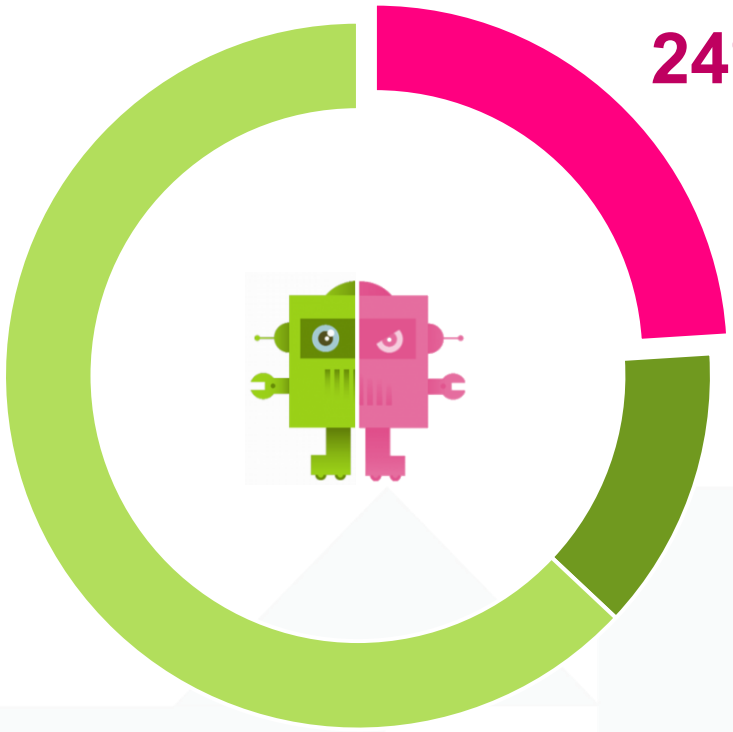
Anomaly Shield v3

Field-proven protection against automated attacks



Automated Threats

Account Aggregation
Account Creation
Ad Fraud
CAPTCHA Defeat
Card Cracking
Carding
Cashing Out
Credential Cracking
Credential Stuffing
Denial of Inventory
Denial of Service
Expediting
Fingerprinting
Footprinting
Scalping
Scraping
Skewing
Sniping
Spamming
Token Cracking
Vulnerability Scanning

Source: OWASP

Hackers love Vulnerability Scanners

Forechecking

Block them early, even before they attack.

Different perspectives

Known
Attack Patterns

Unknown +
Automated Attacks

Request Analysis

Session Analysis

Malicious content?
Known Attacker?

Deviation from "normal"
user behaviour?

Deny Rules
IP Blacklists

Machine
Learning

Mutual complementation

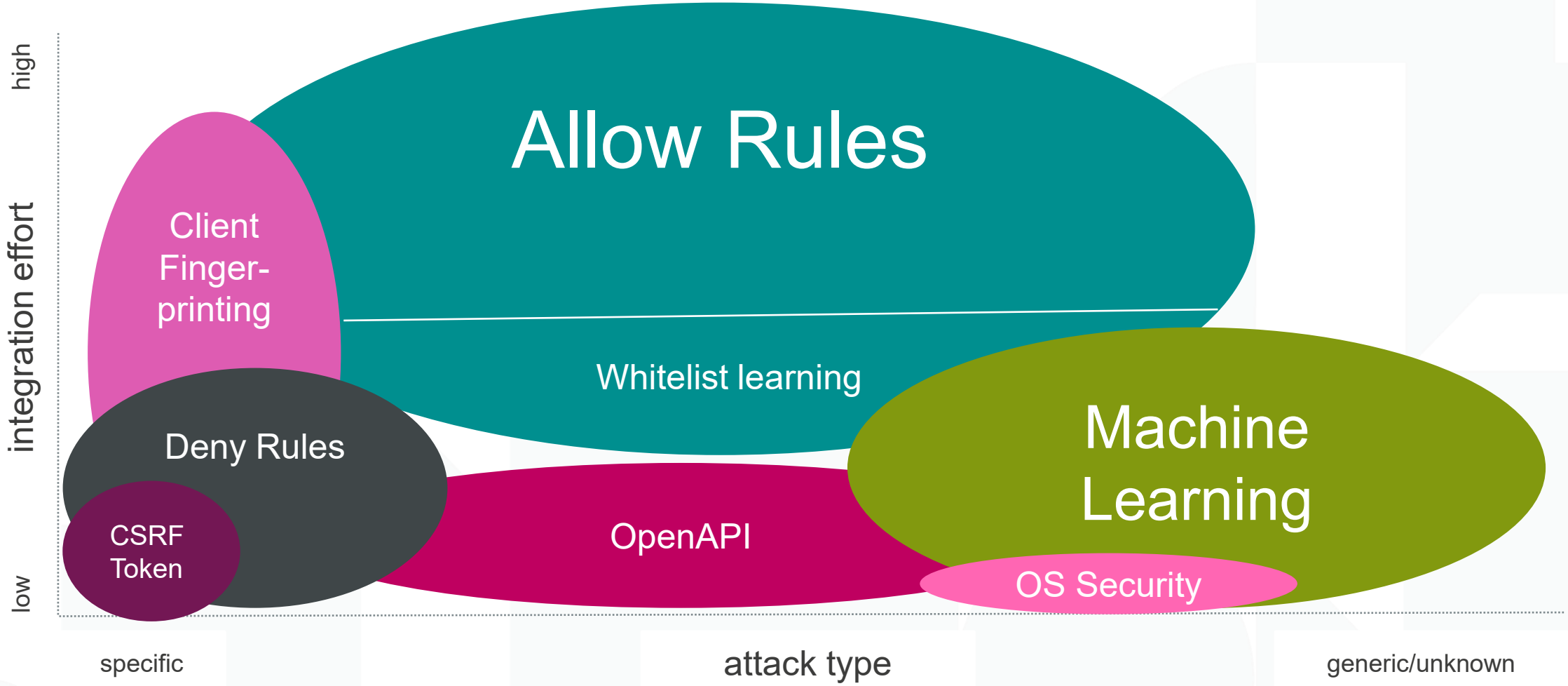
Airlock Gateway

Deny Rules
IP Blacklists

+

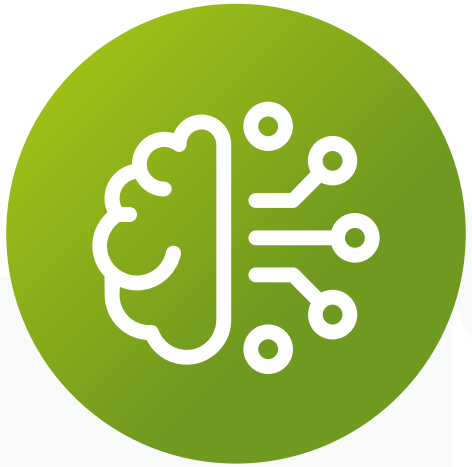
Machine
Learning

Mutual complementation



Anomaly Shield

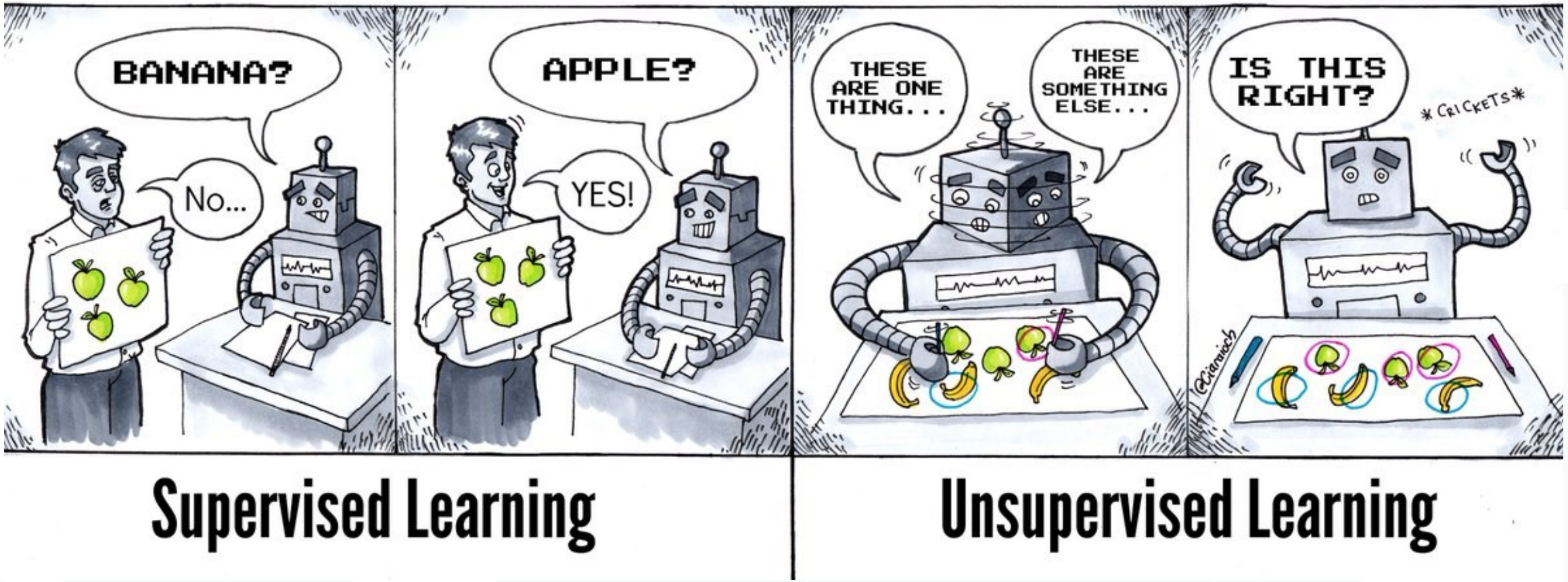
- Reliable detection of behavioural anomalies
- Adapts individually to each business application
- Adjustable sensitivity



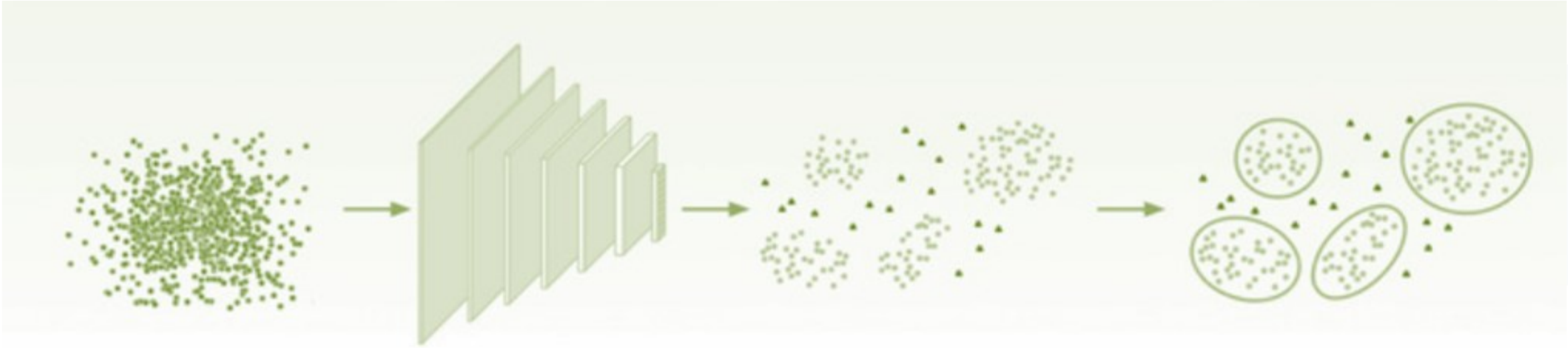
- 100% data protection
- Low maintenance
- High stability, no performance impact

AIRLOCK®

(Un-) Supervised Learning



Unsupervised Learning



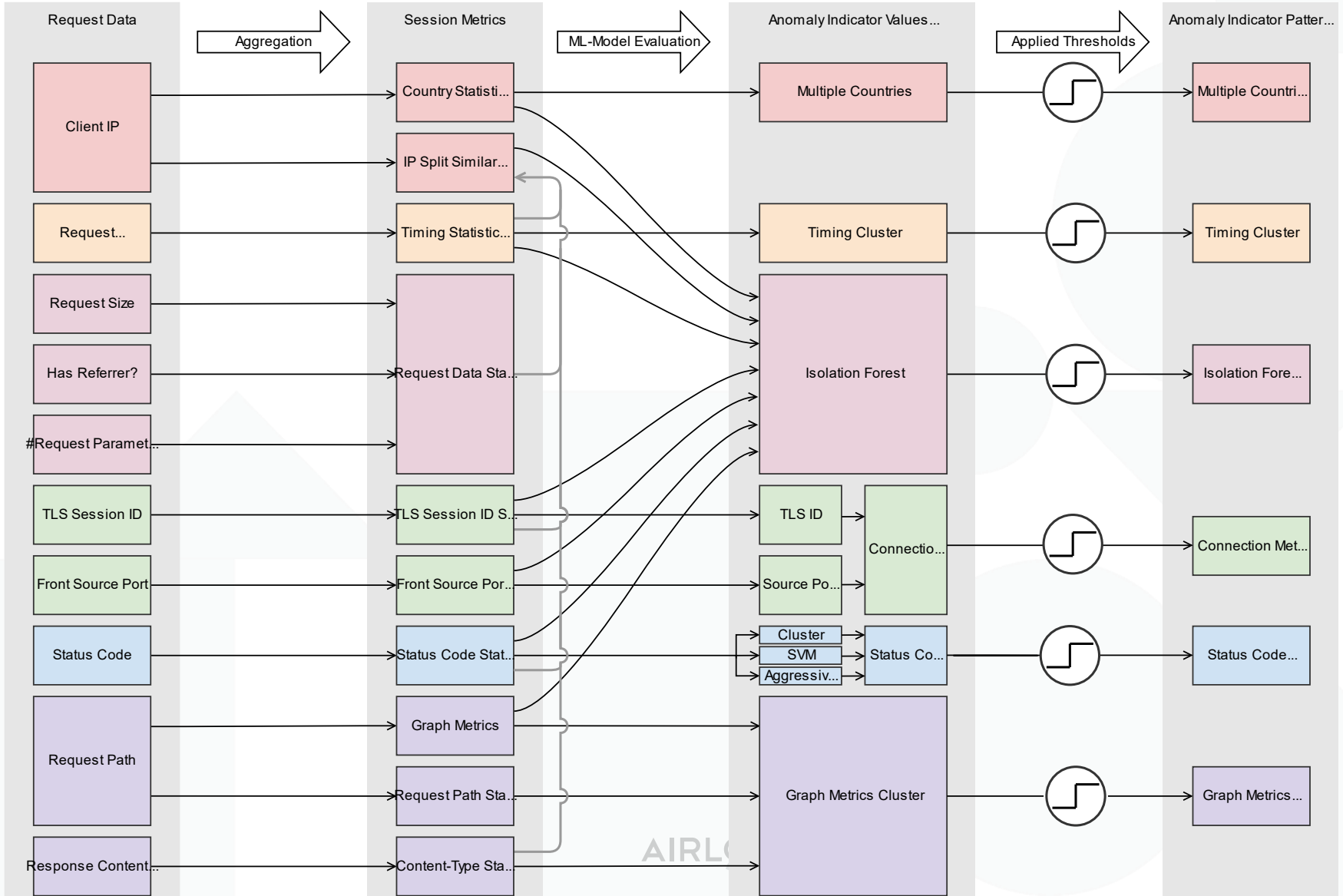
Stage 1

Unsupervised
representation learning

Stage 2

Cluster conditioned
Outlier detection

Under the Hood: Anomaly Shield Models



Under the Hood: Rocket Science?

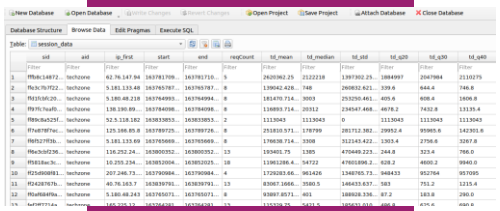
rocket fuel

it’s ok to have “rocket science” here

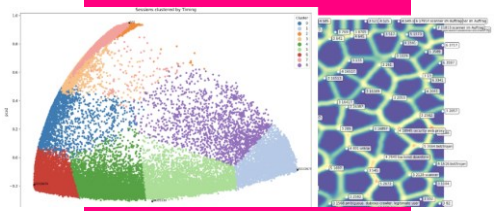
simple configuration

Request data

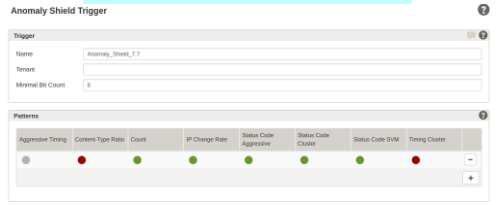
Session metrics



Models



Patterns



Aggregation

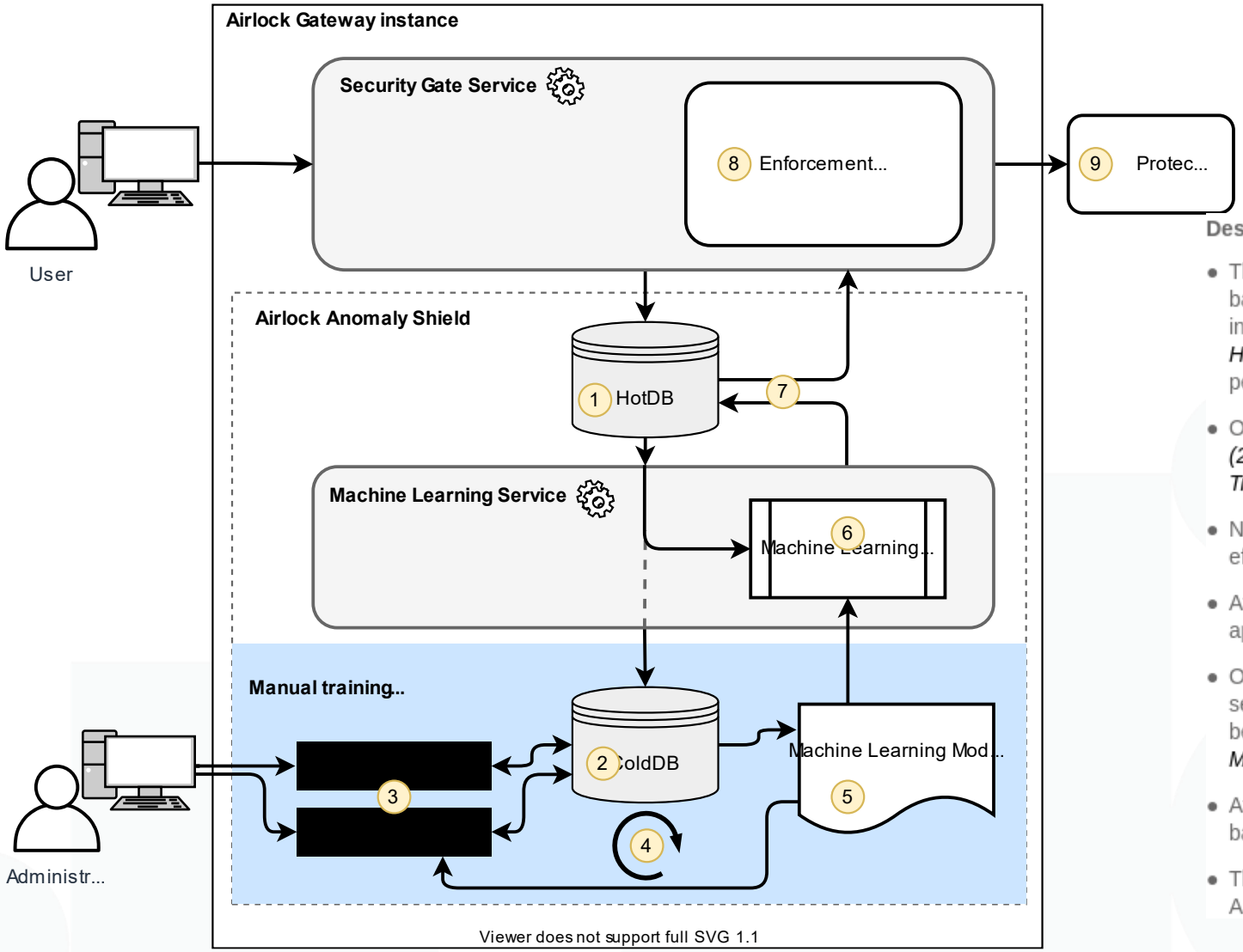
ML Training

Selection

AIRLOCK®

ergon

Under the Hood: Architecture of Anomaly Shield



Description:

- The *Machine Learning Service* of *Airlock Anomaly Shield* requires initial baseline training on user session metrics to detect session anomalies. The initial training data are looped from the *Security Gate Service* through the *HotDB (1)* into the *ColdDB (2)*, where the session metrics are stored persistently.
- Once a sufficient number of user sessions has been collected in the *ColdDB (2)*, the session metrics need to be analyzed and trained using the CLI *Model Trainer and Analytics Tool (3)*.
- Note that the CLI tools can also be used for *dry runs (4)* in order to test the effectiveness of the trained *Machine Learning Model Parameters (5)*.
- After training, the derived *Machine Learning Model Parameters (5)* can be applied to the *Machine Learning Models (6)* of the *Machine Learning Service*.
- Once the *Airlock Anomaly Shield* has been enabled, the *Security Gate Service* sends session live data to the *HotDB (1)*. New HotDB data are automatically being analyzed by the *Machine Learning Service*, based upon the trained *Machine Learning Models (6)*.
- After computing, the resulting anomaly analysis of the live session data is fed back *(7)* to the *Security Gate Service* process through the *HotDB (1)*.
- The Security Gate's *Enforcement Logic (8)* rules are strengthened by Airlock Anomaly Shield 's machine learning service for best application protection *(9)*.

PhD in Data Science??

Save yourself the time!

Application of Airlock Anomaly Shield

Set up

10 min.

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

Collect

> 1 week

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

Configure

10 min.

- Configure sensors
- Start training
- Use generated model

Protect

Continuous Monitoring

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

Anomaly Shield: Evolution

7.6

7.7

Fly-by-wire,
Glas-Cockpit

7.8

More efficient ML sensors,
improved autopilot

all further requests blocked

< 10 Requests

99% of the anomaly sessions are blocked **within 10 Requests**

Vulnerability Scanners

- WP manifest exploit
- .env File Scanners
- PHP Vulnerability Scanner
- Jolokia Vulnerability Scanner
- Python Vulnerability Scanner
- Shellshock (cgi-bin scans)
- Spring Boot Actuator exploit
- Swagger-ui XSS expoit
- Backup scanner
- Mailman input validation vulnerabilities
- Cisco ASA/FTD vulnerabilities

successfully stopped without specific signatures ✓

- Umbraco 4, 6, 7 security issues
- ssh keys scanner
- Horde/IMP Plesk exploit
- ASP.NET session hijacking
- PHPinfo vulnerability
- FCKeditor exploit
- Prometheus exploit
- Confluence Server Webwork OGNL Injection
- RocketChat exploit
- JS libraries insecurities
- SFTP password exposure

AIRLOCK®

Let’s have a look – Demo

AIRLOCK®

Interested?

>>> order@airlock.com