DATA SHEET

CEQUENCE® SECURITY

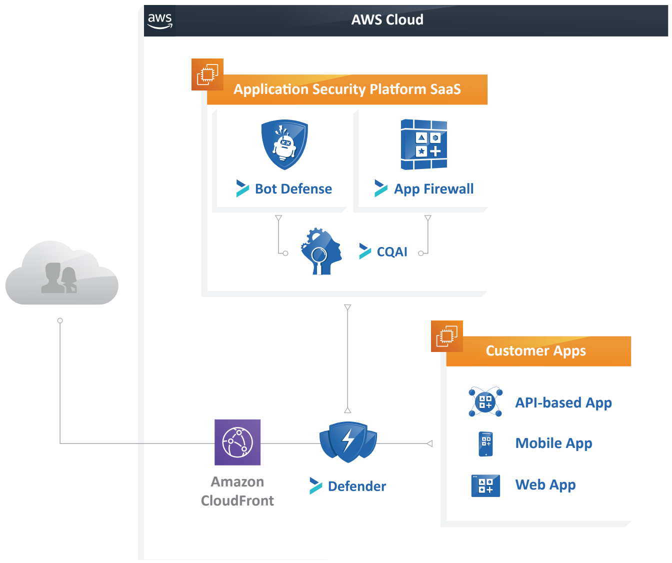
Cequence API Security Platform on AWS

ML-Powered Bot and Vulnerability Exploit Prevention

AWS is fueling the digital transformation for enterprises on a global scale while simultaneously reducing the associated operational burden. As new public facing web or API-based applications are released, bad actors will target them with automated cyberattacks to commit fraud and steal data. The Cequence API Security Platform (ASP) complements native AWS security services with an ML-based approach to detecting and preventing advanced bot attacks and vulnerability exploits.

Cequence ASP Snapshot

- Prevents fraud and data loss caused by bot attacks and vulnerability exploits.
- SaaS approach reduces operational burden while improving your security posture.
- Cequence manages the infrastructure, you manage the data and policies.
- Begin preventing attacks in as little as 24 hours via traffic redirect from Amazon CloudFront or other CDN to the ASP SaaS.
- Agentless approach eliminates need for JavaScript or SDK integration.
- Alternative deployment options include your own Amazon VPC, a datacenter or hybrid environment.



aws partner network

Advanced
Technology Partner

About Cequence Security

Cequence Security is an AWS Advanced Technology Partner and was one of the launch partners for the APN Global Startup Program. Together, we help protect our customers' APIs and web applications from cyberattacks that can cause fraud and data loss. Customers include F500 organizations across multiple vertical markets, and our solution has earned numerous industry accolades. Learn more at https://www.cequence.ai/aws/

At the core of the Cequence ASP is CQAI, a Machine Learning analytics engine that automatically discovers your public facing API and web applications, building an intuitive sitemap for complete visibility while analyzing the traffic to determine intent. CQAI findings can then be used to for policy-based enforcement.

Key Features

- **Dynamic Machine Learning Continuously Discovers Apps and Detects Attacks:** More than 160 customizable, ML-based automation indicators analyze traffic to continually detect and prevent automated attacks and vulnerability exploits – even as they retool to avoid detection. The result: consistent security for APIs and web applications – all managed from a centralized dashboard.
- **Customizable Rules, Policies and Response Options:** Users have full access to the ML-based findings and can use that visibility to enforce flexible mitigation policies. Predefined OWASP Top 10 and PCI DSS 6.6 policies stops exploits and addresses compliance requirements. Attack mitigation options include blocking, rate limiting, geo-fencing and deception. Using deception goes beyond traditional response mechanisms, allowing you to mislead the attacker into believing that their attacks have been successful, such as serving up stale content to price scraper bots.
- **Open, Extensible Platform Integrates with Existing IT Infrastructure:** CQAI findings can be exported to your existing IT infrastructure such as another security device for enforcement, a SIEM, or a REST API endpoint for post-mortem analysis or correlation. The REST API also allows you to import 3rd party threat data or credentials to further enhance CQAI analysis.

Case Study: Preventing Romance Fraud at Zoosk

Challenges	Solution	Results
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.	The Bot Defense 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.	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.