AIRLOCK®
SECURE ACCESS HUB

API

AIRLOCK API

Protects interfaces. Tailor-made.

Application Programming Interfaces (APIs) are the pillars of modern applications and digital services. These interfaces expose sensitive data beyond the company's boundaries to the Internet, from where customers and partners can access it. APIs therefore require special protection and must not only be protected against well-known web attacks (OWASP Top 10) but also against API-specific attacks. Simple and secure access control is an essential component and, together with appropriate monitoring and reporting, forms the foundation for the implementation of digital strategies.

Web security for APIs

Modern applications and services are based on APIs that are integrated into different clients. Clients can be mobile apps, APIs, modern Single-Page Applications (SPAs) or legacy web applications. Due to this variety of application cases, API Security must not be viewed in isolation from classical application security. Therefore, the Airlock API Security Gateway is based on Airlock WAF and comes with a solid filter arsenal for web security.

Advanced API protection

Airlock API offers a range of protective mechanisms that are tailor-made for APIs. JSON Schema and OpenAPI specifications for APIs can be uploaded and enforced via the gateway. Only API calls that meet these specifications will be forwarded to the internal APIs. Innovative functions such as dynamic value endorsement (DyVE) also enable dynamic whitelisting of permitted variables within an API interaction.

API access control

One of the main reasons for using API gateways is to ensure access control to APIs. Airlock API validates access tokens and permits role-based access authorisation for API end points. Airlock API works in conjunction with Airlock IAM to support OAuth 2.0, OpenID Connect 1.0 and SAML 2.0 in protecting access to APIs.

High availability

Airlock API is a reverse proxy with failover and load-balancing functions, efficiently ensuring high availability of connected services. When modifications are made to the application infrastructure (e.g. starting/stoping of additional instances), Airlock API automatically takes over and enables high scalability. TLS is also terminated in advance, relieving the burden on APIs and enabling simple scaling.

Ergon Informatik AG | Merkurstrasse 43 | CH-8032 Zurich | Phone: +41 44 268 89 00 | E-mail: info@airlock.com

API monitoring, statistics and reporting

Built-in dynamic reporting provides an overview of all API access attempts at all times. Access logs for API calls can be forwarded to peripheral systems and, therefore, be used as a basis for monetisation of accesses. Interactive dashboards ensure an overview of both attempted attacks and specification violations, highlighting performance problems and displaying back-end faults.

DevSecOps

Thanks to its comprehensive REST API, Airlock API is easy to integrate into DevOps pipelines. The outcomes of service events in a microservice architecture environment can be tracked automatically via the API gateway. For example, a service update can automatically deploy the new OpenAPI specification to the API gateway.

Deployment

Virtual appliance, hardware appliance, Airlock cloud image.
IAM component on Docker or as self-contained application.

Features:

- **Advanced API protection**
  - Attack filtering in JSON objects
  - OpenAPI enforcement
  - JSON schema validation
  - Dynamic Value Endorsement (DyVE)
- **API access control**
  - OAuth 2.0
  - OpenID Connect 1.0
  - SAML 2.0
  - API Keys
- **PSD2 compliance**
  - NextGenPSD2, STET
  - Dynamic client registration
- **API monitoring**
  - Access statistics
  - Reporting
- **High performance**
  - TLS termination
  - High availability
  - Loadbalancing
- **DOS protection**

Ergon Informatik AG | Merkurstrasse 43 | CH-8032 Zurich | Phone: +41 44 268 89 00 | E-mail: info@airlock.com