DATA SHEET

CEQUENCE SECURITY

Cequence App Firewall

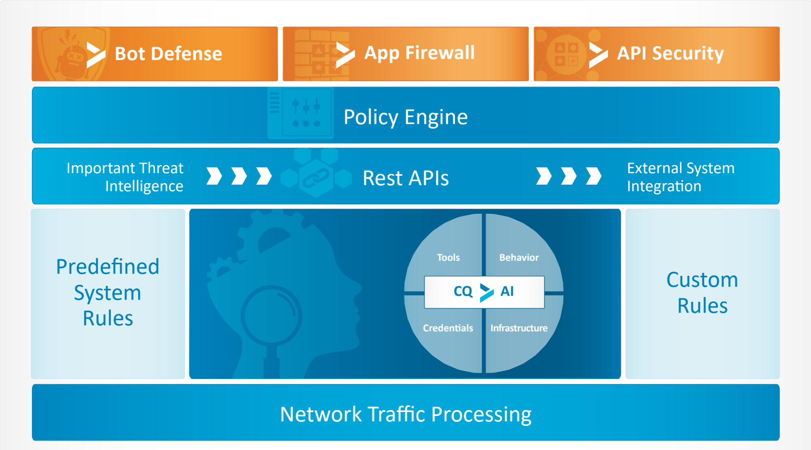
Application Security That Goes Beyond Legacy WAFs

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. Unfortunately, WAFs have become difficult to manage and their traditional change control approach to signature and policy updates can result in false positives and delays into the application development lifecycle, which often impacts user experience. App Firewall takes a new approach, one that uses intelligence and automation to extend far beyond traditional OWASP Top 10 and PCI DSS Section 6.6 focused WAF functionality.

Cequence Application Security Platform with App Firewall

The Cequence Application Security Platform (ASP) is designed to protect your web and mobile applications along with their associated APIs from automated attacks, application business logic abuse and vulnerability exploits. Cequence ASP is the only solution that detects automated attacks against APIs and web applications without cumbersome JavaScript instrumentation or mobile SDK integration requirements. The ASP is comprised of the following components:



CEQUENCE APPLICATION SECURITY PLATFORM

Cequence App Firewall

Complements Bot Defense to provide complete application security in single platform. 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
- › Eliminates deployment bottlenecks by baking security into your application development framework

- **CQAI** uses Machine Learning to automatically and continually discover your public facing APIs and web applications, building an intuitive sitemap for complete visibility. The customizable automation indicators in CQAI analyze the traffic in real-time to determine malicious or benign intent. CQAI findings are then used to enforce policy or exported via a REST-based API to an existing component of your security infrastructure.
- **App Firewall** enforces vulnerability prevention policies based on CQAI findings with a range of response options including blocking, rate limiting, geo-fencing and deception.
- **Bot Defense**, available as a separate license, complements App Firewall by preventing automated attacks against your API and web-based applications.]

Deployed as a SaaS solution, on-prem or in the cloud, Bot Defense and App Firewall helps you strengthen your security posture while reducing the operational burden associated with deploying and managing web application security.

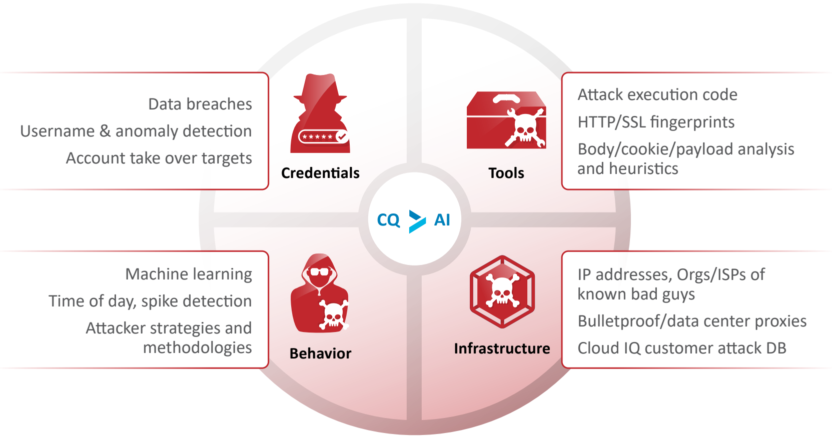
App Firewall Features

Continuous Application Discovery and Visibility

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 uses Machine Learning to analyze your network traffic, automatically building an intuitive site map of your public facing web applications along and any exposed APIs. Newly deployed applications and APIs are automatically discovered and protected as they are deployed. The knowledge of which application and APIs are deployed can then be used to build positive security model enforcement policies – allow specific applications, and deny all else.

Dynamic Machine Learning Minimizes Policy Tuning

Using over 150 customizable ML-based automation indicators, CQAI analyzes your applications based on our Four Pillars of Detection: Credentials, Tools, Infrastructure and Behavior. This multidimensional analysis enabling you to detect and prevent known, as well as unknown vulnerability exploits. The agentless, ML-based approach of CQAI delivers two key benefits. First, it effectively bakes security into your application workflow, eliminating application JavaScript instrumentation and mobile SDK integration penalties such as deployment delays and slow page load times. The second benefit provided is consistent protection against automated attacks against your exposed APIs, effectively eliminating potential security gaps and delivering an opportunity to consolidate application security functions into a single platform.

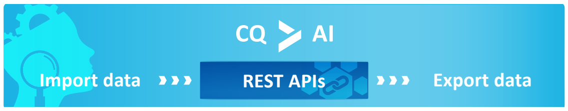

Data breaches
Username & anomaly detection
Account take over targets
Credentials
Tools
Attack execution code
HTTP/SSL fingerprints
Body/cookie/payload analysis and heuristics
CQ AI
Machine learning
Time of day, spike detection
Attacker strategies and methodologies
Behavior
Infrastructure
IP addresses, Orgs/ISPs of known bad guys
Bulletproof/data center proxies
Cloud IQ customer attack DB

Customizable Rules, Policies and Response Options

Application and attack visibility can be translated into policies that enforce a positive security model – allowing what you want while denying all else. Predefined automation indicators 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 be used to create advanced rules. Attack response options include blocking, rate limiting, header-insertion for downstream action and analysis to deception.

Open, Extensible Platform Integrates with Existing IT Infrastructure

As a means of improving your overall security posture, CQAI findings can be exported to your existing IT infrastructure such as another security device for enforcement, a SIEM, or a REST API endpoint for added analysis or correlation. The REST API also allows you to export the attack response results for post-mortem analysis and fine-tuning.

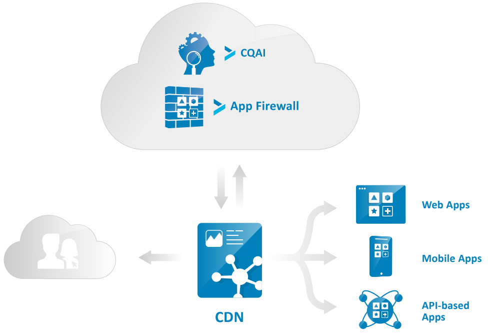


Deployment Options

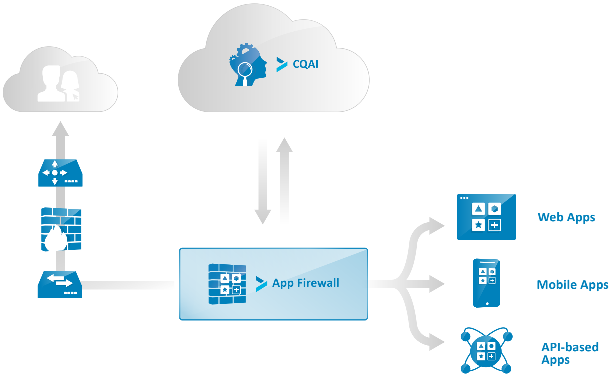
SaaS

App Firewall can be deployed as a SaaS solution to help reduce the operational effort associated with protecting your public facing application infrastructure from automated attacks. Cequence Security deploys and manages the underlying cloud-based infrastructure, ensuring up-time and applying updates to the applications. All policies, data and system configuration elements are managed by you, the customer. Integration with leading CDNs like Amazon CloudFront, Akamai, and Fastly streamlines the deployment, enabling you to quickly begin preventing automated attacks today.

- **CDN Integration:** App Firewall SaaS integrates with your CDN or load balancer to analyze traffic and eliminate the need to deploy any agents that may impact on application performance. Detected attacks can be remediated quickly based on policy with legitimate traffic routed to the origin server or looped back to the CDN then to the application servers. Supported CDN integrations include: AWS CloudFront, Fastly, and Akamai.



- **Proxy Integration:** App Firewall SaaS can be deployed inline, using a lightweight module to integrate with your proxy where it communicates with CQAI in the cloud for ML analysis and policy updates. This approach allows you to deploy exploit prevention closer to the application servers with no changes required to the network edge.



On-Premises or in the Cloud

A distributed, container-based architecture allows Bot Defense to be deployed in a customer managed public cloud, data center and hybrid environment. Bot Defense and App Firewall are deployed as a single component in the line of traffic, sending traffic to CQAI and taking action as dictated by policy. Small and lightweight to ensure low latency and minimal impact, Bot Defense and App Firewall are designed to fail-open in the event of a failure. CQAI and the management dashboard are deployed in a central location, performing analysis, providing visibility, dictating policy and enriching the existing infrastructure through REST-based API import and export capabilities. This distributed approach to deployment allows organizations to quickly and easily support their ever-evolving public facing application infrastructures.