaltet Benutzer, die von aussen auf Applikationen, APIs und Microservices zugreifen wollen und ist entsprechend für grosse Benutzerzahlen skalierbar. Zudem bietet die cIAM-Lösung eine nahtlose User Experience durch optimierte und integrierte Benutzerschnittstellen für Onboarding und Self-Services. Der Umgang mit Social Identities (BYOI) und eine hohe Flexibilität beim Authentisierungsvorgang sind entscheidende Pluspunkte von Airlock IAM.

Starke Authentifizierung mit starker Auswahl

Damit ein Login nicht an den Schwächen eines einzigen Authentisierungsmittels leidet, wird meist eine starke Authentifizierung mit einem zweiten Faktor (auch 2FA oder MFA genannt) eingesetzt. Airlock bietet eine eigene vollständige integrierte und besonders benutzerfreundliche starke Authentifizierung mit Airlock 2FA an. Damit können auch passwortlose Zugriffe einfach und sicher eingerichtet werden.

Airlock IAM unterstützt etliche weitere Authentisierungsmittel und kann diese flexibel kombinieren. So zum Beispiel: FIDO2/WebAuthn, mTAN (SMS), E-Mail OTP, OATH, Matrixkarten, Client-Zertifikate, OneSpan Cronto und Digipass OTP. Neben reinen Authentisierungsfunktionen stehen jeweils auch Verwaltungsfunktionen sowie Self-Services für Endbenutzer zur Verfügung.

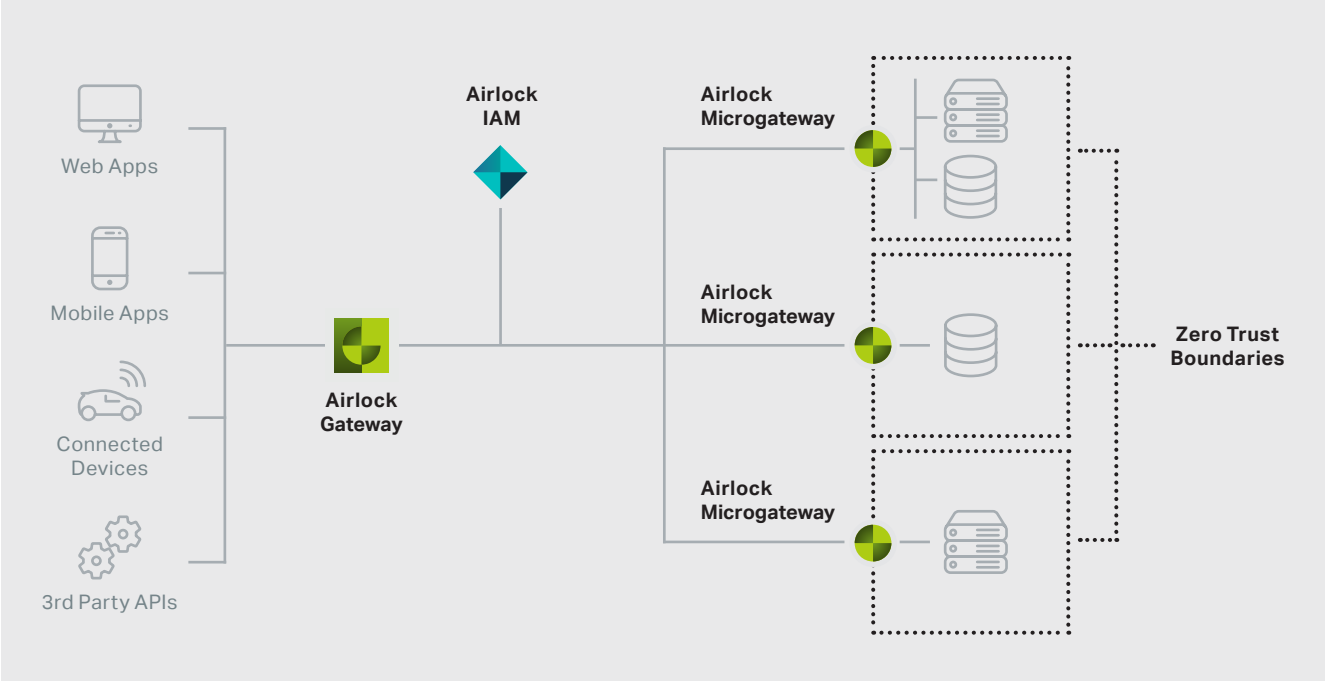
Adaptive Authentifizierung

Airlock IAM kann den Benutzerzugriff auf unterschiedliche Weise dynamisch steuern und bietet für alle Bedürfnisse die optimale Abstimmung zwischen Sicherheit und Benutzerfreundlichkeit. Insbesondere kann die aktuelle Zugriffssituation z. B. vom Arbeitsplatz, von zuhause oder unterwegs, und die Historie eines Benutzers dabei berücksichtigt werden. Es werden u.a. folgende Konzepte unterstützt:

- **Continuous Adaptive Trust (CAT) zur kontinuierlichen Vertrauensanalyse in Kombination mit Airlock Gateway**
- **RBAC/ABAC (Role-/Attribute-based access control)**
- **Risikobasierte Authentifizierung**
- **Re-Authentifizierung und Timeout-Funktionen auf einzelnen Rollen**
- **Umsetzung komplexer Zugriffsrichtlinien mittels Regeln und logischen Operatoren**

Single Sign-On (SSO)

Der Secure Access Hub entkoppelt die Authentifizierung von den Applikationen und kann so als smarte Identitätsweiche fungieren. Je nachdem wo ein Zugriff hingeleitet wird, kann die Identität des authentifizierten Benutzers anders repräsentiert werden. Dadurch wird ein transparenter Single Sign-on möglich, der hohe Sicherheit mit hoher Benutzerakzeptanz verbindet.



Airlock IAM unterstützt diverse SSO- und Federation-Standards wie OpenID Connect, OAuth 2, SAML 2.0, Kerberos und ist in der Lage, Authentisierungsinformationen auch in einfachen HTTP-Headers, Cookies oder als Teil der URL an Zielapplikationen zu propagieren. Für die Anbindung an Legacy-Systeme können mit wenig Aufwand eigene Plug-ins geschrieben werden.

Social Registration und BYOI

Benutzer wollen sich schnell und unkompliziert registrieren und einloggen. Dabei möchten sie bestehende Identitäten wiederverwenden, um nicht noch mehr Passwörter einrichten zu müssen. Wenn Benutzer ihre Identitäten für den Zugriff von aussen mitbringen, spricht man von BYOI (Bring Your Own Identity). Die Alternative zum Passwort-Wirrwarr sind Standards wie OAuth 2.0 und OpenID Connect 1.0. Diese erlauben die Wiederverwendung von Benutzeridentitäten und geben dem Benutzer die Kontrolle über deren Verwendung. Falls man sich dennoch nicht gänzlich auf einen externen Identitätsanbieter wie z. B. Facebook verlassen möchte, kann Airlock IAM diese Identitäten mit einem zweiten Faktor ergänzen, damit eine starke Authentifizierung ermöglicht wird.

Umfassende User-Self-Services

Die Einrichtung von Benutzerkonten und Anmeldeprozessen führen bei Anwendern zu vielen Fragen. Eine zielgerichtete Benutzerführung mit optimierter User Experience ist daher von höchster Bedeutung, um zu verhindern, dass der Helpdesk mit Anfragen überschwemmt wird. Airlock IAM bietet eine Vielzahl von optimierten und integrierten Workflows für Anmeldung, Onboarding und weitere Self-Services. Dazu gehören Kiosk- und Portalfunktionen für die Verwaltung eigener Daten, selbständige Registrierung sowie die Verwaltung von entsprechenden Konten und Authentisierungsmitteln.

Deployment

- **Docker Image**
- **Self-Contained Application für Linux**

Funktionen

- **Benutzerauthentifizierung**
  - Passwort
  - Passwortlos
  - Airlock 2FA (Push, QR Code, OTP, HW Token)
  - FIDO / WebAuthn / Passkeys
  - OATH OTP, MTAN (SMS), E-Mail OTP
  - OneSpan Cronto und Digipass OTP
  - X.509 Client-Zertifikate
  - Adaptiv und risikobasiert
  - Workflow-basiert
  - «Remember Me» Funktion
  - RADIUS Server
- **Request-Authentifizierung**
  - Authentifizierung von REST Calls
  - JWT, OAuth, Basic Auth, Client-Zertifikate, Kerberos, SSO Tickets
- **Benutzerverzeichnisse: Datenbanken, LDAP, MSAD**
- **Benutzer-, Token- und Rollenverwaltung inkl. Helpdesk-Tool**
- **User-Self-Services**
  - Password-Reset
  - Registrierung und Verwaltung von Authentisierungsmitteln (insb. 2. Faktoren)
  - Verwaltung von Sessions und angemeldeten Browsern/Devices
  - Kiosk- und Portalfunktion für eigene Benutzerdaten
  - Diverse weitere Self-Services
- **Weitere**
  - Single Sign-on (SSO): OIDC, OAuth, SAML, Cookies, HTTP-Headers, SSO Tickets, JWT
  - REST APIs für alle Komponenten (Loginapp, Adminapp, Transaction Approval)
  - Identitätsanbieter für OIDC, OAuth, SAML
  - Service Provider für OIDC, OAuth, SAML
  - Social Login und Social Registration
  - Mandantenfähig
  - Hoch skalierbar
  - Sicherheit auf Bankenniveau
  - Individuell erweiterbar
- **Adminapp**
  - Benutzeradministration
  - Verwaltung und Zuweisung von Authentifizierungstoken
  - Verwaltung von Administratoren und technischen Clients
  - Konfigurationsverwaltung und -Editor
  - Erstellen von Authentisierungs- oder Self-Service-Flows ohne Programmieren
  - Flexible Workflowmechanismen mit grosser Bibliothek eingebauter Steps (no code)
  - Erweiterung durch selbstentwickelte Steps (low code)
  - Schrittweises Ändern und Ausprobieren in Echtzeit
  - Visualisierung komplexer Abläufe als Flow-Diagramm
  - Log-Viewer
  - Wartungsmeldungen