CEQUENCE SECURITY

Cequence Bot Defense

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

Introduction

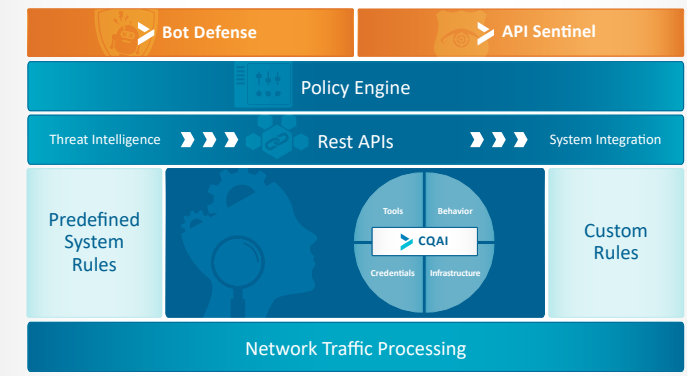
Stolen credentials, attack toolkits, and compromised infrastructure have made it easy for bad actors to launch account takeovers and business logic abuse against your public facing web applications and APIs that can result in fraud or theft. These automated attacks hide in plain sight, masking themselves as legitimate transactions, oftentimes leveraging commercialized toolkits and infrastructure.

Organizations need an open and extensible solution that enables rapid response to increasingly aggressive attacks such as automated shopping and scraping as well as ATO and fake account creation.

Bot Defense Overview

Bot Defense is the only bot mitigation offering that does not require any JavaScript or mobile SDK integration to collect the attack telemetry needed to prevent malicious automated bot attacks that can result in fraud or data loss. Bot Defense leverages CQAI, a patented analytics engine that discovers all web apps and APIs to create a visual site map. Application requests are then analyzed by CQAI's patented ML-based models to detect malicious automated attacks that can then be addressed through mitigation policies.

Bot Defense 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.



CEQUENCE API SECURITY PLATFORM

Bot Defense

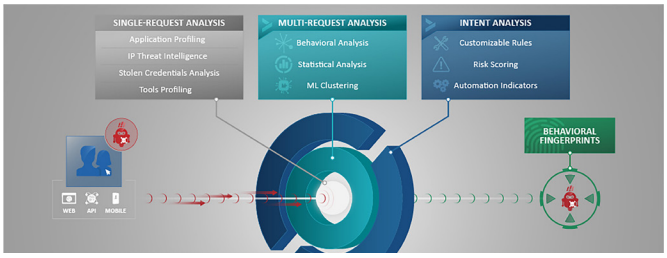
Patented Behavioral Fingerprinting technology consistently detects and protects against ever evolving online attacks without the development friction associated with JavaScript-based offerings. Key benefits include:

- Minimizes fraud related losses caused by account take overs, fake account creation, automated shopping, content/price scraping, and gift card fraud
- Accelerates incident response time with complete visibility into automated attacks against web applications and APIs
- Reduces policy administrative efforts and improves security posture with consistent protection for both web apps and APIs
- Unobtrusive SaaS deployment model enables application protection in hours, not weeks or years

Bot Defense Features

CQAI: No JavaScript or Mobile SDK Required

CQAI eliminates the need for JavaScript or SDK integration with more than 160 ML-based automation indicators that perform a multi-dimensional analysis of your web applications and APIs, resulting in a unique Behavioral Fingerprint that continually tracks sophisticated attacks, even as they retool to avoid detection.



CQAI ML-based Analytics Engine

The CQAI Behavioral Fingerprint enables your team 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., automated shopping, sneaker bots, content/price scraping, and gift card fraud), which are often missed by products requiring the use of JavaScript or an SDK for detection.

> *Cequence AI Bot Defense product outshines the rest with it's most prominent feature: You don't need to integrate an SDK. It's quickly deployed into an AWS infrastructure with multiple options to take a feed of your traffic with real time decisions based on policies you write.*
>
> VP Information Security, Retail/Auction Company
> Gartner Peer Insights 5 Star Review

The CQAI ML-based approach 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 both web apps and 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

Using predefined rules that can be customized, CQAI findings can be translated into policies that enforce a positive security model – allowing what you want while denying all else. Unlike alternative offerings that require professional services to access data or make other changes, 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. Discovered attacks can be mitigated using a range of response options including blocking, rate limiting, geo-fencing and deception, a technique that allows you to mislead and deceive the attacker into believing that their attacks have been successful.

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

Bot Defense SaaS can be enabled to protect your web applications and APIs in as little as 15 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 Bot Defense to be deployed in your data center, your cloud environment, or as a hybrid.

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