AIRLOCK®

Der Wandel der Applikationssicherheit

Oktober 2022

Thomas Kohl
Senior Business Development Manager
International

Airlock – why we are experts

20+ Years

Experiences in Application Security and Access Management

380+

Employees at Ergon, incl. 75 Airlock staffs

Die Bundesregierung

Federal Republic of Germany assigns 4-year framework contract to Airlock in 2021 to deliver security solutions!

International References

in all industries

More than 20 Mio. active identities & +30.000 protected applications

600+

Customers in 15+ countries incl. Middle East, Asia & Australia

250+

Banking customers in Europe

Award Winnings

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2022

SILBER WEB APPLICATION FIREWALLS (WAF) SECURITY INSIDER AWARD 2021

itsecurity AWARD 2019 www.it-security-award.com

Analysts

PRODUCT LEADER ACCESS MANAGEMENT & FEDERATION KUPPINGERCOLE ANALYSTS AG, FEBRUARY 2019

MARKET LEADER ACCESS MANAGEMENT & FEDERATION KUPPINGERCOLE ANALYSTS AG, FEBRUARY 2019

MARKET CHAMPION ACCESS MANAGEMENT & FEDERATION KUPPINGERCOLE ANALYSTS AG, FEBRUARY 2019

Security vs Time to Market

Business speed is more important than ever.
Application developers are shortening their cycles.
How can security keep the pace?

Yesterday

Long
Release
Cycles

Traditional
Websites

Monoliths

Perimeter
Security

Today

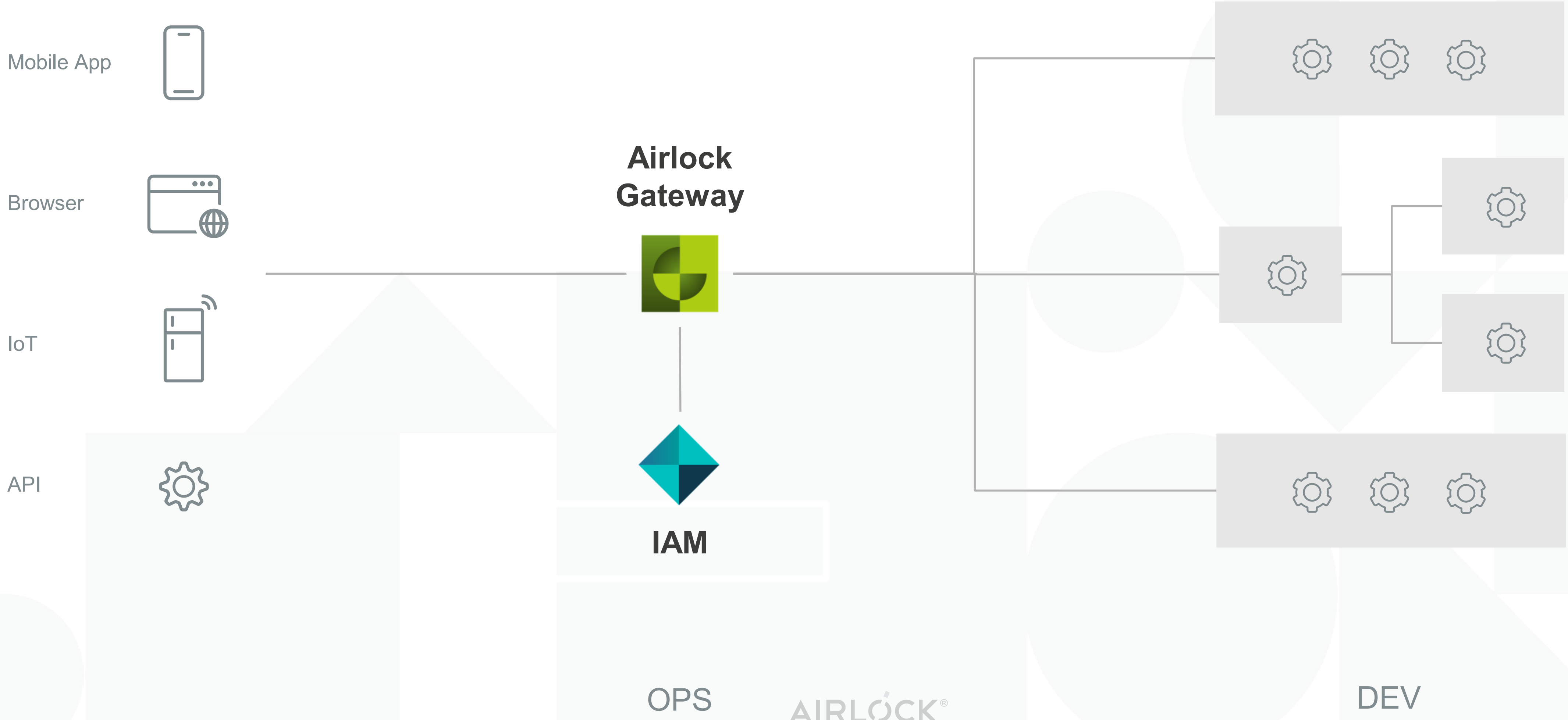
Agile, DevOps
Continuous Delivery

APIs
Mobile Apps
Single-Page Apps

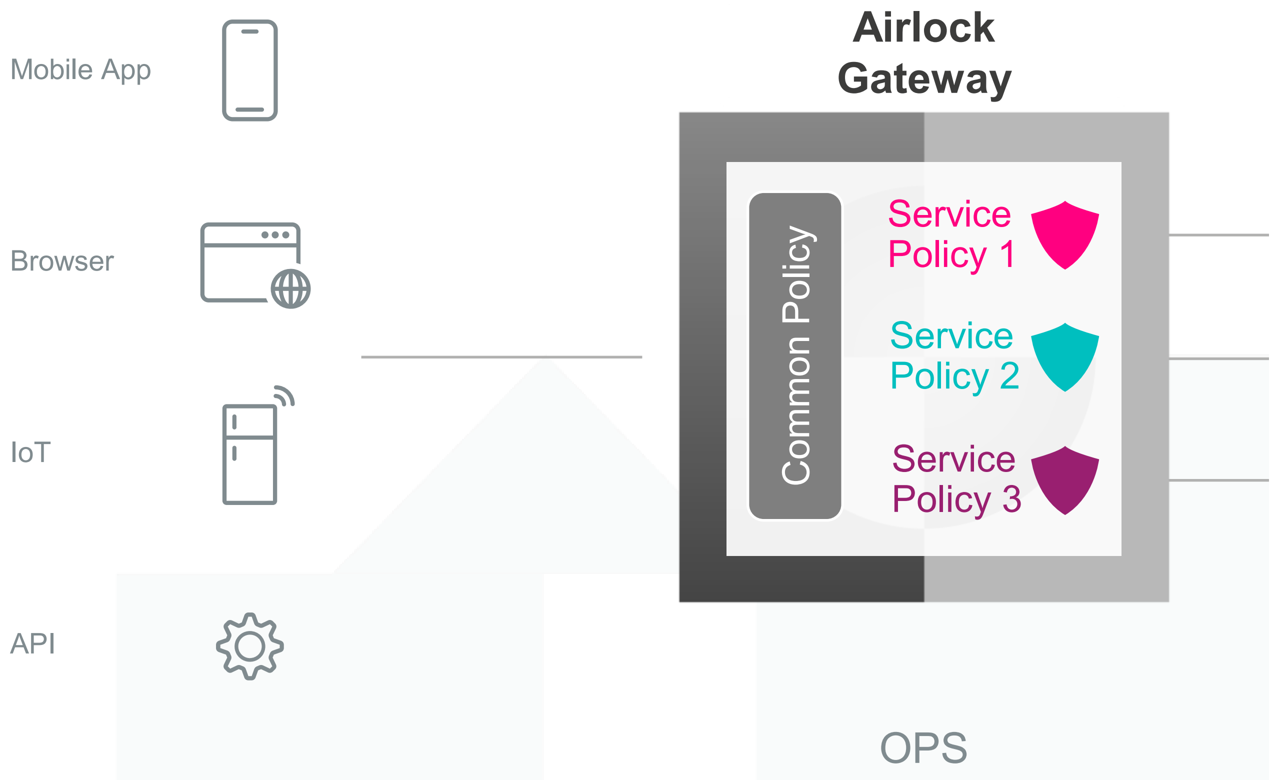
Microservices

Zero Trust

Traditional Architecture



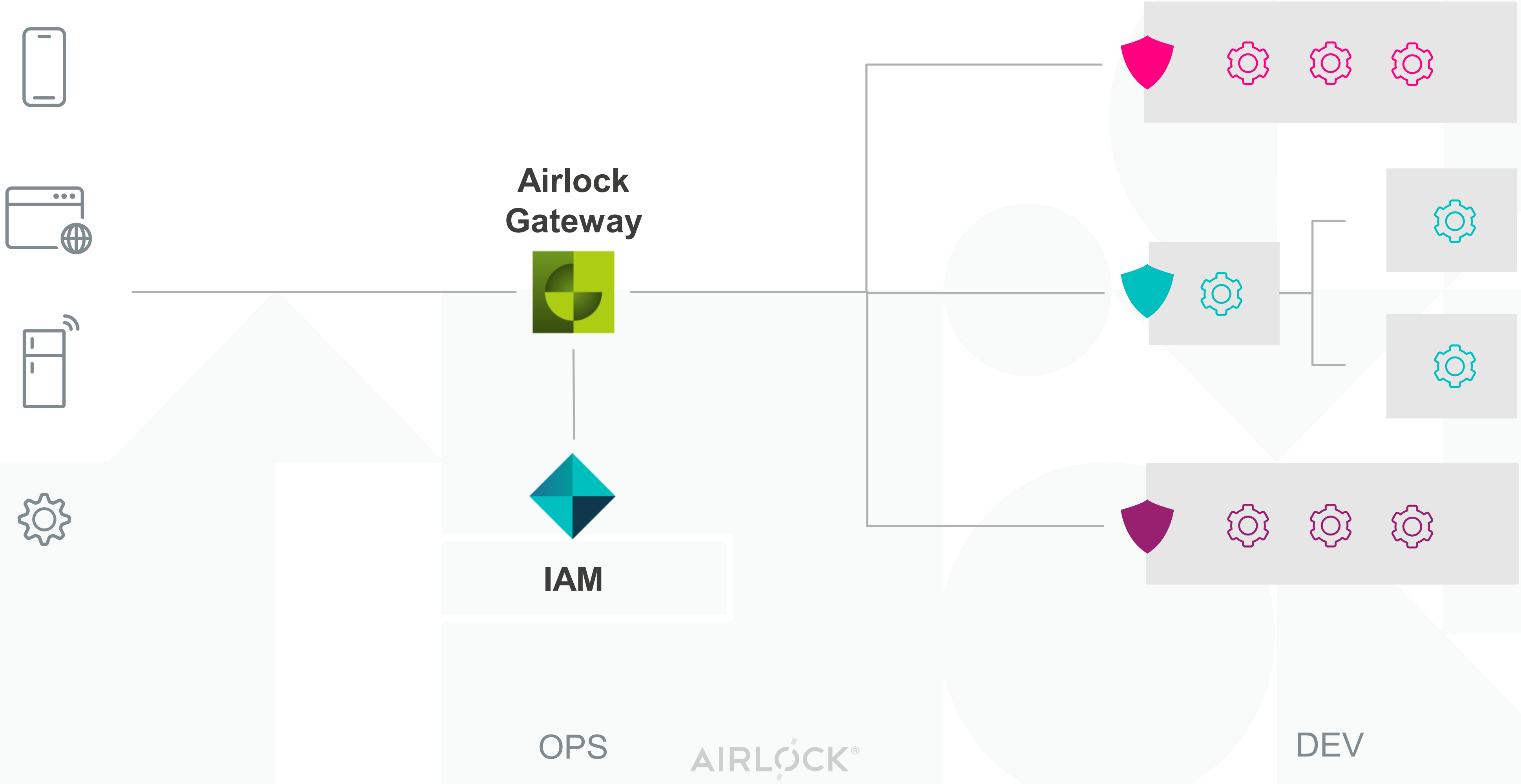
Operations owns all security polic



Problems

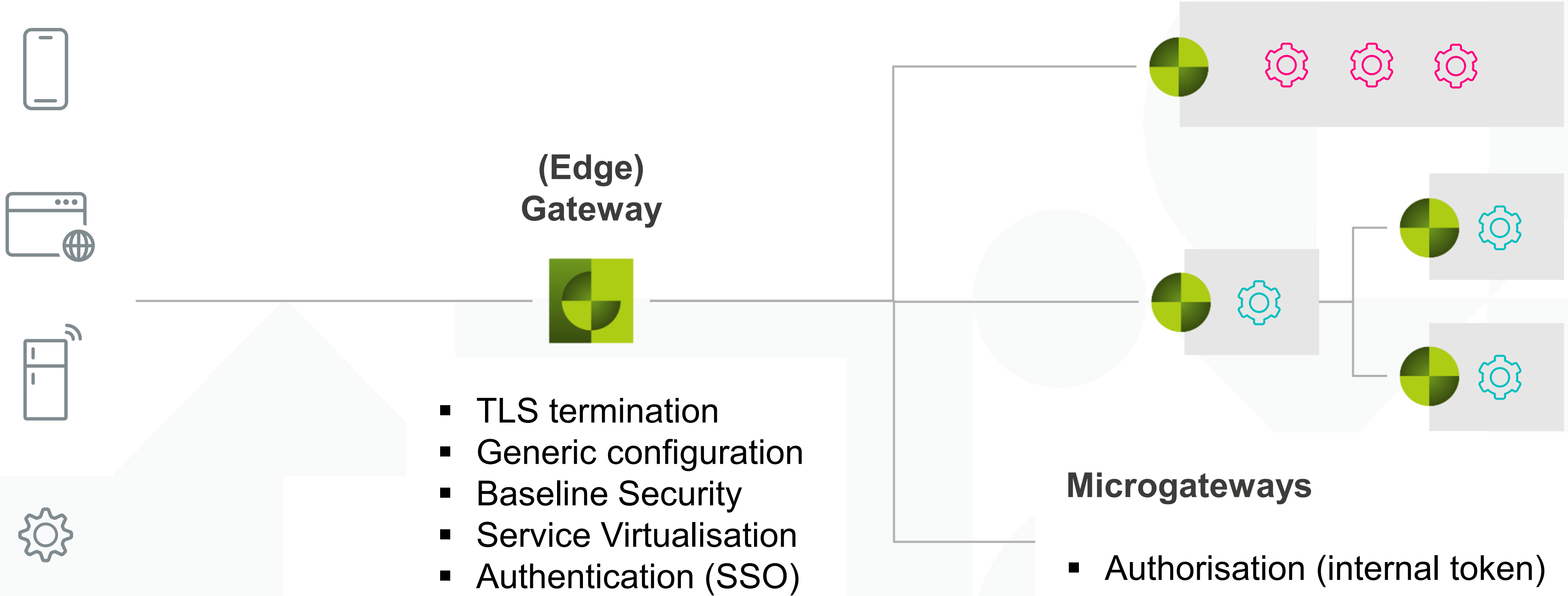
- Integration/Testing is done very late
- Ops do not know much about each service
- Long and costly delays
- Sec/Ops is blamed

App teams own service-specific security policies



AIRLOCK®

Mini-WAF for each API or (Micro-) Service: **Microgateway**



(Edge) Gateway

- TLS termination
- Generic configuration
- Baseline Security
- Service Virtualisation
- Authentication (SSO)
- API Usage Plans

Microgateways

- Authorisation (internal token)
- Attack blocking (OWASP Top 10)
- **Enforce Service Policy with OpenAPI**

OPS

DEV

Anomaly Shield

Field-proven protection against automated attacks

Different perspectives

Known
Attack Patterns

Request Analysis

Malicious content?
Known Attacker?

Deny Rules
IP Blacklists

Unknown +
Automated Attacks

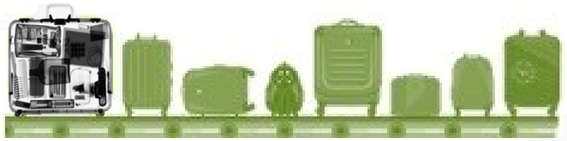
Session Analysis

Deviation from "normal"
user behaviour?

Advanced
Machine
Learning

Mutual complementation

Airlock Gateway

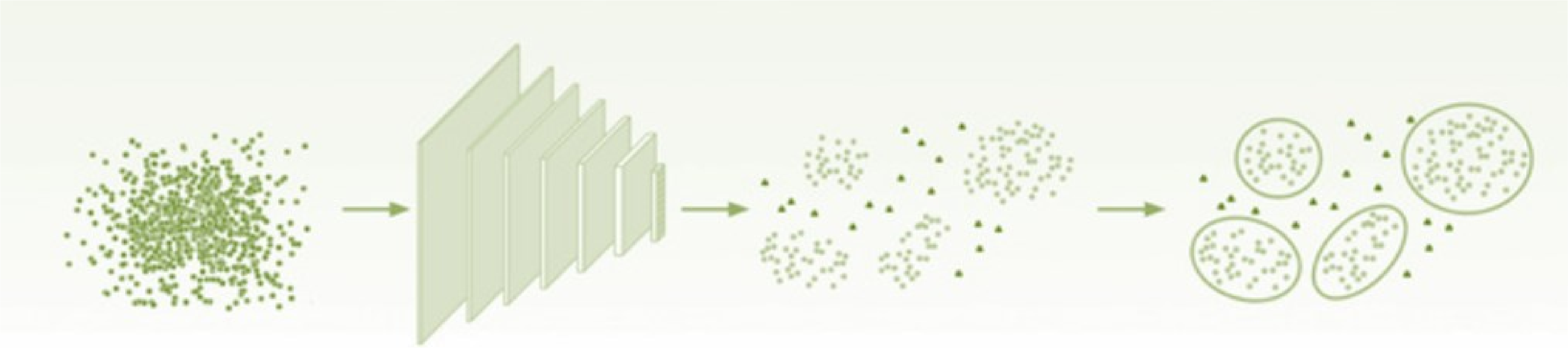


Deny Rules
IP Blacklists

+

Advanced
Machine
Learning

Unsupervised Learning



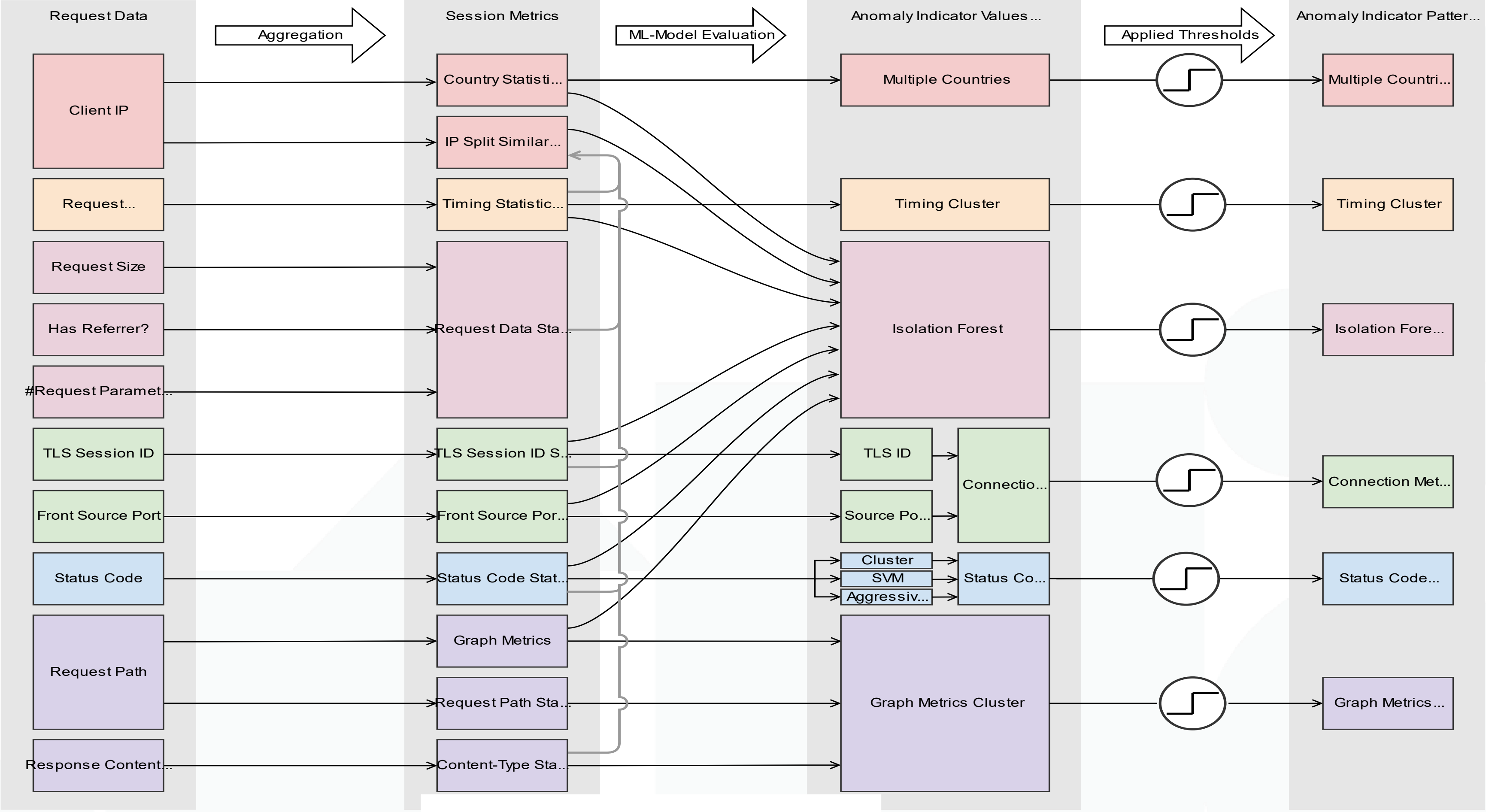
Stage 1

Unsupervised representation learning

Stage 2

Cluster conditioned Outlier detection

ML – Anomaly Shield



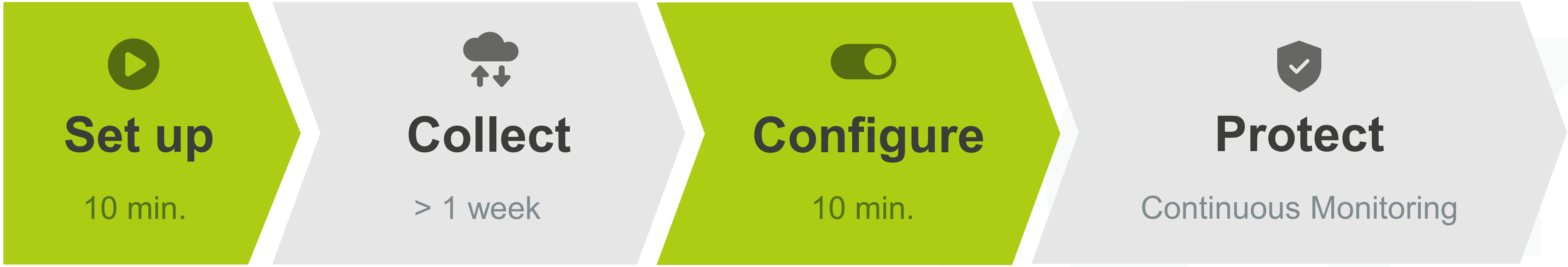
Anomaly Indicators

- ● Multiple Countries
- ● Timing Cluster
- ● Isolation Forest
- ● Connection Metrics
- ● Status Code Meta
- ● Graph Metrics Cluster

PhD in Data Science??

Save yourself the time!

Airlock Anomaly Shield



Set up

10 min.

Collect

> 1 week

Configure

10 min.

Protect

Continuous Monitoring

- Check prerequisites (e.g. session handling)
- Switch on Anomaly Shield
- Exclude pentests and vulnerability scans

- Automatic data collection
- At least 10,000 sessions
- As much “real" traffic as possible from the productive environment.

- Use default sensor configuration
- Start training
- Use generated model

- Protection is active
- Usual monitoring + SIEM
- Kibana and Elastic Search
- Adjust sensitivity if necessary
- No re-learning for normal app adjustments

Thank you very much!

Your personal contacts:

Thomas Kohl
Senior Business Development Manager International
Tel.: +49 170 1613250
Email: thomas.kohl@airlock.com