AIRLOCK API

Schützt Schnittstellen. Massgeschneidert.

Application Programming Interfaces (APIs) sind die Pfeiler moderner Applikationen und digitaler Services. Diese Schnittstellen exponieren sensitive Daten über die Unternehmensgrenze hinaus in das Internet, wo Kunden und Partner darauf zugreifen können. APIs benötigen deshalb besonderen Schutz und müssen nicht nur gegen altbekannte Web-Angriffe (OWASP Top 10) sondern auch gegen API-spezifische Attacken geschützt werden. Eine einfache und sichere Zugriffskontrolle ist dabei ein essentieller Baustein und bildet zusammen mit entsprechendem Monitoring und Reporting das Fundament für die Umsetzung digitaler Strategien.

Web Security für APIs

Moderne Web-Applikationen und Services basieren auf APIs, die in verschiedene Clients integriert werden. Clients können mobile Apps, wiederum APIs, moderne Single-Page Applications (SPAs) oder auch Legacy-Webapplikationen sein. Aufgrund dieser Vielfalt von Anwendungsfällen darf API Security nicht losgelöst von klassischer Applikationssicherheit betrachtet werden. Deshalb basiert der Airlock API Security Gateway auf Airlock WAF und bringt ein solides Filter-Arsenal für Web Security mit.

Advanced API Protection

Airlock API bietet diverse Schutzmechanismen an, die für APIs massgeschneidert sind. JSON-Schema und OpenAPI-Spezifikationen für APIs können auf dem Gateway integriert und durchgesetzt werden. Nur API-Calls, die der Spezifikation entsprechen, werden an die internen APIs weitergeleitet. Innovative Funktionen wie Dynamic Value Endorsement (DyVE) erlauben zudem ein dynamisches Whitelisting von erlaubten Werten innerhalb einer API-Interaktion.

API Access Control

Die Zugriffskontrolle auf APIs ist einer der wichtigsten Gründe für den Einsatz von API Gateways. Airlock API validiert Access Tokens und erlaubt rollenbasierte Zugriffsautorisierung für API-Endpoints. Im Zusammenspiel mit Airlock IAM unterstützt Airlock API Standards wie OAuth 2.0, OpenID Connect 1.0 und SAML 2.0, um Zugriffe auf APIs zu schützen.

High Performance

Airlock API ist ein Reverse-Proxy mit Failover- und Load Balancing-Funktionen. Damit können angebundene Services auf einfache Weise hochverfügbar gemacht werden. Weiters wird TLS vorgängig terminiert, was die APIs entlastet und eine einfache Skalierung ermöglicht.

Ergon Informatik AG | Merkurstrasse 43 | CH-8032 Zürich |Telefon: +41 44 268 89 00 | E-Mail: info@airlock.com

API Monitoring, Statistiken und Reporting

Das eingebaute dynamische Reporting bietet jederzeit Überblick über sämtliche API-Zugriffe. Access Logs zu API Calls können an weiterverarbeitende Systeme geleitet werden und als Basis für die Monetarisierung von Zugriffen verwendet werden. Interaktive Dashboards liefern eine Übersicht der Angriffsversuche und Spezifikationsverletzungen, zeigen Performance-Probleme auf und machen Back-End-Fehler sichtbar.

DevSecOps

Airlock API lässt sich dank eines umfangreichen REST APIs einfach in DevOps Pipelines integrieren. Die Auswirkungen von Service Events in einer Microservice-Architektur lassen sich auf dem API Gateway automatisch nachführen. Beispielsweise kann bei einem Service Update automatisch die neue Open API-Spezifikation auf dem API Gateway bereitgestellt werden.

Deployment

Virtual Appliance, Hardware Appliance, Airlock Cloud Image. IAM Komponente auf Docker oder als Self-Contained Application.

Funktionen:

- **Advanced API Protection**
  - Angriffsfilterung in JSON-Objekten
  - OpenAPI Enforcement
  - JSON Schema Validierung
  - Dynamic Value Endorsement (DyVE)
- **API Zugriffskontrolle**
  - OAuth 2.0
  - OpenID Connect 1.0
  - SAML 2.0
  - API Keys
- **PSD2 Compliance**
  - NextGenPSD2, STET
  - Dynamic Client Registration
- **API Monitoring**
  - Zugriffsstatistiken
  - Reporting
- **High Performance**
  - TLS Terminierung
  - Hohe Verfügbarkeit
  - Load Balancing
- **DOS Schutz**

Ergon Informatik AG | Merkurstrasse 43 | CH-8032 Zürich |Telefon: +41 44 268 89 00 | E-Mail: info@airlock.com