# Stopping Fake Account Creation with Cequence Security

## Bots Abuse Legitimate API Access to Steal Data and Undermine Critical Business Applications

The age of the API has been touted by technologists, investors, and developers. Driven by IoT, mobile, automation, and a desire for openness, APIs have become the preferred method to access business logic and information for many organizations. Most business partners and corporate customers (and even some individuals) don't want to use another app – standard business relationships often now include API access for automatic exchanges of information.

Examples exist in travel, shopping, home, and industrial automation – all places where "good" bots use APIs to do work on behalf of users. Quietly, APIs have been embraced by attackers too, as the underdefended access method to critical business data. With automation – bots – and ever-increasing numbers of open APIs to target, attackers are finding green-field access to attack organizations. The difficulty of defense is compounded by the fact that attackers use the same methods that legitimate users do – automation.

1. Understand attack surface – across browsers, mobile apps, and APIs
2. Understand and differentiate attacks vs. normal app traffic
3. Automatically stop and mitigate attacks
4. Be deployable across different infrastructures and app access methods

## Existing Security Infrastructure Can't Stop API Abuse

Bots abusing API access look like normal network and application traffic. So much of the traditional network security infrastructure – firewalls and IDS/IPS – is blind to business logic attacks like API abuse. To a firewall, it looks like allowed traffic is accessing the API on the appropriate port. To an IDS or IPS tool, it is non-malicious traffic that doesn't exploit a known vulnerability. To a network-level device, a bot abusing an API is entirely indistinguishable from a business partner's aggregator accessing the API.

Many organizations deployed web application firewalls (WAFs) for a mix of compliance and security reasons. While WAFs do take a closer look at application traffic, they remain network devices, and they are typically still looking for traffic that exploits a known vulnerability. They can be tuned for finer-grained inspection, but that usually proves to be more pain than most organizations are willing to undergo – and typically that finer-grained inspection is for browser-based apps, not APIs.

Furthermore, WAFs are often co-located with web servers or load balancers, which, depending on the organization, may not even be in-path for access to some APIs. Unfortunately, for many organizations, WAFs are simply compliance checkbox items and are sidelined as security devices.

Finally, API gateways and anti-bot technologies focus on different problems and are ill-suited to stopping API abuse. API gateways typically focus on authentication and authorization – necessary, but not helpful with differentiating good from bad access. Most anti-bot technology deploys browser-based app protection (or optionally in some cases, a mobile SDK), focused on finding bots that impersonate end users – e.g., they use CAPTCHA as a primary mitigation technique. But in the case of APIs, there is no browser – and thus these types of anti-bot technologies are very limited in an API-first world. Defending API abuse means that the solution has to differentiate between good bots and bad bots.

## What's Needed: A Solution That Sees the API, Can Differentiate Between Access and Abuse, and Flexibly Stops Bad Bots from Harming the Organization

For many organizations, just understanding what APIs they have and the access to them is the first step. Surprisingly, many organizations may not even be aware of all the APIs in use across their infrastructure. Second, a solution has to be able to differentiate normal, desirable access and use of APIs from abuse and attacks as well as immediately send alerts to security teams. Third, a solution should be able to automatically stop attacks – either through its own mitigation capabilities or by working with surrounding infrastructure. Finally, integration flexibility is a requirement for most organizations – therefore it must be deployable in a variety of environments (public/private cloud, virtualization, containers, etc.), with ease – meaning no application changes.

## Cequence Application Security Platform Stops API Abuse

With a flexible, software-only approach, Cequence discovers, detects, and defends. Cequence's Application Security Platform (ASP) first delivers visibility. Far too many security teams don't have a clear picture of the resources they are protecting (in this case, the API) – components, network accessibility, locations, and criticality. Cequence ASP enables security teams to have a complete, automated discovery of the API in operation. In fact, many Cequence customers' initial deployments begin with discovery mode – "first, tell me what I have to protect."

**Cequence ASP spots API abuse.** Cequence is looking only at application level behavior and using machine learning AI to continually learn about what is appropriate for an organization's APIs. Furthermore, Cequence uses similar AI across all customers to understand good and bad bot behavior and the latest tricks attackers use to exploit business logic and dodge enterprise defenses. So Cequence ASP can identify API abuse when other security measures cannot.

- **Behavior** – subtle inconsistencies in presentation vs. actions (how the traffic identifies itself verses how it actually behaves), rates and response, sources and timing, and specific actions within the API
- **Network intelligence** – what's happening around the world – new attack or bot behaviors, new or changing attack infrastructure, newly known botnets
- **Specific to API** – learned or taught behavior particular to the API. It could be known good or known bad.

**Cequence ASP stops attacks.** Depending on how enterprises deploy, Cequence enables in-solution mitigation of abuse and attacks (block, alert, or even misdirect to fool the attacker into thinking that they are successful) or works with surrounding security and application infrastructure (firewalls, load balancers, WAFs) to block attackers and their bots. Furthermore, since Cequence has a native understanding of the API, it can enable an accelerated response for teams to remediate abused APIs – whether that response is to block natively, from infrastructure, or remediate with additional controls on or in the API.

**Cequence ASP deploys in any environment.** Cequence customers have deployed in traditional data centers, in public cloud and private cloud environments, across all sorts of virtualization and container infrastructures. Cequence provides a complete solution across all application access methods (web browser, API, mobile app) without time-consuming changes to the application or its infrastructure.

## API Abuse is Going to Happen – Cequence Makes Sure It Doesn't Happen to Your Organization

Because of the ubiquity of API access, and the expectation of increased API access to more and more business functions across internal and external customers, partners, and other third parties, organizations will continue to expose APIs publicly. This means that malicious actors will continue to attempt to abuse those APIs. Organizations must implement and maintain a strong capability to understand and monitor their exposure, ensure appropriate access, and stop abuse. Cequence delivers.

Learn more about the Cequence Application Security Platform by visiting our website's resources section at cequence.ai/resources or schedule a demo at cequence.ai/demo.

CEQUENCE™ SECURITY

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