CEQUENCE SECURITY

CQ botDefense

Intelligent Automation to Prevent Malicious Bot Attacks

Introduction

Organizations around the world are building feature rich web, mobile and API-based applications as a means of extending their competitive advantage and improving the business. Simultaneously, bad actors are using a rich repository of stolen user information and attack toolkits to programmatically target these public facing applications with malicious transactions that appear to be legitimate, or syntactically correct. These attacks target the business logic of your application, manifesting themselves in the following abusive ways: account take over, fake account creation, content scraping, denial of inventory/ wallet, gift card theft and loyalty program fraud.

Common Business Logic Abuse Attacks

These attacks impact your business in the following ways:

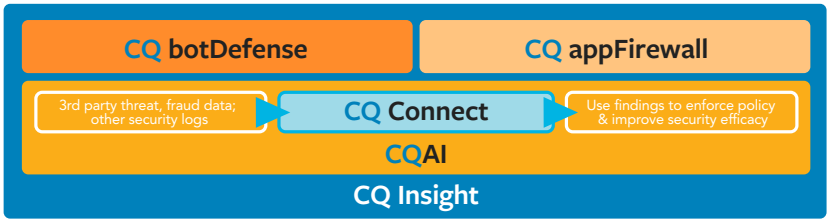
- **Revenue losses** directly attributed to fraud, theft and the process of addressing it.
- **Decline in user-base** from reputation bombing, loss of trust and poor user experience.
- **Increased infrastructure costs** to address the high volume of illegitimate traffic.
- **Degradation of user experience**, application performance and availability.

Traditional approaches to address these automated bots have been a mix of network level protections, Web Application Firewalls and 1st generation bot mitigation tools. These approaches are largely ineffective at protecting your applications against today's sophisticated attacks and are hard to manage, injecting friction into the application development lifecycle and often impacting user experience. What's needed is a new approach, one that provides you with complete visibility and actionable intelligence to protect your application infrastructure.

Cequence Application Security Platform (ASP)

The Cequence Application Security Platform (ASP) protects your web, mobile and API-based application infrastructure from automated attacks, bots, and exploits. CQ botDefense is one of the two security modules available within the ASP.

The intelligence of the platform resides with CQAI, a patented, machine learning, analytics engine that automatically discovers your web, mobile and API-based applications while uncovering threats and vulnerabilities that may lead to data loss or application infrastructure compromise. This provides you with a more complete view of application and threat behavior than other technologies that rely on client context alone. Applications and threats identified by CQAI can then be used to drive policy creation within the two Cequence Security Modules:



Cequence Application Security Platform

- **CQ botDefense** uses the intelligence generated by CQAI to determine the actual intent of the application transactions, allowing you to take mitigative actions if the intent is malicious.
- **CQ appFirewall** leverages CQAI to intelligently extend traditional WAF functionality simplifying administrative effort with predefined application profiles and policy templates while improving security with the ability to prevent unknown, or zero-day attacks.

Additional Cequence ASP elements include CQ Connect and CQ Insight, which allow you to more easily integrate the platform into your existing security infrastructure and to perform centralized management, respectfully.

CQ botDefense: Intelligently Preventing Automated Application Attacks

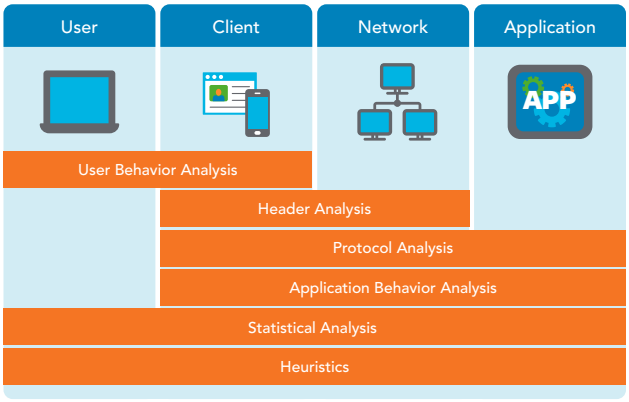
CQ botDefense allows your organization to gain full visibility and control over automated attacks without impacting valid users and beneficial forms of automation. Working collaboratively with CQAI, CQ botDefense first gains a complete understanding of your web, mobile and API-based applications, then detects and mitigates the automated attacks that are targeting them, allowing you to accomplish several key application security objectives:

- **Prevent automated attacks targeting web, mobile and API-based apps.** CQ botDefense continually analyzes your public-facing applications to discover threats that you can mitigate via policy using a range of response options.
- **Bake security into your application infrastructure**. Continual analysis of your applications by CQAI obviates the need for application instrumentation and SDK updates, which means that as new applications or updates are released, they are automatically protected.
- **Seamlessly integrate with your existing infrastructure**. As an integral component of ASP, CQ botDefense allows you to leverage CQ Connect to improve security efficacy and the distributed architecture enables you to deploy application security in the cloud, data center or hybrid locations.

CQ botDefense takes an intelligent approach to preventing automated attacks targeting your modern application infrastructure that may be web, mobile and API-based.

Identify and Prevent Automated Attacks

CQ botDefense harnesses the intelligence of CQAI engine that performs multi-dimensional analysis of the entire application transaction, including heuristics header, protocol, and behavioral analysis. CQAI then correlates across hundreds of client, network, and application traits to separate human from automated traffic, creating a unique fingerprint for each attack.



The fingerprint includes the various channels and their respective application endpoints (e.g., login, registration or account signup) the attackers may be targeting, and the triggers used (e.g., suspicious behaviors exhibited, forged and suspicious sources used, or the URI). The ability to analyze the attack from a variety of different perspectives allows you to conclusively identify the signs of malicious automation down to the level of intent, allowing you to take more informed policy actions. Passive analysis ensures that CQAI continuously tracks evolving bot behavior over long periods to ensure the most accurate detection without any impact on application performance or customer experience.

Customizable Mitigation Options

CQ botDefense allows you to choose from a range of mitigation options that extend beyond traditional signature-based blocking. Mitigation options include alert and block based on the bot fingerprint as well as rate limiting, and geo-fencing based on countries listed by the US Treasury Department Office of Foreign Assets Control.

Using deception as a mitigation technique goes beyond traditional response mechanisms, allowing you to convince the attacker that their malicious efforts have been successful. A deception-based response disturbs the economic factors surrounding the attack, thereby impacting the ability for an attacker to achieve their objective. For example, if credential validation and then resale on the Dark Web is the attack objective, deception will tell the bad actor that the credentials are valid and can be sold for a premium. In reality, the credentials are fake, and essentially worthless.

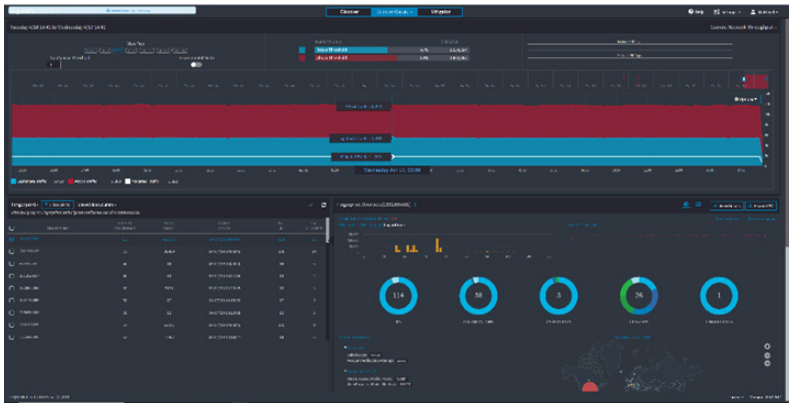


Image 1: Visualize your application traffic and take action on attacks with CQ Insight.

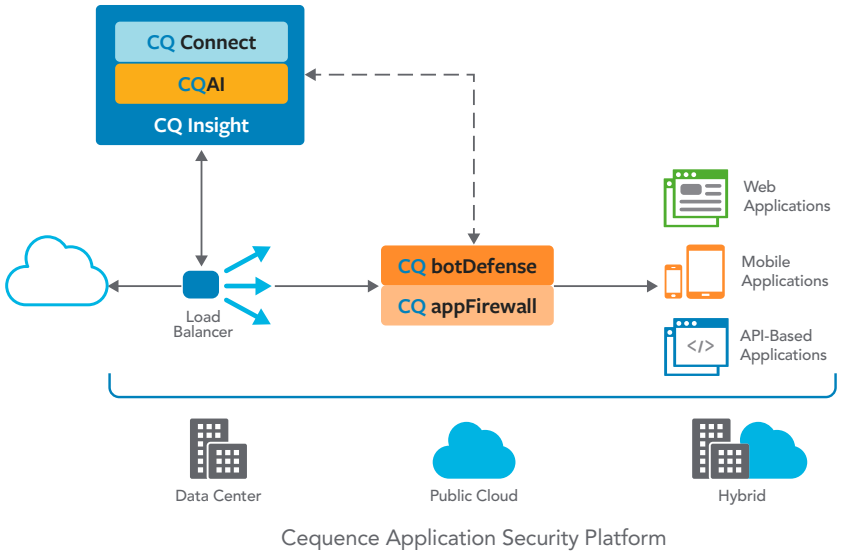
Security that's Baked into your Application Infrastructure

Cloud-native initiatives typically entail moving towards container and micro-services application development methodology that is more agile and iterative. In these scenarios, security must keep pace, moving beyond traditional change-control oriented approach that often injects delay into the application development workflow. CQ botDefense protects all web, mobile, and API applications from automated attacks without the need to customize the application or modify the SDK. CQAI automatically discovers all applications and identifies changes so that the organization remains protected even as developers roll out new apps.

Tighter Integration for a Stronger Security Infrastructure

Too often, security solutions are closed systems, unable to easily export information or import 3rd party data to improve overall security efficacy. CQ Connect, an integral element of Cequence ASP is an open API that allows you to send information on the attack to your existing firewall or WAF for enforcement, or to your SIEM for additional analysis. CQ Connect also allows you to ingest 3rd party data from threat and fraud subscriptions or from your SIEM as a means of enhancing the Cequence findings.

To fully support your hyperconnected application environment, Cequence ASP uses a distributed, container-based architecture that allows you to deploy security wherever your applications are located – in the public cloud, the data center, or hybrid. CQ botDefense is deployed in conjunction with your load balancer so that it is close to the application, continuously sending a copy of all relevant traffic to CQAI and taking action as dictated by policy. Small and lightweight to ensure low latency and minimal impact, CQ botDefense is designed to fail-open in the event of a failure.

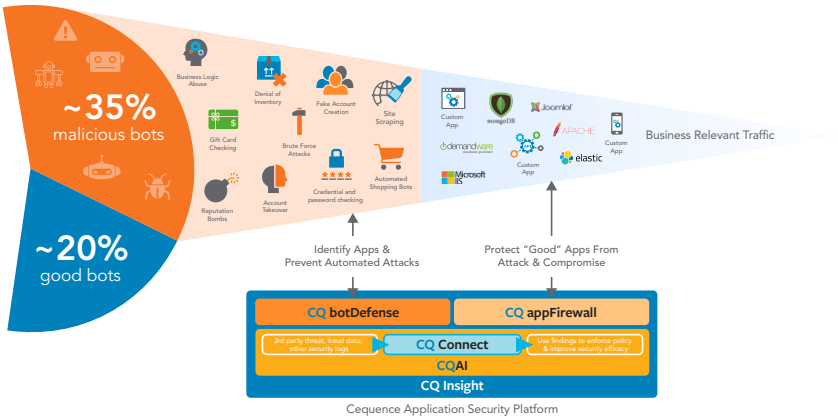


Cequence Application Security Platform

CQAI, CQ Connect and CQ Insight are deployed in a central location, performing analysis, providing visibility, dictating policy and enriching the existing infrastructure through CQ Connect import/export capabilities. This distributed approach to deployment allows organizations to quickly and easily support their ever-evolving public facing application infrastructures.

Consolidating Application Security with CQ appFirewall and CQ botDefense

Malicious bots represent a large portion of your web traffic. CQ appFW and CQ botDefense deliver on the promise of "better together", allowing our customers to improve their application security posture. CQ botDefense blocks malicious bot traffic, immediately reducing your threat footprint and the associated infrastructure load. If CQ appFirewall is enabled, it will then enforce policy to prevent data loss and infrastructure compromise brought on by vulnerabilities in your commercial or custom applications. Cequence ASP provides your team with full visibility into how a specific threat was detected to facilitate confirmation and ongoing analysis.



CQ Insight: Turning Actionable Intelligence into Policy

CQ Insight is the centralized management tool that provides visibility into your applications, their transactions, and any threats that may be hiding in plain sight. Armed with the knowledge of what the intent of your web, mobile and API-based application traffic is, you can build policies to protect your digital assets. Policy examples can include:

- **Quickly understand the characteristics** of your applications and attacks that are targeting them.
- **Deploy policies to prevent automated attacks** such as account takeover, credential stuffing and denial of inventory.
- **Enable attack-specific mitigation techniques** that may vary from alert or block to rate limiting and deception.

In addition to a visual summary of your application traffic and the attacks that may be targeting them, CQ Insight gives you the ability to add and modify custom rules, enable and disable system rules, and configure Cequence ASP.

About Cequence Security

Cequence Security is a venture-backed cybersecurity software company founded in 2015 and based in Sunnyvale, CA. Its mission is to transform application security by consolidating multiple innovative security functions within an open, AI-powered software platform that protects customers web, mobile, and API-based applications – and supports today's cloud-native, container-based application architectures. The company is led by industry veterans that previously held leadership positions at Palo Alto Networks and Symantec. Customers include F500 organizations across multiple vertical markets, and the solution has earned multiple industry accolades. Learn more at www.cequence.ai.

CEQUENCE™ SECURITY
100 Murphy Avenue, Suite 300, Sunnyvale, CA 94086 › 1-650-437-6338 › info@cequence.ai › www.cequence.ai
© 2019 Cequence Security, Inc. All rights reserved. Part#EN01203-3