CEQUENCE SECURITY

Cequence Bot Defense

Innovative, ML-based platform prevents fraud caused by automated attacks

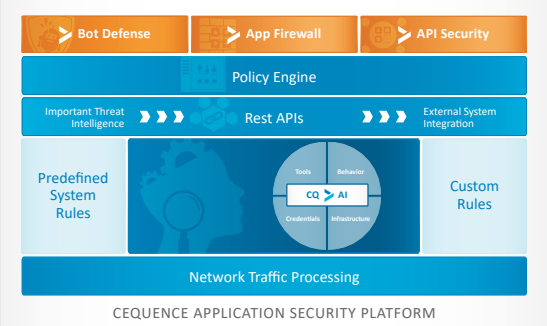
Introduction

Stolen credentials, attack toolkits, and compromised infrastructure have made it easy for bad actors to launch account takeovers and business logic abuse against your public facing applications that can result in fraud or theft. Oftentimes, bad actors will discover and launch their attacks directly against your exposed APIs, bypassing the web form or mobile application completely.

These automated attacks hide in plain sight, masking themselves as legitimate transactions. Organizations need an extensible application security platform that analyzes your traffic, separating benign from malicious intent; supports customizable policies and delivers consistent security for automated attacks across API, web and mobile application channels.

Cequence Application Security Platform with Bot Defense

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

› **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.

Cequence Bot Defense

Can be deployed as a SaaS solution, on premises or in the cloud. Key benefits include:

› Accelerates incident response time with complete visibility into applications and automated attacks

› Minimizes fraud related losses caused by account take overs and fake account creation

› Saves time investigating and preventing attacks such as content/price scraping, denial of inventory, gift card fraud, and denial of wallet

› Eliminates application changes and deployment bottlenecks by baking security into your application development framework

› Consolidates automated attack protection for web, mobile and associated APIs into a single, unified platform

- **Bot Defense** enforces mitigation policies based on CQAI findings with a range of response options including blocking, rate limiting, geo-fencing and deception.
- **App Firewall**, available as a separate license complements Bot Defense by enforcing vulnerability prevention policies based on CQAI findings.

Deployed as a SaaS solution, on-premises or in the cloud, Bot Defense and App Firewall help you reduce the operational burden associated with deploying an application security platform while simultaneously improving your security posture with protection for your public facing applications.

Bot Defense Features

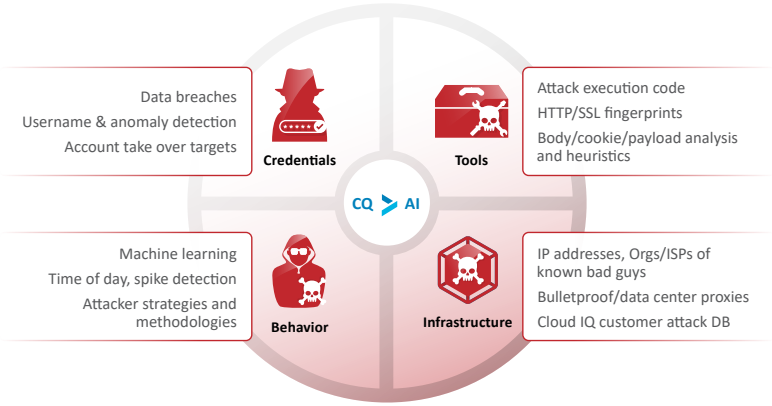
Continuous Discovery and Visibility

Automated attacks can be executed in a variety of ways that include scripting a web form, modifying (spoofing) the mobile application itself and directly targeting the associated APIs. Traditional prevention approaches that use JavaScript and mobile SDKs to collect the necessary telemetry are cumbersome to implement and provide inconsistent protection against attacks that target APIs directly. The unique approach taken by Bot Defense SaaS discovers all the APIs used to support your public facing web and mobile applications, allowing you to protect your customers digital experience with a consistent security policy.

CQAI analyzes your network traffic to automatically build an intuitive site map of all the public facing web and mobile applications along with any exposed APIs. Newly deployed applications and APIs are automatically discovered and protected as they are deployed.

Dynamic Machine Learning

Using over 150 customizable ML-based automation indicators, CQAI determines the intent of each transaction based on our Four Pillars of Detection: Credentials, Tools, Infrastructure and Behavior. This multidimensional analysis is performed out-of-band, enabling you to detect and prevent well-known automated attacks (e.g., account takeovers and fake account creation) as well as those that target application business logic (e.g., content/price scraping, denial of inventory, gift card fraud, and denial of wallet), which are often missed by products requiring JavaScript based detection.



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.

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. Customizable automation indicators can be tailored to your environment to continually detect bot traffic – even as they retool to avoid detection. Discovered attacks can be mitigated using a range of response options including blocking, rate limiting, geo-fencing and deception. Using deception goes beyond traditional response mechanisms, allowing you to mislead the attacker into believing that their attacks have been successful, such as serving up stale content to price scraper bots.

Open, Extensible Platform Integrates with Existing IT Infrastructure

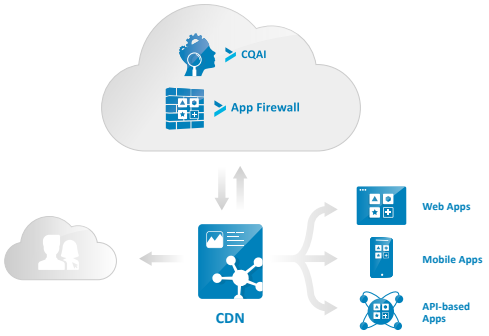
As a means of improving your overall security posture, CQAI findings can be exported to your existing IT infrastructure such as another security device for enforcement, a SIEM, or a REST API endpoint for added analysis or correlation. The REST API also allows you to export the attack response results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

Deployment Options

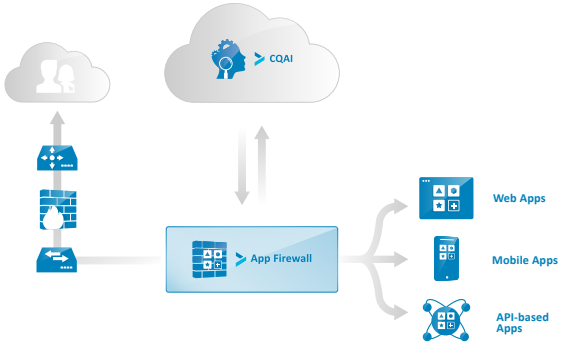
SaaS

Bot Defense 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 Bot Defense SaaS 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 Bot Defense SaaS deployment, enabling you to quickly begin preventing automated attacks today.

- **CDN Integration:** Bot Defense 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. This form of integration allows you to deploy bot protection at the network edge, resulting in a reduction in (malicious) traffic hitting your application server infrastructure. Supported CDN integrations include: AWS CloudFront, Fastly, and Akamai.



- **Proxy Integration:** Bot Defense 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 bot protection 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.

Learn more about the Cequence Application Security Platform family of products at www.cequence.ai.

CEQUENCE SECURITY
100 Murphy Avenue, Suite 300, Sunnyvale, CA 94086 › 1-650-437-6338 › info@cequence.ai › www.cequence.ai