AIRLOCK WAF

Schützt Applikationen. Sicher.

Airlock WAF schützt mit modernen und dynamischen Filtern unternehmenskritische, webbasiert Applikationen. Sie analysiert als zentrale Security-Instanz innerhalb des Airlock Secure Access Hubs jeden http(s) Request auf Angriffe und blockt somit jeglichen Versuch von Datendiebstahl und -manipulation. Im Zusammenspiel mit Airlock IAM und Airlock API besteht somit eine einzigartige Architektur zur Web-Applikationssicherheit.

Einsatz von modernen Webfiltern

Airlock WAF analysiert jeden einzelnen Request zwischen Nutzern und Web-Portalen, -Anwendungen und -Services. Angriffsversuche werden blockiert, noch bevor sie auf interne Systeme zugreifen können. Airlock WAF bietet umfassenden Schutz gegen die OWASP Top 10 Schwachstellen sowie vor modernen Angriffen und ermöglicht das zentrale Management von Security Policies. Dank modularen und innovativen Sicherheitsfunktionen bleiben Unternehmen den Angreifern immer einen Schritt voraus.

Policy Enforcement Point

Im Zusammenspiel mit Airlock IAM und Airlock API wird Airlock WAF zum Policy Enforcement Point, der nur gefilterte, authentisierte und autorisierte Zugriffe erlaubt. Diese Kombination von Access Management mit inhaltlicher Filterung garantiert kompromisslose Sicherheit.

Security Dashboards

Das eingebaute dynamische und grafische Reporting bietet jederzeit Überblick über alle Angriffsversuche. Auch betriebliche Komplikationen wie Performance-Engpässe oder Back-end-Probleme werden erkannt, aufgezeigt und können mit unternehmensspezifischen Eskalationen oder Alarmprozessen kombiniert werden. Mittels interaktivem Drill-Down aus den Dashboards und dank der Anzeige der ursächlichen Logzeilen kann jeder Angriffsversuch exakt analysiert werden.

Plattformunabhängig, hochverfügbar und bedarfsorientiert

Airlock WAF steht als Hardware oder Virtual Appliance sowie als Cloud Image zur Verfügung und ist somit für alle Einsatzszenarien flexibel verfügbar.
Die leistungsstarke Airlock WAF kann im Bedarfsfall, z.B. bei saisonalen Business-Lastspitzen, zu einem aktiven WAF-Cluster mit mehreren Nodes problemlos ausgebaut werden. Der integrierte Loadbalancer unterstützt die geforderte Hochverfügbarkeit für Applikationen und Services im vollen Umfang und spart somit eine zusätzliche Architekturkomponente ein.
Dank der integrierten Let's-Encrypt-Unterstützung lassen sich Zertifikatserneuerungen vollständig in der Airlock WAF automatisieren. Dank flexiblem Lizenzierungsmodell kann auf kundenspezifische Anforderungen eingegangen werden.

Ergon Informatik AG | Merkurstrasse 43 | CH-8032 Zürich |Telefon: +41 44 268 89 00 | E-Mail: info@airlock.com

Zentrale Security-Drehscheibe

Airlock WAF bietet viele Schnittstellen zu weiterführenden Systemen wie SIEM Systemen, Virenscannern, Fraud-Prevention-Systemen oder HSMs. Dank dem integrierten Threat Intelligence Feed reagiert Airlock WAF sofort auf aktuelle Bedrohungslagen aus dem Internet und schützt Systeme vor Gefahren, die gestern noch unbekannt waren. Über eine hochverfügbare ICAP Schnittstelle lassen sich weitere Komponenten integrieren.

DevSecOps

Airlock WAF lässt sich dank eines umfangreichen REST APIs einfach in moderne DevOps-Prozesse integrieren. Bei der frühen Integration der Security in Applikationsentwicklungszyklen, auch in den neuen Docker- und Kubernetes-Philosophien, bietet die Airlock WAF flexible Sicherheit und erlangte Konfigurationen können auf einfachste Weise und somit effizient zwischen den unterschiedlichen Umgebungen transferiert bzw. eingesetzt werden. Auto-Learning-Mechanismen unterstützen beim schnellen Einsatz der Airlock WAF.

Deployment

Virtual Appliance, Hardware Appliance, Airlock Cloud Image

Funktionen:

- **Eindämmung von Applikationsangriffen:**
  - Generische & spezifische Angriffssignaturen
  - Cookie Store
  - Request Validierung
  - CSRF Tokens
- **Zugriffskontrolle**
  - Durchsetzungspunkt für Richtlinien
  - Single Sign-On (SSO)
  - Secure Session Management
- **Dynamic Whitelisting**
  - URL Encryption
  - Form Protection
  - Dynamic Value Endorsement (DyVE)
- **Policy Learning**
  - Automatische Regelvorschläge
- **HTTP(S) Reverse-Proxy**
  - Terminierung
  - OCSP & OCSP Stapling
  - Let's Encrypt Support
  - HSM Integration
  - Service Virtualisierung
  - Content Rewriting
- **Hohe Verfügbarkeit**
  - Failover Cluster
  - Loadbalancing
- **Logging & Reporting**
  - JSON Protokolle & Lucene query syntax
  - Zugriffsstatistik
  - Security Dashboards
  - Performance Dashboards
  - Troubleshooting Dashboards
  - Kundenspezifische Visualisierung
- **SIEM Integration**
  - Splunk App
  - Common Event Format (CEF)
- **Threat Intelligence**
  - Webroot Feed Integration
  - GEO Filterung
- **Konfigurationsmanagement**
  - Staging Support
  - REST API
- **Cloud Image**
  - Kompatibel mit AWS, GCE, Azure
- **ICAP Interface**
- **IBM Trusteer Pinpoint Integration**

Ergon Informatik AG | Merkurstrasse 43 | CH-8032 Zürich |Telefon: +41 44 268 89 00 | E-Mail: info@airlock.com