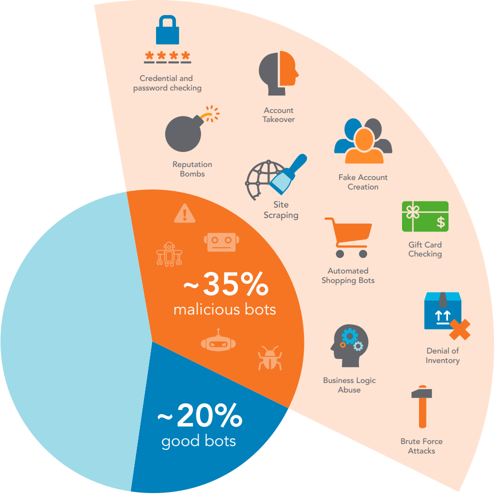
CEQUENCE™
SECURITY

CQ botDefense on Google Cloud Platform

Stop Malicious Bot Attacks Targeting your Web, Mobile, and API-Based Apps

Introduction



Organizations are adopting Google Cloud Platform to leverage the agility that the cloud provides; near immediate access to compute, networking, storage and a rich application infrastructure. Available globally, these resources can quickly expand to meet regional needs, or scale out, to meet performance or capacity demands. Further fueling the drive towards GCP are iterative and agile application development methodologies that leverage containers, microservices and orchestration tools that allow your development teams to rapidly deploy public facing web, mobile and API-based applications on GCP.

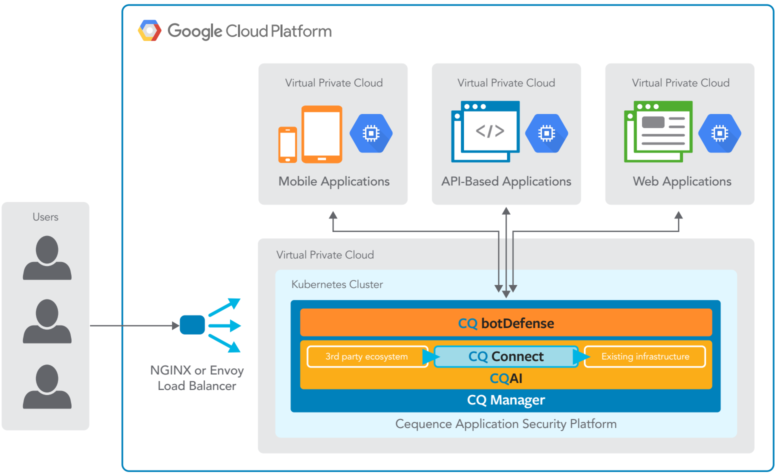
Simultaneously, attackers are using a rich repository of stolen user information and automation toolkits to programmatically target your applications with attacks that appear to be legitimate transactions. These malicious bots represent as much as 35% of the overall web traffic and for some customers, these attacks represent 90% or more of their web traffic, placing significant strain on all aspects of the business. Unless security is embedded into the application development workflow, your cloud-native initiatives can be delayed, or worse, be deployed without attack protection.

Traditional approaches to application security 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)

CQ botDefense is a Cequence ASP security module that allows your organization to fully understand and mitigate automated attacks targeting your public facing web, mobile and API-based applications deployed on GCP.

The intelligence of Cequence ASP resides with CQAI, a machine learning, analytics engine that automatically discovers your applications while uncovering threats and vulnerabilities that may lead to data loss or application infrastructure compromise. CQAI blends multiple techniques



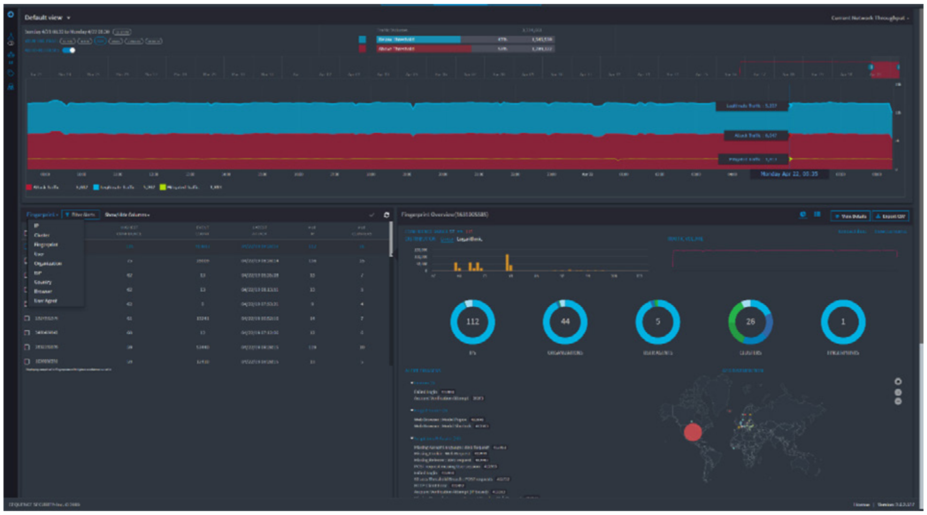
including heuristics header, protocol, and behavioral analysis, correlating across hundreds of client, network, and application traits to separate human from automated traffic. CQAI tracks attack behavior down to the level of intent to further distinguish malicious from benign automation.

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 in CQ botDefense. CQ Connect and CQ Manager allow you to more easily integrate the platform into your existing environment and to perform centralized management, respectfully.

CQ botDefense: Multidimensional AI-Based Bot Detection

C CQ botDefense reveals bots are spoofing their identity, browser, device or other traits, and exposes attack toolkits masquerading as valid browsers or mobile applications. Behavioral analysis of both user and application reveals signs of application abuse and fraud.

Additionally, by learning the unique behaviors of attackers, CQ botDefense can identify the intent of detected automation to distinguish malicious from benign automation such as valid content aggregators. CQ botDefense provides customers with full visibility into how a specific threat was detected, for easy confirmation and ongoing analysis. Behavior and statistics are tracked and auditable at a variety of levels to reveal anomalies in individual IP addresses, the organization, ASN, or geography.



Customizable Mitigation Options

CQ botDefense allows you to choose from a range of mitigation options that extend beyond traditional signature-based blocking. CQAI continuously tracks evolving bot behavior over long periods to ensure the most accurate detection without any impact on application performance or customer experience. 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.

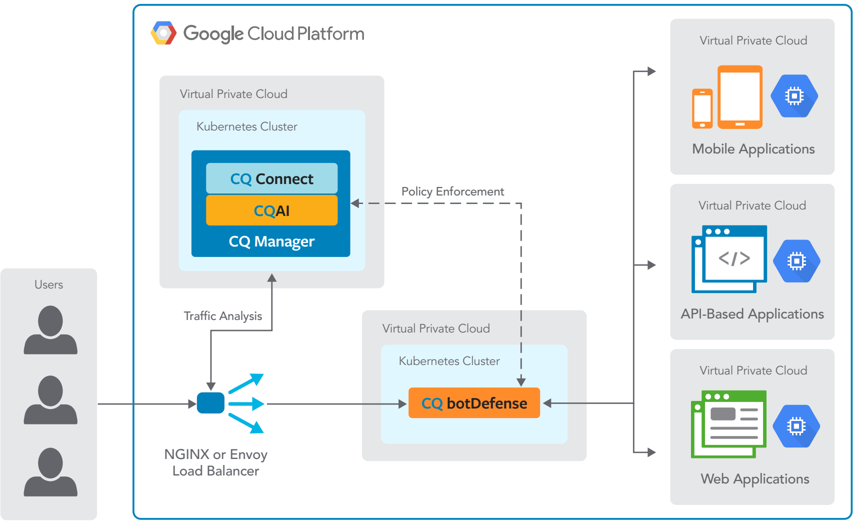
Using deception as a mitigation technique goes beyond traditional response mechanisms, allowing you to convince the attacker that their malicious efforts have been successful. A deception-based response disturbs the economic factors surrounding the attack, thereby impacting the ability for an attacker 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.

Embedding Security into Application Development Workflow

Cloud-native initiatives typically entail moving towards container and microservices 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-based applications from automated attacks without requiring additional instrumentation or SDK modifications. CQAI automatically discovers all applications and identifies changes so that the organization remains protected even as developers roll out new applications. CQ botDefense is also able to correlate across different application interfaces, fingerprinting an attacker that first targets a mobile application, then recognize that same attacker when they shift their attack to a web or API-based application.

Integrate With, and Extend Your Existing 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.



Cequence ASP uses a distributed, container-based architecture deployed in GKE. Traffic is analyzed by CQAI and if an attack is detected CQ botDefense can take 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.

As shown in the diagram, CQ AI, CQ Connect and CQ Manager are deployed separately, in 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.

CQ Manager: Turning Actionable Intelligence into Policy

CQAI provides the intelligence and analytics for Cequence ASP while CQ Manager 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 Manager gives you the ability to add and modify custom rules, enable and disable system rules, and configure Cequence ASP.