CEQUENCE

Datasheet

Cequence API Spartan

ML-based API Attack Prevention

Introduction

The ubiquity of APIs combined with their ease of use and flexibility have made them the top target for attackers. Even perfectly coded APIs can be subject to business logic abuse as part of a large scale account takeover or shopping bot campaign. Mass fake account creation and content scraping campaigns are executed against high quality production APIs. Attackers are also finding and exploiting API vulnerabilities introduced by coding errors inadvertently released to production. Organizations need an open and extensible API protection solution that detects and prevents the full spectrum of API attacks including those that target correctly coded APIs and those that target API vulnerabilities as defined by the OWASP API Security Top 10 list.

API Spartan at a Glance

- **Reduces policy administrative** efforts and improves security posture with consistent protection for both web apps and APIs.
- **Accelerates incident response time** with complete visibility into automated attacks against APIs and web applications.
- **Improves the bottom line** High efficacy bot protection results in IT resource and manpower savings.
- **Ensures fraud prevention** that blocks unauthorized fraudulent activity from affecting your users or your business operations.
- **Unobtrusive SaaS deployment model** enables high efficacy protection in minutes, not weeks or years.

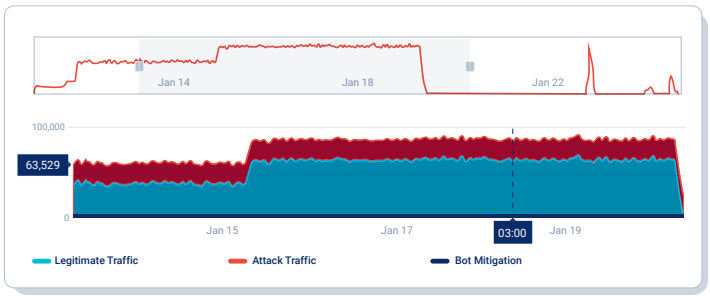
API Spartan Overview

API Spartan can fully protect your APIs by detecting and preventing cyberattacks natively in real-time with near zero false positives. It does not require any integration with JavaScript, mobile SDK, or web application firewall (WAF) to stop attacks that target your APIs. API Spartan leverages an ML-based analytics engine to analyze API and web application requests to protect your APIs from a full range of OWASP API and Web Top 10 lists and automated API attacks that ensure your business operations are never impacted.

API Spartan Features

Continuous Behavior-based API Threat Detection

API Spartan leverages the behavioral fingerprint created by the ML-based analytics engine to continuously track sophisticated attacks, even as they retool to avoid detection. Supported by the largest API threat database in the world, with millions of behavioral and malicious infrastructure records the analysis results are translated into out-of-the-box policies that can be implemented on high efficacy protection on day-one.



Stay Ahead of Attackers with Policy Customization and Automation

Unlike alternative offerings that require professional services to create policy or make changes all rules and policies can be customized to fit your unique traffic and detection requirements by your team or using assistance from our CQ Prime Threat Research Team. Policies can be modified in many ways, such as granular filtering on transaction elements such as request header, request body and query parameters allow you to selectively analyze API traffic and minimize the impact on all other traffic. The result is high-efficacy detection of attacks on your perfectly coded APIs as well as OWASP related API vulnerability exploits. As attacks escalate and change tactics, ML Auto Pilot can be used to automatically analyze findings and adjust policies in real-time to maintain prevention efficacy while conserving your valuable security resources.

Mitigate Attacks Natively and in Real Time

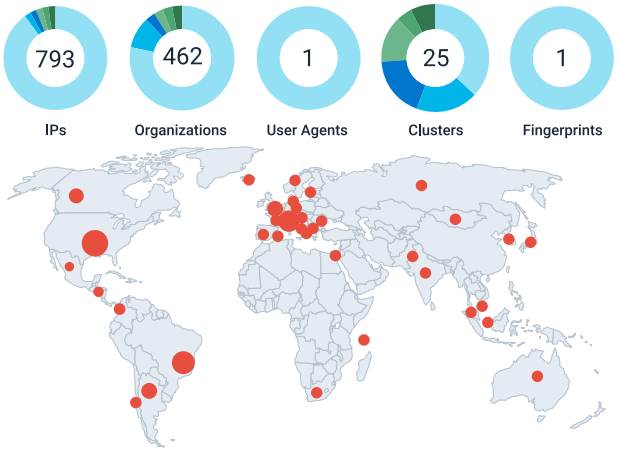
Discovered attacks can be mitigated natively, without the need to signal a WAF or other third-party solution, thereby ensuring you have end-to-end control over your API attack detection and mitigation. Flexible response options include logging, blocking, rate limiting, geo-fencing and deception, a technique that allows you to mislead attacker into believing that their attacks have been successful.

Fraud Prevention That Protects Your Users

Cequence Fraud Prevention delivered on API Spartan allows organizations to protect users from online fraud. Fraud teams can craft granular fraud policies that accurately detect and block unauthorized actions. Cequence empowers fraud teams to take back control, enabling them to be aware of the exact moment when fraudulent transactions take place, ensuring they are blocked so that they never disrupt your users or your business.

Integrates and Complements your Existing Infrastructure

API Spartan is an **open, extensible solution** with a rich, graphical user interface that allows your team to quickly analyze attacks, make policy decisions, and generate reports. Granular role-based administration enables access to specific features for different users or groups. REST-based APIs allow you to import third-party data to enhance 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

API Spartan SaaS **can be enabled** to protect your APIs and web applications in as little as 15 minutes and can immediately begin reducing the operational burden associated with preventing attacks that can result in fraud, data loss and business disruption. Alternatively, the modular architecture allows API Spartan to be deployed in your data center, your cloud environment, or a hybrid infrastructure.

API Threat Detection and Mitigation Partnership

In the event that your team needs assistance, the **CQ Prime Threat Research team**, curators of our database of API attack behaviors, malicious infrastructure, stolen credentials and toolkits, can be called upon to provide periodic guidance, or as a licensed service extension of your team where they work side by side to prevent threats. It's your choice.

API Spartan and the Unified API Protection Solution

As an integral component of the **Cequence Unified API Protection solution**, API Spartan provides your team with ML-based detection and prevention of automated attacks against your APIs and web applications. Organizations that have adopted an API first development methodology are using the Cequence Unified API Protection solution to view their API attack surface with **API Spyder**; then creating a run-time API inventory and monitoring compliance with **API Sentinel** while protecting them from exploits and business logic abuse with API Spartan and eliminating vulnerabilities with API testing.

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