AIRLOCK®

Airlock Microgateway Webinar

4. November 2021

Dr. Martin Burkhart
Head of Product Management Airlock

Stefan Dietiker
Product Manager Airlock Microgateway

Agenda

1. Why do we need Microgateways?

2. Airlock Microgateway News

3. Demo with Airlock Microgateway

Use Q&A window for questions

Past

Long Release Cycles

Classic
HTML Websites

Monoliths

Perimeter Security

Today

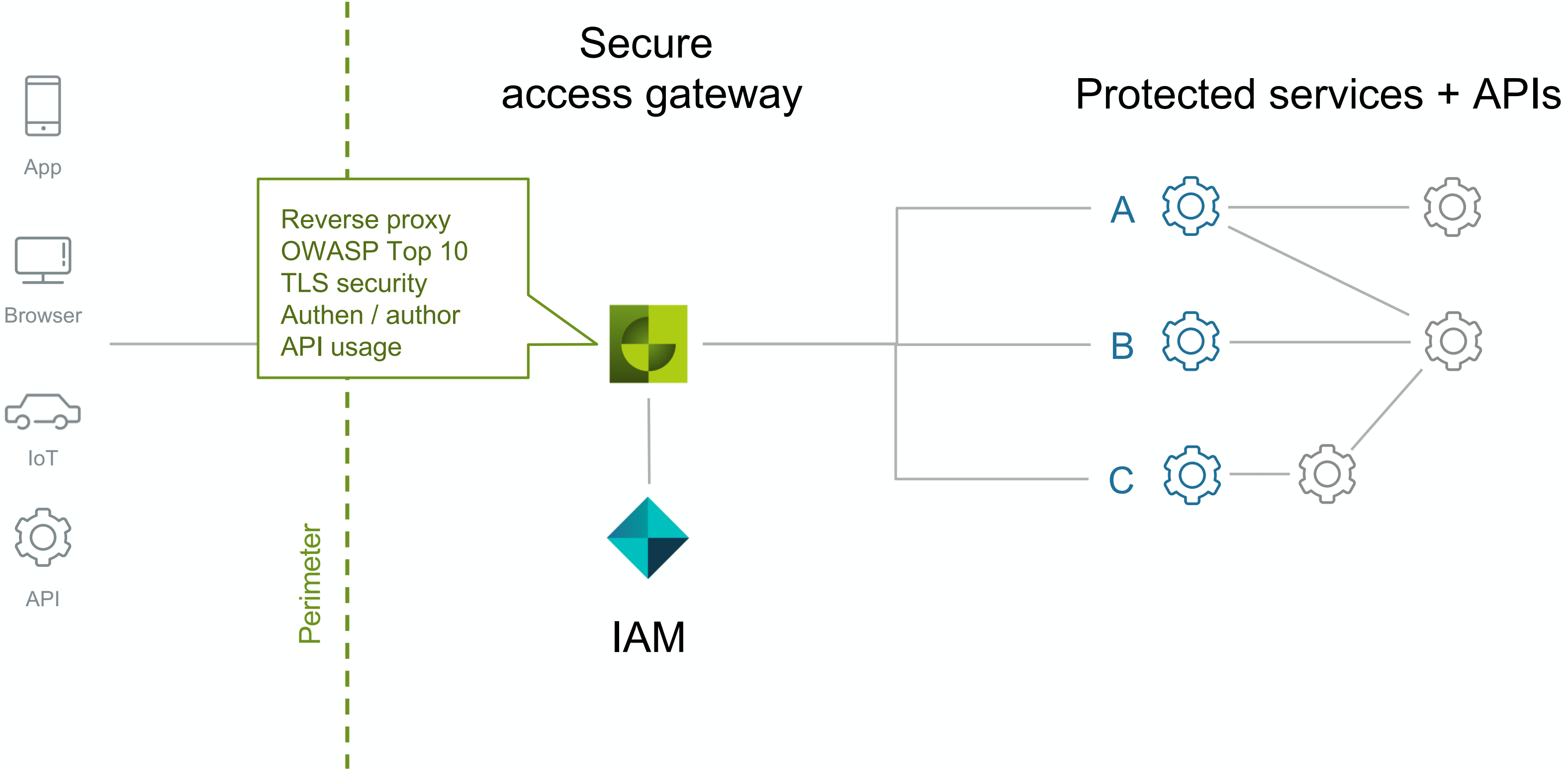
Agile, DevOps
Continuous Delivery

APIs
Mobile Apps
Single-Page Apps

Microservices

Zero Trust

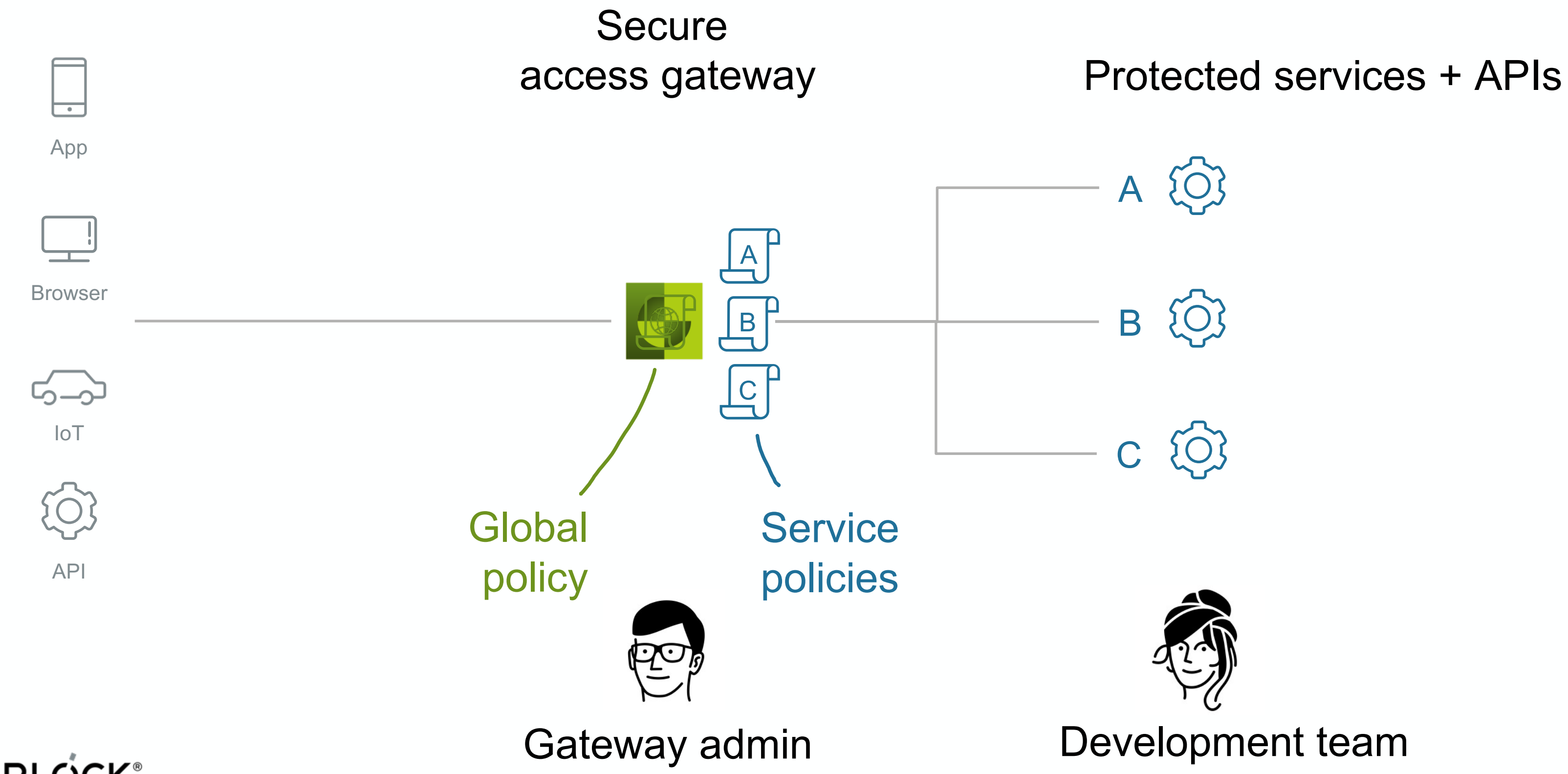
Classic architecture



AIRLOCK®

ergon

Classic architecture - policies



Two distinct perspectives

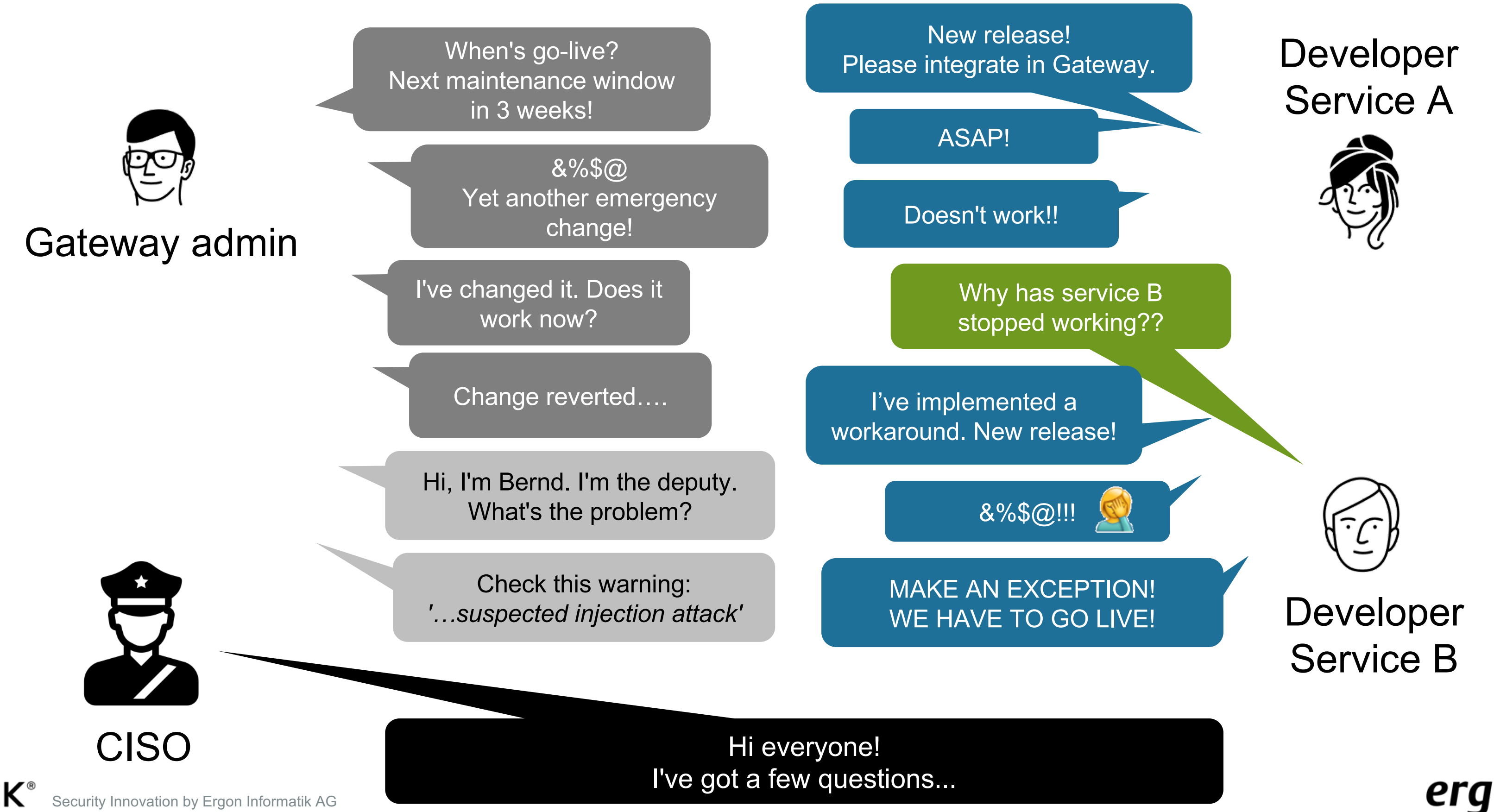
- Publish service **securely**
- Understands little about the service
- Fears false positives

Gateway admin

- Release service **quickly**
- Understands little about operations
- Everything works here!

Development team

The delivery back-and-forth



Developer Service A

Gateway admin

Developer Service B

CISO

New release!
Please integrate in Gateway.

When's go-live?
Next maintenance window in 3 weeks!

ASAP!

&%$@
Yet another emergency change!

Doesn't work!!

I've changed it. Does it work now?

Why has service B stopped working??

Change reverted….

I’ve implemented a workaround. New release!

Hi, I'm Bernd. I'm the deputy. What's the problem?

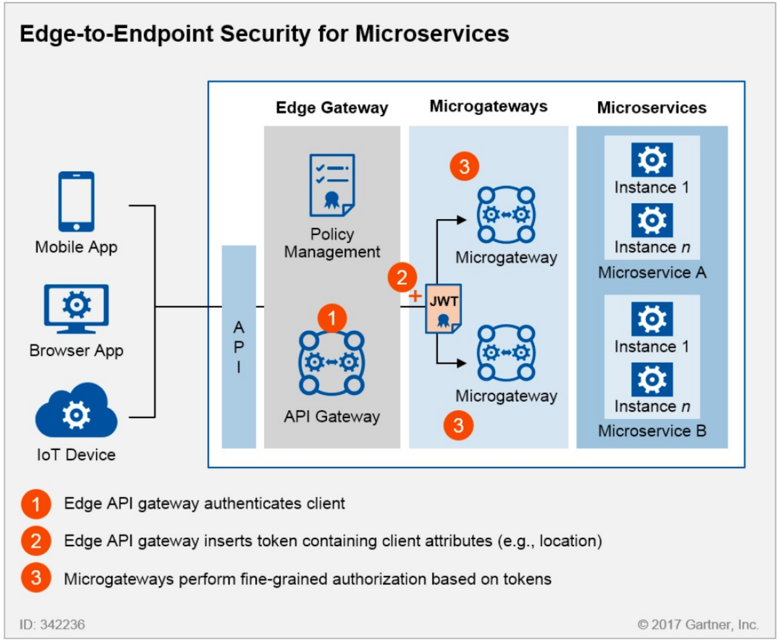
&%$@!!! 🤦

Check this warning:
'…suspected injection attack'

MAKE AN EXCEPTION!
WE HAVE TO GO LIVE!

Hi everyone!
I've got a few questions...

Architectures for Securing Microservices



Edge-to-Endpoint Security for Microservices

1 Edge API gateway authenticates client

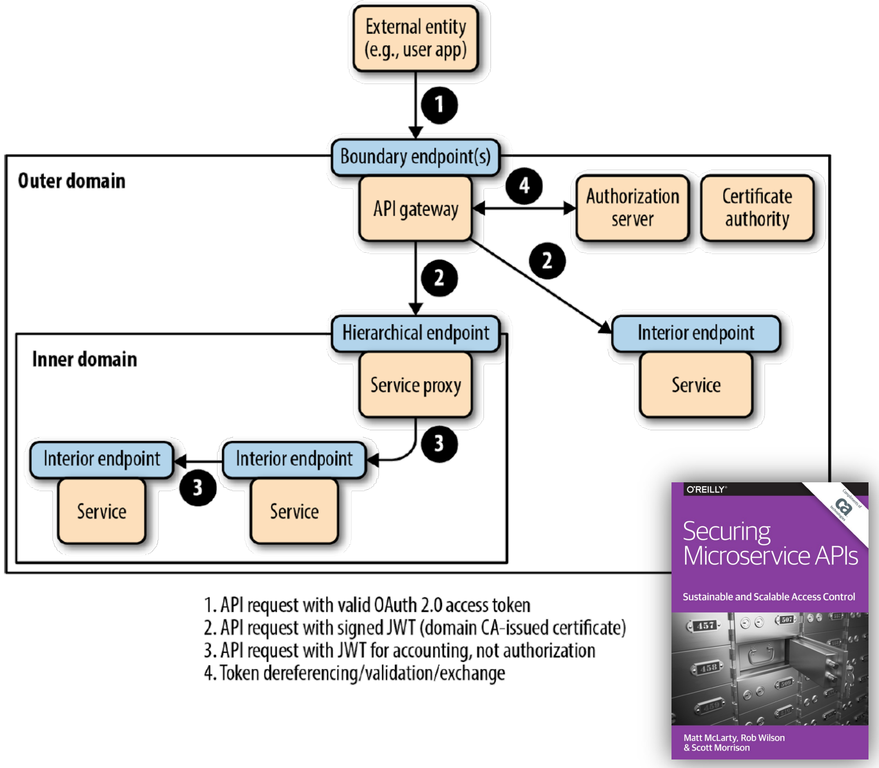
2 Edge API gateway inserts token containing client attributes (e.g., location)

3 Microgateways perform fine-grained authorization based on tokens

ID: 342236

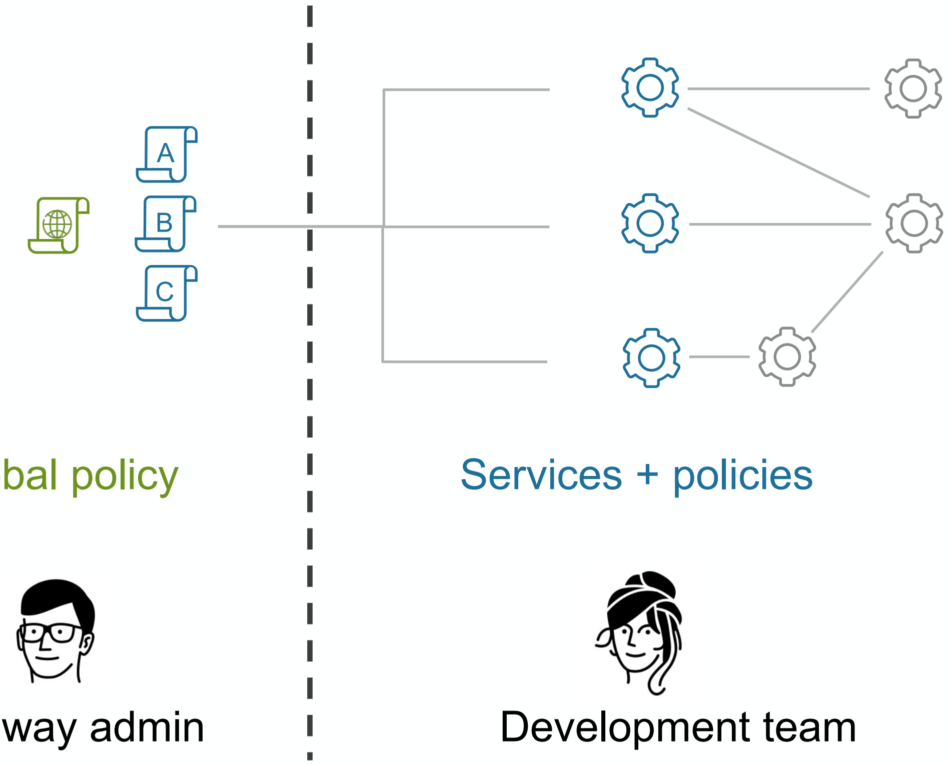
© 2017 Gartner, Inc.

How to Build an Effective API Security Strategy, Gartner



1. API request with valid OAuth 2.0 access token
2. API request with signed JWT (domain CA-issued certificate)
3. API request with JWT for accounting, not authorization
4. Token dereferencing/validation/exchange

Solution: Organisation



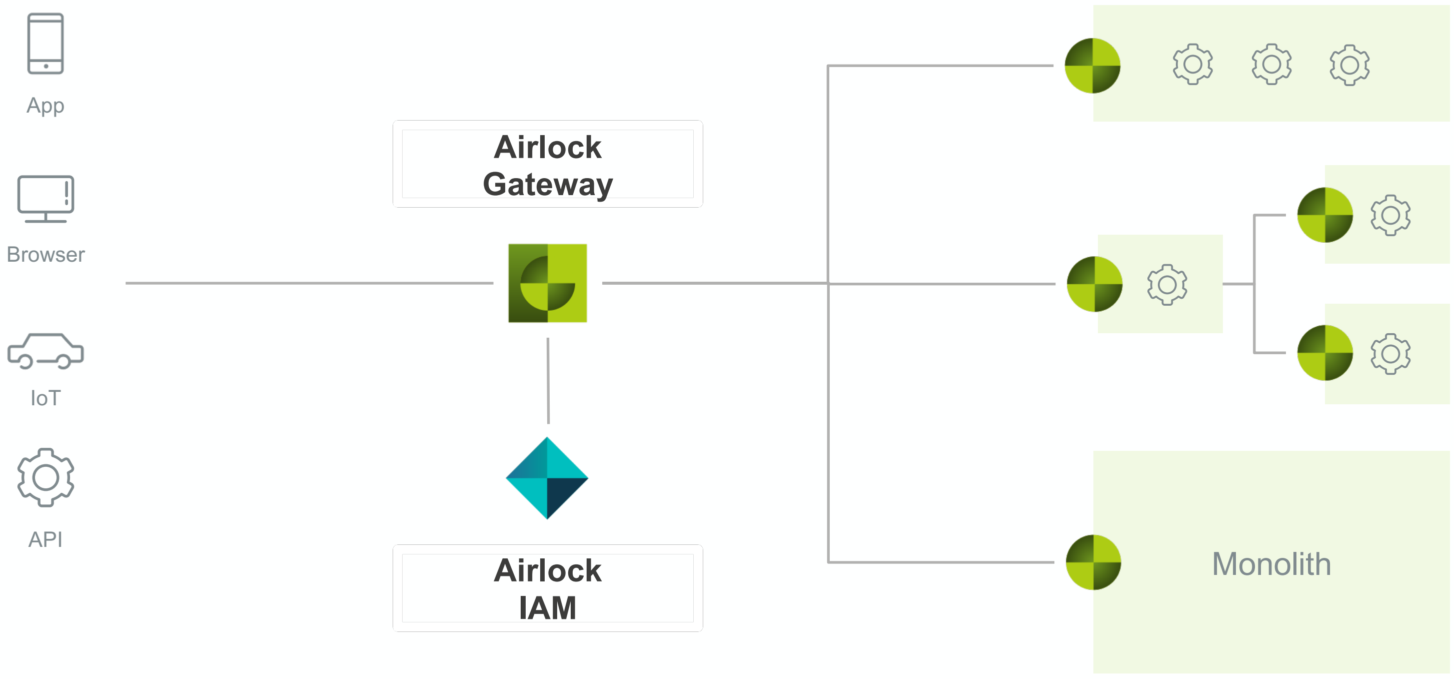
Global policy

Services + policies

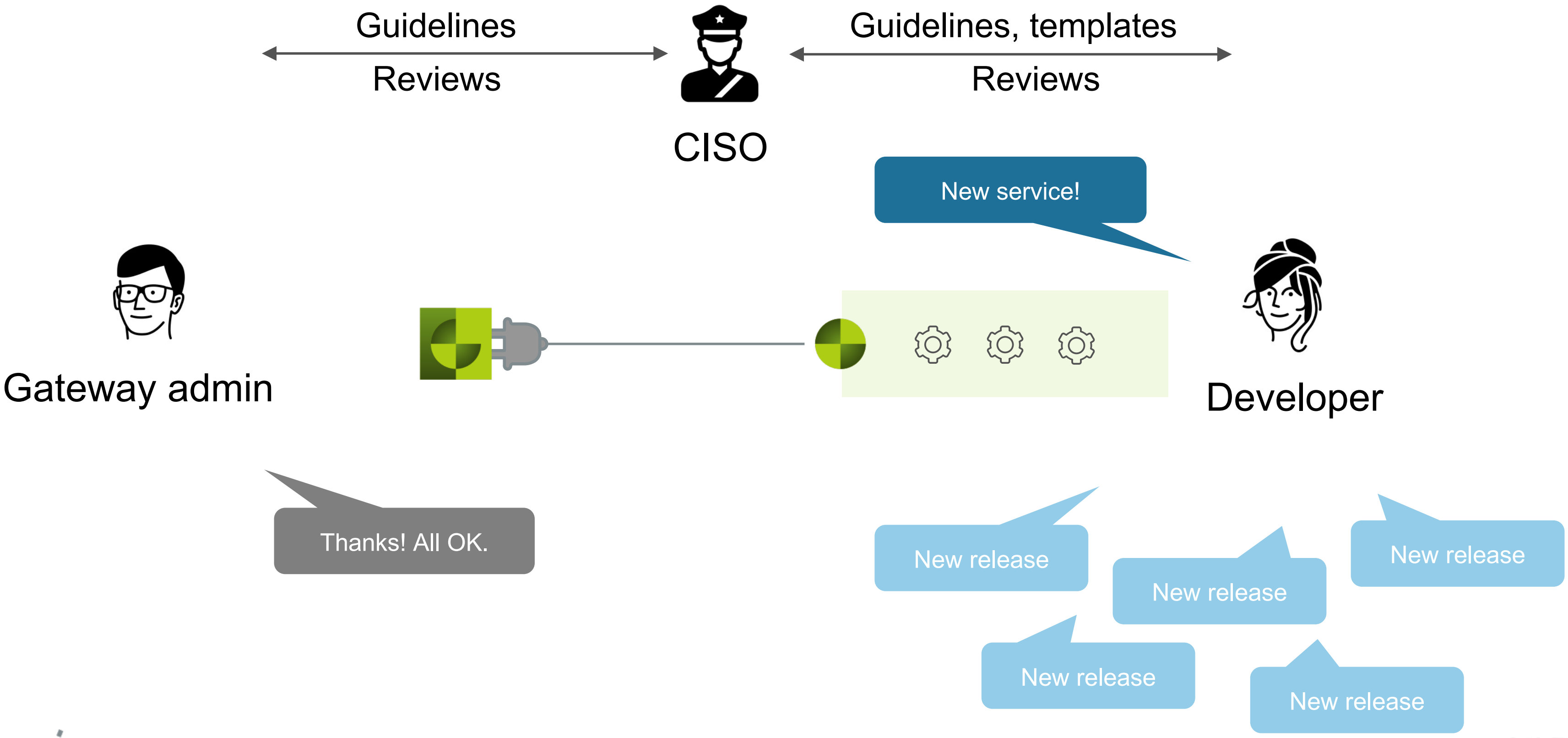
Gateway admin

Development team

Zero-trust architecture with Microgateways



Software deployment with Microgateways



Guidelines

Reviews

CISO

Guidelines, templates

Reviews

New service!

Gateway admin

Developer

Thanks! All OK.

New release

New release

New release

New release

New release

Airlock Microgateway News

Overview

2.1

Gateway Core: 7.6

Update from 2.0 is non-breaking

Substantial extension of DSL

Community Edition (Freemium Model)

Premium Edition

- License unlocks premium features

3.0

Gateway Core: Update to 7.7

Update Breaking for JWT Configuration

JWKS Support (JSON Web Key Sets)

YAML Schema for validation and IDE Support

Various extensions to the DSL

Enhanced Minikube-Example with GitOps

Tutorials for self-study

Release 2.1

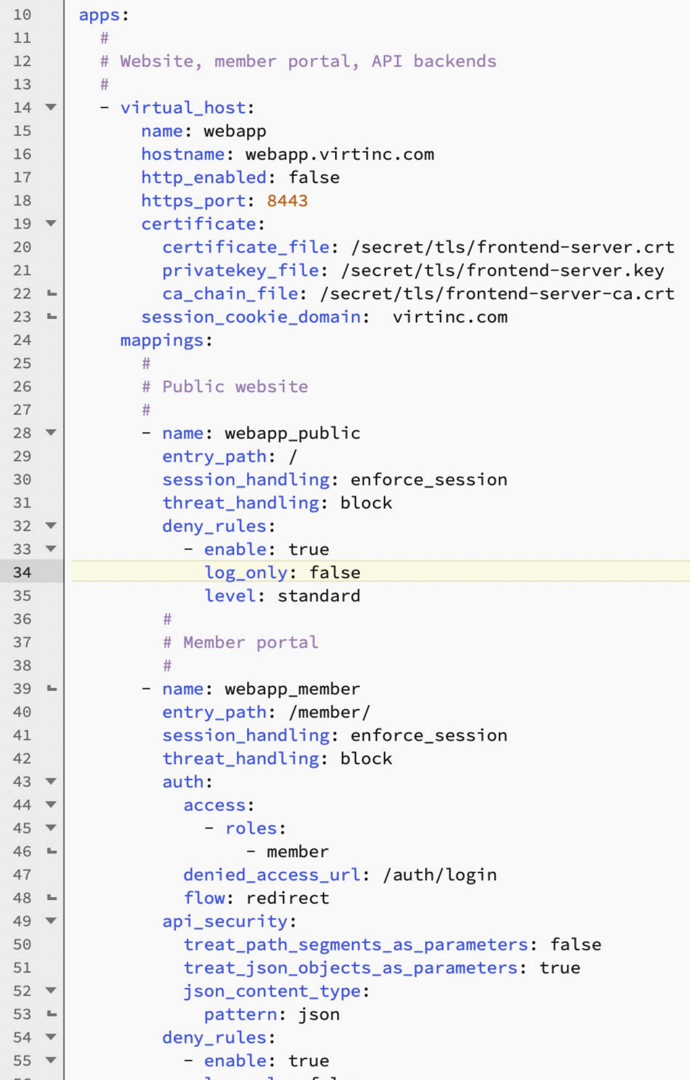
Extension of DSL

Advantages:

- Easily automate configuration changes
- Use developer tooling (e.g. GIT)
- No workarounds using mapping templates

New Settings:

- Custom Deny Rules
- Custom Allow Rules (Path+Method)
- Custom Request/Response Actions
- JSON Rewriting
- Client Certificates
- Error Page Replacement
- Passthrough/Encrypted Cookies
- CSRF Token
- Remote IP Settings
- VH Aliases, etc.



```yaml
apps:
  #
  # Website, member portal, API backends
  #
  - virtual_host:
      name: webapp
      hostname: webapp.virtinc.com
      http_enabled: false
      https_port: 8443
      certificate:
        certificate_file: /secret/tls/frontend-server.crt
        privatekey_file: /secret/tls/frontend-server.key
        ca_chain_file: /secret/tls/frontend-server-ca.crt
      session_cookie_domain:  virtinc.com
    mappings:
      #
      # Public website
      #
      - name: webapp_public
        entry_path: /
        session_handling: enforce_session
        threat_handling: block
        deny_rules:
          - enable: true
            log_only: false
            level: standard
        #
        # Member portal
        #
      - name: webapp_member
        entry_path: /member/
        session_handling: enforce_session
        threat_handling: block
        auth:
          access:
            - roles:
                - member
          denied_access_url: /auth/login
          flow: redirect
        api_security:
          treat_path_segments_as_parameters: false
          treat_json_objects_as_parameters: true
          json_content_type:
            pattern: json
        deny_rules:
          - enable: true
```

Airlock Microgateway Freemium Model

Feature	Community Edition (free)	Premium Edition
DevSecOps Support Container, GitOps-friendly configuration, Mgmt via K8S, Helm Charts	✓	✓
Monitoring and Reporting Structured Logs, Prometheus interface, Kibana dashboards	✓	✓
Standard Application Protection (OWASP Top 10) DoS and bot protection, TLS termination, SQLi and XSS filters, cookie protection, request sanity checks	✓	✓
Access Control with Airlock IAM (separate License) Multi-Factor Authentication (MFA), Identity Federation & much more	✓	✓
Advanced Application Protection OpenAPI schema enforcement, more Deny- and Allow-Rules, CSRF tokens, HTTP parameter pollution, multipart parser, etc.	Log only	✓
Access Control using Tokens Verification of JSON Web Tokens (JWT), Access Control using claims	Log only	✓
Support	Community Support	Premium Support

Community Support

Public Forum

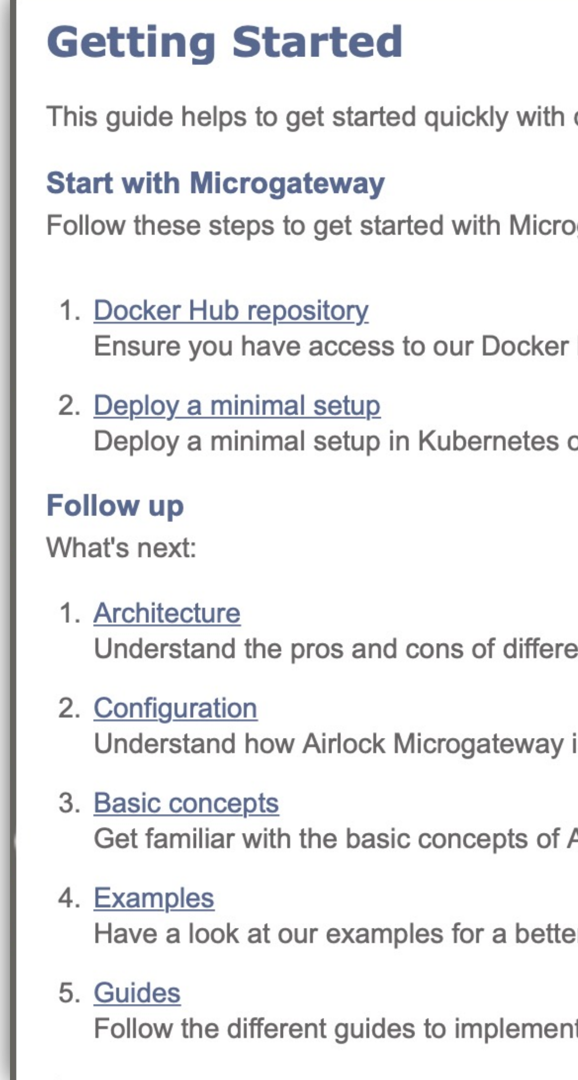
- https://forum.airlock.com/
- Requires account for questions and commenting
- Airlock moderation

Support Level by Airlock

- Hints, pointers to documentation and best practices
- no case analyses
- no guaranteed response times
- complex cases require premium support

Documentation

- Microgateway documentation significantly enhanced!
- Goal: don’t require Airlock Gateway know-how
- Structured around tasks of engineers
- Synergies with Airlock Academy



Getting Started

This guide helps to get started quickly with

Start with Microgateway

Follow these steps to get started with Micro

1. Docker Hub repository
   Ensure you have access to our Docker
2. Deploy a minimal setup
   Deploy a minimal setup in Kubernetes

Follow up

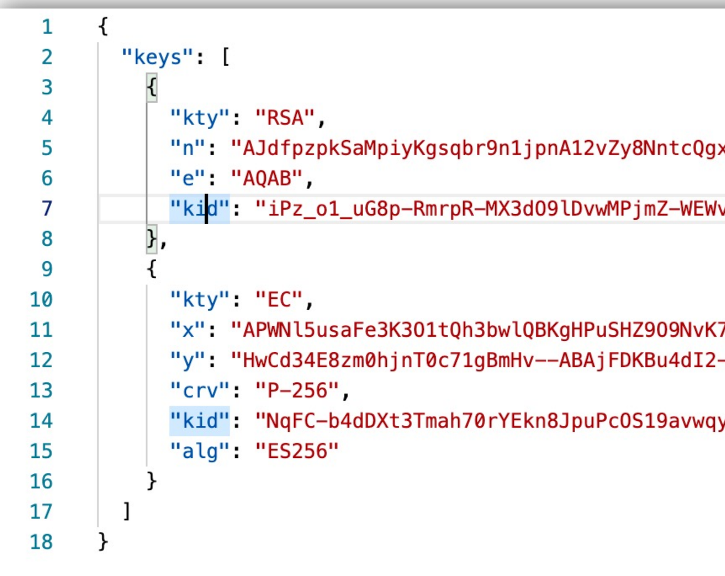
What's next:

1. Architecture
   Understand the pros and cons of differe
2. Configuration
   Understand how Airlock Microgateway i
3. Basic concepts
   Get familiar with the basic concepts of A
4. Examples
   Have a look at our examples for a bette
5. Guides
   Follow the different guides to implement

Release 3.0

JWKS (JSON Web Key Sets)

- Extends the JWT Access Control feature
- Keys locally in “keys” array or
- Key servers remote via URL
- Updating of keys
  - on (re-)load of configuration
  - every 7200s (expert setting)
- JWKS are cached, in case server unreachable (e.g. after a reboot)

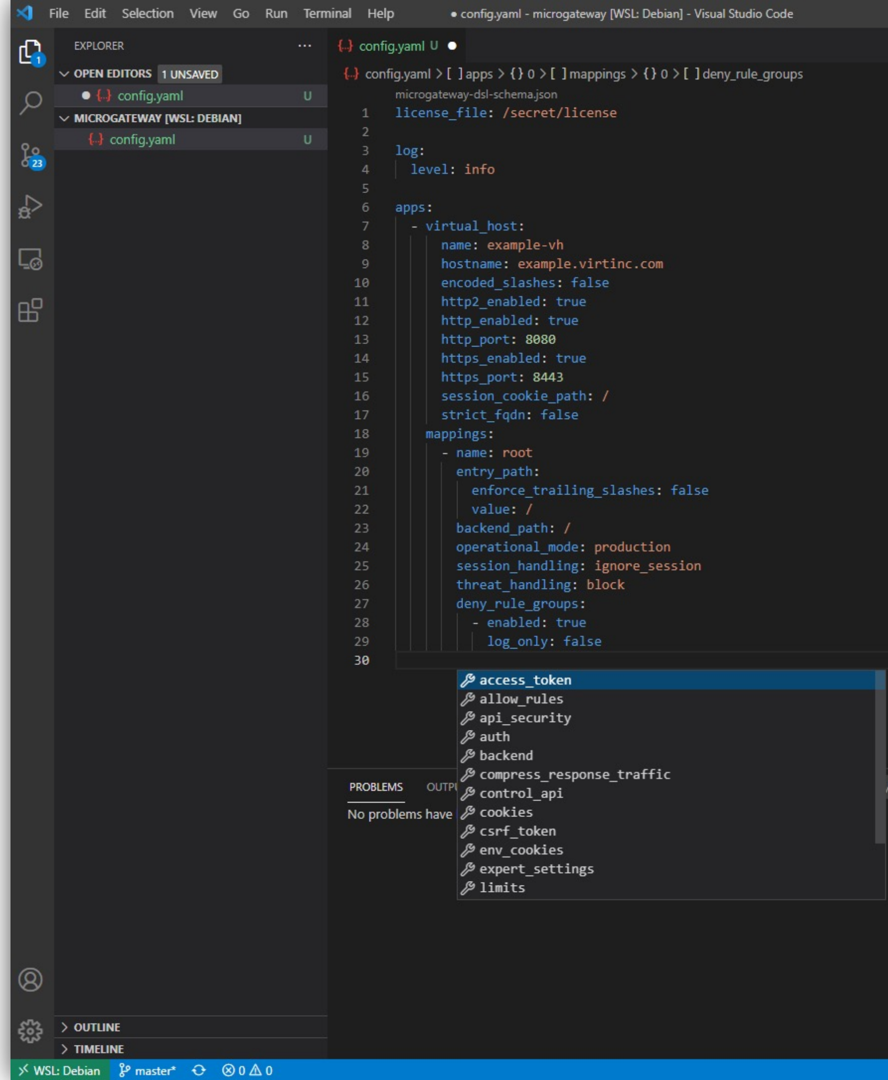


```
{
  "keys": [
    {
      "kty": "RSA",
      "n": "AJdfpzpkSaMpiyKgsqbr9n1jpnA12vZy8NntcQgx
      "e": "AQAB",
      "kid": "iPz_o1_uG8p-RmrpR-MX3dO9lDvwMPjmZ-WEWv
    },
    {
      "kty": "EC",
      "x": "APWNl5usaFe3K3O1tQh3bwlQBKgHPuSHZ9O9NvK7
      "y": "HwCd34E8zm0hjnT0c71gBmHv--ABAjFDKBu4dI2-
      "crv": "P-256",
      "kid": "NqFC-b4dDXt3Tmah70rYEkn8JpuPcOS19avwqy
      "alg": "ES256"
    }
  ]
}
```

YAML Schema

- Validation of config.yaml
- IDE support for
  - Documentation in tooltip
  - Syntax check
  - Code completion and suggestions

AIRLOCK



```yaml
license_file: /secret/license

log:
  level: info

apps:
  - virtual_host:
      name: example-vh
      hostname: example.virtinc.com
      encoded_slashes: false
      http2_enabled: true
      http_enabled: true
      http_port: 8080
      https_enabled: true
      https_port: 8443
      session_cookie_path: /
      strict_fqdn: false
    mappings:
      - name: root
        entry_path:
          enforce_trailing_slashes: false
          value: /
        backend_path: /
        operational_mode: production
        session_handling: ignore_session
        threat_handling: block
        deny_rule_groups:
          - enabled: true
            log_only: false

```

Tutorials

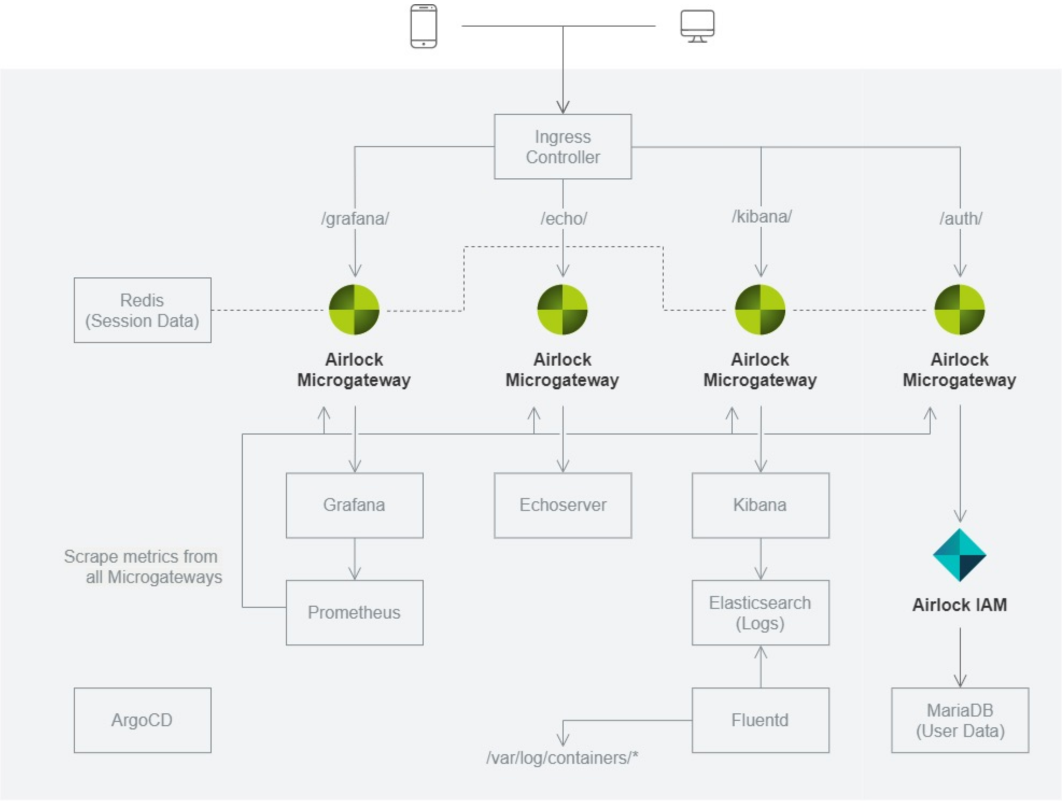
Exercises to learn in self-study about Microgateway:

- Getting started
- Protecting a backend service
- OpenAPI
- Deny rules

Demo of
Airlock Microgateway

Demo Architecture

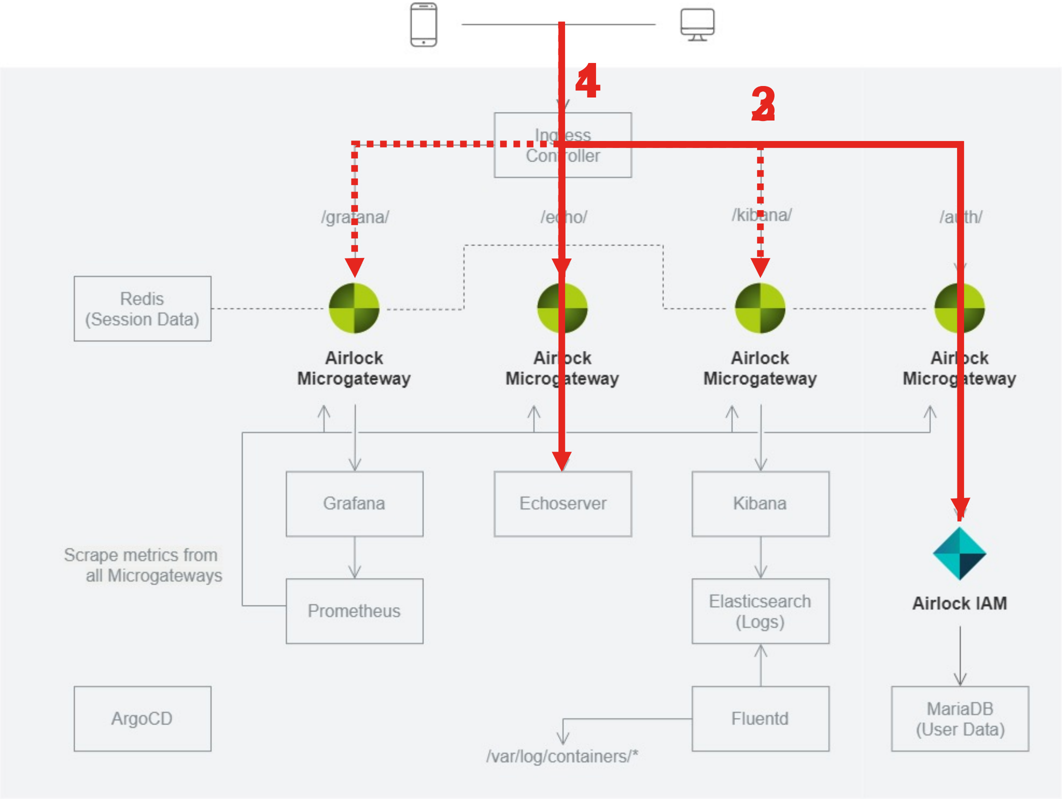
- Services protected by Airlock Microgateway
- Authentication using Airlock IAM
- Integration in Kibana
- Integration in Grafana



https://github.com/ergon/airlock-minikube-example

Use Case: Authentication

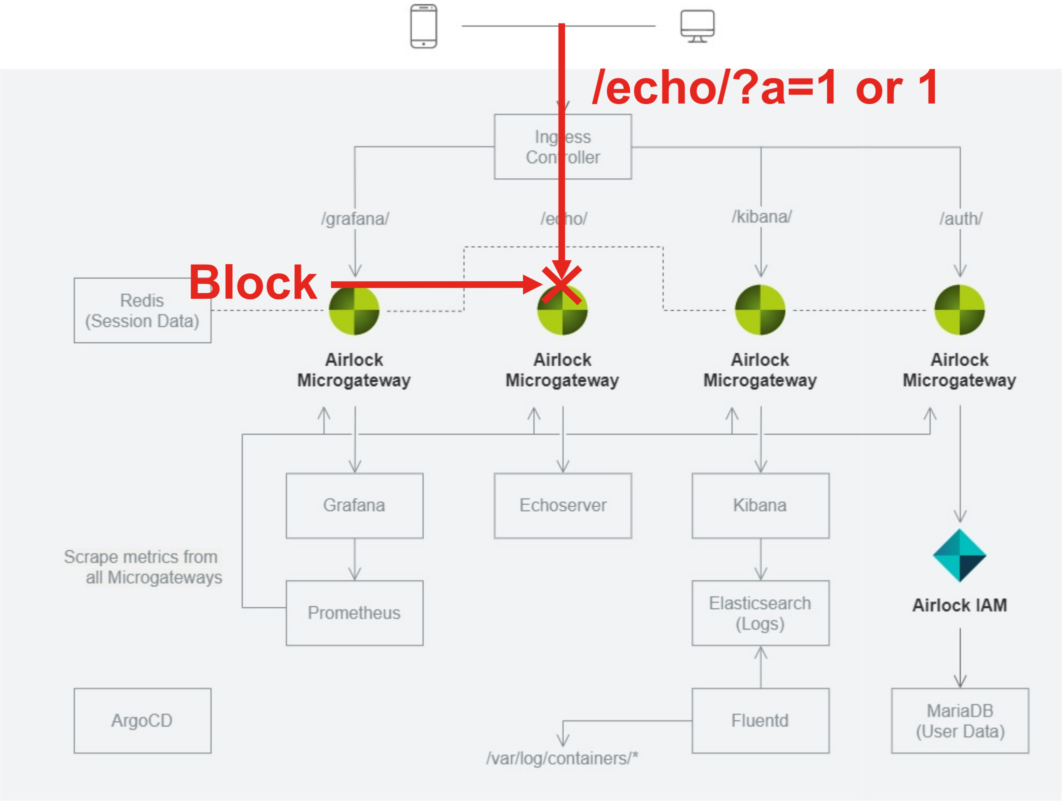
- **Upstream Authentication**
  - Federation using JWT
  - Single Sign-On



https://github.com/ergon/airlock-minikube-example

Use Case: Deny Rules

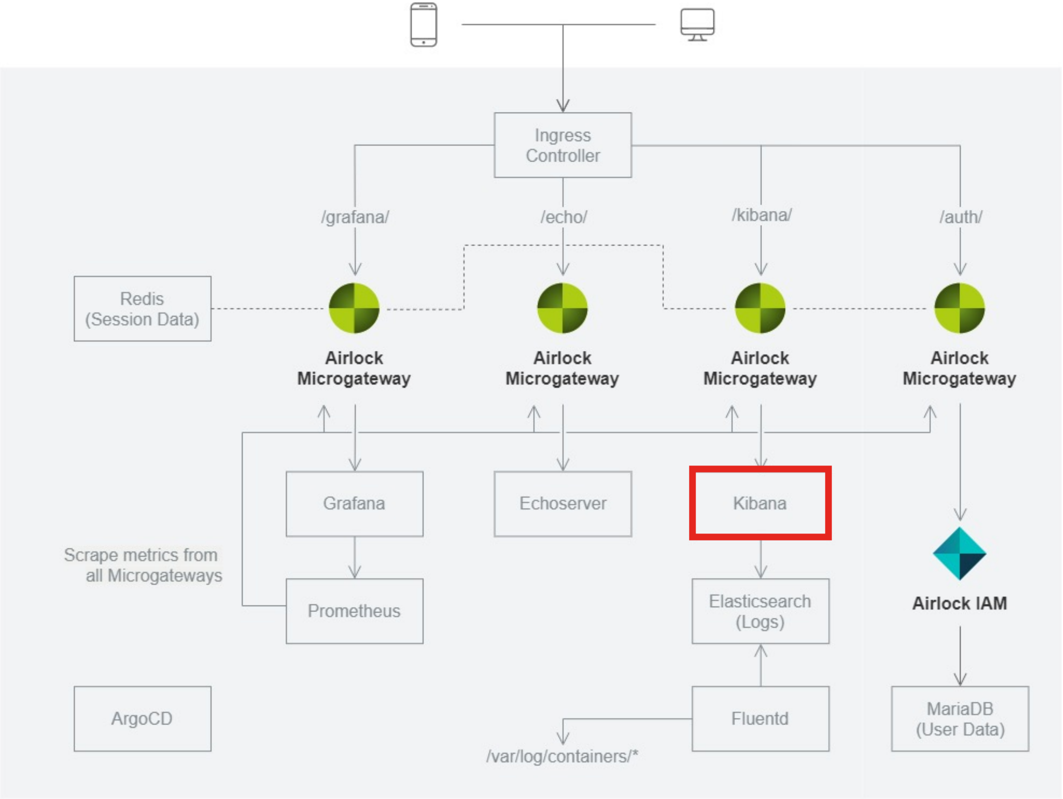
- **Deny Rules**
  - Protection against many OWASP Top 10 risks



https://github.com/ergon/airlock-minikube-example

Use Case: Logging & Reporting

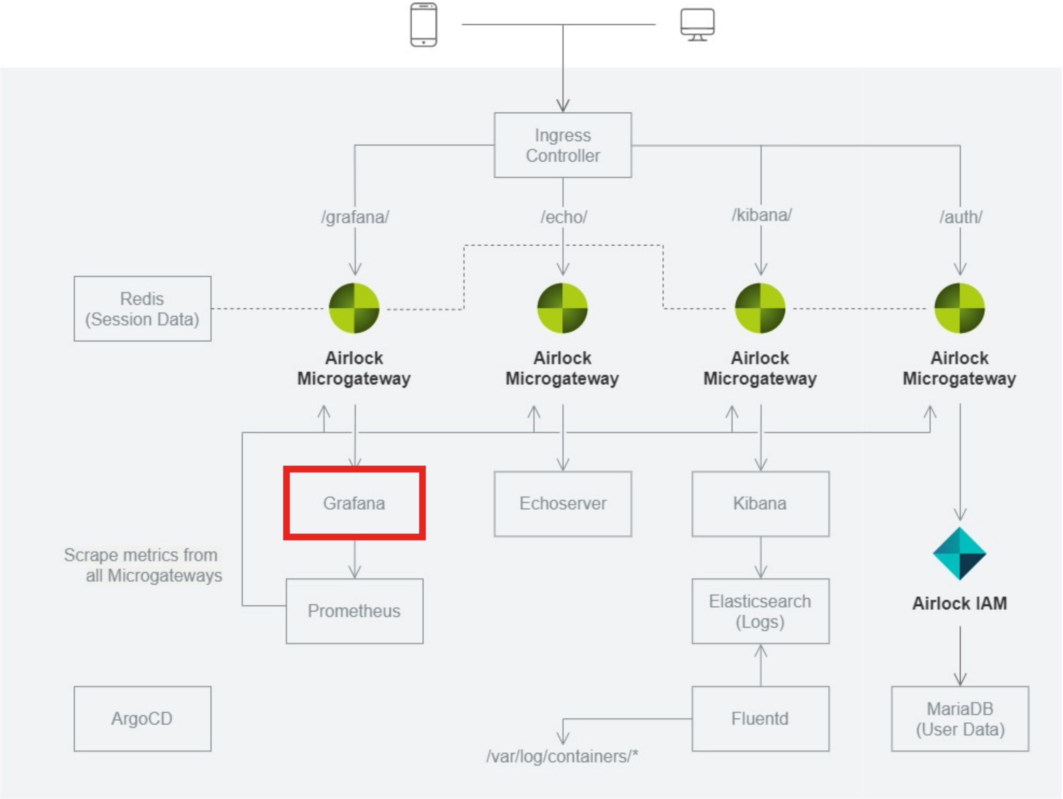
- **Logging and Reporting**
  - Easy troubleshooting
  - Visualization of traffic



https://github.com/ergon/airlock-minikube-example

Use Case: Metrics

- **Metrics**
  - Visualization of Prometheus metrics in Grafana



https://github.com/ergon/airlock-minikube-example

Demo

AIRLOCK®

Thanks for your attention!

www.airlock.com/microgateway

docs.airlock.com/microgateway/latest/

Dr. Martin Burkhart
martin.burkhart@airlock.com

Stefan Dietiker
stefan.dietiker@airlock.com