AIRLOCK
by ergon

Airlock App for Splunk

The Airlock App for Splunk® provides aggregated reports of security issues and application usage. The various dashboards allow network administrators to quickly investigate security issues or troubleshoot application and performance problems.

Dashboards

All dashboards allow grouping of statistics by various filters like virtual hosts, mappings, countries and so on.

The Airlock App for Splunk contains the following dashboards:

– Overview:
Dashboard to get a quick overview about the Airlock WAF environment. This dashboard provides summary views for all available dashboards. These reports give a quick high-level overview of what is going on in the network. The main plot from each dashboard and statistics per virtual host and mapping are included. PDF versions of the management reports can be scheduled for periodic delivery by email with low effort.

– Session statistics:
Detail dashboard with session count and user statistics. This dashboard presents all traffic in terms of sessions rather than requests. Predefined filters allow differentiation between authenticated and anonymous user sessions.

– Traffic statistics:
Detail dashboard with request count and bandwidth information. This dashboard gives a quick overview of all traffic running through Airlock WAF. With a single click, customers' origin countries or most popular web application can be identified.
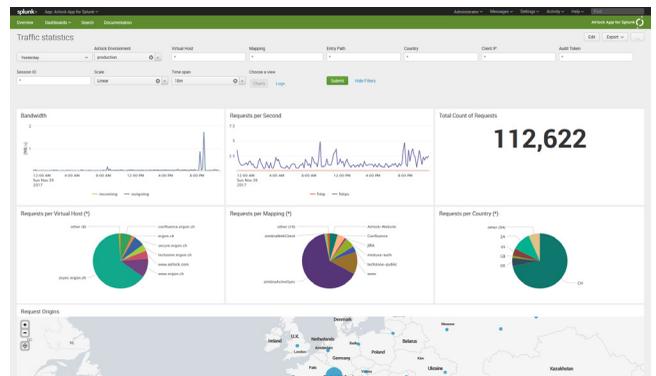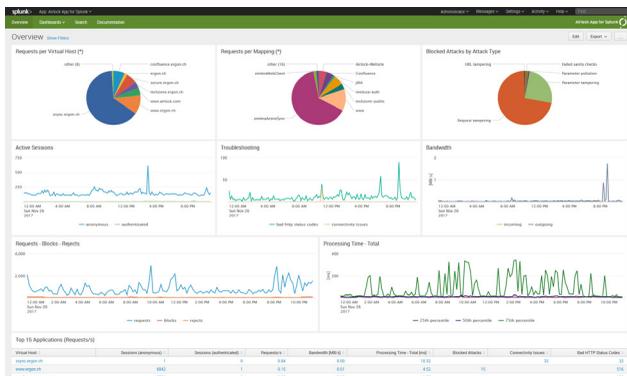
– Attacks:
Detail dashboard with requests, which were blocked.
Use the Attacks dashboard to investigate security issues.
Pre-defined filters allow quick investigation of why requests were blocked, e. g., due to missing whitelist rules, triggered blacklist rules or DoS attack prevention.

– Connectivity issues:
Detail Dashboard with connectivity statistics.
This Dashboard shows all connectivity problems to the back-end applications. If an application can not be reached, the reasons can be found in this dashboard.
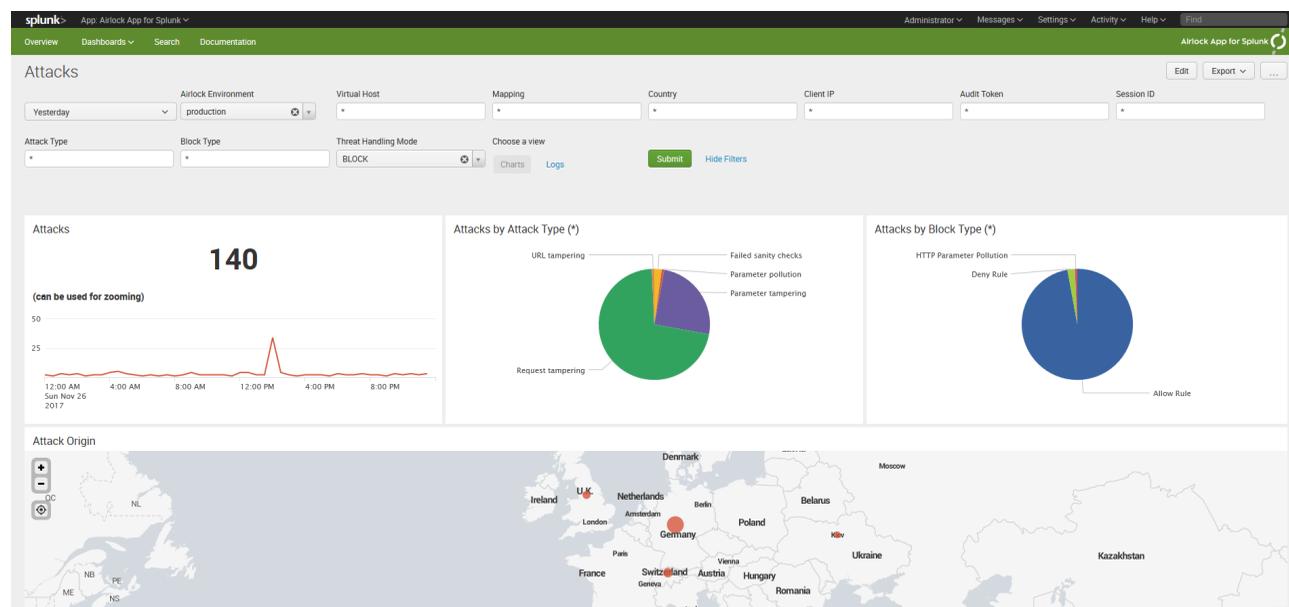
– Rejected requests:
Detail dashboard with requests, which were rejected.
The reason for the rejection might lie in a misconfiguration of Airlock WAF, system sizing or be caused by environment issues (network or back-end) .Use this dashboard as a starting point for debugging application issues.

– Performance:
Detail dashboard with performance statistics.
This dashboard monitors performance of individual back-end applications. Detailed statistics are computed for assessing back-end responsiveness, response processing time or time spent in ICAP filters.

– Request analyzer:
Detail Dashboard with request statistics.
The dashboard shows all bad http status codes like 4xx and 5xx codes.

Your benefits:
– Ready-to-use product
– Tailored Airlock WAF dashboards
– More dashboards to come
– Management reports
– Splunk field definitions for Airlock logs
– High flexibility with custom search queries
– Maintenance by Ergon

The Airlock App for Splunk is sold as an optional module for Airlock WAF. For sales inquiries, please contact sales@airlock.com.

About Ergon Informatik AG and Airlock Suite

Founded in 1984, Ergon Informatik AG is a leading developer of bespoke software solutions and products. The cornerstone of our success: 270 highly qualified IT specialists who are committed to creating value for the client, anticipating technological trends and designing solutions that generate competitive advantage. Ergon focuses on implementing major B2B projects.

Airlock Suite deals with the issues of filtering and authentication in one complete and coordinated solution – setting standards for usability and services. Airlock protects more than 30.000 applications, 15 million identities at more than 400 customers with a net promotor score of +53. The security Suite was launched on the market in 2002.

Ergon, the Ergon logo, «smart people smart software» and Airlock are registered trademarks of Ergon Informatik AG.

ergon

Ergon Informatik AG
Merkurstrasse 43
CH–8032 Zürich

+41 44 268 89 00
www.airlock.com
twitter.com/ErgonAirlock