AIRLOCK®
SECURE ACCESS HUB

FACTSHEET

Kubernetes-basierter Schutz für APIs und Microservices.

Airlock Microgateway

www.airlock.com

Airlock Microgateway hilft DevOps- und Applikationsteams, ihre Services mit wenig Aufwand vor unerlaubtem Zugriff zu schützen. Es kombiniert modernes Traffic Management über die Kubernetes Gateway API mit Web Application and API Protection (WAAP) und Identity Enforcement – für mehr Agilität in der Entwicklung und Sicherheit am richtigen Ort.

Applikationssicherheit sollte von Anfang an Teil der Entwicklungspipeline sein. Wer sich erst kurz vor der Inbetriebnahme darum kümmert, riskiert Verzögerungen und gefährliche Kompromisse. Mit Airlock Microgateway können Entwickler Sicherheitsregeln selbst definieren und durchsetzen.

Dafür braucht es eine Sicherheitskomponente, die

- leichtgewichtig und automatisierbar ist,
- vom Applikationsteam kontrolliert werden kann,
- und einfach in die Entwicklung integriert ist.

Was ist Airlock Microgateway?

Airlock Microgateway schützt APIs, Microservices und Webanwendungen direkt im Kubernetes-Cluster. Es kombiniert Traffic Management über die Gateway API mit vorgelagerter Authentisierung und Autorisierung in einer schlanken Sicherheitslösung.

Das Microgateway folgt «Secure-by-Default»-Prinzipien: Nur geprüfte Anfragen von Benutzern, Services oder Clients erreichen geschützte Services. Gleichzeitig werden eingehende Requests gezielt auf bekannte Angriffe, fehlerhafte API-Aufrufe und missbräuchliche Zugriffsmuster geprüft.

Vorteile

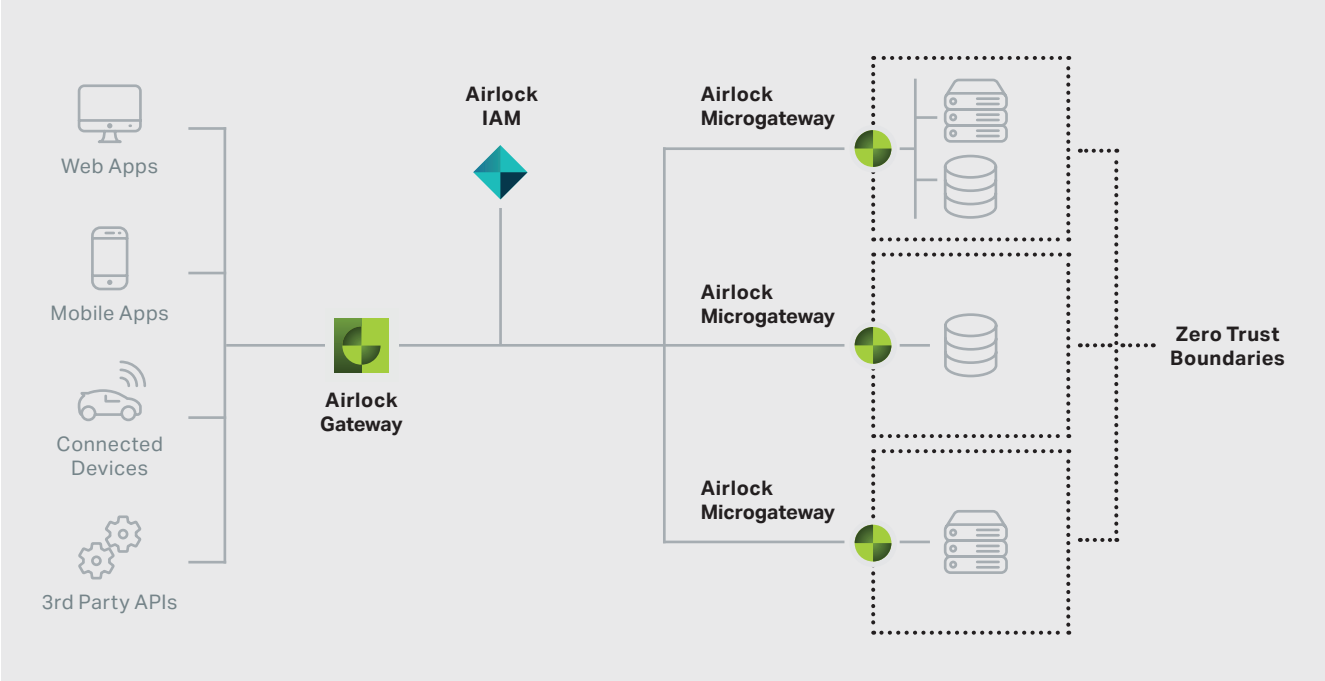
Gateway API statt Legacy Ingress
Airlock Microgateway unterstützt Unternehmen beim Wechsel von klassischen Ingress-Setups zur Kubernetes Gateway API. Damit wird Microgateway zur modernen, standardbasierten Alternative für Kubernetes-Traffic-Management.

Gateway API ist der Nachfolger von Ingress API und löst diverse Pain Points der alten Implementierung. Dank der Community Edition können alle den neuen Standard implementieren. Kostenlos und ohne Lizenz.

Starker Schutz für Anwendungen und APIs
Airlock Microgateway blockiert Angriffe, setzt API-Schemas durch und schützt Identitäten, wodurch ein zuverlässiger Schutz sowohl für Web- als auch für API-Workloads gewährleistet wird.

Identitätszentrierte Sicherheit
Nur authentifizierte und autorisierte Anfragen erreichen Ihre Dienste. Das minimiert Risiken und entlastet Ihre Anwendungen von Sicherheitsaufwand.

Nahtlose Integration
Dank nativer Kubernetes-Integration, Gateway-API und GitOps-fähigen Workflows lässt sich Microgateway einfach bereitstellen, leicht bedienen und nahtlos in containerbasierte Architekturen und Cloud-Strategien integrieren.



Microgateway kann unabhängig von Airlock Gateway und Airlock IAM betrieben werden.

kubernetes aws Google Cloud Azure OPENSHIFT

Einsatzgebiete

- **Gateway-API-basierte Alternative zu Ingress**
  Nutzen Sie Microgateway als moderne Alternative zu klassischen Ingress-Setups. Microgateway nutzt die Kubernetes-Gateway-API, um sowohl interne als auch externe Workloads zu sichern.
- **Kubernetes-native WAAP**
  Airlock Microgateway prüft eingehende Requests, setzt API-Schemas durch und blockiert bekannte Angriffsmuster. So werden interne und externe Workloads geschützt, bevor schädlicher Traffic die Applikation erreicht.
- **Zero Trust für moderne und klassische Webanwendungen**
  Authentisierung, Autorisierung und Prüfung für jede Anfrage über Webanwendungen, APIs und Legacy-Workloads hinweg durchsetzen.
- **Integration externer Identitätsanbieter**
  Mit der Token-Exchange-Funktion lassen sich Identitäten nahtlos über externe Anbieter hinweg verbinden. So bleiben Zugriffe über verschiedene Identity Provider, Security-Zonen und Services hinweg kontrollierbar.

Auf Ihre Architektur zugeschnitten

Eigenständig eingesetzt bietet Airlock Microgateway Sicherheit auf Service-Ebene, vorgelagerte Authentisierung, API-Schutz und Zero-Trust-Durchsetzung direkt über die Kubernetes Gateway API.

Je nach Anforderung kann Airlock Microgateway optional auch mit Airlock Gateway und Airlock IAM eingesetzt und zu einer mehrschichtigen Sicherheitsarchitektur kombiniert werden. So entsteht ein durchgängiger Schutzansatz für klassische und cloud-native Anwendungen. Beide Ansätze werden vollständig unterstützt und lassen sich passend zur bestehenden Architektur umsetzen.

Entwickelt für die Cloud

Airlock Microgateway ist für dynamische Cloud-Umgebungen entwickelt und unterstützt Teams beim sicheren Betrieb moderner Applikationen.

- Bereit für Kubernetes-Umgebungen wie AKS, GKE, EKS, k3s, OpenShift und Rancher.
- Helm Chart für die einfache Provisionierung
- Kubernetes Operator für den einfachen Betrieb
- Dokumentation unter docs.airlock.com/microgateway

Funktionen

- Mehrstufige Sicherheits-Filter zum Schutz vor bekannten Attacken (OWASP Top 10)
- Zugriffskontrolle mittels OIDC, JWT oder mTLS, um nur authentifizierten Benutzern den Zugriff auf geschützte Dienste zu ermöglichen.
- Reverse-Proxy-Funktionen mit Regeln für die Weiterleitung von Anfragen, TLS-Terminierung sowie Unterstützung für HTTP/1.1, HTTP/2 und HTTP/3
- Einsatz als Ingress Controller oder als In-Cluster-Gateway unter Verwendung der Kubernetes Gateway API
- API-Sicherheitsfunktionen wie JSON-Parsing, Durchsetzung der OpenAPI-Spezifikation oder GraphQL-Schema-Validierung.
- Deklarative Konfiguration über Kubernetes Custom Resource ermöglicht Automatisierung und Integration in DevSecOps-Prozesse.
- Zertifiziert für Red Hat OpenShift für den zuverlässigen Betrieb in Kubernetes-Umgebungen im Enterprise-Bereich

Bezugsformen

- Lizenzfreie und kostenlose Community Edition als Ingress für Ihre Applikationen und APIs.
- Premium Edition mit Sicherheits-Funktionen und Support für Enterprise-Szenarien.

Kubernetes-nativer Schutz von APIs und Microservices

—

Jetzt in unserem virtuellen Labor testen

airlock.com/labs/micro-gateway/