AIRLOCK®
SECURE ACCESS HUB

FACTSHEET

Detecting bots with machine learning

Airlock Anomaly Shield

www.airlock.com

Forechecking disrupts the sporting opponent before he can even launch an attack. Airlock Anomaly Shield detects unwanted bots and automated attacks based on their behavior and catches undesired actions in the early stages. Behavior-based anomaly detection complements classic, rule-based protection of web applications and APIs.

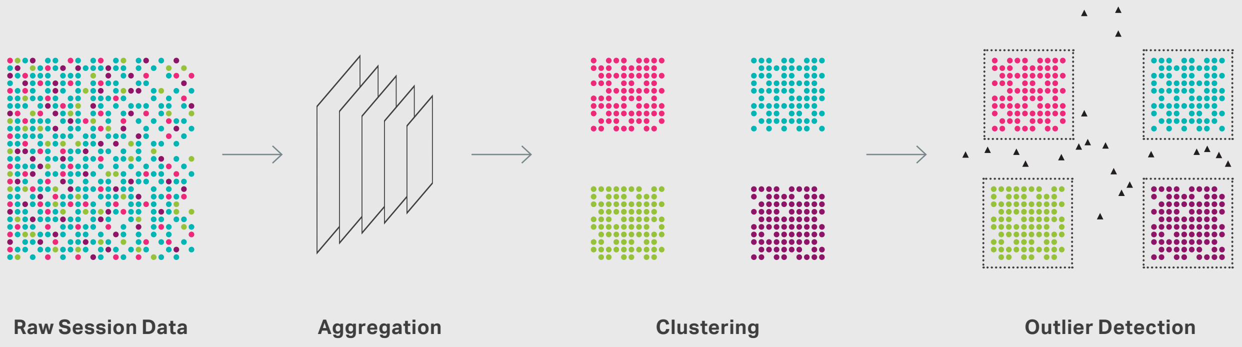
Anomaly detection and bot management

Web application firewalls and API gateways inspect every single request and usually decide immediately whether it is an attack or whether the request is forwarded. These rule-based protection systems provide very reliable protection, especially against known types of attacks. Malicious bots and automated attacks, however, are not so easy to detect. Therefore, a different approach is required here. The actions of a bot can only be distinguished from a real user if the behaviour is analysed over several requests. Anomaly detection aims to model the characteristics of legitimate traffic for reference. By comparing automated bot requests to the reference model, bots can be identified as outliers and combated. Airlock Anomaly Shield reliably detects malicious bots, automated attacks or vulnerability scans within a few requests.

Field of application

- Countering automated attacks
- Detection and mitigation of undesired bot activity such as content scraping, denial of service, credential stuffing, etc.
- Forechecking:
  Deterring hackers in the reconnaissance phase, e.g. by preventing vulnerability scans.

Anomaly Detection



How Airlock Anomaly Shield works

Airlock Anomaly Shield learns during deployment how real users of an application behave. In order to optimise the precision and effectiveness, the raw data is processed and aggregated in a space-saving way prior to the unsupervised learning. The machine learning models generated in the training phase accurately map the characteristics of the business application. During operation, all active sessions are permanently compared with the learned behaviour. If the deviation is too large, the session is marked as an outlier. Whether an anomaly is only logged or whether the session is terminated and the IP address blocked can be controlled separately for each application.

Set up →
10 min

Collect Data →
> 1 week

Configure →
10 min

Protect →
Continuous monitoring

Malicious bots: Characteristics and examples

Bots often behave very similarly to human users. Nevertheless, they can be recognised by their behaviour over time. The following anomalies occur very frequently when analysing bot traffic:

- **Unusually large number of requests** within a short period of time
- **Unexpectedly high error rate** or bounce rate
- **Abnormal sequence of page views**
- **Irregular sender addresses** or TLS sessions

Vulnerability Scanner
Hackers use automated tools to find vulnerable systems. With the help of bots, they often scan many systems simultaneously for possible security vulnerabilities. The individual steps of a scan are often not clearly recognisable as an attack - after all, the attacker wants to stay under the radar for as long as possible.

Web and API Scraping
In content scraping, a bot downloads all the content of a website, often with the aim of abusing the data obtained. Here, too, the attacker makes an effort to pretend to be a normal user. However, to cope with the large amount of data, many more page views are required. Airlock Anomaly Shield was developed to combat such scraping attacks and other types of malicious traffic.

Credential Stuffing
Credential stuffing exploits that the same password is often used for multiple services for laziness. Attackers can thus attempt to compromise user accounts by trying stolen credentials on many systems. A strong protection against credential stuffing is to detect bots. Two-factor authentication or CAPTCHAs can also be considered as countermeasures, but these are often perceived as a hassle by end users.

Denial-of-Service Attacks
In a denial-of-service (DoS) attack, a malicious actor attempts to make a service inaccessible to its intended users. The system is flooded with application requests until normal traffic can no longer be processed. Through behavioural analysis, DoS attacks can be detected at the application level and stopped before they set up damage.

Advantages

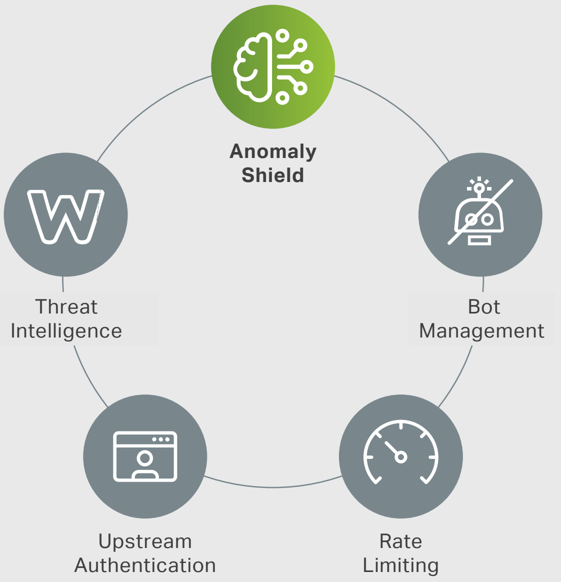
- **Quick setup without data science know-how:** Configuration and maintenance are possible within minutes, even without any machine learning knowledge.
- **Defence against unknown types of attacks:** The application-specific training results in a positive security model. As a result, unknown bots or zero-day attacks can also be detected because the protection is not based on signatures.
- **100 % data protection and control:** Neither the training data nor the anomaly decisions ever leave the Airlock Gateway cluster.
- **Adjustable sensitivity:** In case of an increase in false positives/negatives, the sensitivity can be adjusted for each sensor.
- **High throughput:** The anomaly detection takes place in the background and is decoupled from the normal request flow. A delay of the data traffic is excluded by the asynchronous assessment.

Complete Bot Protection

For optimal application protection, the combination of various bot management functions in Airlock Secure Access Hub® is recommended:

- **Threat Intelligence:** BrightCloud Threat Intelligence Service from Webroot uses real-time reputational data to block rogue IP addresses.
- **Rate limiting and DoS protection:** If the number of requests or sessions per IP is particularly high, DoS protection prevents applications from being overloaded. Especially with APIs, the data throughput is also limited depending on the user identity.
- **Upfront authentication:** To ensure that only authorised users can access the application, unidentified visitors are redirected to the Airlock IAM login page, for example.
- **Bot Management:** Detects bots and requires that all callers return cookies. Many automated bots cannot pass this hurdle because they do not have a cookie store. Search engine bots must also access from the IP range of the respective search engine. In the event of repeated violations of the security rules within a short period of time, an IP is placed in quarantine. During the quarantine, no more requests are accepted from these IPs.

Completion with additional bot protection measures



Would you like to try Airlock Anomaly Shield?

If you are interested in Airlock Anomaly Shield, please contact us via email at **order@airlock.com**. We will be happy to provide you with a test licence to test the bot detection in log-only mode.