

Modernizing security architecture with Airlock Microgateway

Health Info Net AG (HIN)



“In healthcare, the requirements for protecting sensitive data are particularly high. That is why we place great importance on security, digital sovereignty, and long-term reliability when selecting our technology partners. What we value about Airlock Microgateway is that it is developed by Ergon, a Zurich-based company with extensive experience in the Swiss banking and public sectors.”

Mohammad Alavi, CTO at HIN

Health Info Net AG (HIN) has been securely connecting organizations and professionals across the Swiss healthcare sector since 1996. When its infrastructure, which had evolved over many years, could no longer meet the growing demands for flexibility, automation, and independence, HIN decided to chart a new course. Together with specialized partners, HIN created a Kubernetes-native, GitOps-based architecture built on open standards—with Airlock Microgateway as a central component for protecting web applications and APIs.

A network trusted across Switzerland

More than 50,000 professionals and institutions—including hospitals, medical practices, pharmacies, laboratories, insurers, and public authorities—use HIN to securely exchange sensitive health data.

Where protecting health data is a core business, security and availability are non-negotiable. At the same time, the infrastructure must keep pace with new digital services and growing demands. This is precisely where the modernization began.

When legacy infrastructure reaches its limits

The existing infrastructure had served HIN well for many years. However, as its digital services evolved, the demands for flexibility, automation, and scalability increased. Making changes to the infrastructure was time-consuming, and new services could no longer be deployed at the desired pace. Implementing changes through tickets sometimes took more than two weeks, while numerous custom solutions increased the effort required for maintenance and updates.

The upstream security architecture had also evolved over many years and had become correspondingly complex. Implementing new requirements involved considerable effort. At the same time, HIN wanted to give development teams greater autonomy, increase process automation, and reduce its dependence on individual technologies and infrastructure providers.

The key challenges were:

- ▶ **Limited adaptability:** Static configurations and time-consuming changes made agile deployment cycles more difficult.
- ▶ **High security and compliance requirements:** Granular security policies for sensitive health data could no longer be efficiently scaled using manual processes.
- ▶ **Technology dependencies:** Custom proxy logic and hosting structures restricted HIN's strategic freedom.
- ▶ **Distributed responsibilities:** Infrastructure, platform, security, and application teams needed an operating model that clearly separated their responsibilities.

For HIN, it was therefore clear that replacing individual components would not be enough: what was needed was a fundamental modernization of the security and operating architecture.

Project Phoenix: Guiding principles for the new platform

With *Project Phoenix*, HIN initiated this transformation. Inspired by the book *The Phoenix Project*¹, the goal was to build a standardized, automated, and resilient platform in which development, operations, and security work closely together.

¹ The Phoenix Project: A Novel About IT, DevOps, and Helping Your Business Win by Gene Kim (Author), Kevin Behr (Author), George Spafford (Author)

Six guiding principles shaped the project:

1. **GitOps and traceability:** Changes should be centrally documented, versioned, and fully traceable for auditing purposes.
2. **Security first:** Data protection, compliance, and security should be considered from the outset.
3. **Dual-vendor strategy:** Dependencies should be reduced and resilience increased.
4. **Open standards:** Proprietary, isolated solutions should be replaced with standardized, portable approaches.
5. **Automation and agility:** Repeatable processes should simplify operations and enable new services to be delivered more quickly.
6. **Faster time to market:** New services should be delivered more quickly and cost-effectively.

In this way, HIN linked the technical modernization to a broader objective: greater control over its infrastructure and operating processes.

A partner ecosystem with clearly defined responsibilities

These requirements led to a target architecture based on a Kubernetes platform that can be operated through automated processes, meets high security requirements, and does not depend on a single provider.

To achieve this, HIN deliberately relies on specialized partners. Red Hat OpenShift provides the Kubernetes platform, while VSHN is responsible for operating it and supports HIN with architecture and migration. With cloudscale.ch and Exoscale, HIN uses two independent cloud providers. This allows the company to reduce its dependence on a single infrastructure provider and increase the platform's resilience. With Microgateway, Airlock provides Kubernetes-native protection for web applications and APIs. Additional technology partners are integrated into the identity and authentication architecture.

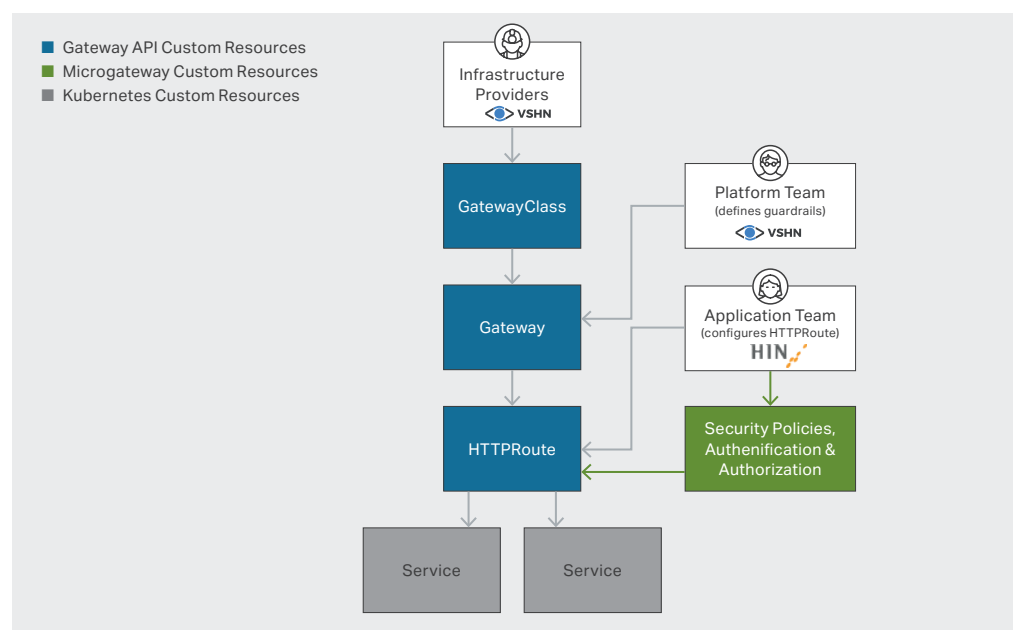
Responsibilities are also clearly distributed within the platform. The resource and role model of the Kubernetes Gateway API supports this division of responsibilities.

We were able to consistently implement the Gateway API's clear separation of roles with Airlock Microgateway. Using the declarative configuration model, the platform team defines the guardrails, while the application teams manage their own routes and security policies. This simplifies collaboration across multiple teams and partners and makes operations more efficient.



Andreas Gruhler,
Cloud Architect at HIN

Role-oriented operating model based on the Kubernetes Gateway API. VSHN provides the platform and gateways, with Airlock Microgateway as the Gateway API implementation, while HIN manages application routes and security policies.



Why HIN chose Airlock Microgateway

To protect its web applications and APIs, HIN was looking for a solution that could be integrated into OpenShift, its GitOps-based operating model, and its existing IAM landscape while still providing sufficient flexibility to meet specific requirements. Configuration changes needed to take effect without a restart, and the security component also had to fit the distributed operating model used by HIN and its partners.

Airlock Microgateway met these requirements as a Kubernetes-native implementation of the Gateway API. For routing, HIN therefore uses the standardized resource model of the Kubernetes Gateway API instead of a proprietary routing model. The solution extends this model with Web Application and API Protection and identity-based access control and is certified for Red Hat OpenShift.

Another decisive factor in HIN's dual-vendor strategy is that the security architecture is not tied to a specific cloud provider. As a cloud-agnostic, Kubernetes-native solution, Airlock Microgateway can be operated consistently across HIN's OpenShift environments. This means that the security layer also remains portable across different cloud infrastructures.

The existing identity infrastructure can be integrated using standards such as OIDC. OAuth 2.0 Token Exchange and extension options using ICAP or Lua also make it possible to meet specific requirements.

How HIN combines routing, application protection, and identity

HIN uses Airlock Microgateway for three central tasks in the new architecture. At the cluster entry point, the solution brings routing, application protection, and identity-based access control together in a Kubernetes-native component.

- ▶ **Routing with Gateway API:** HIN defines its application routes using the standardized resource model of the Kubernetes Gateway API. Airlock Microgateway implements this configuration and controls which traffic is directed to which service.
- ▶ **Web Application and API Protection:** Strong security defaults protect web applications and APIs from the outset, including against known attack patterns covered by the OWASP Top 10.
- ▶ **Identity-aware proxy:** For interactive browser access, Airlock Microgateway acts as an OIDC Relying Party and therefore integrates with HIN's existing identity infrastructure using an established standard. At the same time, this integration enables seamless single sign-on.

This capability is particularly relevant for HIN: In addition to traditional browser access, the platform must also secure third-party applications and technical devices. For OAuth-based access, Airlock Microgateway accepts the supplied access token and can use OAuth 2.0 Token Exchange to obtain a token for accessing the downstream service.

For particularly sensitive applications or paths, HIN can also require a higher authentication level. Users who have already been authenticated are then specifically redirected to an additional authentication step. Access to the protected resource is granted only once the required trust level has been reached.

The combination of standardization and extensibility was decisive for us: Airlock Microgateway is built on the Kubernetes Gateway API, integrates natively into OpenShift, and supports our IAM integration through open standards such as OIDC and OAuth 2.0 Token Exchange. At the same time, we can meet highly specific requirements, for example using ICAP for malware scanning or Lua.



Andreas Gruhler,
Cloud Architect at HIN

Security policies become part of the development process

A key advantage of the new architecture is its declarative configuration. Routes and security policies are managed, versioned, reviewed, and automatically deployed through Git. This allows Airlock Microgateway to fit seamlessly into HIN's DevSecOps model: Security is integrated directly into development and operating processes as code.

As a result, changes remain traceable and can be reviewed and approved before rollout. Test, pre-production, and production environments can be operated according to the same principles, while rollouts can be automated in a controlled manner.

The migration of the existing configurations also follows this approach. A purpose-built script automatically converts existing configurations into Gateway API and Microgateway manifests, which are then deployed through Argo CD. The gradual migration and accompanying end-to-end tests enabled HIN to modernize its business-critical environment in a controlled manner without having to migrate the entire environment at once.

From migration to modern platform operations

The modernization is changing not only the technology, but also the way HIN develops and operates its digital platform.

- **Greater control and resilience:** HIN can operate its applications across two independent cloud infrastructures. The security layer remains cloud-independent and can be deployed in both OpenShift environments according to the same principles.
- **Greater security:** Airlock Microgateway enforces application protection and identity-based access control directly in front of the services. Capabilities such as step-up authentication enable additional levels of protection for particularly sensitive access.

- **Greater efficiency and agility:** Automation and "Security Policy as Code" accelerate deployments—from several hours to just a few minutes.
- **Greater freedom for development:** The established DevOps culture with clearly distributed responsibilities relieves development teams of routine tasks and supports the faster evolution of digital services.

The foundation for future digital healthcare services

With the new platform, HIN has fundamentally realigned its security architecture. Open standards, clear responsibilities, and automated processes create an environment that can evolve flexibly and reduces dependencies on individual technologies and providers.

Airlock Microgateway integrates application protection and identity-based access control directly into this Kubernetes-native operating model. This makes security an integral part of development and operations.

HIN has therefore created a flexible and automatable foundation for continuing to develop digital healthcare services securely in the future.

Airlock Microgateway impressed us because the solution fully supports our security principles while also being consistently designed for container-based architectures. The cloud-native and scalable architecture, as well as the close technical collaboration, were key factors for us.



Mohammad Alavi,
CTO at HIN

Health Info Net AG (HIN)

Health Info Net AG (HIN) was founded by physicians for physicians in 1996. Today, HIN supports healthcare professionals and institutions in Switzerland with digital services for simple, secure, and privacy-compliant communication and collaboration. The platform is particularly well known for HIN Mail, which is used to send millions of encrypted emails every year.

HIN protects sensitive health data, ensures its availability, and thereby contributes to digital sovereignty in the Swiss healthcare sector. Its objective is to simplify administrative processes and give healthcare professionals more time for their patients.

About Airlock – security innovation by Ergon Informatik AG

The Airlock Secure Access Hub combines the key IT security issues of filtering and authentication into a well-coordinated overall package that sets standards in terms of usability and services. The Secure Access Hub provides all the key functions required for modern IT security in this field – from a web application firewall (WAF) acclaimed by specialist journalists and a customer identity and access management (CIAM) system trusted by Swiss banks, to API security that meets the latest requirements. The Airlock IT security solution protects more than 20 million active digital identities and 30,000 backends from over 550 customers all over the world.

You can find further information at www.airlock.com. Airlock is a security innovation from Swiss software company Ergon Informatik AG.

Ergon Informatik AG was founded in 1984 and is a leader in the production of customised software solutions and software products. 300 highly qualified IT specialists who quickly anticipate new technology trends and ensure key competitive advantages with innovative solutions thanks to their outstanding specialist knowledge form the basis of this success. Ergon Informatik mainly implements large-scale projects in the B2B sector.

Ergon Informatik AG
Merkurstrasse 43
8032 Zurich, Switzerland
+41 44 268 89 00
info@airlock.com

airlock.com

ergon

Copyright © 2026 Ergon Informatik AG. All Rights Reserved. All technical documentation that is made available by Ergon Informatik AG is the copyrighted work of Ergon Informatik AG and is owned by Ergon Informatik AG. Ergon, the Ergon logo, «smart people – smart software» and Airlock are registered trademarks of Ergon Informatik AG. Microsoft and ActiveDirectory are registered trademarks or trademarks of Microsoft Corporation in the United States and /or other countries. Other products or trademarks mentioned are the property of their respective owners.