CEQUENCE SECURITY

Cequence Application Security Platform

ML-Powered Platform for Stronger Application Security

Introduction

Organizations that increasingly rely on APIs to power their business are often targeted by attacks that can cause online fraud, business logic abuse, exploits and unintended data leakage. Traditional approaches to preventing these attacks often require multiple point solutions that are largely ineffective and are hard to manage. What's needed is an innovative, ML-based platform that provides you with complete visibility and actionable intelligence to protect your modern application infrastructure.

Cequence Application Security Platform

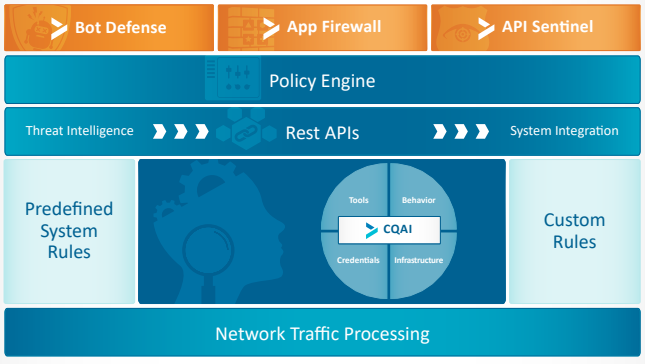
The Cequence Application Security Platform solves these challenges with the only Web and API Protection (WAAP) offering that unifies runtime API visibility, security risk monitoring, and patented behavioral fingerprinting technology to consistently detect and protect against ever evolving online attacks.

- **CQAI** uses customizable Machine Learning models to analyze web applications and APIs resulting in a unique Behavioral Fingerprint that determines malicious or benign intent. Findings are then used for policy enforcement or exported via a REST-based API to an existing component of your security infrastructure.
- **Bot Defense** enforces mitigation policies based on CQAI findings with a range of response options including blocking, rate limiting, geo-fencing and deception.
- **App Firewall** complements Bot Defense by enforcing vulnerability exploit prevention policies based on CQAI findings.
- **API Sentinel** integrates with your API management infrastructure to identify, inventory and analyze all your APIs allowing to discover and mitigate security gaps before they are published or exploited by attackers.

Cequence Application Security Platform

Delivers the most effective and adaptive web and API protection solution that enables your business to remain resilient in today's ever-changing business and threat landscape. Key benefits include:

- Eliminates security gaps that can result in compromise or data loss caused by shadow and non-conforming APIs with continuous discovery and monitoring
- Improves developer productivity by eliminating JavaScript and mobile SDK integration requirements
- Protects your applications with advanced security features in a matter of hours, not weeks or years



CEQUENCE APPLICATION SECURITY PLATFORM

Deployed as a SaaS solution, the Cequence ASP can begin protecting your applications in a matter of hours, with the most effective and adaptive protection from online fraud, business logic attacks, exploits and unintended data leakage. As a result, your applications and your business will remain resilient against today's ever-changing business and threat landscape.

CQAI: No JavaScript or Mobile SDK Required

CQAI uses more than 160 ML-based automation indicators to perform a multi-dimensional analysis of your web applications and APIs, resulting in a unique Behavioral Fingerprint that continually tracks sophisticated attacks, even as they retool to avoid detection. The in-depth analysis performed by CQAI brings the added benefit of identifying benign forms of automation such as approved content aggregators, that can then be managed with separate policies.

CQAI ML-based Analytics Engine

Bot Defense and App Firewall: Customizable Rules, Policies and Response Options

Application and attack analysis findings can be used to create and enforce custom policies that result in a positive security model – allowing what you want while denying all else. Predefined policies for OWASP Top 10 and PCI DSS 6.6 stops exploits and addresses compliance requirements. Discovered attacks can be mitigated using a range of response options including blocking, rate limiting, geo-fencing and deception, a technique that allows you to mislead the attacker into believing that their attacks have been successful.

> *We chose Cequence after extensive market research and found the Cequence AI platform to offer the best solution for the attacks we most often face.*
>
> Manager, Security and Risk Management, Financial Services, Gartner Peer Insights 5 Star Review

API Sentinel: Runtime API Inventory and Security Analysis

API Sentinel integrates with your API infrastructure to discover and inventory all your public facing APIs including shadow and unmanaged. Discovered APIs are continuously tracked and analyzed for specification conformance. Non-conforming APIs can be flagged and addressed by development to eliminate security gaps before they are published or discovered and exploited by bad actors.

Easily Integrates with Existing Infrastructure

REST-based APIs allow you to import 3rd party data to enhance CQAI analysis, or you can export the findings to your existing IT infrastructure for post-mortem analysis, correlation, or enforcement by your firewall or other security device.

Deploys in Minutes

Cequence ASP can be enabled to protect your web applications and APIs in as little as 60 minutes and can immediately begin reducing the operational burden associated with preventing attacks that can result in fraud or data loss. Alternatively, the modular, container-based architecture allows the ASP to be deployed in your data center, your cloud environment, or as a hybrid.

CEQUENCE SECURITY
100 Murphy Avenue, Suite 300, Sunnyvale, CA 94086 › 1-650-437-6338 › info@cequence.ai › www.cequence.ai