AIRLOCK®
SECURE ACCESS HUB

FACTSHEET

Kubernetes-native protection of APIs and microservices.

Airlock Microgateway

www.airlock.com

Airlock Microgateway helps DevOps engineers and application teams protect their services from unauthorized access with minimal effort. It combines modern traffic management via the Kubernetes Gateway API with Web Application and API Protection and Identity Enforcement – enabling greater development agility and security in the right place.

Application security should be part of the development pipeline from the very first second. Taking care of it only shortly before going live risks delays and dangerous compromises. Developers know their services best, which is why they should be able not only to define security rules, but also to enforce them directly.

This calls for a security component that:

- ▶ is lightweight and automatable
- ▶ is controlled by the application team itself
- ▶ and can be easily integrated into development

What is Airlock Microgateway?

Airlock Microgateway protects APIs, microservices and web applications directly in the Kubernetes cluster. It combines traffic management via the Gateway API with upstream authentication and authorization in a lightweight component.

Microgateway follows secure-by-default principles: It enforces that only verified requests from users, services or clients can access protected applications and services. At the same time, it filters incoming requests for known attacks, invalid API calls, and abusive access patterns.

Benefits

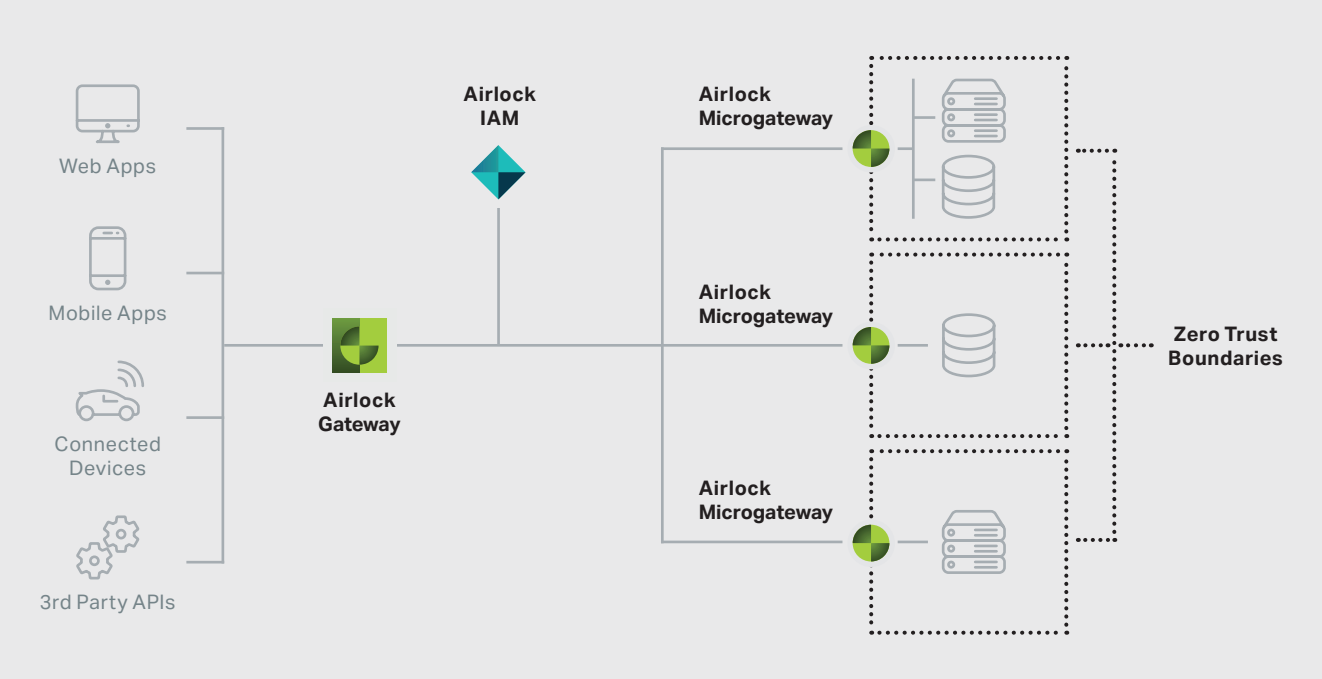
Gateway API instead of legacy ingress
Airlock Microgateway supports organizations in moving from traditional ingress setups to the Kubernetes Gateway API. This makes Microgateway a modern, standards-based alternative for Kubernetes traffic management.

Gateway API is the successor to the Ingress API and addresses several pain points of the previous implementation. With the Community Edition, teams can adopt the new standard free of charge and without a license.

Strong protection for applications and APIs
Airlock Microgateway blocks attacks, enforces API schemas and secures identities, ensuring reliable protection for both web and API workloads.

Identity-aware security
Only authenticated and authorized requests reach your services, reducing risk and relieving your applications from security overhead.

Seamless fit for your Kubernetes platform
With native Kubernetes integration, Gateway API support and GitOps-ready workflows, Microgateway is easy to deploy, simple to operate, and integrates seamlessly into container-based architectures and cloud strategies



Microgateway can run independently of Airlock Gateway and Airlock IAM.

kubernetes aws Google Cloud Azure OPENSHIFT

Use Cases

- **Gateway API-based alternative to ingress**
  Use Microgateway as a modern alternative to traditional ingress setups. Microgateway uses the Kubernetes Gateway API to secure both internal and external workloads.
- **Kubernetes-native WAAP**
  Airlock Microgateway inspects incoming requests, enforces API schemas, and blocks known attack patterns. This protects internal and external workloads before malicious traffic reaches the application.
- **Zero trust for modern and classical web apps**
  Enforce authentication, authorization and inspection for every request across web apps, APIs and legacy workloads.
- **Third-party identity integration**
  With Token Exchange, identities can be connected seamlessly across external providers. This keeps access controllable across different identity providers, security zones, and services.

Tailored to your architecture

Airlock Microgateway operates as a fully standalone Kubernetes-native WAAP. It provides service-level security, upstream authentication, API protection, and Zero-Trust enforcement directly via the Kubernetes Gateway API.

Depending on your requirements, Airlock Microgateway can also be combined with Airlock Gateway and Airlock IAM to create a multi-layered security architecture. This provides consistent protection for both classic and cloud-native applications. Both approaches are fully supported and can be implemented in line with your existing architecture.

Designed for the cloud

Airlock Microgateway is built for dynamic cloud environments and helps teams operate modern applications securely.

- Ready for use in Kubernetes environments such as AKS, GKE, EKS, k3s, OpenShift and Rancher

- Helm chart for easy provisioning
- Kubernetes Operator for simplified operation
- Documentation on docs.airlock.com/microgateway

Features

- Multi-level security filters for protecting against known attacks (OWASP Top 10)
- Access control using OIDC, JWT or mTLS to allow only authenticated users to access protected services
- Reverse proxy capabilities with request routing rules, TLS termination and HTTP/1.1, HTTP/2 and HTTP/3
- Runs as Ingress Controller or in-cluster Gateway using the Kubernetes Gateway API
- API security features like JSON parsing, OpenAPI specification enforcement or GraphQL schema validation
- Declarative configuration via Kubernetes Custom Resource enables automation and integration into DevSecOps processes.
- Certified for Red Hat OpenShift for reliable operation in enterprise Kubernetes environments.

Editions

- Free Community Edition for using Airlock Microgateway as an ingress solution for your applications and APIs.
- Premium Edition with security features and support for enterprise scenarios.

Kubernetes-native protection of APIs and microservices

—

Try it in our virtual lab

airlock.com/labs/micro-gateway/

Ergon Informatik AG | Merkurstrasse 43 | CH-8032 Zurich | Phone: +41 44 268 89 00 | Email: info@ergon.ch