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 to protect their services against unauthorized or malicious access with little effort. This increases agility and provides high security at the right place from the beginning.

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 and can therefore not only define the security rules themselves but also enforce them.

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

Benefits

Strong protection for your 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 at the edge
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 fits any cloud strategy.

What is Airlock Microgateway?

Modern application security is embedded into the development workflow and follows DevSecOps principles. Airlock Microgateway is purpose-built for this model. It is a lightweight WAAP solution, optimized for Kubernetes environments and designed to integrate seamlessly into container-native architectures.

Microgateway follows secure-by-default principles. It enforces that only authenticated and authorized users can access applications and services, and it filters all incoming requests against known attack patterns. This delivers strong, consistent protection while maintaining the scalability required in modern Kubernetes environments.

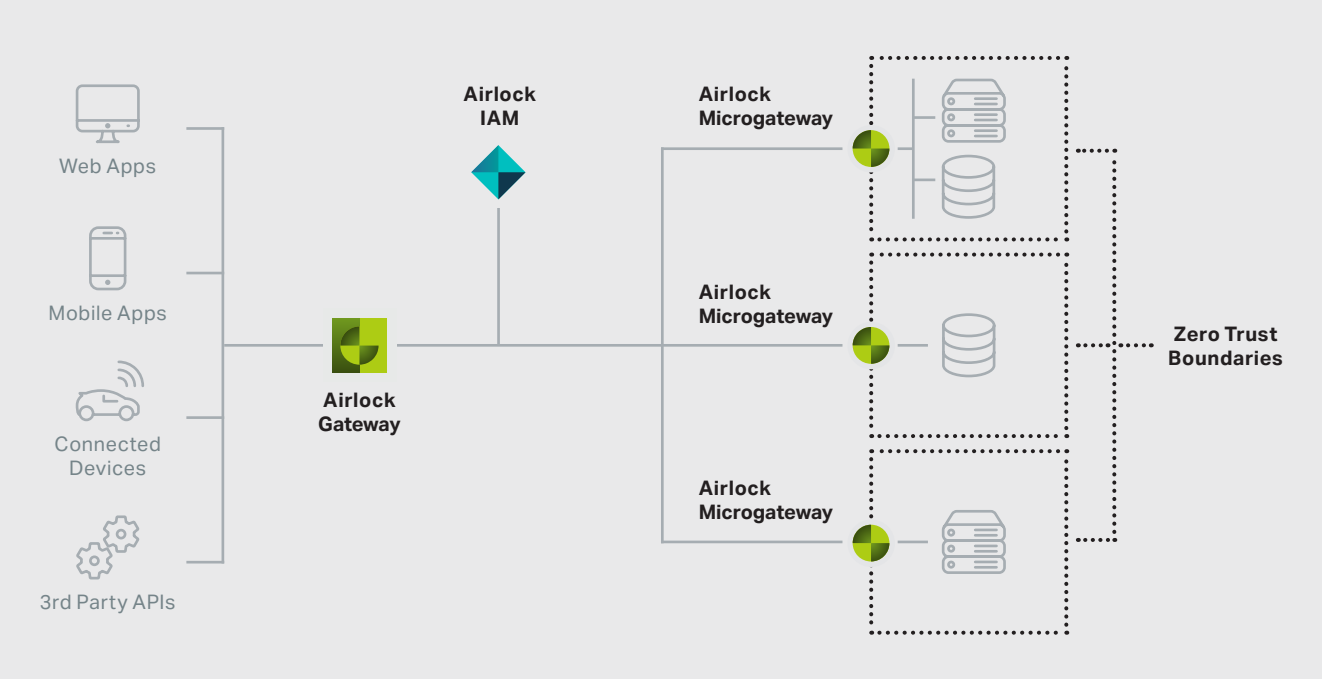
Features

- 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
- Run as Ingress Controller or in-cluster Gateway using the Kubernetes Gateway API

Kubernetes-native protection of APIs and microservices

Try it in our virtual lab

airlock.com/labs/micro-gateway/



Microgateway can also run independently of Airlock Gateway and Airlock IAM.

kubernetes aws Google Cloud Azure OPENSHIFT

- 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.

Use Cases

- **Kubernetes-native WAAP via Gateway API**
  Use Microgateway as an Ingress replacement with the Kubernetes Gateway API to secure both internal and external workloads.
- **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**
  Use the Microgateway Token Exchange feature to seamlessly bridge identities across third-party providers.

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. Customers can choose to run Microgateway on its own for a lightweight, Kubernetes-first setup or combine it with Airlock Gateway for a layered security architecture. Both approaches are fully supported, and each comes with its own benefits.

Designed for the cloud

- Ready for use in Kubernetes environments: AKS, GKE, EKS, k3s, OpenShift, Rancher, …
- Helm charts for easy provisioning
- Kubernetes Operator for simplified operation
- Documentation on docs.airlock.com/microgateway

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