AIRLOCK®
SECURE ACCESS HUB

FACTSHEET

Kubernetes-nativer Schutz von APIs und Microservices.

Airlock Microgateway

www.airlock.com

Das Airlock Microgateway hilft DevOps-Engineers und Applikationsteams, ihre Services mit wenig Aufwand vor unerlaubtem oder bösartigem Zugriff zu schützen. Dies erhöht die Agilität und sorgt von Anfang an für hohe Sicherheit am richtigen Ort.

Applikationssicherheit sollte von der ersten Sekunde an Teil der Entwicklungspipeline sein. Wer sich erst kurz vor der Inbetriebnahme darum kümmert, riskiert zeitliche Verzögerungen und gefährliche Kompromisse. Die Entwickler kennen ihre Services am besten, entsprechend können sie die Sicherheitsregeln nicht nur selbst definieren, sondern auch durchsetzen.

Dafür braucht es eine Sicherheitskomponente, die

- leichtgewichtig und automatisierbar ist,
- vom Applikations-Team selbst kontrolliert wird
- und einfach in die Entwicklung integrierbar ist.

Vorteile

Agilität durch klare Zuständigkeiten
Die servicespezifischen Sicherheitsregeln werden durch die Entwickler definiert und vom Microgateway durchgesetzt. Die Koordination mit dem Netzwerkadministrator entfällt weitgehend.

Skalierung und hohe Verfügbarkeit
Dank der schlanken Architektur skaliert das Microgateway in jeder Kubernetes-Umgebung. Die Konfiguration per Kubernetes Custom Resource erlaubt die Automatisierung und Integration in Dev(Sec)Ops-Prozesse.

Massgeschneiderter und kontinuierlicher Schutz
Die Service-Spezifikation im OpenAPI-Format deklariert die erlaubten Aufrufe und dient sowohl als Dokumentation als auch als Sicherheits-"Allow List".

Was ist das Airlock Microgateway?

Das Airlock Microgateway ist ein leichtgewichtiges Security Gateway, das speziell für den Einsatz in Kubernetes-Umgebungen konzipiert wurde. Es wird unmittelbar vor der Applikation positioniert, so kommt niemand daran vorbei.

Das Microgateway basiert auf den bewährten Sicherheitsprinzipien der Airlock Gateway Appliance. Nur authentisierte und autorisierte Benutzer erhalten Zugriff auf Applikationen und Services. Gleichzeitig werden eingehende Requests gezielt gegen bekannte Angriffe gefiltert. So vereint das Microgateway effektiven Schutz mit einer hohen Skalierbarkeit.

Funktionen

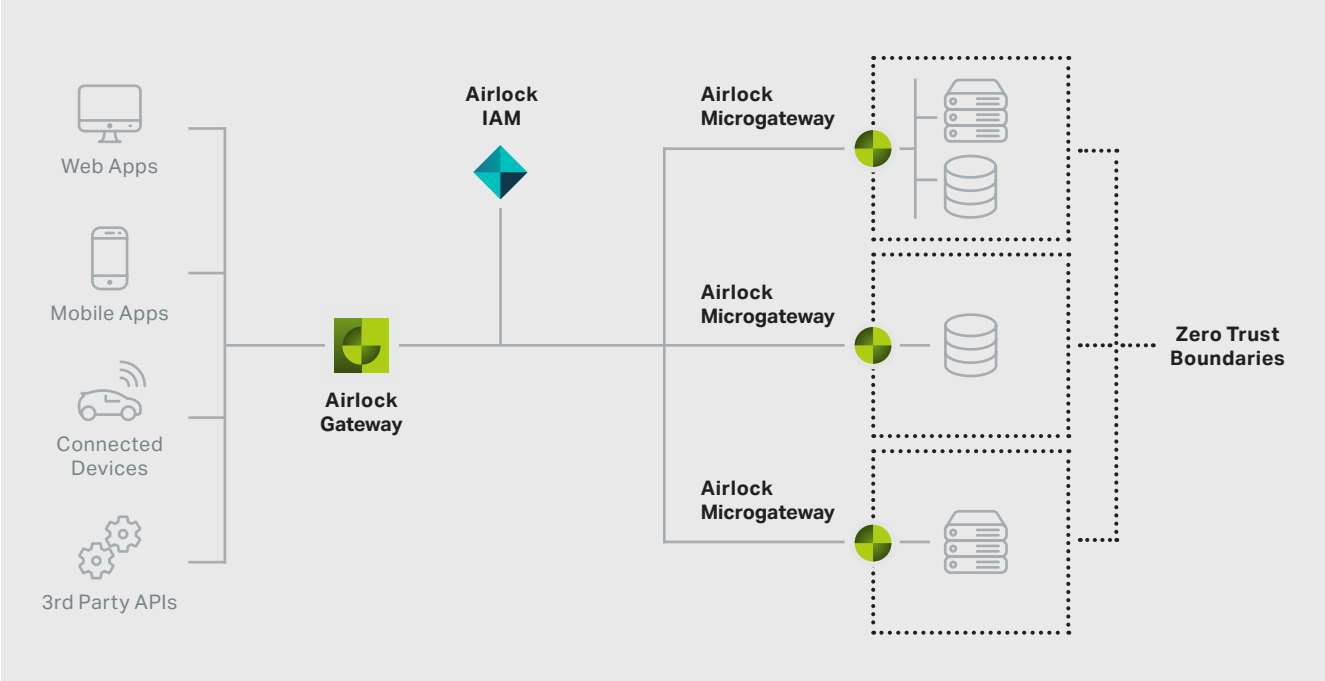
- Mehrstufige Sicherheits-Filter zum Schutz vor bekannten Attacken (OWASP Top 10)
- OpenAPI Schema Protection für eine engmaschige Service-Absicherung: Nur was explizit deklariert ist, wird akzeptiert.
- Zugriffsverwaltung im Zusammenspiel mit Airlock IAM oder anderem Identity Provider mit OIDC-Protokoll.
- Authentifizierungs-Check (u.a. JWT-Token Validierung)
- Textbasierte Konfiguration per Kubernetes Custom Resource zur einfachen Automatisierung
- Load Balancing: Verteilung der Last auf mehrere Service-Instanzen

Kubernetes-nativer Schutz von APIs und Microservices

—

Jetzt in unserem virtuellen Labor testen

airlock.com/labs/micro-gateway/



kubernetes aws Google Cloud Azure OPENSHIFT

Einsatzgebiet

- **Agiler Schutz von Microservices**
  dank einfacher Einbindung in moderne Service-Architekturen.
- **Zero Trust für Monolithen**
  Herkömmliche Applikationen profitieren von der schlanken Sicherheitsprüfung. Die Platzierung unmittelbar vor der Applikation folgt dem Zero Trust Prinzip.
- **Integrations-Gateway für Entwickler**
  Das Microgateway wird bereits während der Entwicklung und zum Testen eingesetzt. Damit werden Integrationshürden früh aus dem Weg geräumt.

Abgestimmt auf Airlock Gateway und IAM

Mit der Einführung des Microgateways wird das zentrale Airlock Gateway nicht ersetzt, sondern vielmehr ergänzt: Die applikationsspezifischen Regeln werden im Microgateway gepflegt und bei Bedarf werden generische Security-Einstellungen auf Airlock Gateway konfiguriert. Dazu gehören insbesondere Intrusion Prevention oder vorgelagerte Authentifizierung, die weiterhin möglichst weit vorne erledigt werden müssen. So profitiert jede Applikation von den zentralen Sicherheitskomponenten wie API-Gateway, Web Application Firewall und Access Management. Und jede Komponente kann sich auf ihre Stärken konzentrieren.

Konzipiert für die Cloud

- Bereit für den Einsatz in Kubernetes-Umgebungen: aks, gks, eks, k3s, OpenShift, Rancher, …
- Container Images verfügbar auf Quay.io
- Helm Charts für die einfache Provisionierung
- Kubernetes Operator für den einfachen Betrieb
- Dokumentation auf docs.airlock.com