Cequence Security on AWS
Prevent Fraud Caused by Account Takeovers and API-based Business Logic Abuse

Challenges: Automated attacks hide in plain sight
Stolen credentials, attack toolkits, and compromised infrastructure make it easy for bad actors to launch automated bot attacks against public facing API and web applications deployed on AWS.

By hiding in plain sight, looking like legitimate transactions, and oftentimes, targeting your exposed APIs directly, these attacks are difficult to detect and prevent with traditional security measures, such as a WAF, firewall, or identity management solution.

CQ botDefense: Innovative, ML-based platform prevents automated attacks
Complementing native AWS security features, CQ botDefense prevents fraud and theft caused by bot attacks against your API and web applications deployed on AWS. CQ botDefense uses machine-learning automation indicators to automatically and continually analyze your public facing applications, building an intuitive sitemap for complete visibility. Each transaction is analyzed to determine if it is legitimate or if it is part of a bot attack such as an account takeover, fake account creation, or business logic abuse. Malicious traffic can be automatically mitigated using a variety of response options including block, rate limit and deception. Alternatively, the results can be sent to another element of your AWS infrastructure for additional analysis or an alternative incident response.

Key Features
› Dynamic Machine Learning Continuously Discovers Apps and Detects Attacks: An agentless, ML-based analytics engine automatically and continually analyzes your application traffic, building an intuitive site map of your public facing web and mobile applications along with any exposed APIs. Customizable, ML-based automation indicators analyze traffic to detect and prevent automated account takeovers and API-based business logic abuse. The result: consistent security for web and mobile applications along with any exposed APIs.

› Customizable Rules and Policies: The knowledge of apps in use and those under attack can be translated into customizable policies that enforce a positive security model – allowing what you want while denying all else.

› Open, Extensible Platform: A rich management interface and a REST API allow you to control all aspects of your deployment and import or export data to enhance your security posture or perform post-mortem analysis and policy fine-tuning. Deployed as a SaaS offering hosted on AWS or as a customer managed image in your Amazon VPC, CQ botDefense allows you to place application security in the location that best suits your security and architecture requirements.

CQ botDefense is available on AWS Marketplace as a SaaS offering or it can be deployed on an EC2 instance in your Amazon VPC, providing you with flexible deployment options.
Customer Case Study: Preventing Romance Fraud Caused by Account Takeovers

<table>
<thead>
<tr>
<th>Challenges</th>
<th>Solution</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zoosk helps people connect and find romantic love. Unfortunately, bad actors have seized on the popularity of Zoosk as an opportunity to scam unsuspecting users and commit fraud through automated account takeover and fake account creation attacks.</td>
<td>The CQ botDefense ML-based analytics engine detects and prevents automated attacks targeting more than 25 Zoosk mobile application APIs. The analysis is done out of band, requiring no agents or mobile SDK with the results used for policy enforcement.</td>
<td>Romance scams associated with account takeovers, averaging $12,000 per incident, were stopped along with any incidental damage to the Zoosk reputation. Security induced friction was eliminated resulting in developer productivity goals being met consistently.</td>
</tr>
</tbody>
</table>

About Cequence Security

Cequence Security is a Select Technology partner and one of the launch partners for the APN Global Startup Program. The Cequence Application Security Platform with CQ botDefense complements native AWS security by preventing highly automated attacks on public facing applications. The agentless, ML-based approach effectively eliminates security induced delays by baking automated attack protection into your application workflow. As development teams publish new applications and updates, they are automatically discovered and protected by CQ botDefense. Learn more at www.cequence.ai/aws