AIRLOCK®
SECURE ACCESS HUB

WAF

AIRLOCK WAF

Protects applications. Securely.

Airlock WAF protects mission-critical, web-based applications with modern and dynamic filters. As a central security instance within the Airlock Secure Access Hub, it analyses every http(s) request for attacks and thus blocks any attempt at data theft and manipulation. In combination with Airlock IAM and Airlock API, a unique architecture for web application security exists.

Filtering of application-based attacks

Airlock WAF analyses traffic between users and services. Attempted attacks on applications are blocked before they can reach the in-house systems. Airlock WAF provides comprehensive protection against the OWASP Top 10 vulnerabilities and enables centralised management of security policies. Thanks to these innovative security functions, you can always stay ahead of attackers.

Policy enforcement point

Working in conjunction with Airlock IAM, Airlock WAF serves as a policy enforcement point for security guidelines, allowing only filtered, authenticated and authorised access. This combination of access management and content filtering guarantees security, with no compromises.

Security dashboards

Thanks to built-in dynamic reporting, decision makers have an overview of attempted attacks at all times. Operational problems such as performance bottlenecks or back-end problems are also displayed. Interactive drill-down from the dashboards, along with the display of the log lines causing the issue, facilitate the in-depth analysis of every attempted attack. In addition, Airlock is CEF certified, which enables integration with common SIEM solutions. For Splunk there is even an in-house Airlock Splunk App available.

Reverse proxy functionality and high availability

Airlock WAF is a reverse proxy that makes it possible to virtualise in-house services and applications for external access. The integrated load balancer also ensures the high availability of applications and services. Even complex issues such as the configuration of TLS security and certificate management can be dealt with upstream on the central proxy. Thanks to integrated Let's Encrypt support, certificate renewals can even be completely automated.

All-round flexible

Efficient and powerful configuration options allow full adaptability without customisation and future updates become easy. Thanks to a flexible licensing model, customer-specific requirements can be met.

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

AIRLOCK®
SECURE ACCESS HUB

Central hub

Airlock WAF provides a host of interfaces with peripheral systems such as SIEM systems, virus scanners, fraud-prevention systems and HSMs. Thanks to its integrated threat intelligence feed, Airlock WAF reacts immediately to real-time threat situations on the Internet, protecting systems from new and potentially harmful hazards. Additional components can be integrated via the high-availability capable ICAP interface.

DevSecOps

With its comprehensive REST API, Airlock WAF is easy to integrate into modern DevOps pipelines and can be supplied as hardware, virtual appliance or cloud image. Early integration of the security in application development cycles, including the new Docker- and Kubernetes-philosophies, allows Airlock WAF to offer flexible security. Attained configurations can, therefore, easily and efficiently be transferred between the different environments. Auto-learning-mechanisms support fast deployment of Airlock WAF.

Deployment

Virtual appliance, hardware appliance, Airlock cloud image

Features:

- **Mitigation of application attacks:**
  - Generic & specific attack signatures
  - Cookie store
  - Request validation
  - CSRF tokens
- **Access control**
  - Policy enforcement point
  - Single Sign-On (SSO)
  - Secure session management
- **Dynamic whitelisting**
  - URL Encryption
  - Form Protection
  - Dynamic Value Endorsement (DyVE)
- **Policy learning**
  - Automatic rule suggestions
- **HTTP(S) reverse-proxy**
  - TLS termination
  - OCSP & OCSP stapling
  - Let's Encrypt support
  - HSM integration
  - Service virtualisation
  - Content rewriting
- **High availability**
  - Failover cluster
  - Loadbalancing
- **Logging & reporting**
  - JSON logs & Lucene query syntax
  - Access statistics
  - Security dashboards
  - Performance dashboards
  - Troubleshooting dashboards
  - Custom visualisations
- **SIEM integration**
  - Splunk app
  - Common Event Format (CEF)
- **Threat intelligence**
  - Webroot feed integration
  - GEO filtering
- **Configuration management**
  - Staging support
  - REST API
- **Cloud image**
  - Compatible with AWS, Google Cloud, Azure
- **ICAP interface**
- **IBM Trusteer Pinpoint integration**
- **Protection of MS applications**

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