CEQUENCE

Solution Brief

Cequence Fraud Prevention

Introduction

Skyrocketing levels of fraud, enabled by the adoption of digital commerce have overwhelmed fraud teams as they combat fraud campaigns that target their organizations. The surge in fraud has led to increased financial losses, decreased customer trust, and damaged brand loyalty. Banks, insurance, and fintech institutions are looking for a fraud prevention solution that enables them to accurately detect fraudulent activity as it occurs - blocking unauthorized actions in real time before they cause harm to their users and their business.

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 have taken place, ensuring they are blocked so that they never disrupt your users or your business.

Cequence Fraud Prevention Features

Customize to Your Fraud Use Case

Customers can implement very granular security policies that can match any organization’s fraud use case. Cequence Fraud Prevention includes a customizable rules engine that allows fraud analysts to define their own customer detection criteria. Cequence also allows fraud detection teams to upload their own proprietary datasets that can include lists of known rouge user accounts or high-risk users. Once uploaded, such data can be looked up by defined fraud policies that will upon matching a desired criterion, enable instant remediation and alert generation.

Prevent Fraud in Real Time

Once deployed, Cequence monitors all transactions to determine if they are made by legitimate authorized users or if they are made by fraudulent bad actors. Cequence monitors in real-time, immediately surfacing any anomalous behavior as it happens. Once transactions match configured fraud policy, customers have actions available that include blocking the unauthorized fraudulent transaction or generating an alert so that the fraud team can investigate further. Customers also have the capability to authorize their own private API which can suspend their customer account and, by extension the fraudulent transaction.

Automate Regulatory Compliance

Customers can deploy Cequence to monitor transactions ensuring that they can prevent financial fraud and money laundering while providing suspicious activity reports when unusual behavior is detected. Cequence can help you stop fraudulent activity while ensuring you comply with government regulations such as Electronic Fund Transfer Act and Bank Secrecy Act (BSA).

Fraud Prevention at a Glance

- ✓ **Granular and complex policies** can be implemented to satisfy any fraud use case.
- ✓ **Blocks fraudulent activity** as it occurs ensuring unauthorized actions never disrupt your business.
- ✓ **Rapid deployment** ensures customers can deploy in a matter of days not weeks.
- ✓ **Incident forensics** analyzes transactions to gain key insights into details of each fraud campaign.

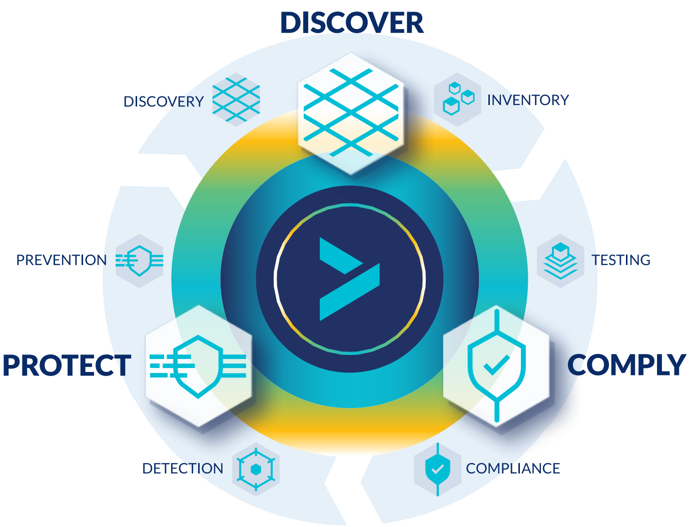
Deploy in Minutes

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.

Extend Your Fraud Team

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.

The Cequence Unified API Protection Solution



DISCOVER
with
COMPLY
with
PROTECT
with

API Spyder

Discovery: Viewing an organization's API attack surface from a threat actor perspective to know the unknown.

Inventory: Performing a comprehensive multi-cloud API inventory, including all existing APIs and connections.

API Sentinel

Testing: Integrating API protection into development, which shifts API security left within the organization, so risky code doesn't go live.

Compliance: Keeping APIs in compliance with specifications, standards and regulations such as OWASP and ensuring ongoing API governance.

API Spartan

Detection: Continuous scanning for threats, including subtle business logic abuse, fraud, and automated malicious activity from bots.

Prevention: Employing countermeasures such as alerts, real-time blocking, deception, without the need for added third-party data security tools.