DATA SHEET

Cequence App Firewall

Application Security That Goes Beyond Legacy WAFs

Introduction

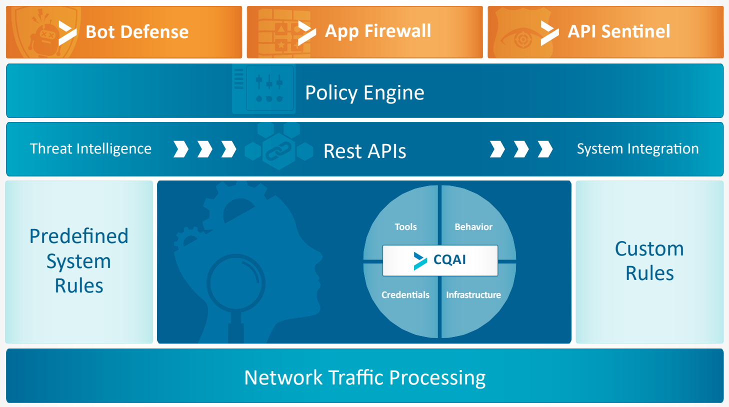
Data breach announcements resulting from the use of an application component that has an unpatched vulnerability have become a regular occurrence. Historically, organizations have addressed these risks using a Web Application Firewalls (WAF), focusing heavily on the OWASP Top 10 and PCI regulatory compliance requirements.

Traditionally, WAFs are difficult to manage and their traditional change control approach to signature and policy updates can result in false positives and delays in the application development lifecycle, which can impact user experience.

App Firewall Overview

Cequence App Firewall takes a new approach to blocking application vulnerability exploits, one that uses intelligence and automation to extend web app and API protection beyond traditional OWASP Top 10 and PCI DSS Section 6.6 focused WAF functionality.

The App Firewall is part of the Cequence API Security Platform, the only offering that unifies runtime API visibility, security risk monitoring, and patented behavioral fingerprinting technology to consistently detect and protect against ever evolving online attacks. When deployed as an add-on to Bot Defense, the App Firewall can strengthen your security posture while reducing the operational burden associated with deploying and managing web application security.



CEQUENCE API SECURITY PLATFORM

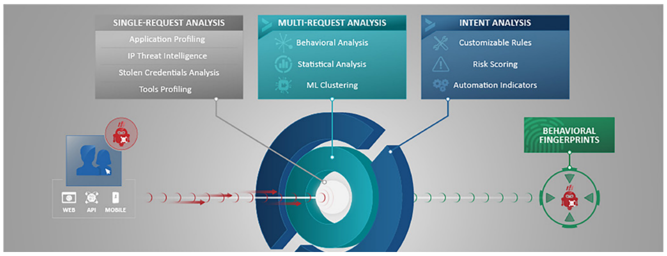
Cequence App Firewall

Complements Bot Defense to consistently detect and protect against ever evolving online attacks without the development friction associated with alternative offerings. Key benefits include:

- Accelerates incident analysis and response time with complete visibility into which applications may be at risk
- Minimizes the need to constantly tune security policies associated with traditional, old-school WAFs
- Consolidates WAF, automated bot attack protection and API security into a single, unified platform
- Protects your applications with advanced security features in a matter of hours, not weeks or years

App Firewall Features

CQAI: Maximum Visibility, Minimal Policy Tuning



CQAI ML-based Analytics Engine

Traditional WAFs focus on known application states and known-bad threats making them relatively ineffective at detecting new, zero-day exploits. Gaining visibility into all of the publicly exposed applications and APIs is the first step towards preventing data loss caused by bad actors taking advantage of vulnerability exploits. CQAI analyzes your network traffic, automatically building an intuitive site map of your web applications and APIs. Newly deployed applications and APIs are automatically discovered and protected as they are deployed.

> *Cequence was a very easy integration and proved their value almost immediately. We really like their visibility and ability to pick out a bad actor in a crowd of good customers. They are setting the bar for machine learning and AI in this domain.*
>
> Director IT Security, Retail
> Gartner Peer Insights 5 Star Review

Using over 160 customizable ML-based automation indicators, CQAI performs a multi-dimensional analysis of your applications to create a unique Behavioral Fingerprint that detects known, as well as unknown vulnerability exploits. Findings are then translated into attack prevention policies.

Customizable Rules, Policies and Response Options

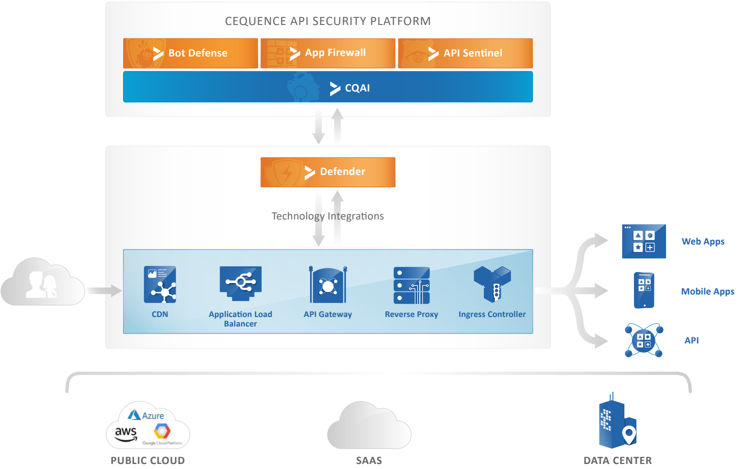
Whereas some WAF offerings require the use of professional services to make generate queries or make execute system changes, the App Firewall policy creation and management can be performed by your team or in conjunction with the Cequence Threat Monitoring Service with support provided by our CQ Prime Research Team. Predefined ML models and system rules can be tailored using criteria such as the specific application, HTTP payload, OWASP Top 10, geo-location or time of day. Lua and ModSecurity scripting can also be used to create advanced App Firewall rules. Attack response options include blocking, rate limiting, header-insertion for downstream action and analysis.

Easily Integrates with Existing Infrastructure

REST-based APIs allow you to import 3rd party data to enhance CQAI analysis, or you can export the findings to your existing IT infrastructure for post-mortem analysis, correlation, or enforcement by your firewall or other security device.

Deploys in Minutes

The App Firewall can be enabled to protect your web applications and APIs in as little as 60 minutes and can immediately begin reducing the operational burden associated with preventing attacks that can result in fraud or data loss. Alternatively, the modular, container-based architecture allows the App Firewall to be deployed in your data center, your cloud environment, or as a hybrid.


CEQUENCE API SECURITY PLATFORM
Bot Defense
App Firewall
API Sentinel
CQAI
Defender
Technology Integrations
CDN
Application Load Balancer
API Gateway
Reverse Proxy
Ingress Controller
Web Apps
Mobile Apps
API
Azure
aws
Google Cloud Platform
PUBLIC CLOUD
SAAS
DATA CENTER