Die Zukunft der Applikationssicherheit: Continuous Adaptive Trust

Oktober 2022

Thomas Kohl
Senior Business Development Manager
International

Ergon Informatik AG

Core Business:

Business Software Development

Founded: 1984

Employees: 380+*

Learners: 10

Turnover 2021: CHF 63 Mio.

Headquarter: Zurich (Switzerland)

* 84% with university degree

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!

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

International References

in all industries

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

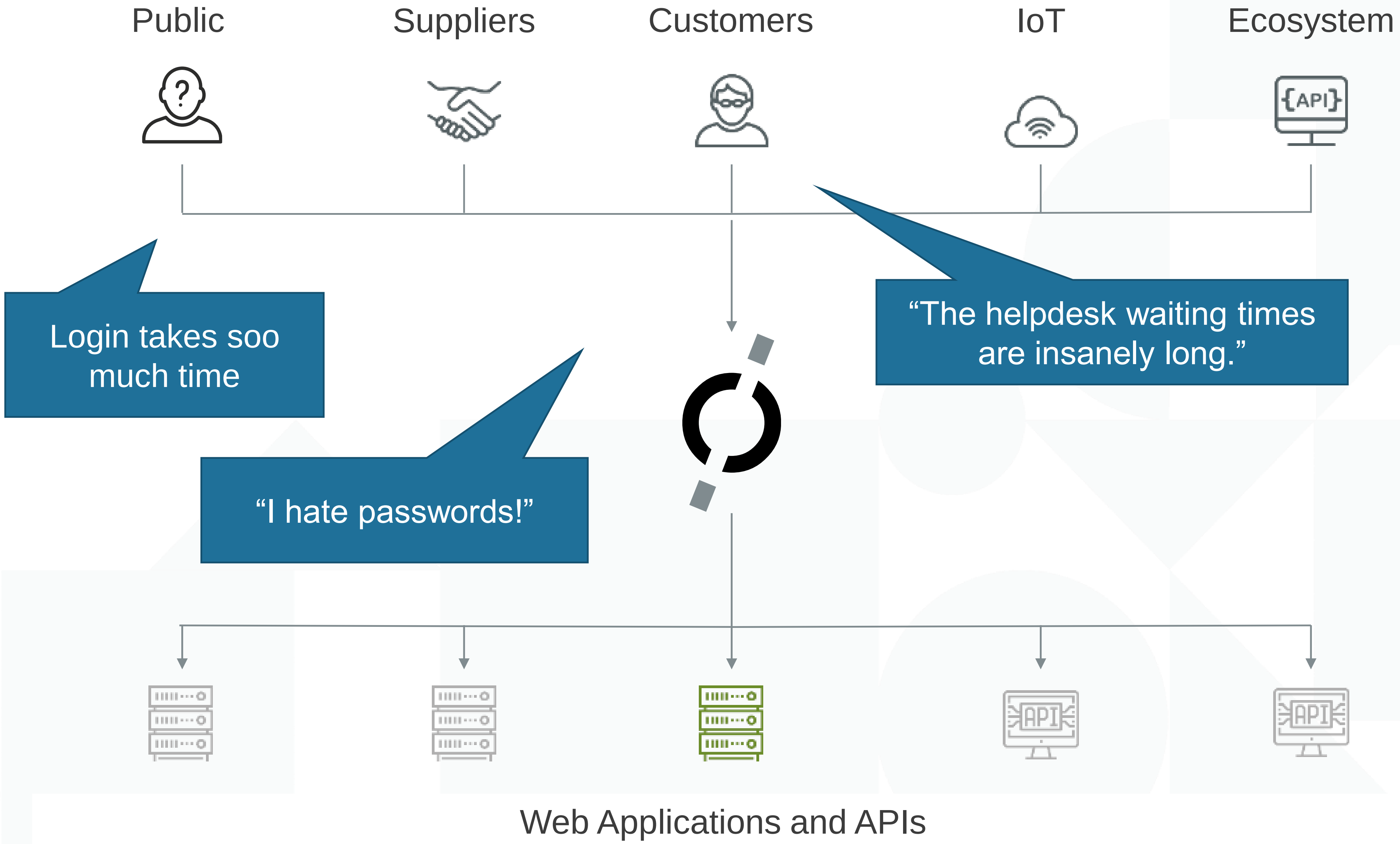
Analysts

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

External challenges

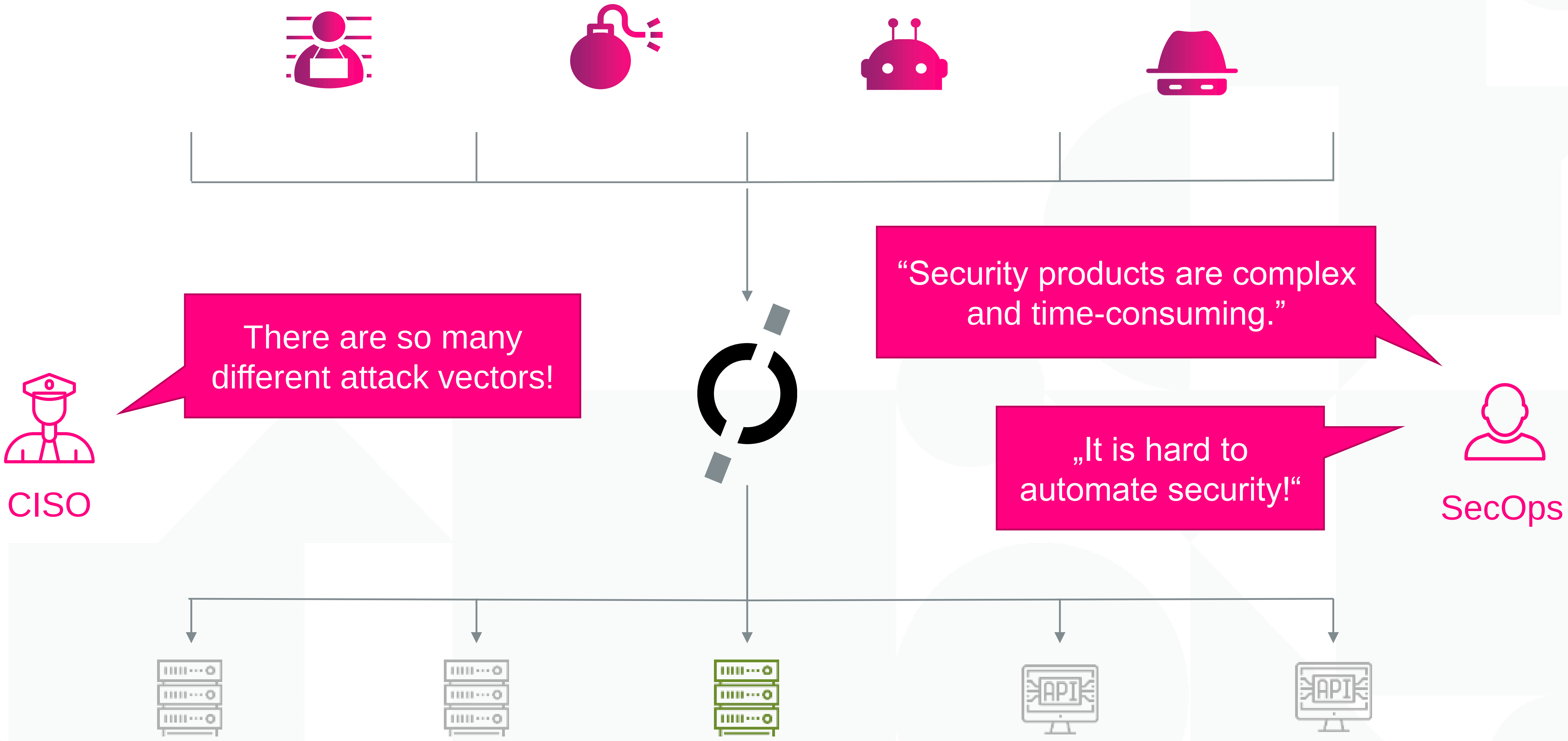


Login takes soo much time

“I hate passwords!”

“The helpdesk waiting times are insanely long.”

Internal challenges



There are so many different attack vectors!

CISO

“Security products are complex and time-consuming.”

„It is hard to automate security!“

SecOps

Web Applications and APIs

Different kinds of attack vectors and how to protect

Known Bad Guys

OWASP Top 10 + 0-day attacks

Bots & Scanners

Unauthorized Users

Threat Intelligence

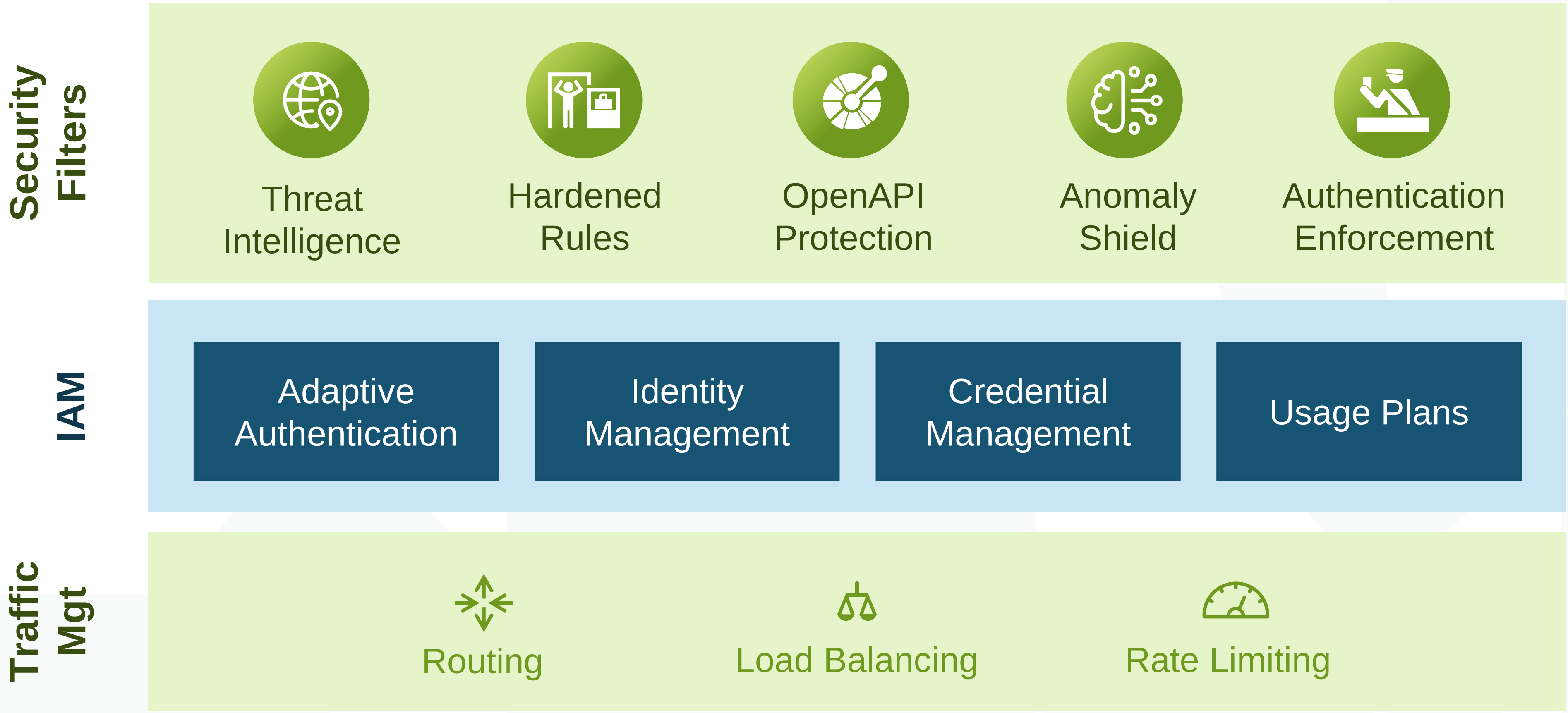
Hardened Rules

OpenAPI Protection

Anomaly Shield

Authentication Enforcement

Web Application and API Protection (WAAP)



Security Filters

Threat Intelligence

Hardened Rules

OpenAPI Protection

Anomaly Shield

Authentication Enforcement

IAM

Adaptive Authentication

Identity Management

Credential Management

Usage Plans

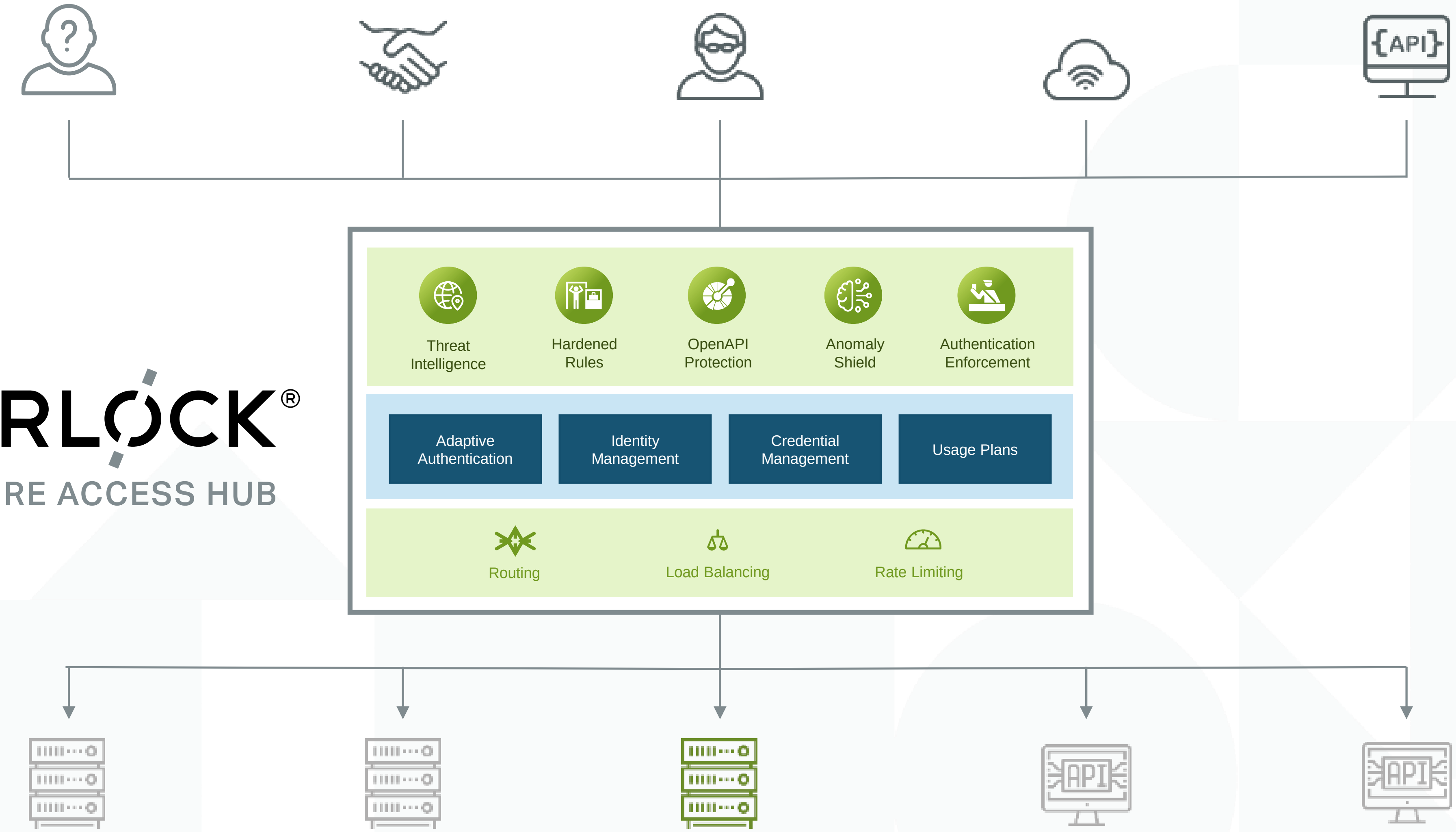
Traffic Mgt

Routing

Load Balancing

Rate Limiting

A modern WAAP solution



AIRLOCK®

SECURE ACCESS HUB

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

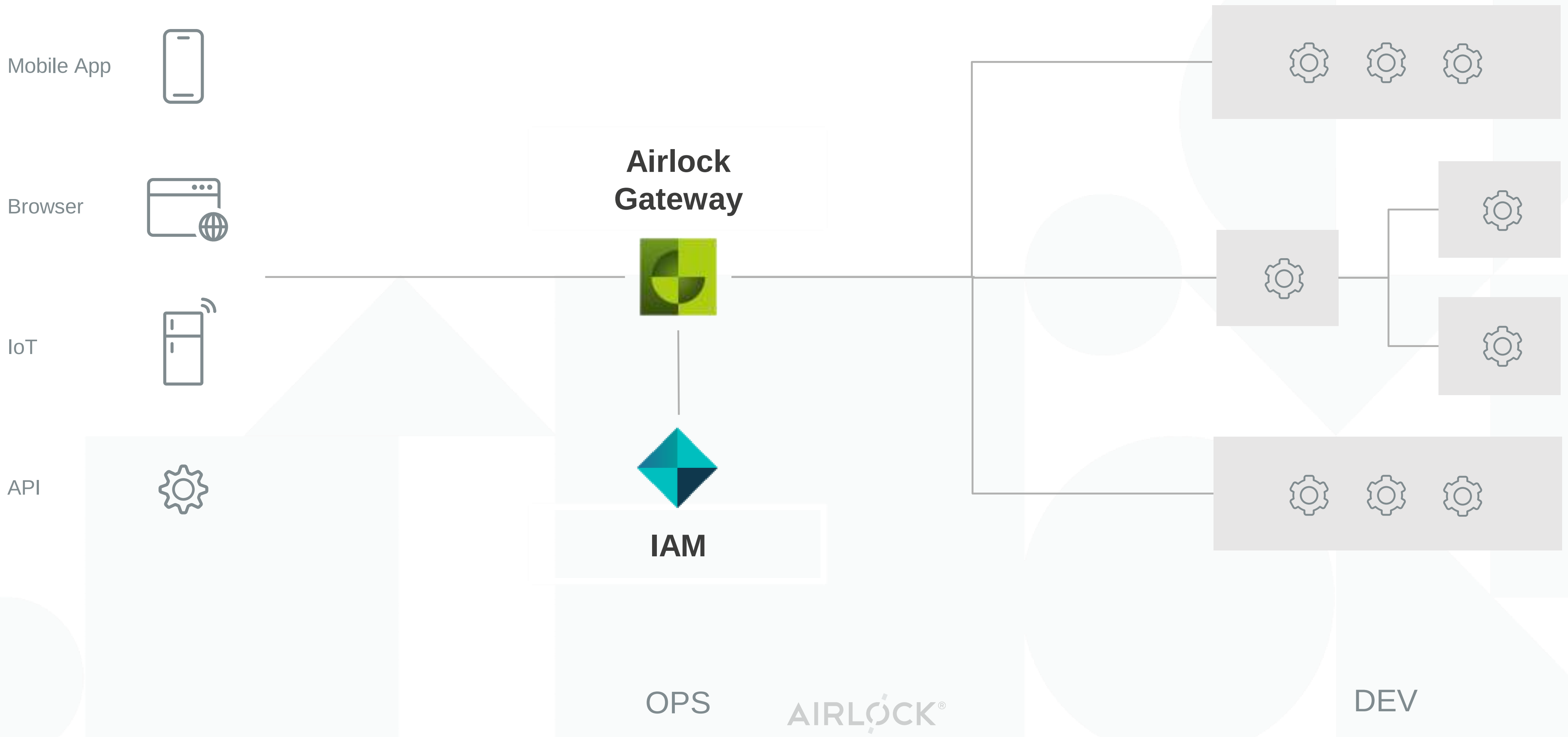
Agile, DevOps
Continuous Delivery

APIs
Mobile Apps
Single-Page Apps

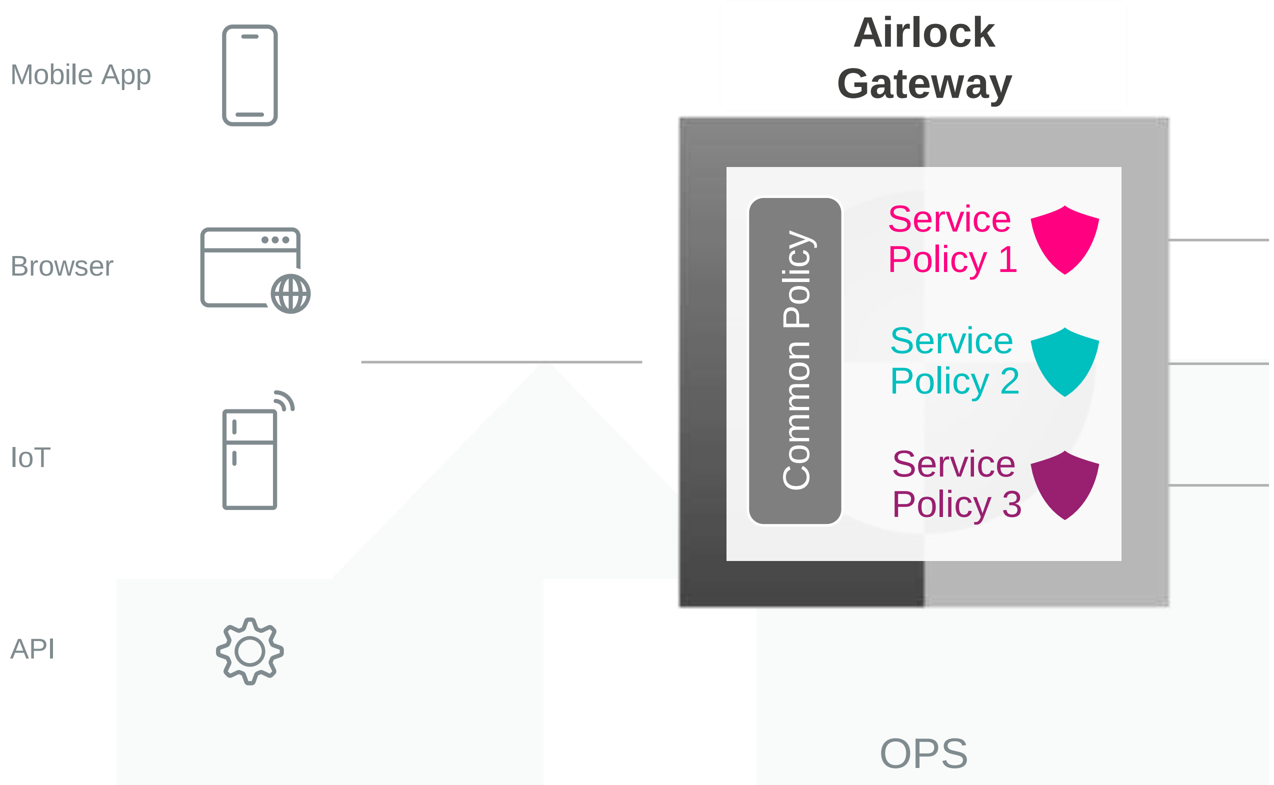
Microservices

Zero Trust

Traditional Architecture



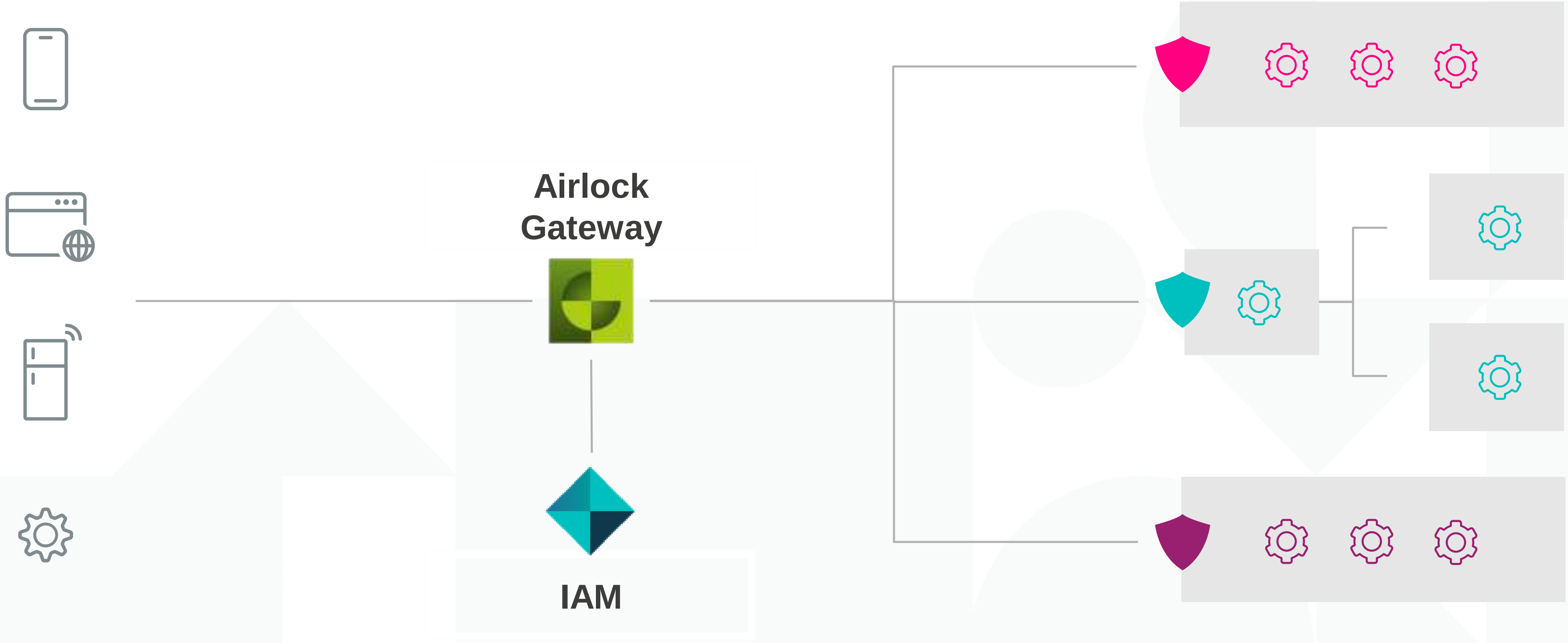
Operations owns all security polic



Problems

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

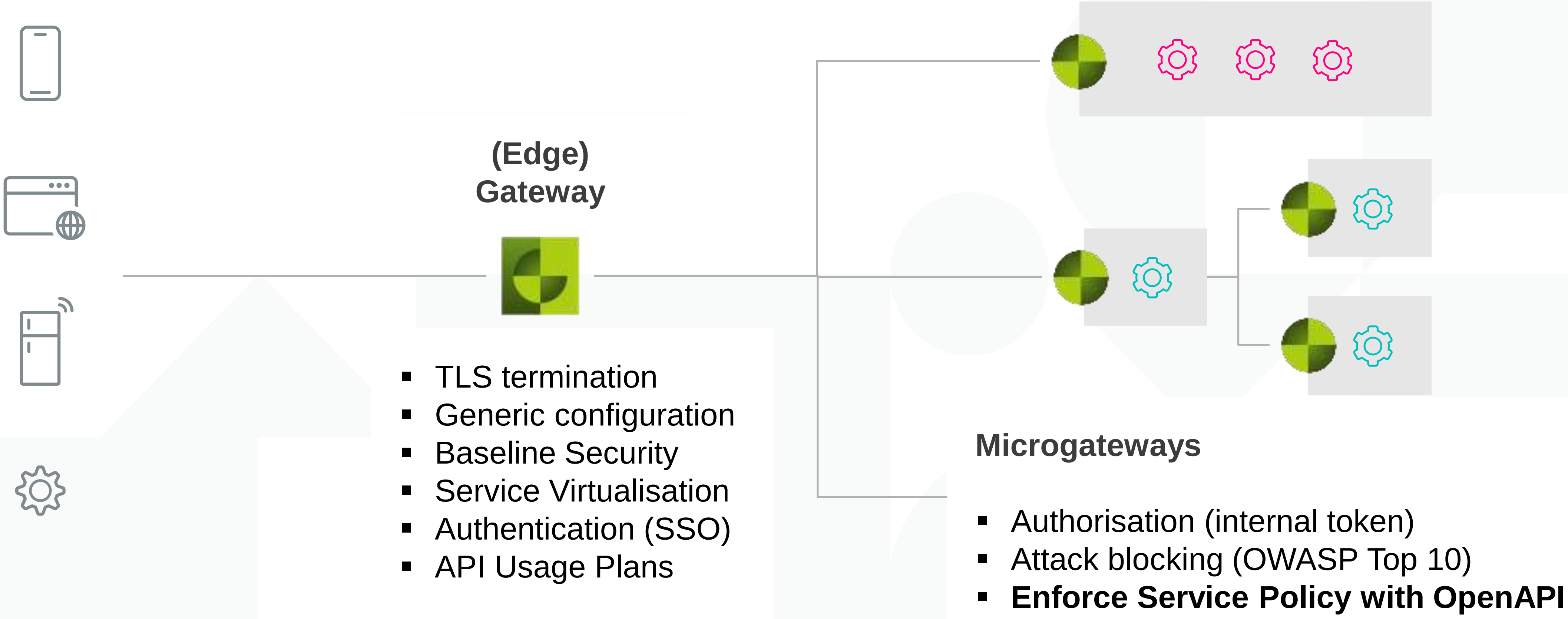
App teams own service-specific security policies



OPS

DEV

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

Security vs User Experience

You can have both:
high security *and* a great UX.

Continuous Adaptive Trust - a combination of Gateway and IAM

Risk minimisation
Continuous balance between trust level and required security level

Optimal user experience
Lower entry barrier,
Security remains in the background

Holistic approach

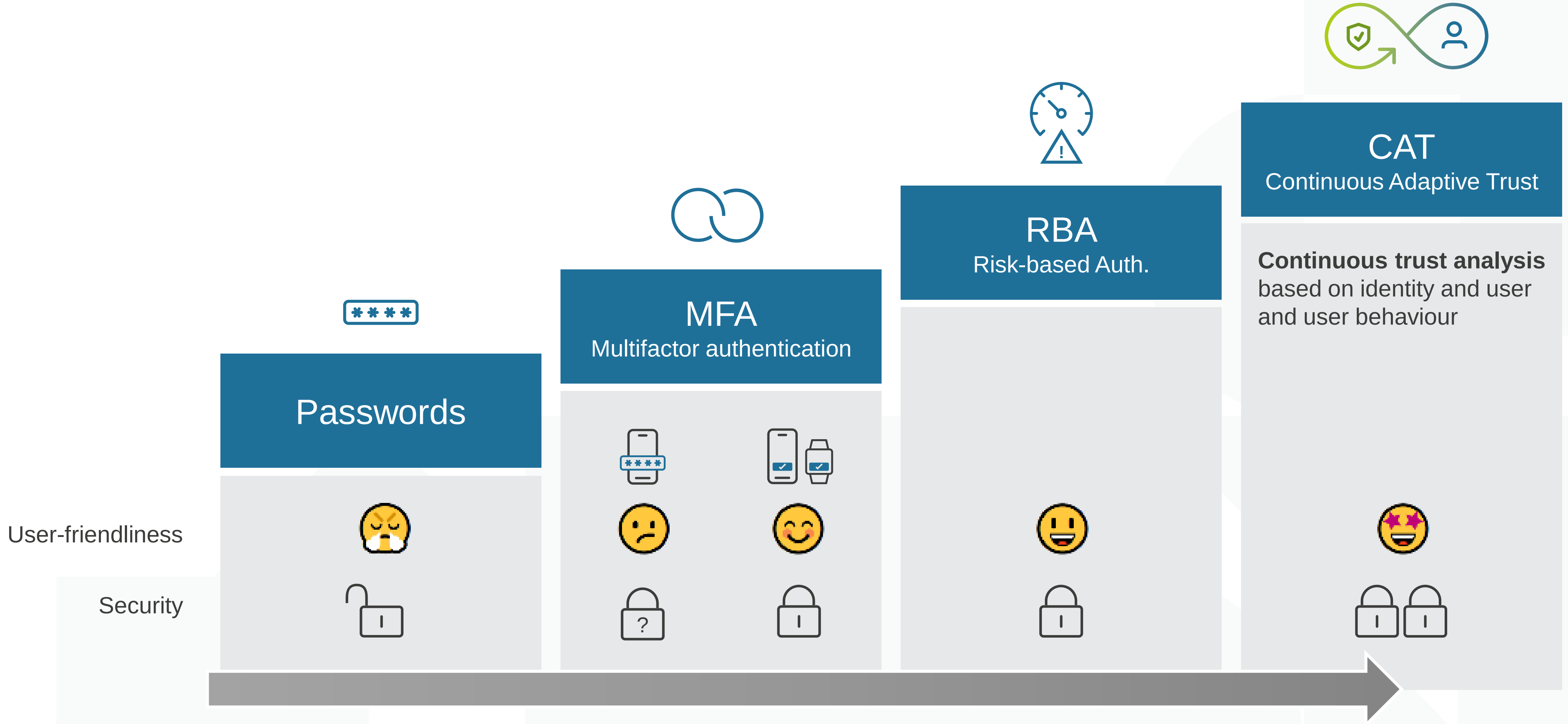
Negative Security Model

- **Multi-level filtering detects known attack patterns**
- Normalization prevents filter evasion
- Policy learning to handle false positives with ease
- No app knowldge needed
- Continuous hardening e.g. with bug bounties

Positive Security Model

- **Blocks everything that is not allowed**
- Manual rules require deep application knowledge
- Enforce existing schema declarations (JSON, OpenAPI)
- Machine Learning + Anomaly Detection

User-friendly and secure



Passwords

MFA
Multifactor authentication

RBA
Risk-based Auth.

CAT
Continuous Adaptive Trust

Continuous trust analysis based on identity and user and user behaviour

User-friendliness

Security

AIRLOCK® Source: "Shift Focus From MFA to Continuous Adaptive Trust", Gartner 2021

AIRLOCK®

Get more details about on our booth 111, hall 7A!

AIRLOCK®

Thank you very much!

Your personal contacts:

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