AIRLOCK®

Der Wandel zu moderner Applikationssicherheit

20. Oktober 2022

Tim Rückforth
Business Development,
Ergon Informatik

Security
vs.
Time to Market

Geschwindigkeit von Innovationen ist für Unternehmen wichtiger denn je. Die Anwendungsentwickler verkürzen ihre Zyklen.
Wie kann die Sicherheit damit Schritt halten?

Gestern

Lange Release-Zyklen

Traditionelle Webseiten

Monolithen

Perimeter Sicherheit

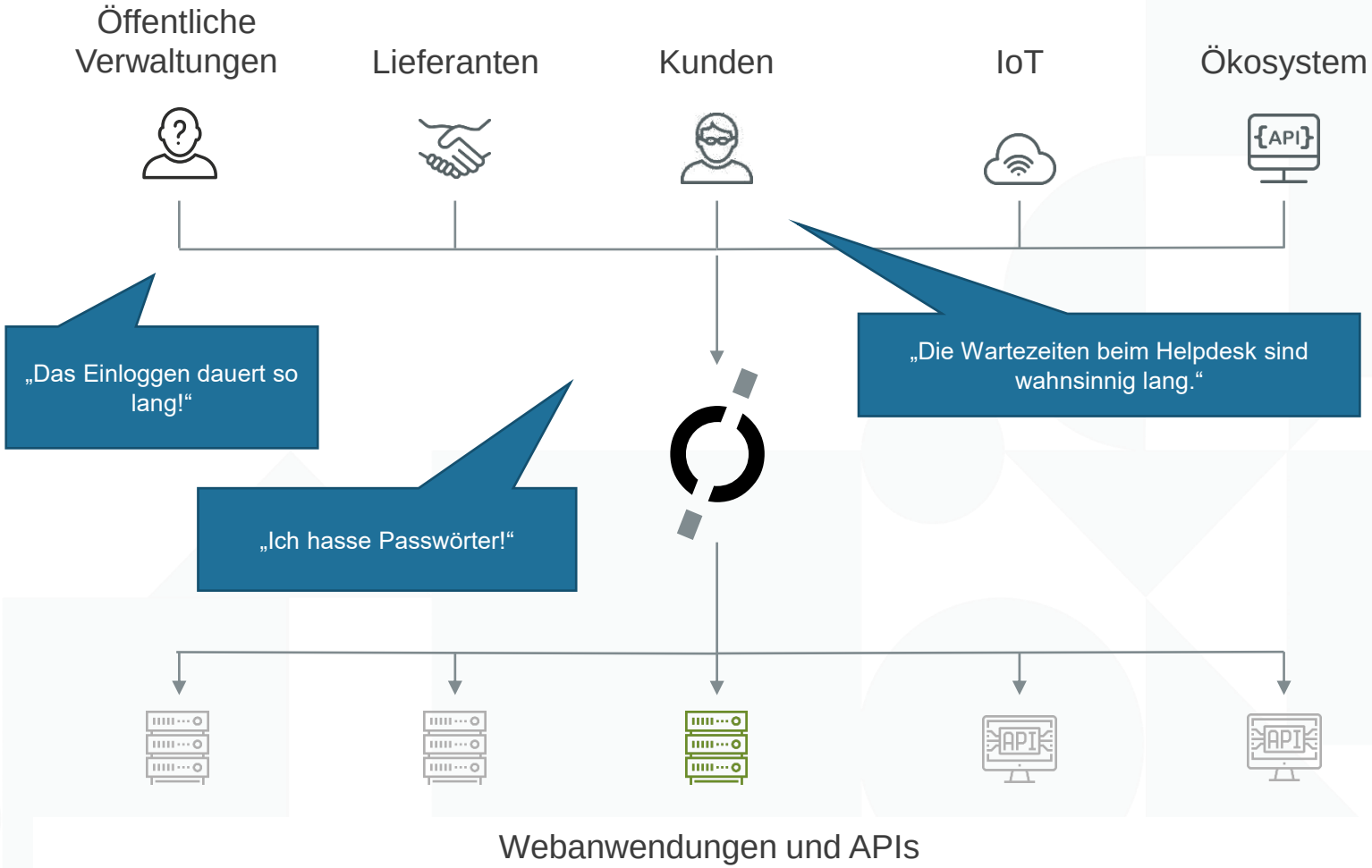
Heute

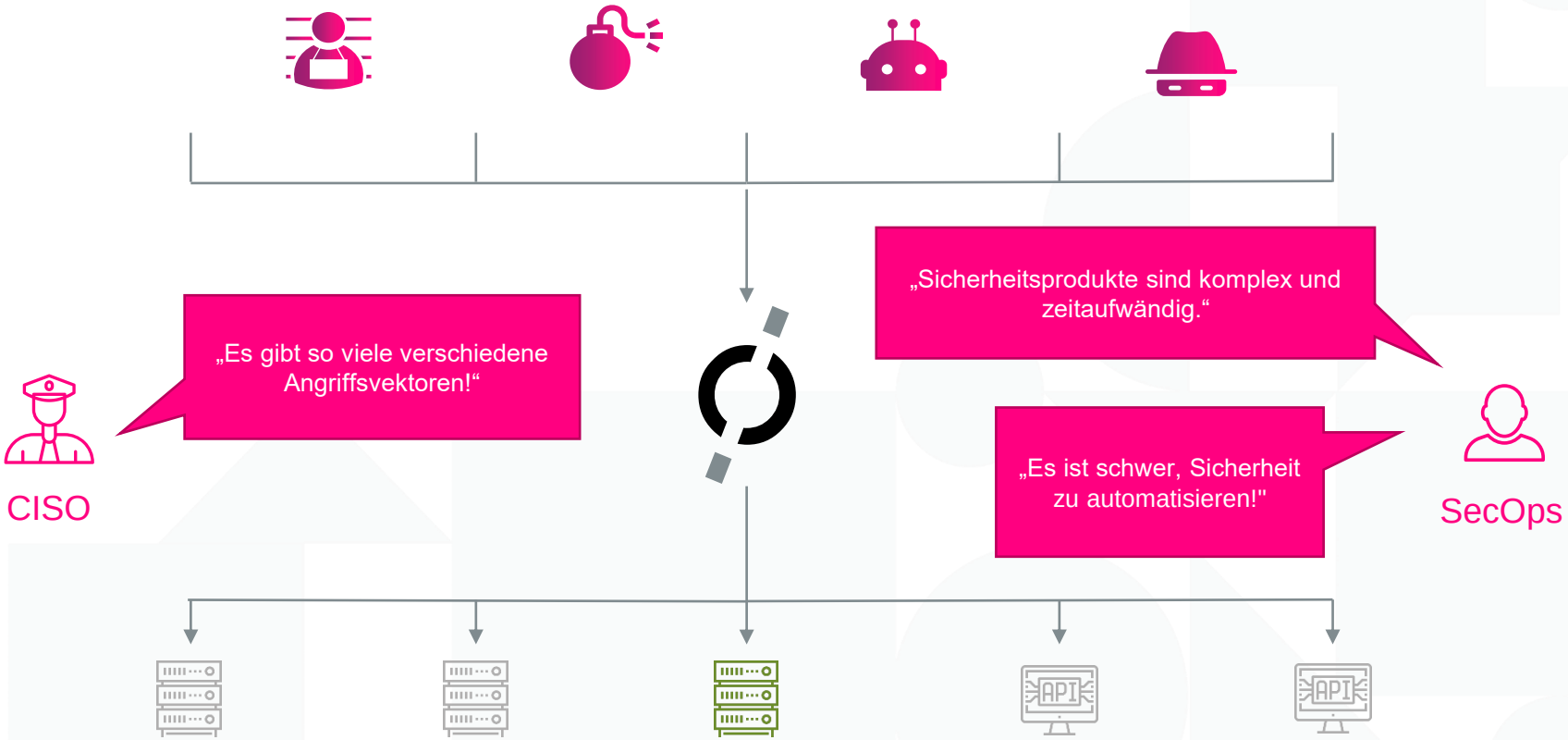
Agil, DevOps
CI/CD

APIs
Mobile Anwendungen
Single-Page-Apps

Microservices

Zero Trust


Öffentliche Verwaltungen
Lieferanten
Kunden
IoT
Ökosystem
{API}
„Das Einloggen dauert so lang!“
„Die Wartezeiten beim Helpdesk sind wahnsinnig lang.“
„Ich hasse Passwörter!“
API
API
Webanwendungen und APIs



Webanwendungen und APIs

Bekannte
Bad Guys

OWASP Top 10 +
0-Day-Angriffe

Bots &
Scanner

Unauthorized
Users

Threat
Intelligence

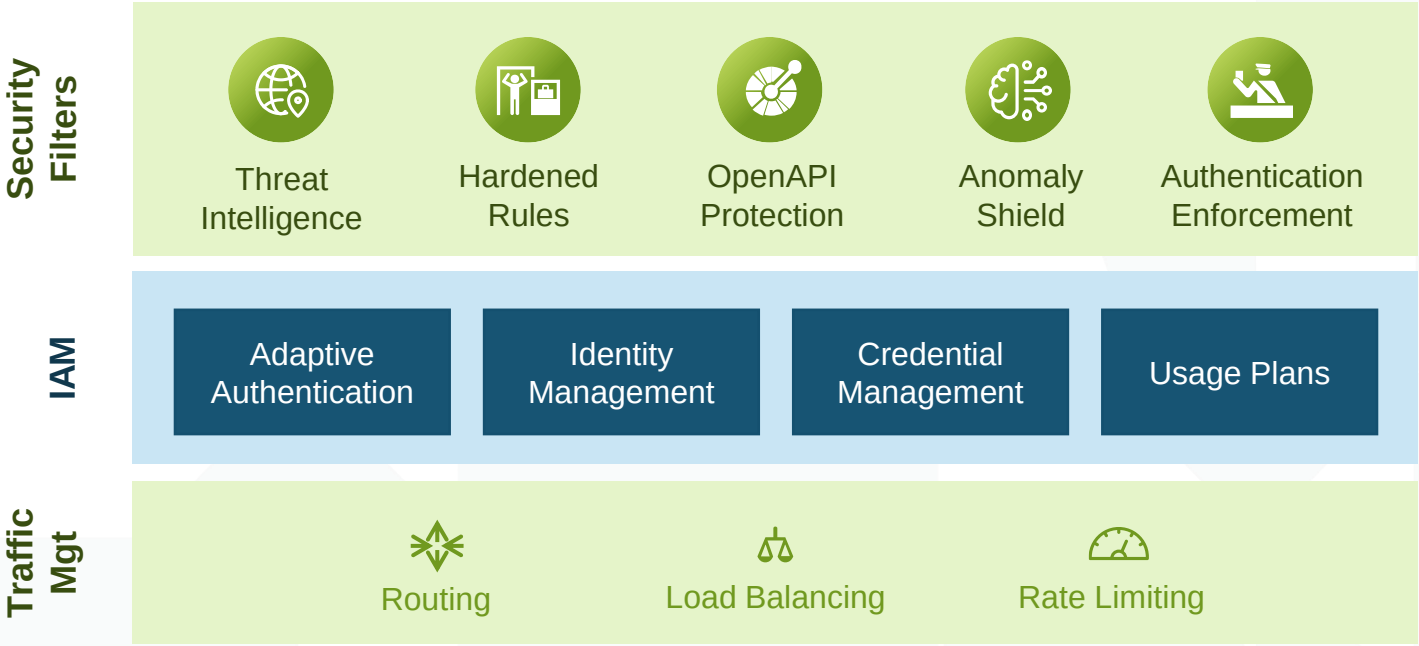
Hardened
Rules

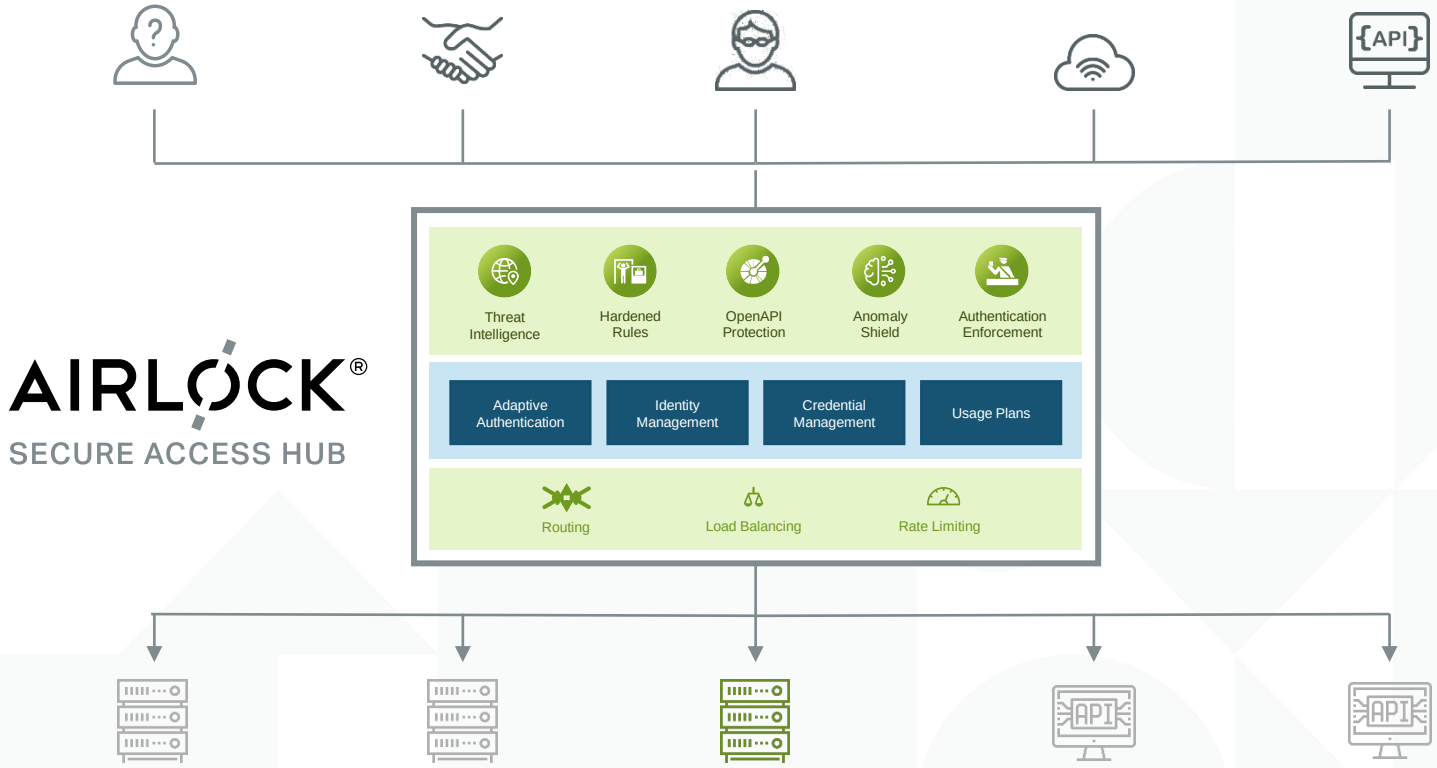
OpenAPI
Protection

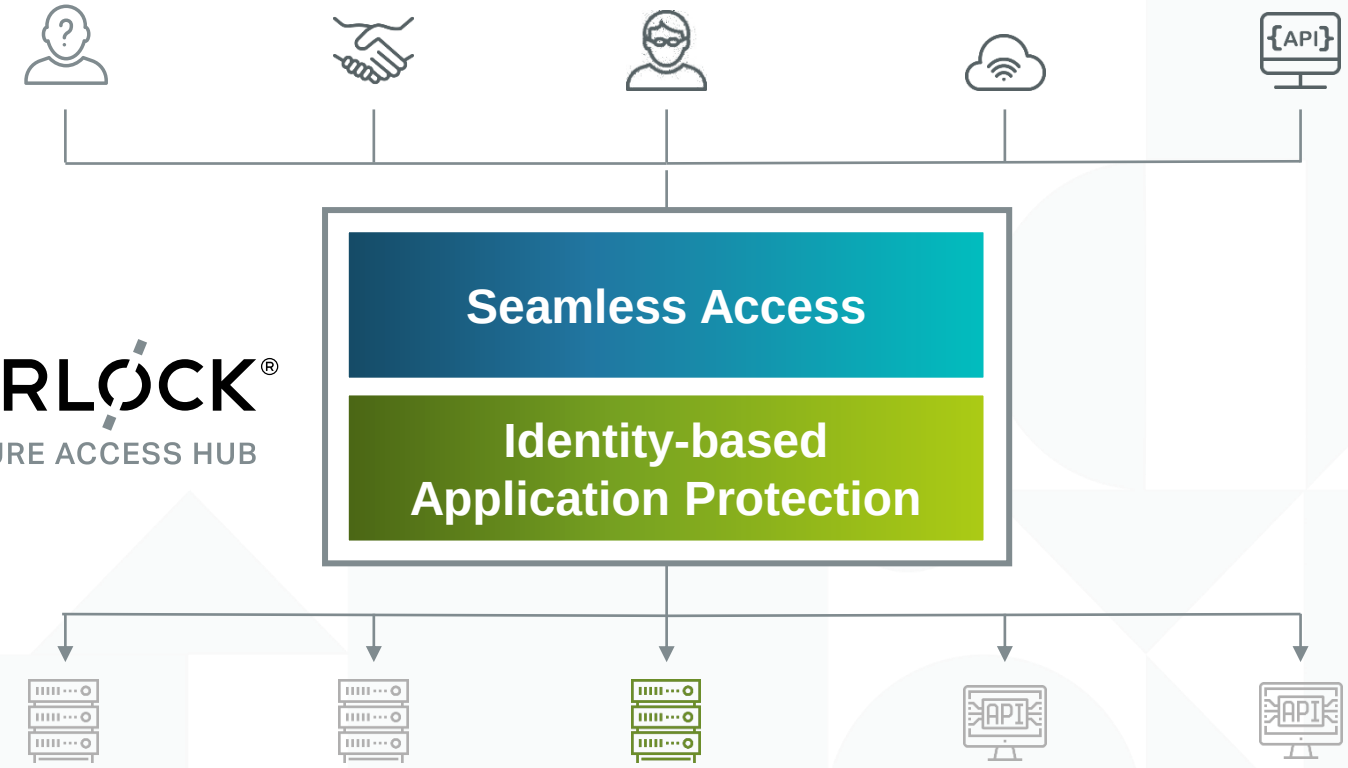
Anomaly
Shield

Authentication
Enforcement

Web Application und API Protection (WAAP)



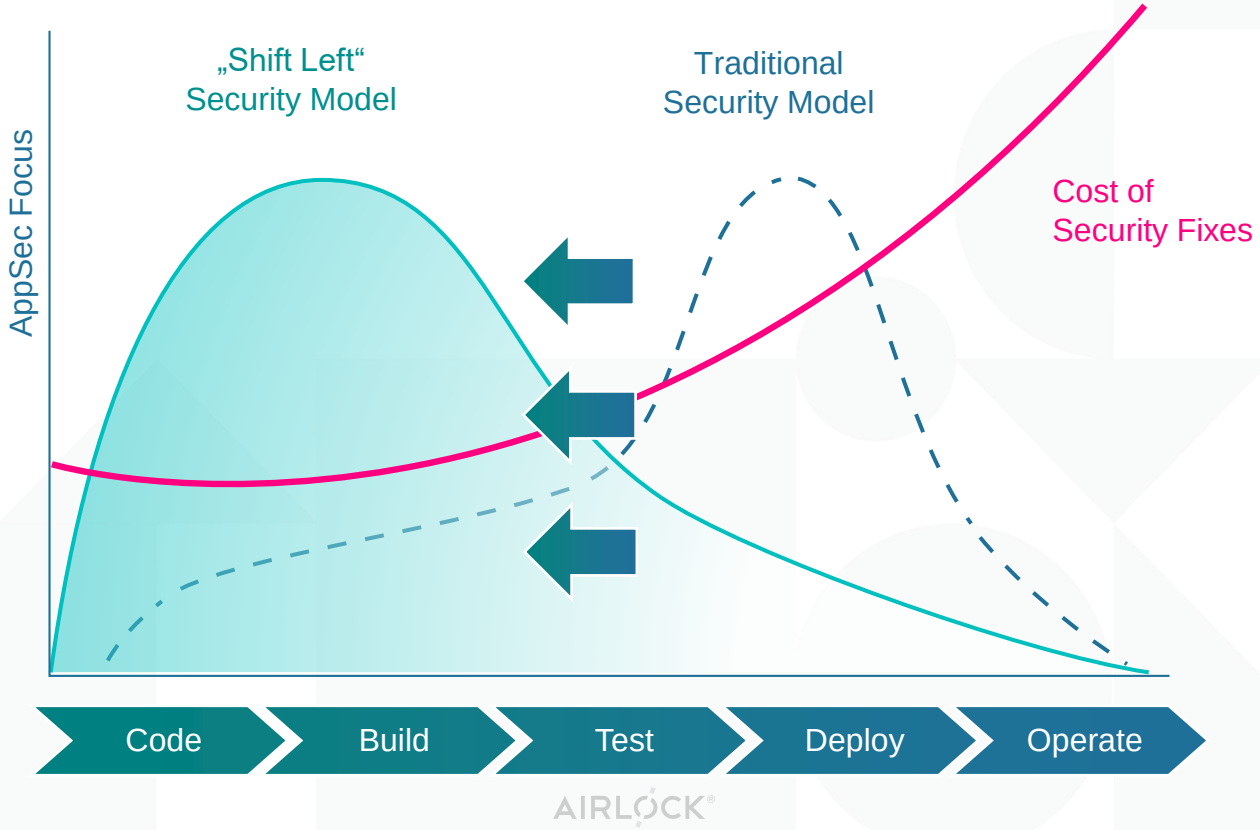

AIRLOCK®
SECURE ACCESS HUB
{API}
Threat Intelligence
Hardened Rules
OpenAPI Protection
Anomaly Shield
Authentication Enforcement
Adaptive Authentication
Identity Management
Credential Management
Usage Plans
Routing
Load Balancing
Rate Limiting
API
API



AIRLOCK®
SECURE ACCESS HUB

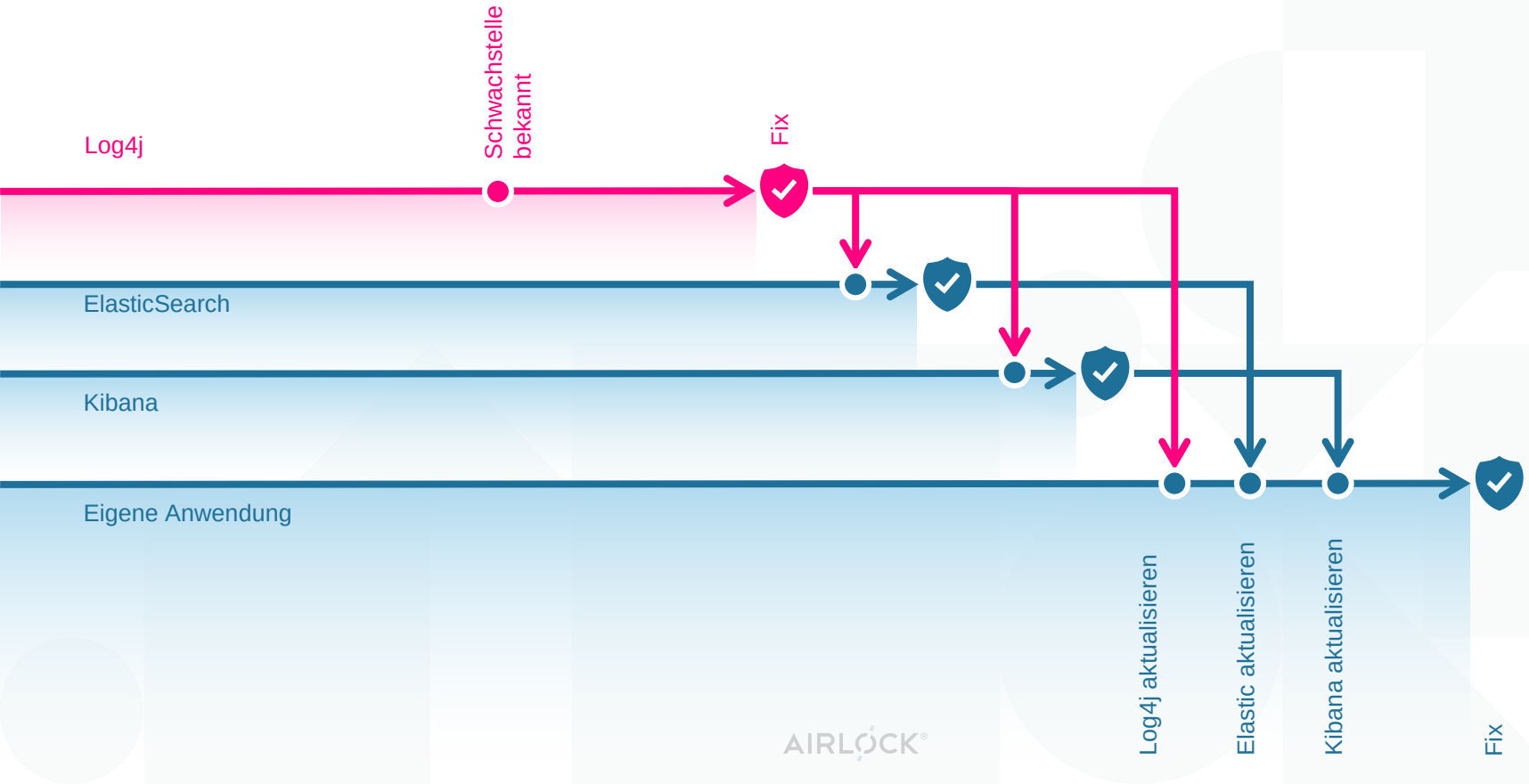
DevSecOps in der Praxis

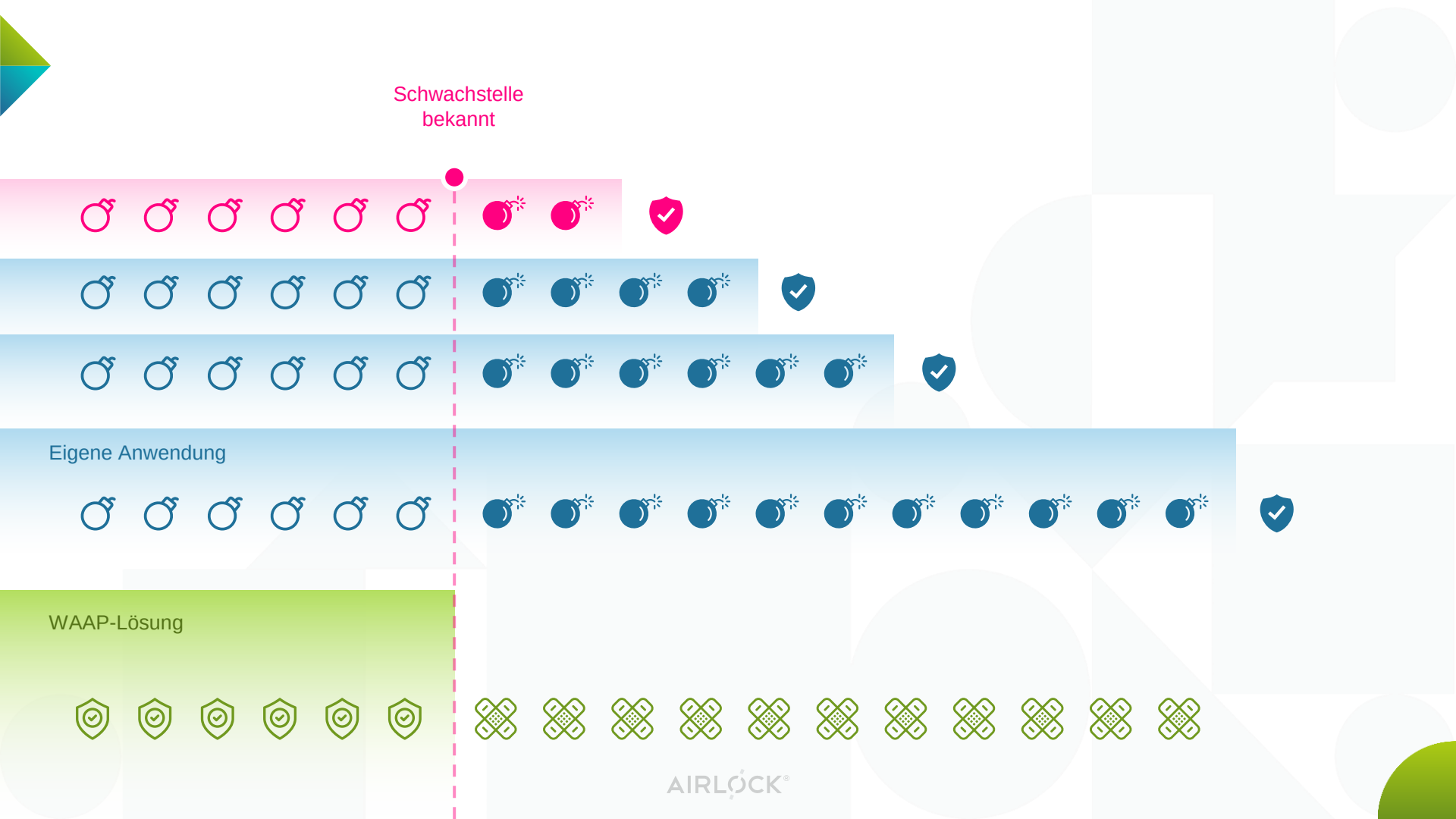
Cost of Security Fixes




APPLICATION
SECURITY
TESTING
LOG4SHELL

Open-Source-Abhängigkeiten




Schwachstelle
bekannt
Eigene Anwendung
WAAP-Lösung
AIRLOCK®

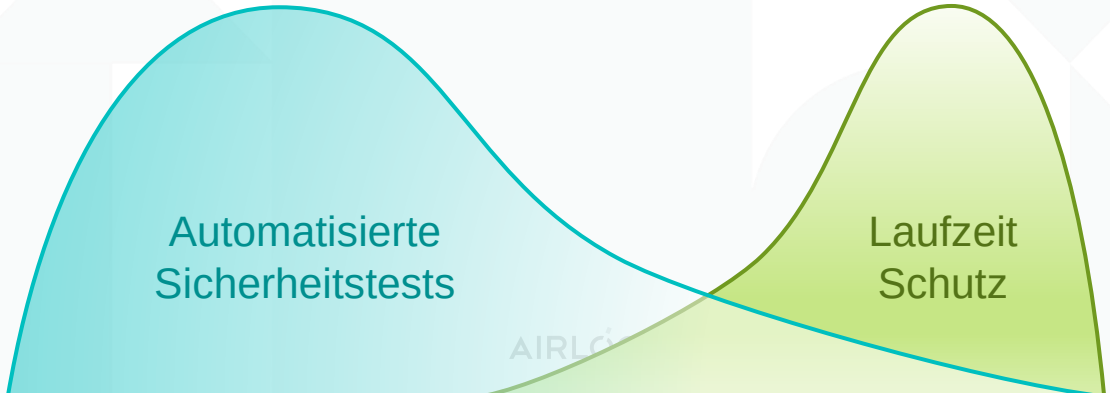
Shift Left

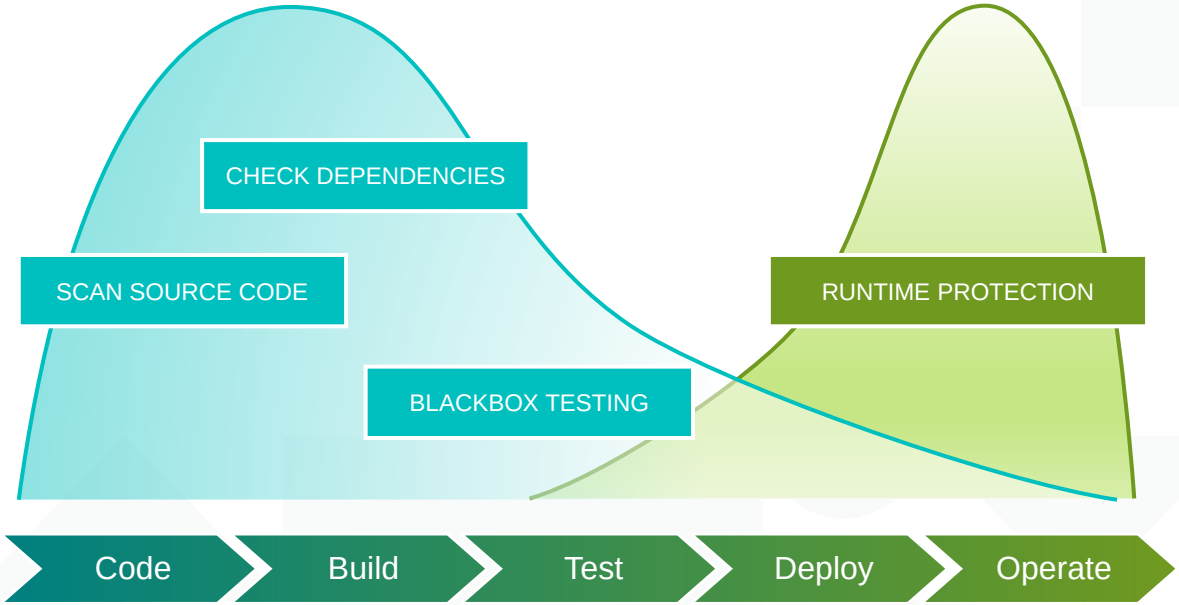
Verlagerung des Sicherheitsschwerpunkts an den Anfang des Lebenszyklus der Softwareentwicklung und -bereitstellung

Shield Right

Schützen Sie die Anwendungen und APIs zur Laufzeit und darüber hinaus.

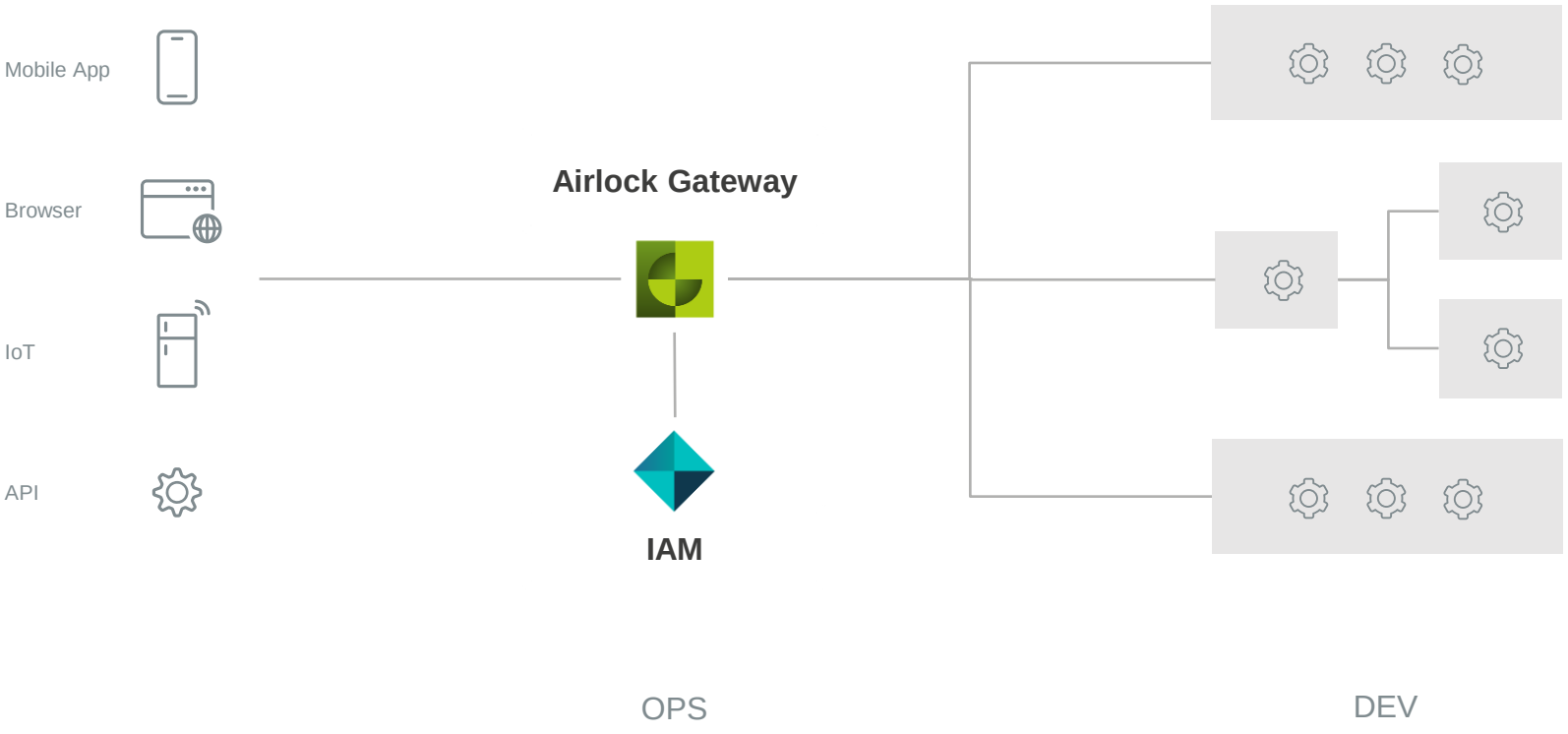
- Entschärfung unbekannter Angriffe
- Virtuelles Patchen
- Zeit zum Patchen gewinnen, Kosten sparen



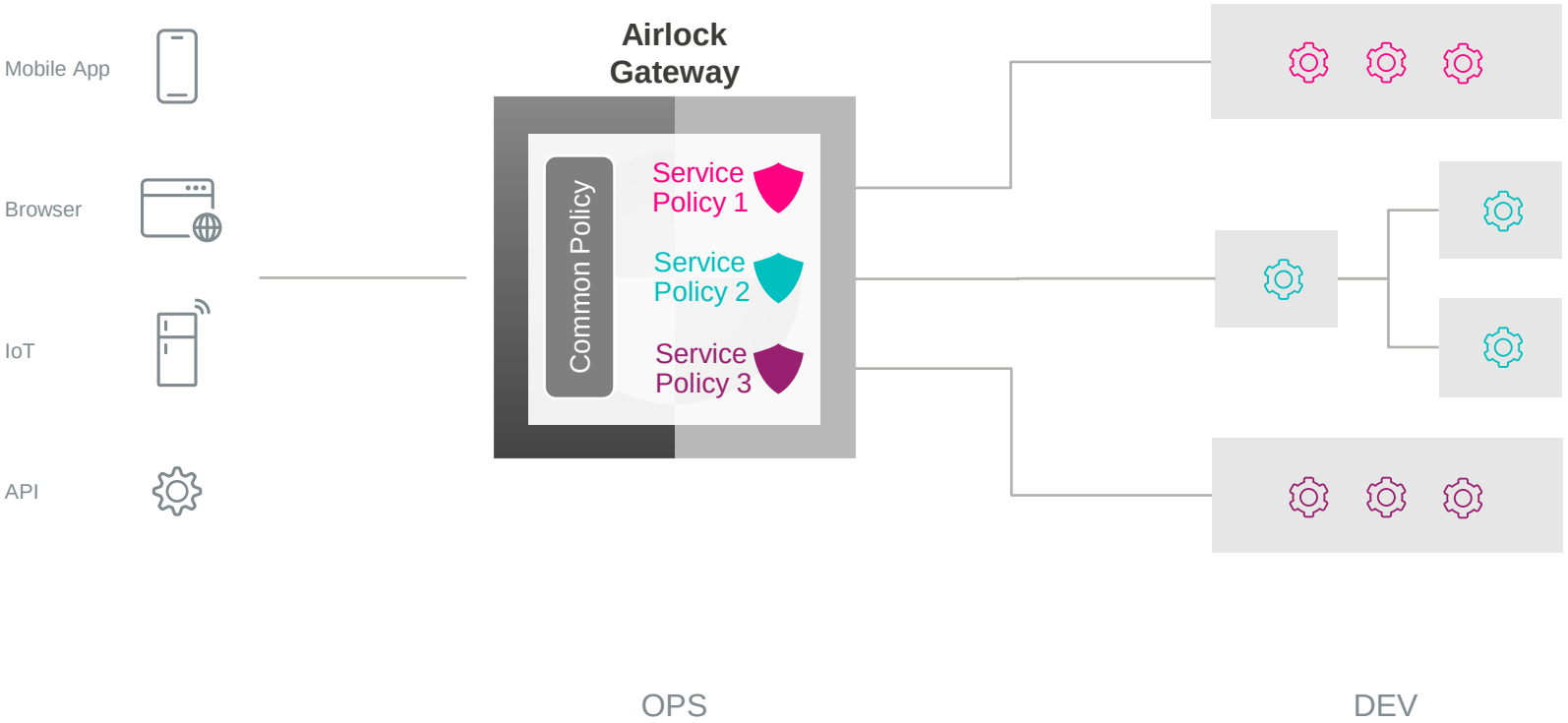


Security in allen Phasen
= DevSecOps und Zero Trust

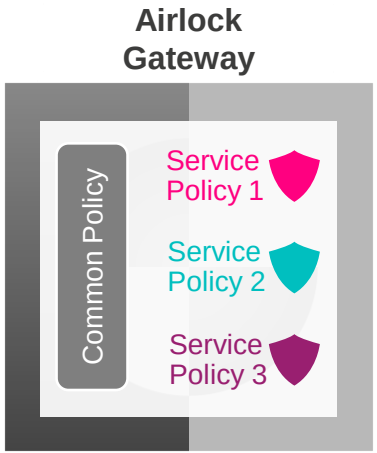
Traditionelle Architektur



Der Betrieb ist für alle Security Policies verantwortlich



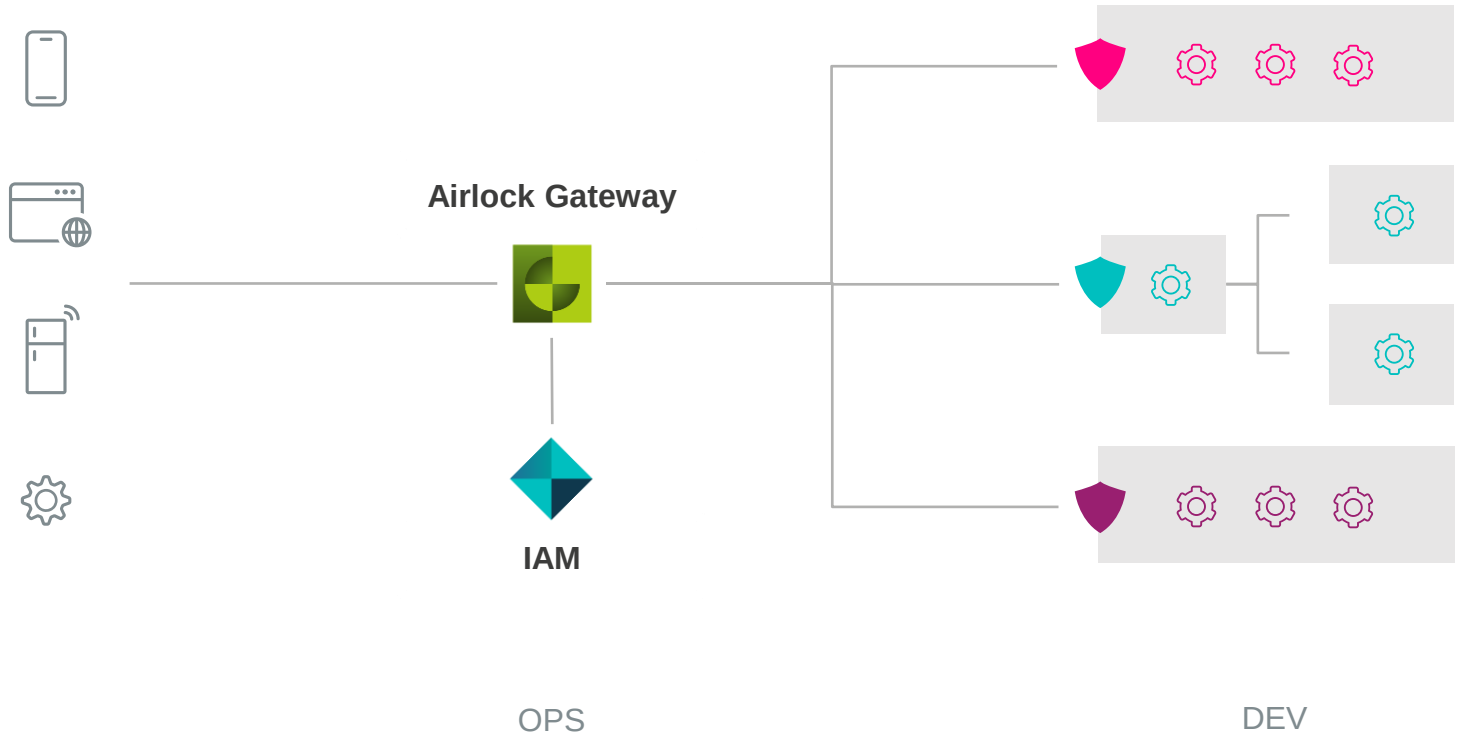
Ops ist für alle Sicherheitsrichtlinien zuständig



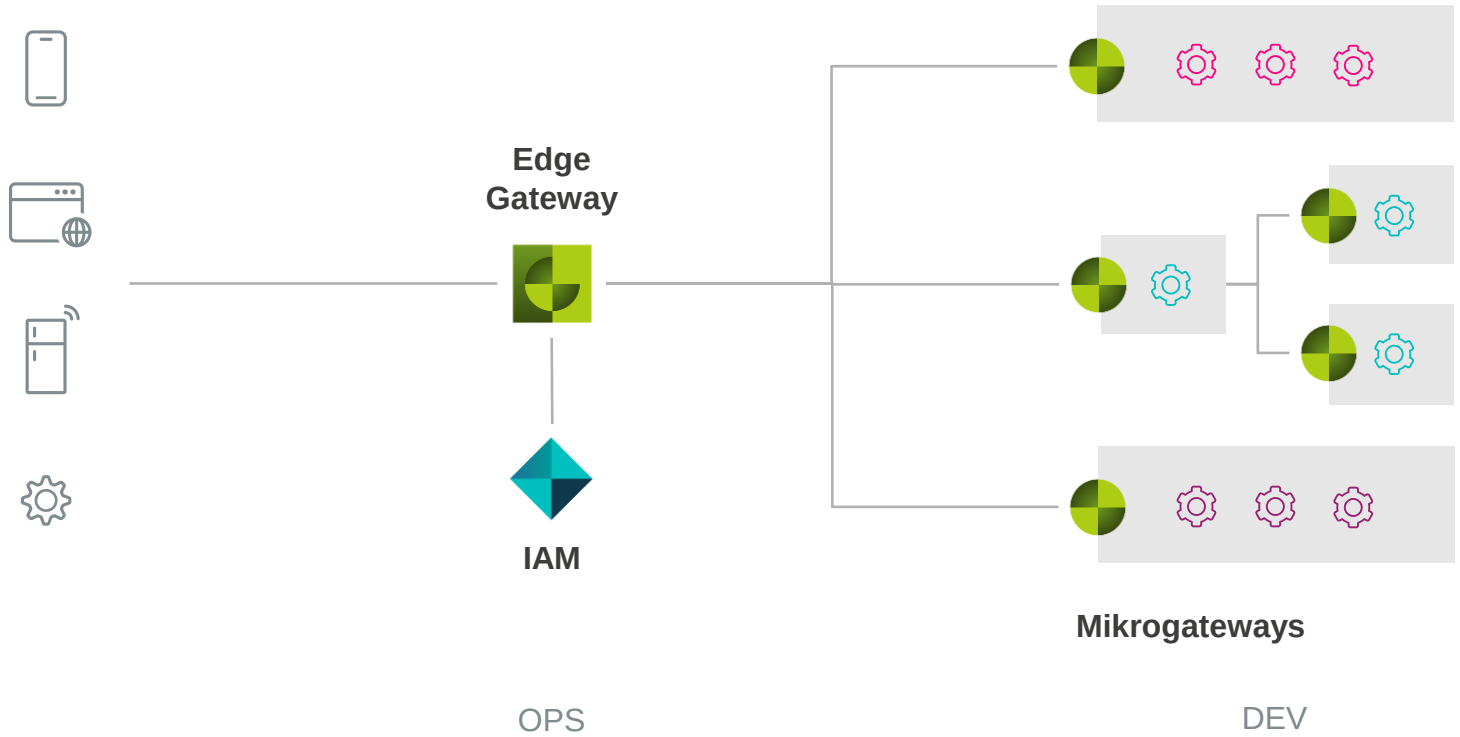
Probleme

- Integration/Prüfung erfolgt sehr spät
- Ops wissen nicht viel über jeden Dienst
- Lange und kostspielige Verzögerungen
- Sec/Ops wird beschuldigt

App-Teams besitzen Service-spezifische Security Policies



Mini-WAF für jede API und jeden (Mikro-) Service: Microgateway



Microgateway: Cloud-native

kubernetes

EKS

Amazon
Elastic Kubernetes Service

AKS

Azure
Kubernetes Service

GKE

Google
Kubernetes Engine

Airlock Microgateway

Kontinuierlicher
Anwendungsschutz
für die DevSecOps-Welt

- ☑ Frühzeitige Integration während der Entwicklung und der Tests
- ☑ Automatisierung (alles als Code)
- ☑ Zero Trust durchsetzen