AIRLOCK by ergon

Hewlett Packard Enterprise

Integrated security for your applications with HPE Security ArcSight and Airlock

Airlock Suite deals with the issues of filtering and authentication in one complete and coordinated solution

About HPE Security

HPE is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading products from HPE Security ArcSight, HPE Security Fortify, and HPE Security—Data Security, the HPE Security Intelligence Platform uniquely delivers the advance correlation and analytics, application protection, and data security to protect today's hybrid IT infrastructure from sophisticated cyber threats.

AIRLOCK by ergon

Airlock Suite deals with the issues of filtering and authentication in one complete and coordinated solution – setting standards for usability and services. Airlock Suite, our security product, was launched on the market in 2002 and is now protecting more than 30.000 back-ends and 15 million identities around the globe.

Integrated Security for applications

- With the Airlock CEF integration into HP ArcSight our customers do not only receive a full protection of their applications, identities and data but also full insights into possible attacks, performance or application issues.

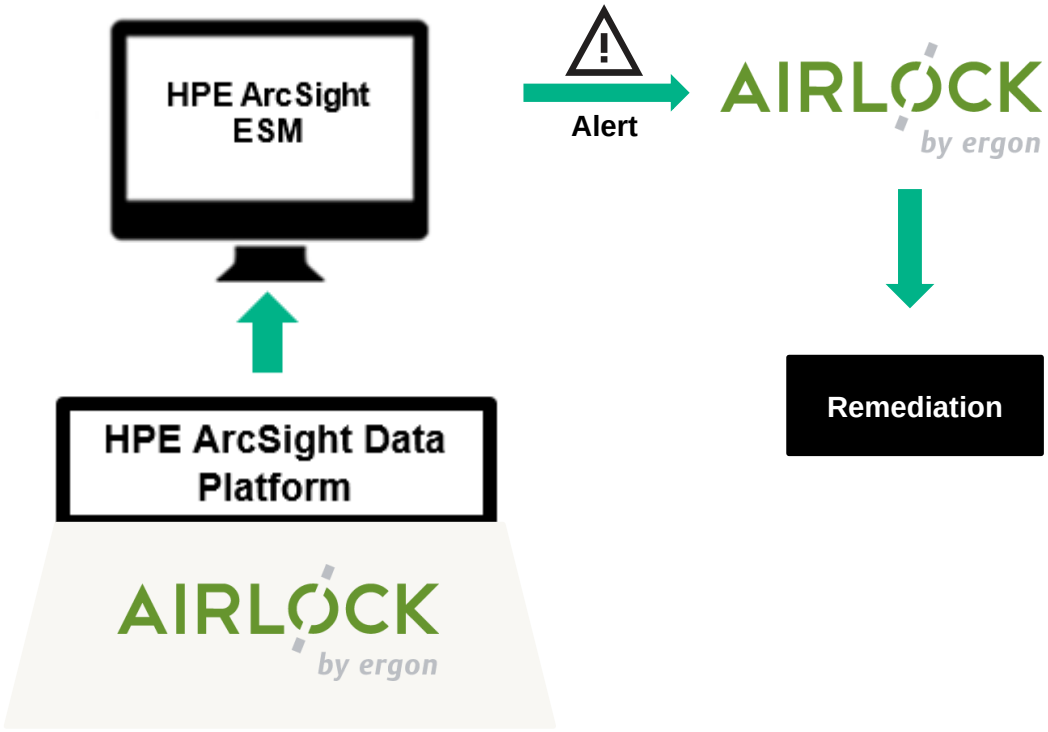
Better together

The Airlock Web Application Firewall (Airlock WAF) offers a unique combination of protective mechanisms for web applications and APIs. It protects against OWASP top 10 vulnerabilities through a host of smart features. Together with Airlock IAM, access management for applications and APIs can be fully integrated in Airlock WAF. Detected attacks can be blocked or just logged. In conjunction with HPE ArcSight, the user is provided a comprehensive and company-wide view of security events and incidents. Using HPE ArcSight, attacks detected by Airlock WAF are put in perspective and can be correlated with attacks on different systems and layers.

https://www.airlock.com/en/products/airlock-waf/

Key Benefits:

- Aggregation of security incidents across systems
- Correlation of security incidents with activity in other sources
- Identifying hot spots of activity
- Anomaly detection in traffic patterns
- Full protection of applications against OWASP Top 10 with Airlock WAF and Airlock IAM
- Upstream authentication and authorization



Use cases:

- Aggregation of security incidents across systems
- Security incidents on a single installation can easily be aggregated with incidents on different systems. This allows identification of an attack's size and scope, e.g., does it pertain to single hosts or is it company-wide?
- Correlation of security incidents with activity in other sources
- Airlock WAF analyzes HTTP(S) traffic. Correlation of incidents with events from other sources, e.g., anti-malware scanners, IDS systems, data leakage prevention or suspicious login attempts allows getting the big picture and analyzing potential attacks in-depth.
- Identifying hot spots of activity
- Correlation and aggregation of events allows identification of hot spots of an ongoing attack, e.g., the originating regions or targeted applications.
- Anomaly detection in traffic patterns
- Statistical anomalies in observed traffic patterns may be the starting point for a more thorough investigation. Include Airlock WAF's detailed content inspection features in your analysis to find proof of malicious activities.

More Info

For additional HPE Security information visit: http://www.hpe.com/software

For additional Partner information visit: https://www.airlock.com/en/products/airlock-waf/