CEQUENCE

Solution Brief

Cequence Unified API Protection Solution

An Ideal RSA Silver Tail Replacement

Bringing Antifraud and Bot Mitigation (Security) Together

Much like Silver Tail, the Cequence Unified API Protection solution prevents fraud caused by account takeovers and fake account creation by analyzing application traffic collected from a range of network elements that are close to the applications being protected. Cequence UAP with CQAI automatically identifies your public-facing web applications and APIs, then immediately analyzes them using patented, ML-based analytics to uncover fraudulent activity.

CQAI uses more than 180 rules that can be customized to deliver "Analyst Workbench" like functionality that fraud analysts have become accustomed to with Silver Tail. CQAI discovers malicious activity and graphically displays it for viewing and data manipulation purposes. The REST-based API can be used to export the findings to external systems such as SIEMs and antifraud solutions, thereby encouraging security and antifraud team collaboration. In addition to export, the findings can also be used by security teams to immediately mitigate the malicious activity.

Analyze and Discover Fraudulent Activity with Less Effort

The Cequence Unified API Protection solution with CQAI uses a combination of customizable ML-models and an open, extensible platform to enable Silver Tail users to discover and address fraudulent activity with less effort.

Minimizes Analyst Manpower Dependency

The CQAI ML-based analytics engine performs the bulk of the analysis and eliminates the need for dedicated security analysts to be constantly monitoring and querying to detect bot attacks. Instead, some of those resources can be utilized to customize CQAI to look for "hard to find" attacks, such as those that are low and slow.

Customizable Analytics

CQAI includes a rich set of predefined ML-models, rules and policies that will look for malicious activity using volumetric patterns, known indicators of automation and business logic abuse as well as known malicious infrastructure (IP addresses, organization, country, etc.). ML-models, rules and policies are fully customizable, allowing your analyst team to fine-tune their investigation to address your unique requirements. A powerful set of Kibana-based query tools enables your team to perform more in-depth analysis of the raw data as needed.

Real-time Detection

CQAI is a streaming analytics engine, processing data as soon as it is sensed on the network to provide actionable results to both the antifraud and security teams, in real time.

Open Platform Facilitates Integration

Cequence UAP REST-based APIs allow you to import 3rd-party information from external systems such as threat feeds or credential dumps that can enhance the CQAI analysis and findings. The APIs also allow you to export findings to external systems for added analysis or mitigation.

Flexible Mitigation Options

In addition to the ability to export the CQAI findings, Cequence UAP offers a variety of mitigation options including block, alert, rate limit and geo fence. Responses can be customized per application with an agnostic approach to IP address and HTTP header field rotation. A deception option allows you deliver fake responses that appear to be real application responses.

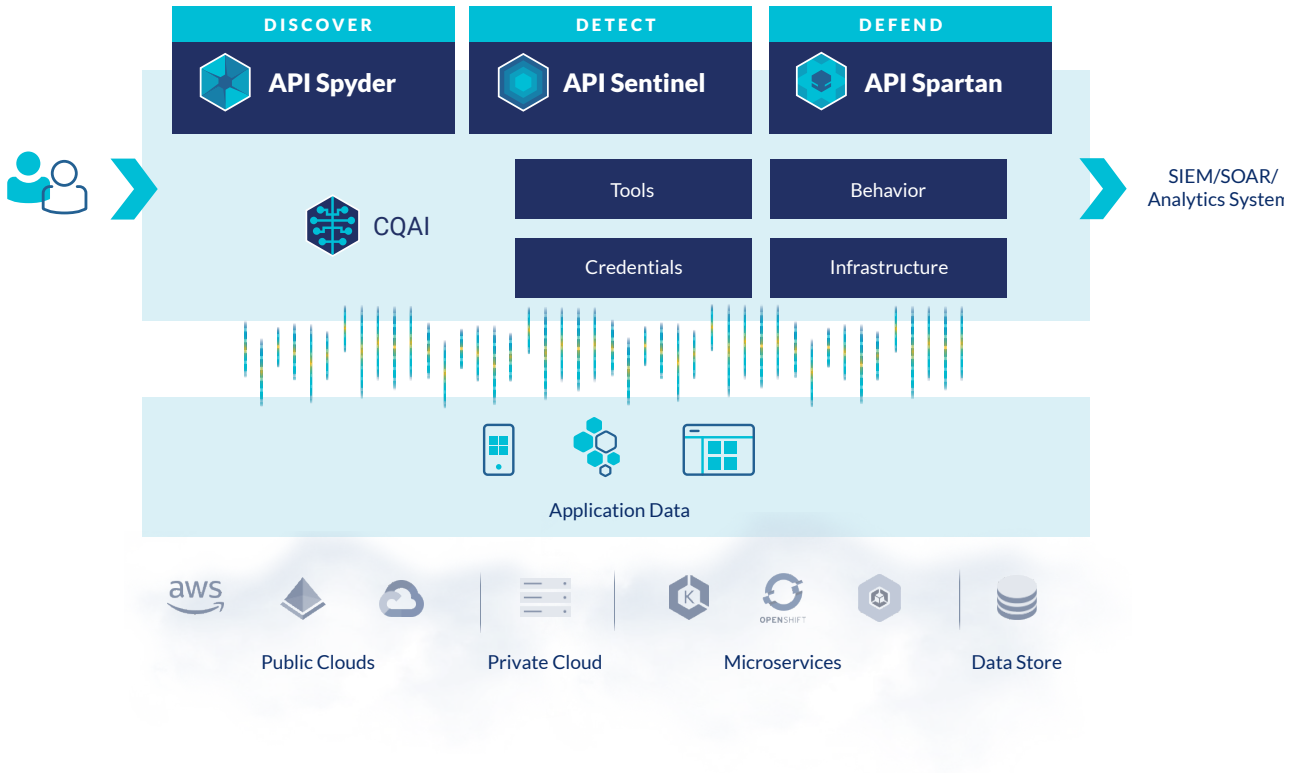
API, Web and Mobile Application Protection

Cequence UAP uses an agentless, ML-based approach to protect web and mobile applications along with their respective APIs without requiring any application changes or integration.

Bringing Antifraud and Bot Mitigation (Security) Together

Much like Silver Tail, the Cequence Unified API Protection solution prevents fraud caused by account takeovers and fake account creation by analyzing application traffic collected from a range of network elements that are close to the applications being protected. Cequence UAP with CQAI automatically identifies your public-facing web applications and APIs, then immediately analyzes them using patented, ML-based analytics to uncover fraudulent activity.

CQAI uses more than 180 rules that can be customized to deliver "Analyst Workbench" like functionality that fraud analysts have become accustomed to with Silver Tail. CQAI discovers malicious activity and graphically displays it for viewing and data manipulation purposes. The REST-based API can be used to export the findings to external systems such as SIEMs and antifraud solutions, thereby encouraging security and antifraud team collaboration. In addition to export, the findings can also be used by security teams to immediately mitigate the malicious activity.



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