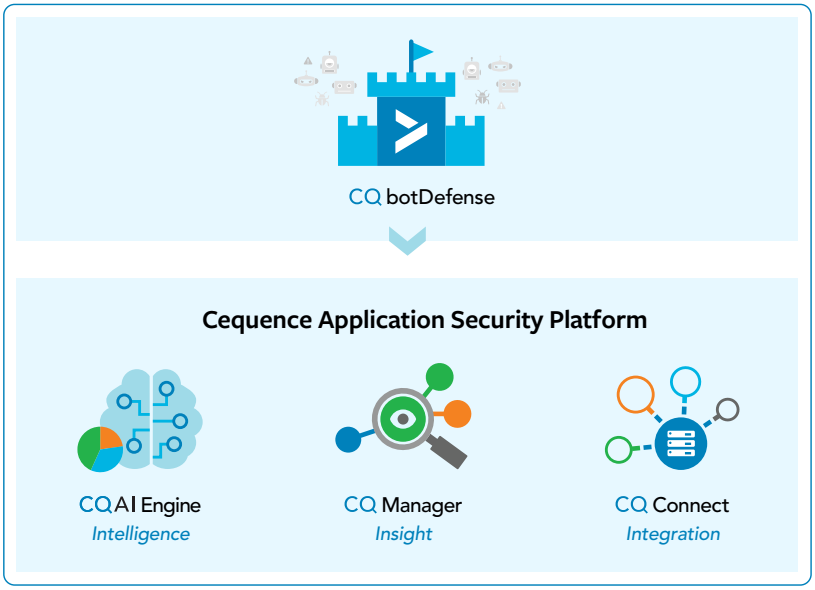
CEQUENCE SECURITY

CQ botDefense

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

Malicious bots account for more than 30% of all Internet traffic, but if your organization is a target for bot attacks, that percentage could be much higher. The CQ botDefense module works with the Cequence ASP platform to give organizations the fine-grained visibility and control needed to stop bots and automated attacks without impacting valid users and beneficial forms of automation.



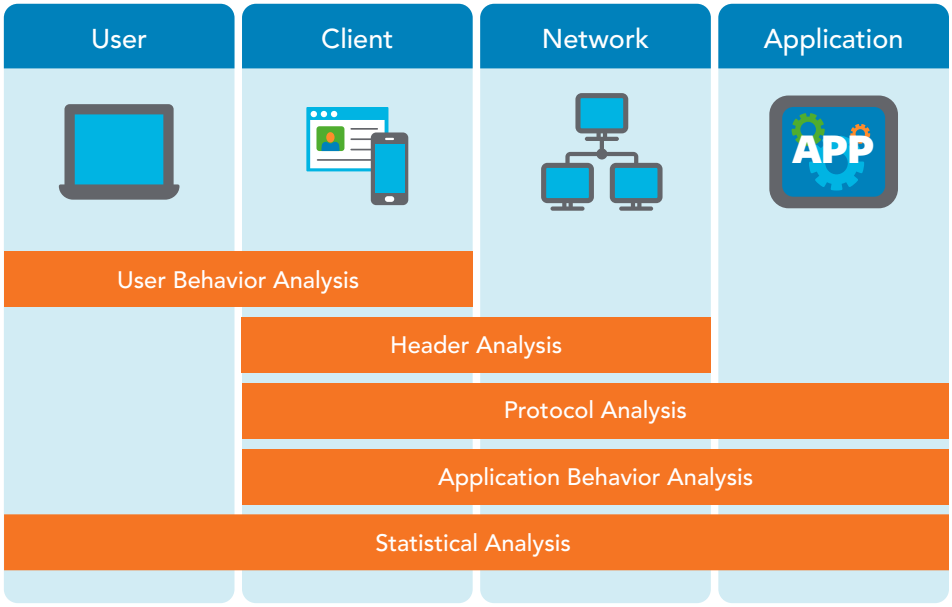
Protection From Malicious Automation

CQ botDefense harnesses the patent-pending intelligence of the CQAI analytics engine to separate human from automated traffic, and tracks behavior down to the level of intent to further distinguish malicious from benign automation. This allows Cequence to detect and defend against a wide variety of attack types including but not limited to:

Multidimensional AI-Based Bot Detection

CQ botDefense, working with Cequence ASP, represents a new approach to AI-based bot detection. Cequence analyzes and correlates across hundreds of client, network, and application traits to identify the signs of malicious automation and attacks conclusively down to the level of intent. The underlying CQAI analytics engine blends multiple techniques such as header analysis, protocol analysis, and behavioral analysis of both the user and application to establish a complete view of every interaction.

CQAI 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, the solution can identify the intent of detected automation to distinguish malicious from benign automation such as valid content aggregators.



Additionally, Cequence provides customers with full visibility into how a specific threat was detected, for easy confirmation and ongoing analysis. Behavior and stats are tracked and auditable at a variety of levels to reveal anomalies in individual IP addresses, the organization, ASN, or geography.

Deploy Once, Discover and Protect All Apps

CQ botDefense protects all web, mobile, and API applications from automated attacks without the need to customize the application. Cequence automatically discovers all applications and identifies changes so that the organization remains protected even as developers roll out new apps. CQ botDefense also has the intelligence to correlate across different application interfaces. For example, the solution can fingerprint an attacker first targeting a mobile application, then recognize that same attacker when he shifts to attacking the API.

Passive Detection, Active Mitigation, and Deception

Cequence uses a blended approach to the detection and mitigation of automated threats. Passive analysis ensures that CQAI can continuously analyze evolving bot behavior over long periods to deliver the most accurate detection, and without any performance impact on the application.

When CQ botDefense discovers malicious automation, staff can choose a variety of active responses that will trigger based on policy. Depending on the threat, this could include blocking, rate limiting DoS behaviors, or active deception of other automated attacks. CQ Connect, the API integration tool within the platform, also allows Cequence to trigger actions such as blocks in a WAF or firewall. Likewise, information can be routed to specific staff analysts, for example, sending suspicious accounts to the fraud team for review.

Deception offers a particularly powerful counter to automated attacks. For instance, deception can make an attacker believe a credential stuffing attack was successful. This disrupts the attack, feeds the attacker back bad data, and allows security teams to observe the attackers next steps and long-term intent, all while preventing the attacker from consuming resources of the actual application.

You can also learn more about the Cequence Application Security Platform by visiting our website's resources section: cequence.ai/resources.

CEQUENCE™ SECURITY
100 Murphy Avenue, Suite 300, Sunnyvale, CA 94086 › 1-408-978-3258 › info@cequence.ai › www.cequence.ai