AIRLOCK®
SECURE ACCESS HUB

FACTSHEET

Schützt Webapplikationen und APIs.

Airlock Gateway

www.airlock.com

Airlock Gateway schützt unternehmenskritische, webbasierte Applikationen und APIs vor Angriffen und unerwünschten Besuchern. Als zentrale Security-Instanz untersucht es jeden HTTP(S)-Request auf Angriffe und blockt somit jeglichen Versuch von Datendiebstahl und -manipulation. Im Zusammenspiel mit Airlock Microgateway und Airlock IAM besteht somit eine einzigartige Architektur für mehr Webapplikationssicherheit.

Applikationen und APIs mit einer umfassenden Lösung schützen

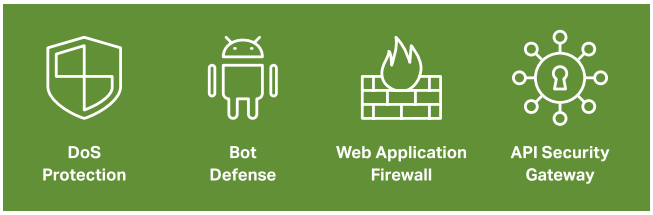
Webapplikationen, mobile Apps und die dahinter verborgenen APIs sind die Pfeiler der Digitalisierung. Der Schutz dieser Anwendungen bedingt einen ganzheitlichen Ansatz, der die Funktionen einer modernen Web Application Firewall (WAF) mit einem API Security Gateway vereint. Deswegen spricht man auch von Web Application + API Protection (WAAP).

Negative und positive Sicherheitsmodelle kombiniert

Negative Filter (Block-Listen) erkennen bekannte Angriffsarten wie Injections oder Cross-Site-Scripting (XSS). Smarte Erkennungsmuster blockieren im Gegensatz zu Signaturen nicht nur einzelne Schwachstellen, sondern ganze Familien von Angriffen. Eine vorgängige Normalisierung sorgt dafür, dass die Filter nicht mit anderen Codierungen umgangen werden können. Dank dem Threat Intelligence Feed erkennt Airlock Gateway jederzeit potenzielle Gefahrenquellen wie Botnetze oder verdächtige Zugriffe über das TOR-Netzwerk.

Noch höhere Sicherheit wird mit einem positiven Sicherheitsmodell erreicht: Dabei wird alles blockiert, was nicht explizit erlaubt wurde. Manuell erstellte Allow-Listen erfordern allerdings viel Anwendungs-Know-how und sind aufwändig zu warten. Im Vergleich dazu reagiert der Anomaly Shield automatisch und praktisch wartungsfrei auf Abweichungen vom normalen Verhalten. Mittels Machine Learning erkennt er sogar Bots oder Content Crawler, die sich eigentlich als normale Benutzer ausgeben.

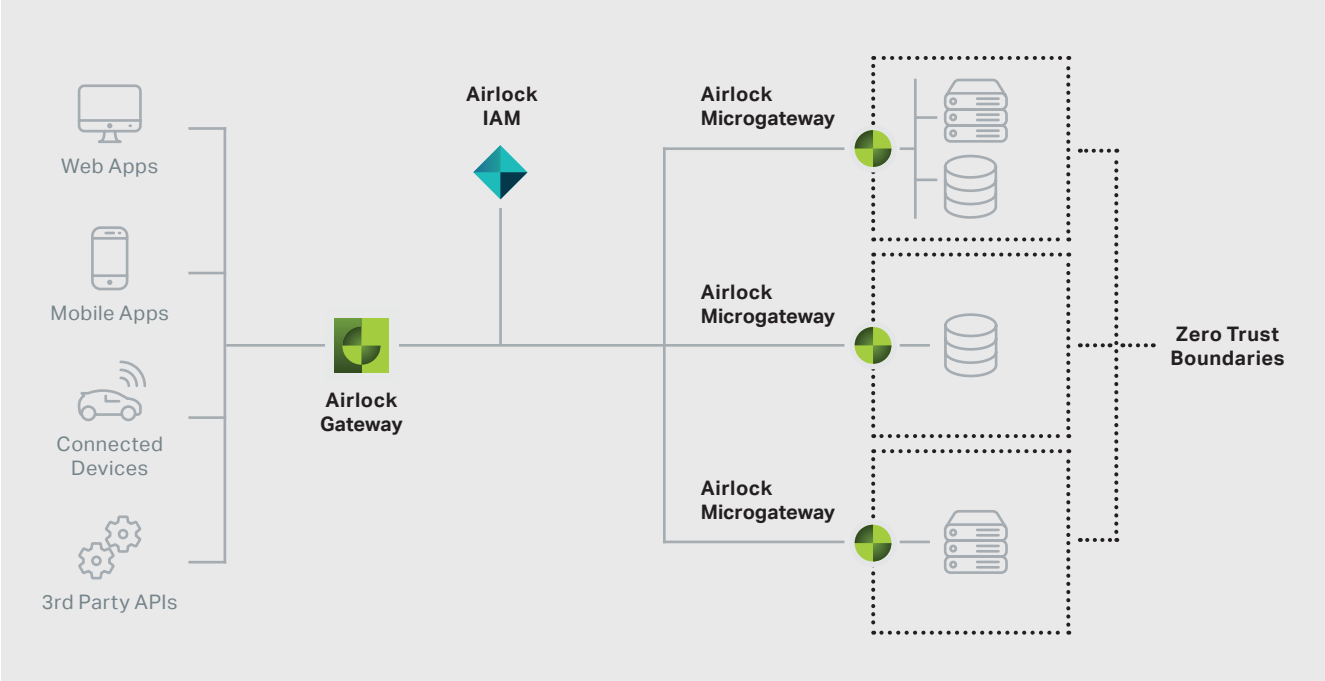
Viele Entwickler verfolgen heute einen „API first"-Strategie und legen die Schnittstellen eines APIs fest, noch bevor eine Zeile Code geschrieben wird. Ein solches JSON- oder OpenAPI-Schema dient der Dokumentation und definiert gleichzeitig, was erlaubt ist. Airlock Gateway kann für die Einhaltung dieses Schemas sorgen und alles blockieren, was davon abweicht.



Identitätszentrierte Zugriffskontrolle und Single Sign-on

Die häufigste Schwachstelle von Webapplikationen und APIs ist eine fehlerhafte Zugriffskontrolle. Ein Angreifer kann in der Folge heikle Daten stehlen, ändern oder sogar löschen.

Im Zusammenspiel mit Airlock IAM sorgt Airlock Gateway dafür, dass jede Benutzeridentität authentifiziert und ihre Zugriffe autorisiert werden. Airlock IAM bestimmt die Berechtigungen anhand diverser Informationen, z.B., Benutzerrollen, Sensitivität und Kontext des Zugriffs oder der Authentisierungsstärke und leitet diese an Airlock Gateway weiter. Dabei werden Identity Federation-Standards wie OAuth 2.0, OpenID Connect 1.0 und SAML 2.0 unterstützt. Bei APIs können auch API Keys zum Einsatz kommen. Ein Benutzer muss sich nur einmal anmelden, um auf alle angeschlossenen Anwendungen zuzugreifen. Dank Identity Propagation funktioniert der Single Sign-on auch mit proprietären Legacy-Systemen, welche nicht die neusten Standards unterstützen oder nicht verändert werden können.



Zentrale Security-Schnittstelle

Airlock Gateway bietet viele Schnittstellen zu weiterführenden Systemen wie SIEM-Lösungen, Virenscannern, Fraud-Prevention-Systemen oder HSMs. Dank dem integrierten Threat Intelligence Feed reagiert Airlock Gateway sofort auf aktuelle Bedrohungslagen aus dem Internet und schützt z. B. vor Botnetzen und anderen Gefahren, die gestern noch unbekannt waren. Über eine hochverfügbare ICAP-Schnittstelle lassen sich weitere Komponenten einfach anbinden.

Hochverfügbar und Cloud-unabhängig

Airlock Gateway ist ein Reverse-Proxy mit Failover- und Load Balancing-Funktionen. Damit können angebundene Services auf einfache Weise hochverfügbar gemacht werden. Das leistungsstarke Airlock Gateway kann im Bedarfsfall, z. B. bei saisonalen Lastspitzen, problemlos zu einem Cluster mit mehreren aktiven Knoten ausgebaut werden. Das integrierte Load Balancing gewährleistet die geforderte Hochverfügbarkeit für Applikationen und Services und kann somit eine zusätzliche Architekturkomponente einsparen.

Airlock Gateway steht als Virtual Appliance oder als Cloud Image zur Verfügung und bietet somit höchste Flexibilität in allen Einsatzszenarien. Zum Schutz von Container-Anwendungen und Microservices empfehlen wir Airlock Microgateway, das Cloud-native Pendant mit dem bewährten Sicherheitskern von Airlock Gateway.

Deployment

- **Virtual Appliance**
- **Cloud Image für Azure, AWS und Google Cloud**

Funktionen

- **Eindämmung von bekannten und unbekannten Angriffen**
  - Ganzheitliche WAF mit positiven und negativen Filtern
  - Smarte Block-Listen zur Erkennung bekannter Angriffsmuster
  - Protokollvalidierung und Normalisierung (gegen Filterumgehung)
  - Session-basierte Anomalie-Erkennung
  - Dynamisches Whitelisting
  - Durchsetzung von Schnittstellen-Spezifikationen
  - Virtual Patching
  - Vorgelagerte Authentifizierung
- **API Protection**
  - Angriffsfilterung in JSON-Objekten
  - OpenAPI Enforcement
  - JSON Schema-Validierung
  - API Keys
  - Dynamic Client Registration
  - Durchsatzbegrenzung (Throttling)
- **Denial-of-Service und Bot Protection**
  - Schutz vor DoS-Angriffen auf Layer 7
  - Erkennung automatisierter Angriffe, Bots und Content Crawler
- **Threat Intelligence**
  - Webroot Feed Integration
  - GEO-Filterung
- **HTTP(S) Reverse-Proxy**
  - TLS-Terminierung
  - OCSP & OCSP Stapling
  - Let's Encrypt Support
  - HSM Integration
  - Service Virtualisierung
  - Content Rewriting
- **Weitere Schutzfunktionen**
  - Cookie Protection
  - CSRF Tokens
  - URL Encryption
  - Form Protection
  - Dynamic Value Endorsement (DyVE)
  - ICAP-Schnittstelle
  - IBM Trusteer Pinpoint Integration
  - Vorlagen zum Schutz von Microsoft Applikationen
- **Zugriffskontrolle***
  - Single Sign-on (SSO)
  - Durchsetzungspunkt für Zugriffsrichtlinien
  - Secure Session Management
  - Auswertung von JSON Web Tokens (JWT)
  - Anbindung von JWKS Servern
- **Hochverfügbarkeit**
  - Failover Cluster (aktiv-passiv, aktiv-aktiv)
  - Load Balancing und Health Checks
- **Logging & Reporting**
  - Stukturierte Logs (JSON)
  - Lucene query syntax
  - Zugriffsstatistik
  - Vordefinierte Dashboards (z.B. Security, Performance, Troubleshooting)
  - Kundenspezifische Visualisierung
- **SIEM-Integration**
  - Integration u.a. in Splunk, Logpoint, ArcSight
  - Common Event Format (CEF-zertifiziert)
- **Konfigurationsmanagement**
  - Automatische Regelvorschläge (Policy Learning)
  - Staging Support
  - Automatisierung per REST-API
- **Cloud Image (kompatibel mit AWS, Google Cloud, Azure)**

* im Zusammenspiel mit Airlock IAM