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 very little effort. This increases agility and provides high security at the right place from beginning.

Application security should be part of the development pipeline from the very first second. Anyone who only takes care of it shortly before going live risks delays and dangerous compromises. The developers know their services the 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

Agility with clear responsibilities
The service-specific security rules are defined by the developers and enforced by the Microgateway. This means much of the coordination work with the network administrator is no longer necessary.

Scaling and high availability
Thanks to its lightweight architecture, the Microgateway can scale in any Kubernetes environment. Configuration via Kubernetes Custom Resource allows automation and integration into Dev(Sec)Ops processes.

Tailored and continuous protection
The service specification in OpenAPI format declares the allowed requests and serves both as documentation as well as a security allow list.

What is Airlock Microgateway?

Airlock Microgateway is a lightweight security gateway specially designed for use in Kubernetes environments. It is positioned directly in front of the application, so it can't be avoided.

The Microgateway is based on the proven security core of the Airlock Gateway Appliance. Airlock Microgateway enables you to protect your applications and microservices with the tried-and-tested Airlock security features against attacks, while also providing a high degree of scalability.

Features

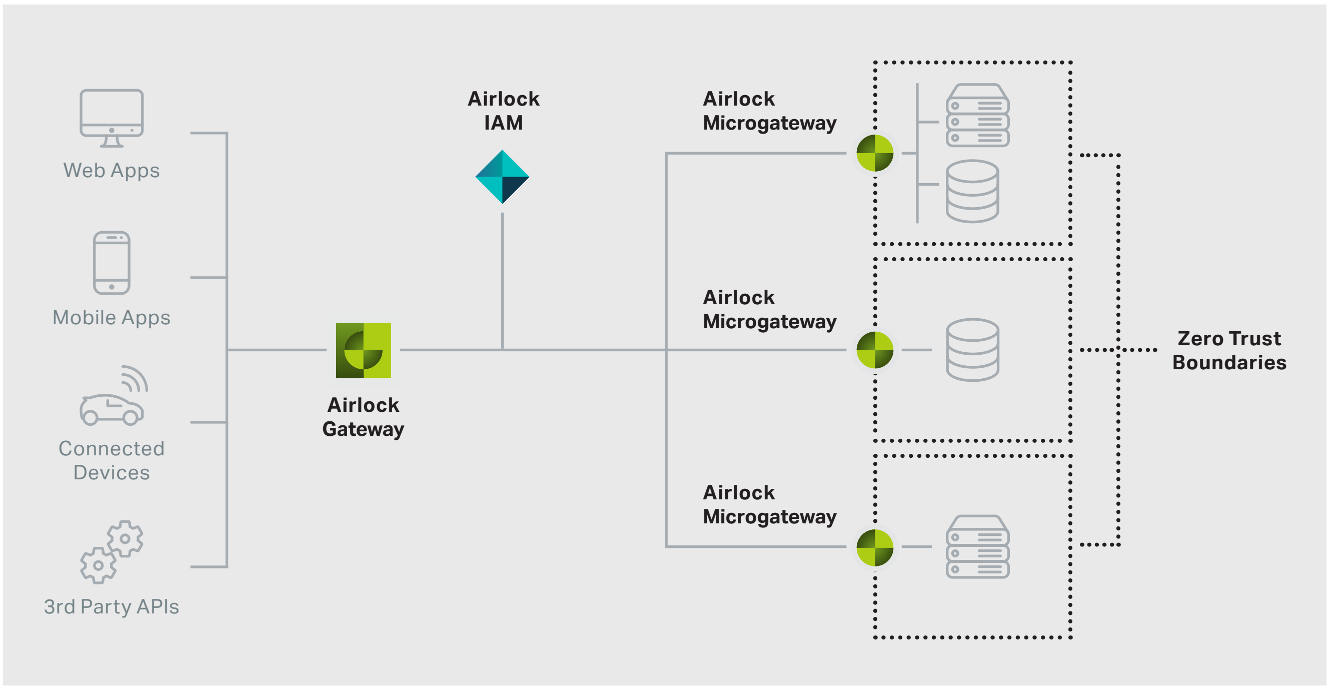
- ▶ Multi-level security filters for protecting against known attacks (OWASP Top 10)
- ▶ OpenAPI Schema Protection for close-meshed API security: Only what is explicitly declared is accepted
- ▶ Access management in combination with Airlock IAM or another identity provider using the OIDC protocol.
- ▶ Authentication check (including JWT token validation)
- ▶ Text-based configuration via Kubernetes Custom Resource for easy automation
- ▶ Load balancing: load distribution across multiple service instances

Kubernetes-native protection of APIs and microservices

—

Try it in our virtual lab

airlock.com/labs/microgateway/



kubernetes aws Google Cloud Azure OPENSHIFT

Use Cases

- **Agile protection for microservices** thanks to easy integration into modern service architectures.
- **Zero trust for monoliths** Conventional applications benefit from the streamlined security check. Positioning directly in front of the application follows the principle of zero trust.
- **Integration gateway for developers** The Microgateway is used already during development and for testing. This enables integration hurdles to be cleared at an early stage.

Tailored to Airlock Gateway and IAM

Introducing the Microgateway does not replace the central Airlock Gateway; it's an ideal complement. The application-specific rules are maintained in the Microgateway. Other generic security settings can be configured on the Airlock Gateway as needed.

In particular, this includes intrusion prevention or upstream authentication, which still need to be dealt with as far ahead as possible. This way, each application benefits from the central security components like the API gateway, web application firewall and access management. And each component can focus on its strengths.

Designed for the cloud

- Ready for use in Kubernetes environments: aks, gks, eks, k3s, OpenShift, Rancher, ...
- Container images available on Quay.io
- Helm charts for easy provisioning
- Kubernetes Operator for simplified operation
- Documentation on docs.airlock.com