AIRLOCK®

Airlock Microgateway Webinar

4. November 2021

Dr. Martin Burkhart
Head of Product Management Airlock

Stefan Dietiker
Product Manager Airlock Microgateway

Agenda

1. Warum brauchen wir Microgateways?

2. Airlock Microgateway News

3. Demo mit Airlock Microgateway

Fragen bitte gleich im Q&A Fenster stellen

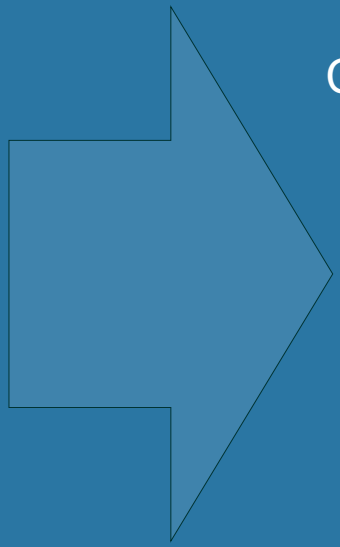
Gestern

Lange Release-Zyklen

Klassische Webseiten

Monolithen

Perimeter-Sicherheit



Heute

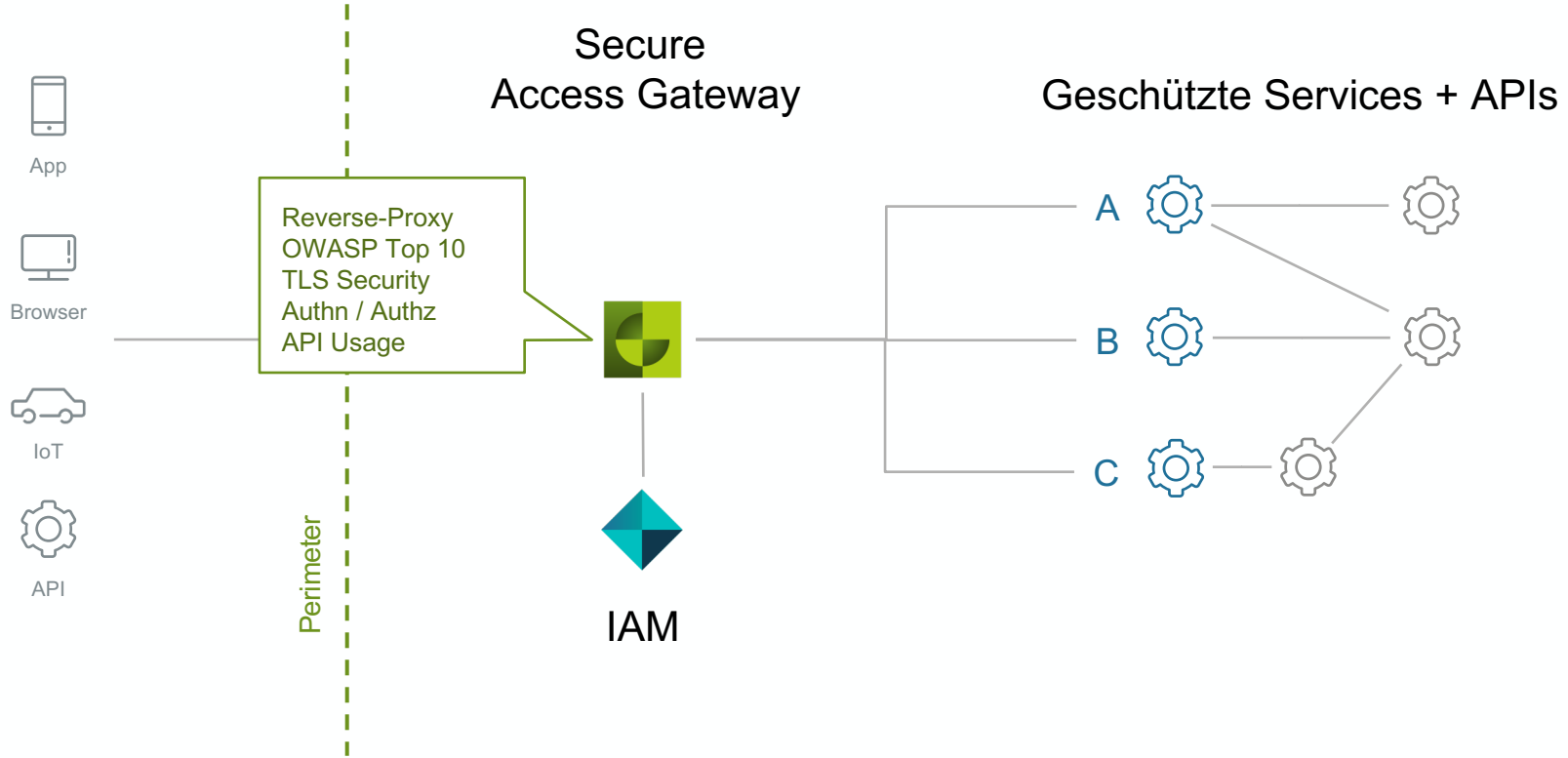
Agile, DevOps
Continuous Delivery

APIs
Mobile Apps
Single-Page Apps

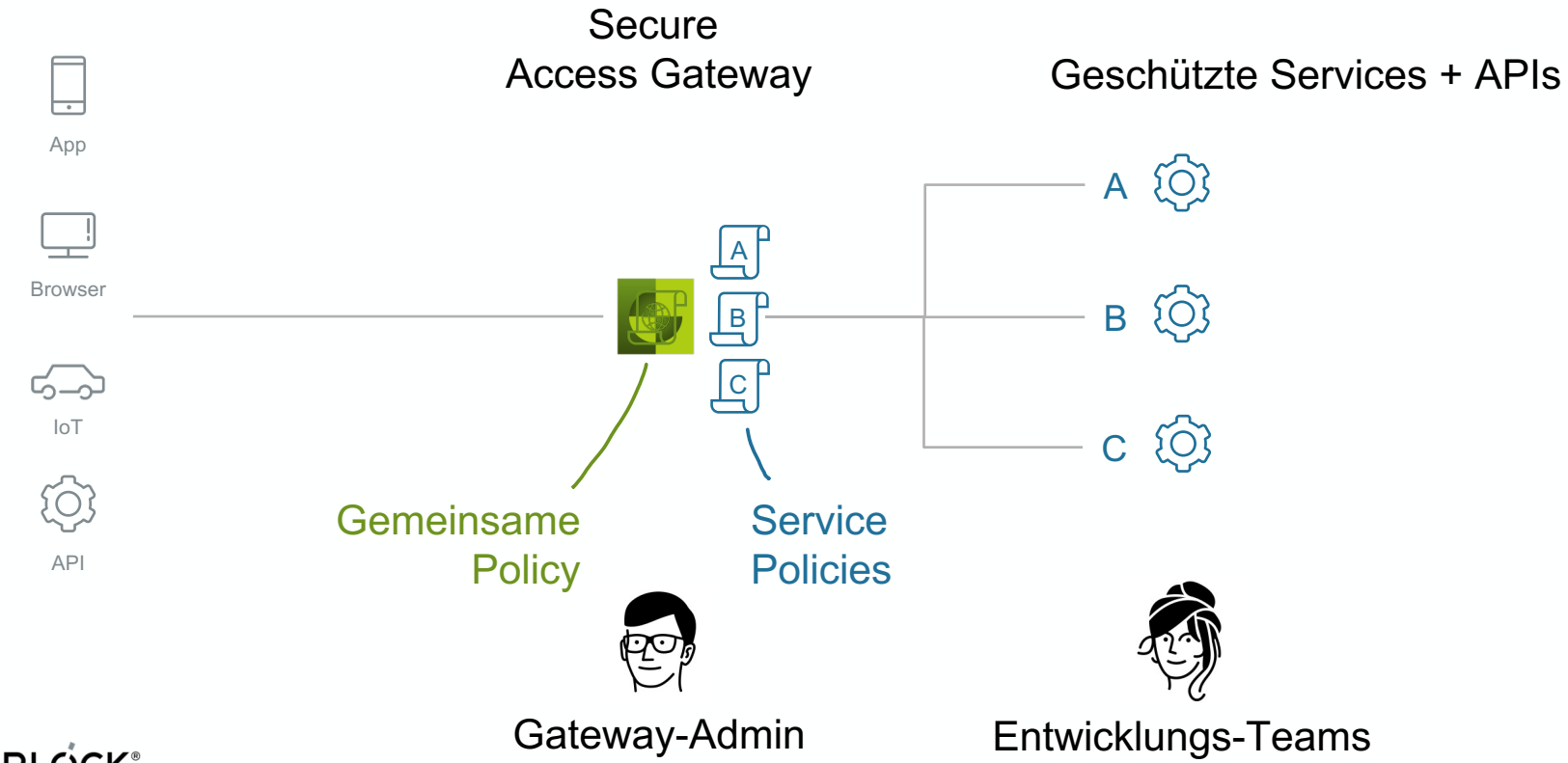
Microservices

Zero Trust

Klassische Architektur



Klassische Architektur - Policies



Der fehlende Blick über den Tellerrand

- Service **sicher** freischalten
- versteht wenig vom Service
- fürchtet False-Positives

Gateway-Admin

- Service **schnell** freischalten
- verstehen wenig von Betrieb
- Es funktioniert doch alles!

Entwicklungs-Teams

Delivery «Ping Pong»

Gateway Admin

Wann ist Go-live?
Nächstes Wartungsfenster
in 3 Wochen!

&%$@
Schon wieder ein
Emergency Change!

Hab was umgestellt.
Geht's jetzt?

Change reverted….

Hallo, ich bin Bernd. Ich bin der
Stellvertreter. Um was geht's?

Schau mal diese Warnung:
"…suspected injection attack"

CISO

Neuer Release!
Bitte auf Gateway integrieren.

ASAP!

Funktioniert nicht!!

Warum läuft Service B
nicht mehr??

Hab einen Workaround
implementiert!
Neuer Release!

&%$@!!!

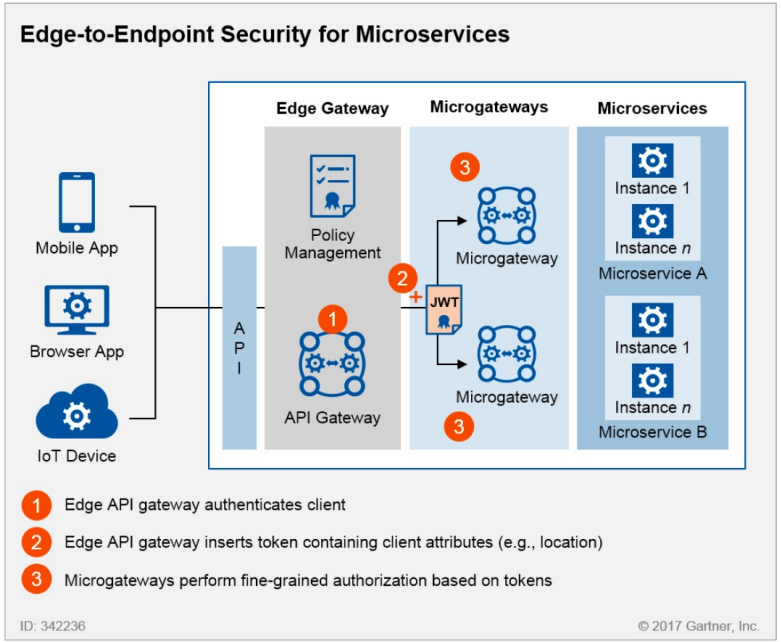
MACH EINE EXCEPTION!
WIR MÜSSEN LIVE GEHEN!

Entwickler
Service A

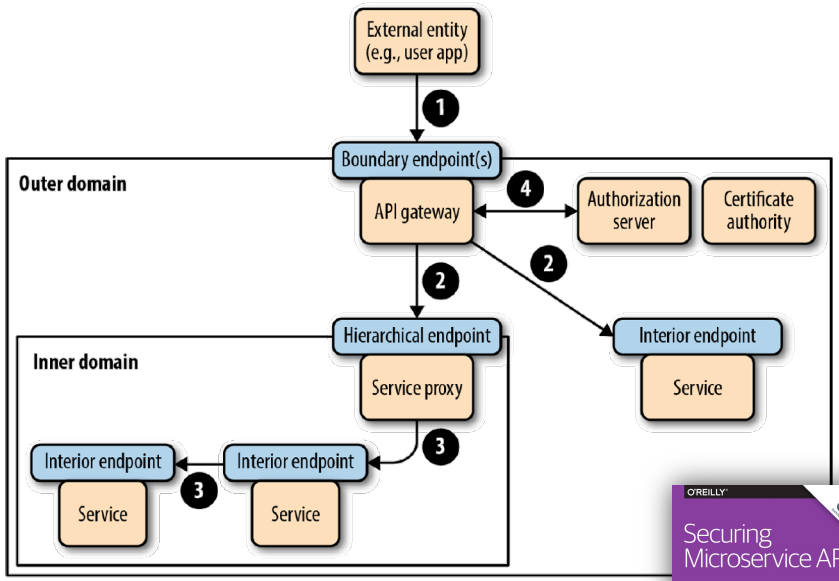
Entwickler
Service B

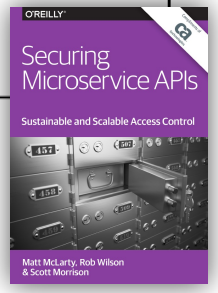
Hallo zusammen!
Ich hätte da noch ein paar Fragen…

Architekturen für sichere Microservices

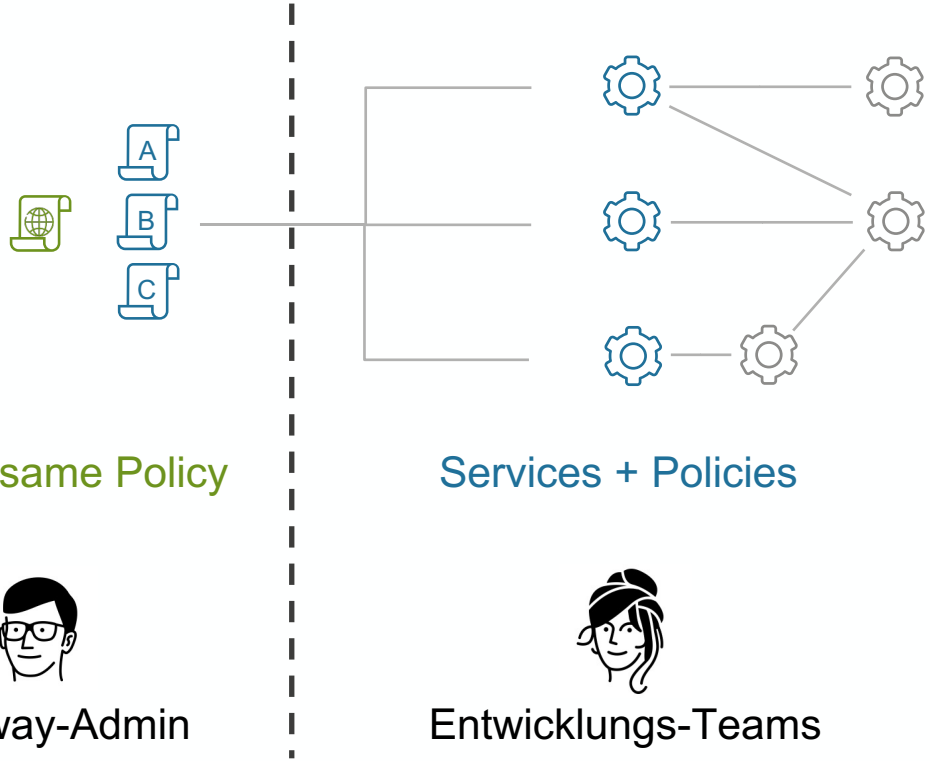


How to Build an Effective API Security Strategy, Gartner

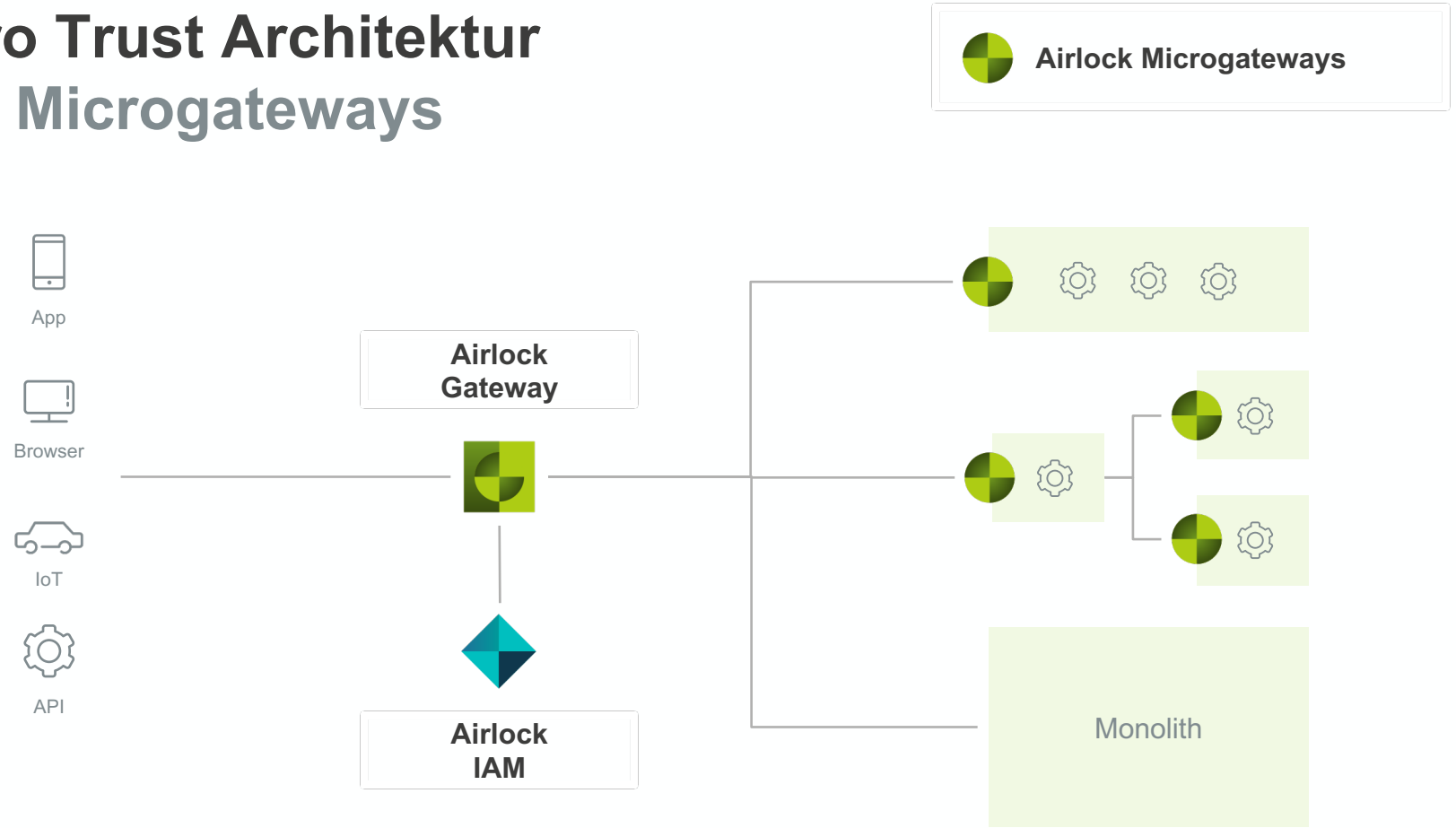




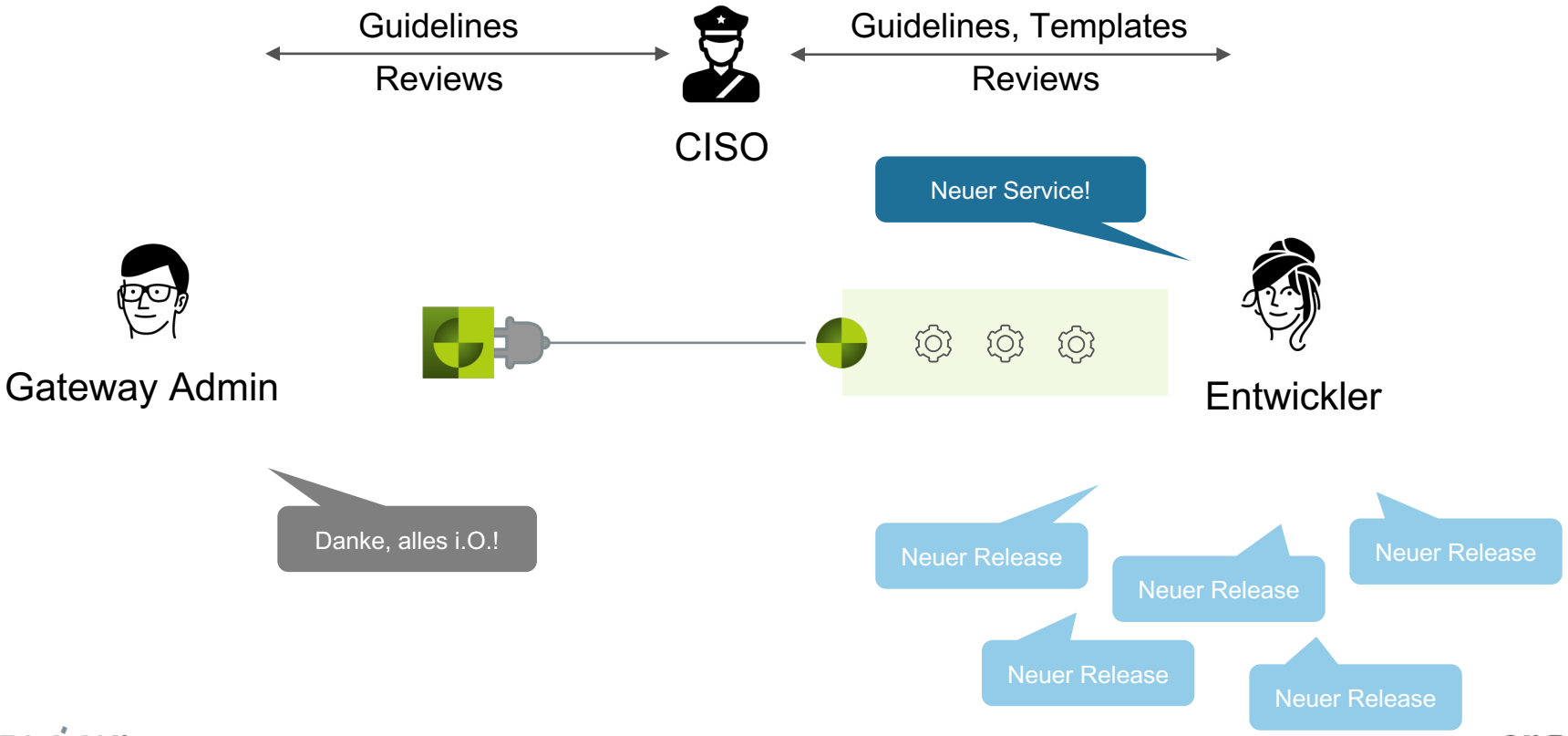
Lösung: Organisation



Zero Trust Architektur
mit Microgateways



Software Deployment mit Microgateways



Airlock Microgateway News

Überblick

2.1

Gateway Core: 7.6

Update von 2.0 ist non-breaking

Komplettierung der DSL

Community Edition (Freemium Modell)
- Frei verfügbar auf Docker Hub
- Lizenzloser Modus hat Basisfunktionalität

Premium Edition
- Einspielen einer Lizenz schaltet Premium Funktionen frei

3.0

Gateway Core: Update auf 7.7

Update Breaking für JWT Config

JWKS Support (JSON Web Key Sets)

YAML Schema für Validierung und IDE Unterstützung

Diverse DSL Erweiterungen

Erweitertes Minikube-Example mit GitOps

Tutorials für Selbststudium

Release 2.1

Komplettierung der DSL

Vorteile:

- Automatisierbarkeit der Konfiguration
- Nutzung von Entwicklertools (z.B. GIT)
- Keine Workarounds über Mapping Templates

Neue 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.

```
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 Lizenz-Modell

Funktion	Community Edition (gratis)	*Premium* Edition
DevSecOps Unterstützung Container, GitOps-freundliche Konfiguration, Mgmt via K8S, Helm Charts	✓	✓
Monitoring und Reporting Strukturierte Logs, Prometheus Schnittstelle, Kibana Dashboards	✓	✓
Standard Applikationsschutz (OWASP Top 10) DoS und Bot Protection, TLS Terminierung, SQLi and XSS Filter, Cookie Schutz, Request Sanity Prüfung	✓	✓
Access Control mit Airlock IAM (separate Lizenz) Multi-Factor Authentisierung (MFA), Identity Federation & Vieles mehr	✓	✓
Erweiterter Applikationsschutz OpenAPI Schema Enforcement, Mehr Deny- und Allow-Rules, CSRF Tokens, HTTP Parameter Pollution, Multipart Parser, etc.	Log only	✓
Access Control mittels Tokens Verifikation von JSON Web Tokens (JWT), Zugriffkontrolle anhand Claims	Log only	✓
Support	Community Support	Premium Support

Community Support

Öffentliches Forum

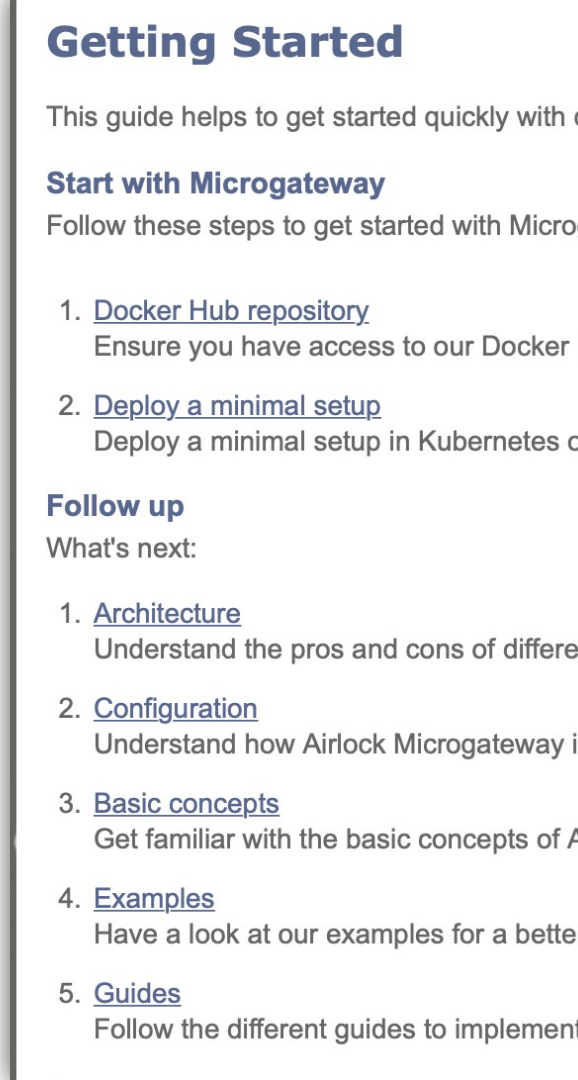
- https://forum.airlock.com/
- Benötigt Account zum Fragen stellen und kommentieren
- Airlock moderiert

Support Level seitens Airlock

- Hinweise auf Doku und Tips
- Keine Fallanalysen
- Keine garantierte Antwort(zeit)
- Komplizierte Fälle erfordern Premium Support

Dokumentation

- Microgateway Dokumentation wurde eigenständig
- Ohne Airlock Gateway Basiswissen nutzbar
- Struktur orientiert sich an Arbeitschritten eines Engineers
- Nutzt Synergien mit Academy



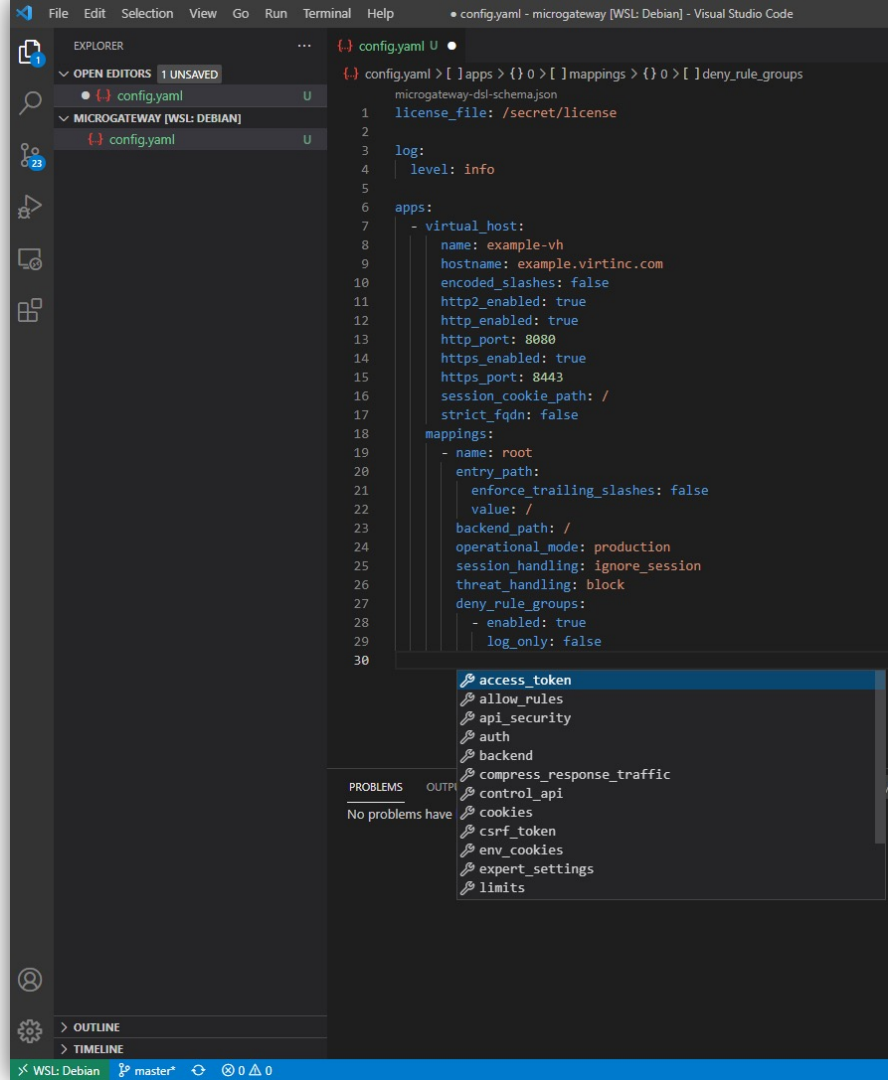
Release 3.0

JWKS (JSON Web Key Sets)

- Basis Features: JWT Access Control
- Keys lokal in “keys” Array oder
- Key Servers remote via URL
- Aktualisierung der Keys
  - bei (Re-)Load der Konfiguration
  - spätestens alle 7200s (Expert Setting)
- JWKS werden gecachet, falls Server nicht erreichbar (z.B. nach Reboot)

YAML Schema

- Validierung des Config.yaml Files
- IDEs unterstützen das im Editor
  - Doku im Tooltip
  - Syntax Check
  - Code Completion



AIRLOCK

Tutorials

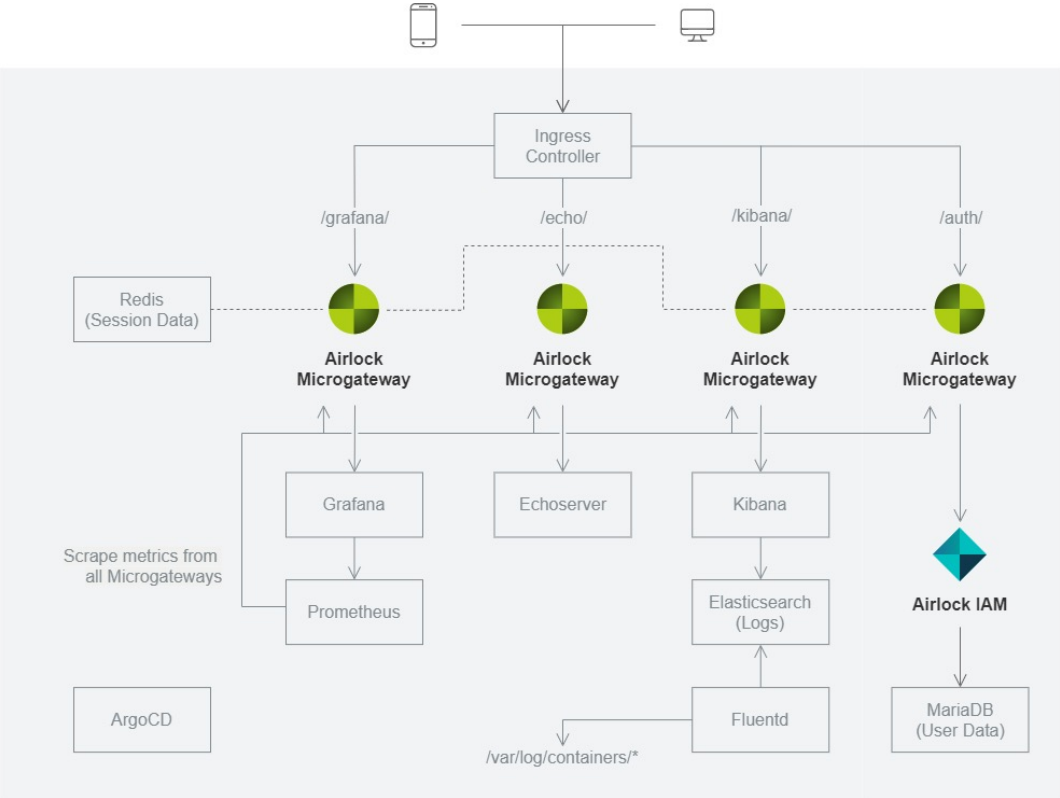
Übungen, um im Selbststudium den Microgatway kennenzulernen:

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

Demo mit Airlock Microgateway

Demo Architektur

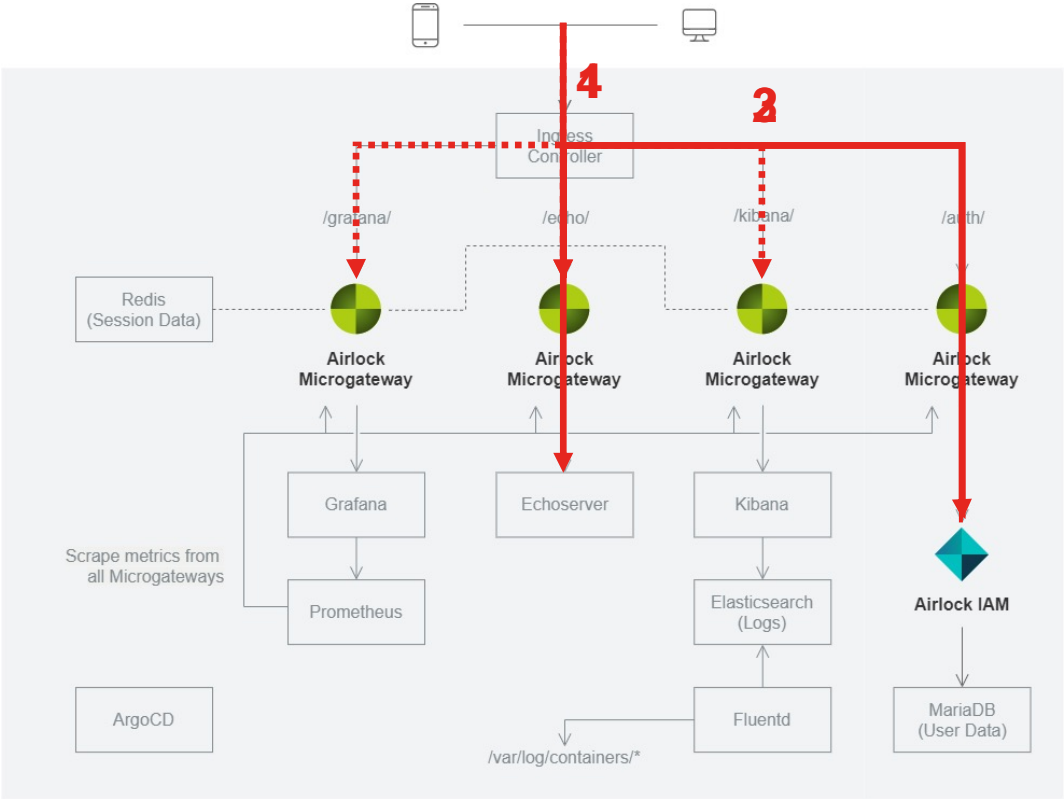
- Services geschützt mit Airlock Microgateway
- Authentisierung durch Airlock IAM
- Integration in Kibana
- Integration in Grafana



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

Anwendungsfall: Authentisierung

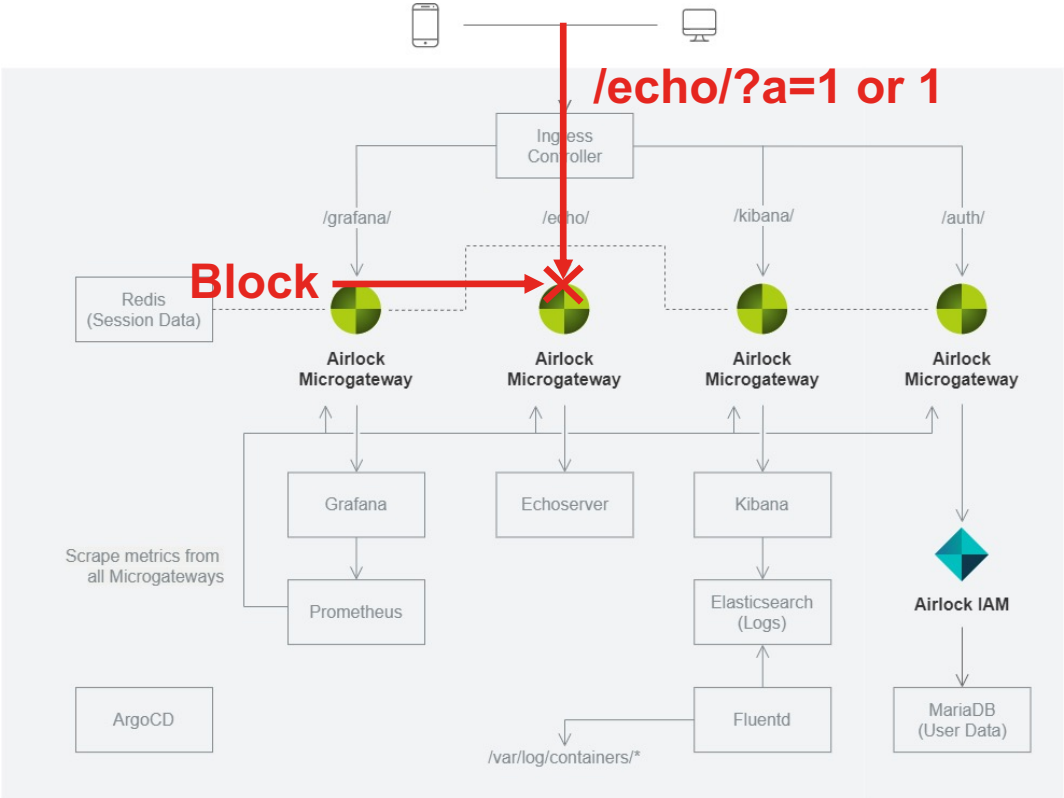
- **Vorgelagerte Authentisierung**
  - Föderieren mit JWT
  - Single Sign-On



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

Anwendungsfall: Deny Rules

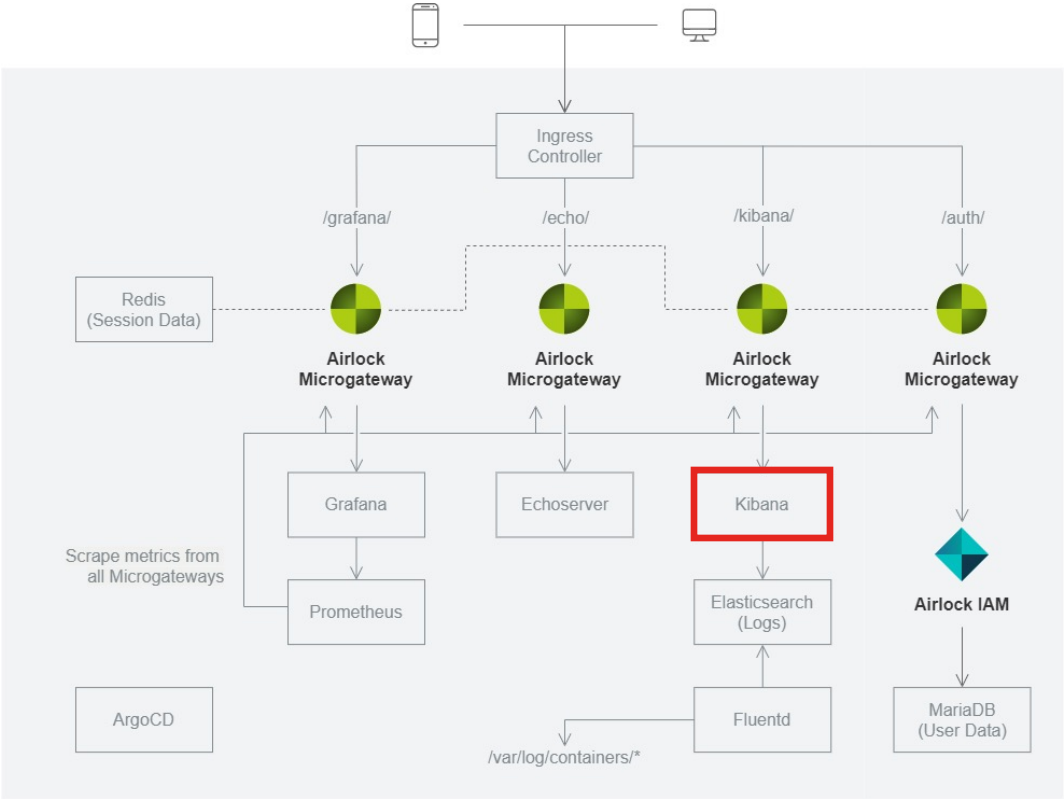
- **Deny Rules**
  - Schutz gegen OWASP Top10 Risiken



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

Anwendungsfall: Logging & Reporting

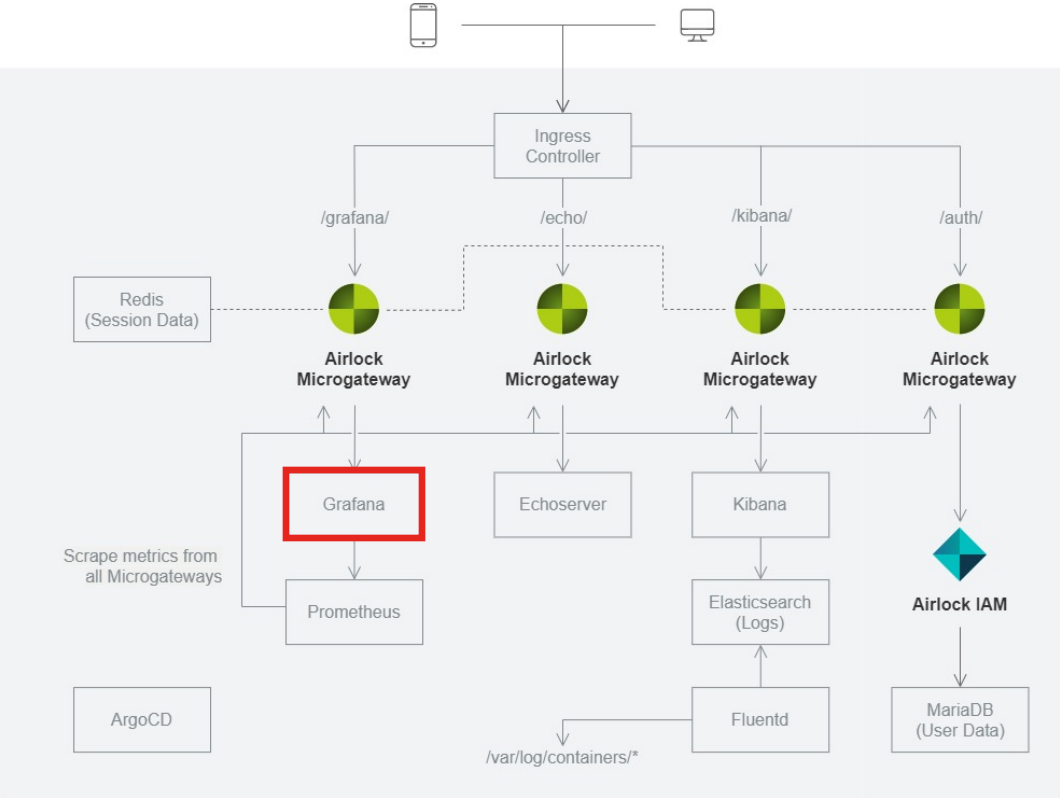
- **Logging and Reporting**
  - Einfaches Troubleshooting
  - Visualisieren des Traffics



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

Anwendungsfall: Metriken

- **Metriken**
  - Darstellen von Prometheus Metriken in Grafana



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

Demo

AIRLOCK®

Vielen Dank!

www.airlock.com/microgateway

docs.airlock.com/microgateway/latest/

Dr. Martin Burkhart
martin.burkhart@airlock.com

Stefan Dietiker
stefan.dietiker@airlock.com