AIRLOCK®
SECURE ACCESS HUB

FACTSHEET

Protects Web Applications and APIs.

Airlock Gateway

www.airlock.com

Airlock Gateway protects business-critical, web-based applications and APIs from attacks and unwanted visitors. Providing a central security service, it examines every HTTP(S) request for attacks and blocks any attempt to steal and manipulate data. Combined with Airlock Microgateway and Airlock IAM, this creates a unique architecture for greater web application security.

Protect applications and APIs with a comprehensive solution

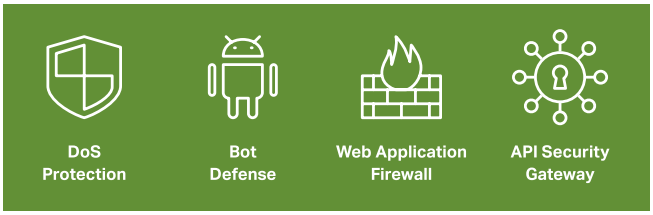
Web applications, mobile apps, and the associated APIs are the keystones of digitization. Protecting these applications requires a holistic approach that combines the functions of a modern web application firewall (WAF) with an API security gateway. This concept is also called web application and API protection (WAAP).

Combining negative and positive security models

Negative filters (block lists) detect known forms of attacks, such as injections or cross-site scripting (XSS). Unlike signatures, smart detection patterns block not only individual vulnerabilities but entire families of attacks. Prior normalization helps prevent circumvention of the filters with other forms of code. Thanks to the threat intelligence feed, Airlock Gateway recognizes potential hazard sources such as botnets or suspicious access via the TOR network at all times.

A positive security model achieves an even higher level of security. It blocks everything that has not explicitly been allowed. However, manually created allow lists require extensive application knowledge and are time-consuming to maintain. In contrast, the anomaly shield automatically responds to deviations from normal behavior and needs almost no maintenance at all. Using machine learning, it even detects bots or content crawlers that masquerade as normal users.

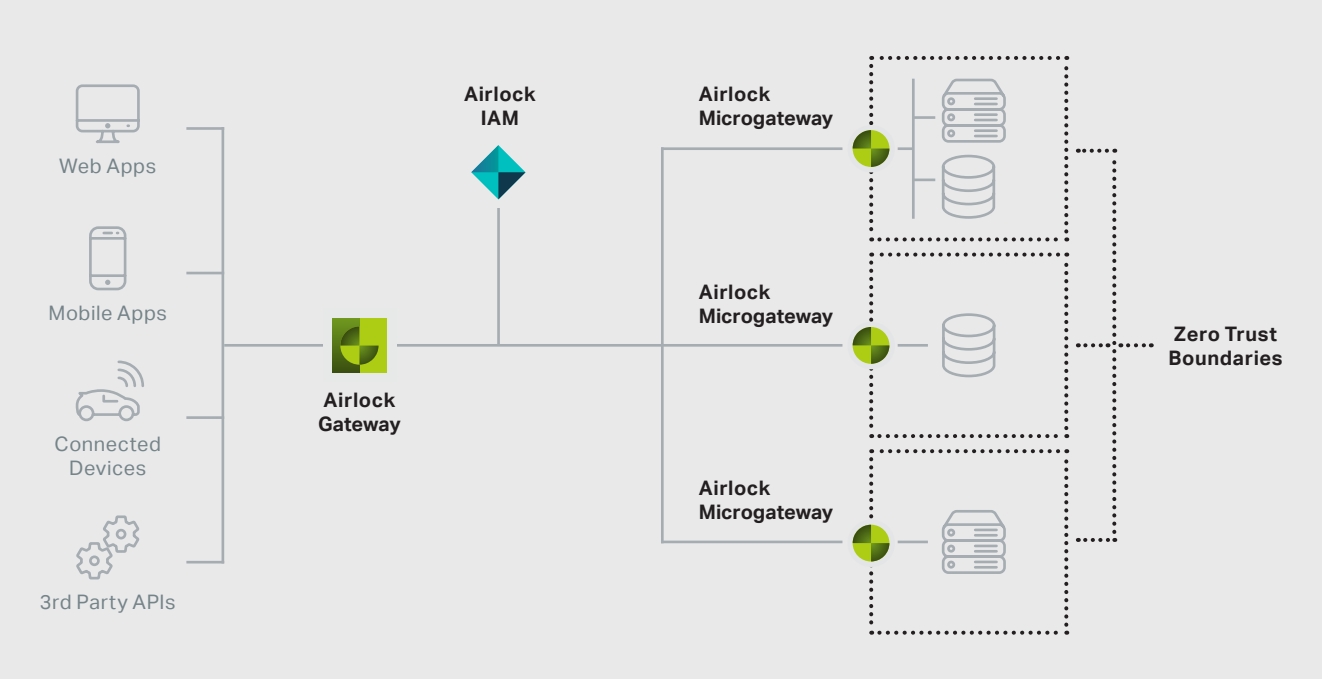
Many developers today pursue an "API first" strategy and define the API interfaces before writing a line of code. A JSON or OpenAPI scheme facilitates documentation and also defines what is allowed. Airlock Gateway can enforce adherence to this scheme and block everything that deviates from it.



Identity-centric access control and single sign-on

The most common vulnerability in web applications and APIs is found in ineffective access control. As a result, an attacker can steal, modify, and even delete sensitive data.

Combined with Airlock IAM, Airlock Gateway ensures that every user identity is authenticated and its access is authorized. Airlock IAM determines permissions based on various information, e.g. user roles, sensitivity and context of access or context of access or authentication strength and forwards them to Airlock Gateway. Identity federation standards such as OAuth 2.0, OpenID Connect 1.0, and SAML 2.0 are supported in this process. API keys can also be used with APIs. A user only needs to log in once to access all connected applications. Thanks to identity propagation, single sign-on also works with proprietary legacy systems that do not support the latest standards or which cannot be changed.



docker kubernetes aws Google Cloud Azure OPENSHIFT

Central security interface

Airlock Gateway offers plenty of interfaces to further systems such as SIEM solutions, virus scanners, fraud prevention systems or HSMs. The integrated threat intelligence feed allows Airlock Gateway to respond immediately to current threat situations from the internet and protects against botnets and other dangers that were only discovered in the last 24 hours. A high-availability ICAP interface enables the easy integration of additional components.

Highly available and cloud independent

Airlock Gateway is a reverse proxy with failover and load balancing functions. This easily enables connected services to become highly available. The highly performant Airlock Gateway can conveniently be upgraded to a cluster with multiple active nodes when needed, such as for seasonal peaks in load. Integrated load balancing ensures the required high availability for applications and services, thereby saving on an additional architecture component.

Airlock Gateway is available as a virtual appliance or cloud image, offering extreme flexibility in all deployment scenarios. To protect container applications and microservices, we recommend Airlock Microgateway – the cloud-native equivalent with the proven security core of Airlock Gateway.

Deployment

- **Virtual appliance**
- **Cloud image for Azure, AWS, and Google Cloud**

Functions

- **Containing known and unknown attacks**
  - Holistic WAF with positive and negative filters
  - Smart block lists for detecting known attack patterns
  - Protocol validation and normalization (against filter circumvention)
  - Session-based anomaly detection
  - Dynamic whitelisting
  - Enforcement of interface specifications
  - Virtual patching
  - Upstream authentication
- **API protection**
  - Attack filters in JSON objects
  - OpenAPI enforcement
  - JSON scheme validation
  - API keys
  - Dynamic client registration
  - Throttling
- **Denial-of-service and bot protection**
  - Protection against DoS attacks on Layer 7
  - Detection of automated attacks, bots, and content crawlers
- **Threat intelligence**
  - Webroot feed integration
  - GEO filters
- **HTTP(S) reverse proxy**
  - TLS termination
  - OCSP and OCSP stapling
  - Let's Encrypt support
  - HSM integration
  - Service virtualization
  - Content rewriting
- **Additional protection features**
  - Cookie protection
  - CSFR tokens
  - URL encryption
  - Form protection
  - Dynamic value endorsement (DyVE)
  - ICAP interface
  - IBM Trusteer Pinpoint integration
  - Templates to protect Microsoft applications
- **Access control***
  - Single sign-on (SSO)
  - Enforcement point for access rules
  - Secure session management
  - Evaluation of JSON Web Tokens (JWT)
  - Connection of JWKS servers
- **High availability**
  - Failover cluster (active-passive, active-active)
  - Load balancing and health checks
- **Logging and reporting**
  - Structured logs (JSON)
  - Lucene query syntax
  - Access statistics
  - Predefined dashboards (e.g. security, performance, and troubleshooting)
  - Customer-specific visualization
- **SIEM integration**
  - Integration in Splunk, Logpoint, ArcSight and others
  - Common event format (CEF-certified)
- **Configuration management**
  - Automatic rule suggestions (policy learning)
  - Staging support
  - Automation via REST API
- **Cloud image (compatible with AWS, Google Cloud, and Azure)**

* in combination with Airlock IAM