CEQUENCE

Solution Brief

Cequence Fraud Prevention

Introduction

The rapid adoption of digital commerce has enabled ever-increasing levels of fraud that threaten to overwhelm unprepared organizations. The surge in digital fraud has led to increased financial losses, reduced customer trust, and damaged brand loyalty. Organizations need a fraud prevention solution that accurately detects fraudulent activity as it occurs and blocks unauthorized actions in real time before they cause harm to their users and their business.

Cequence Fraud Prevention enables organizations to protect users from online fraud. Fraud teams can craft granular, organization-specific 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 users or the business.

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 don't disrupt business.
- **Rapid deployment** ensures customers can deploy in a matter of hours.
- **Incident forensics** analyzes transactions to gain key insights into details of each fraud campaign.

Cequence Fraud Prevention Features

Customizable to Support a Variety of Fraud Use Cases

Organizations can develop and implement very granular security policies that can match their particular fraud use cases. Cequence provides 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 rogue 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

Cequence monitors all transactions to determine if they are made by legitimate authorized users or 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 the offending 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).

Deploy in Minutes

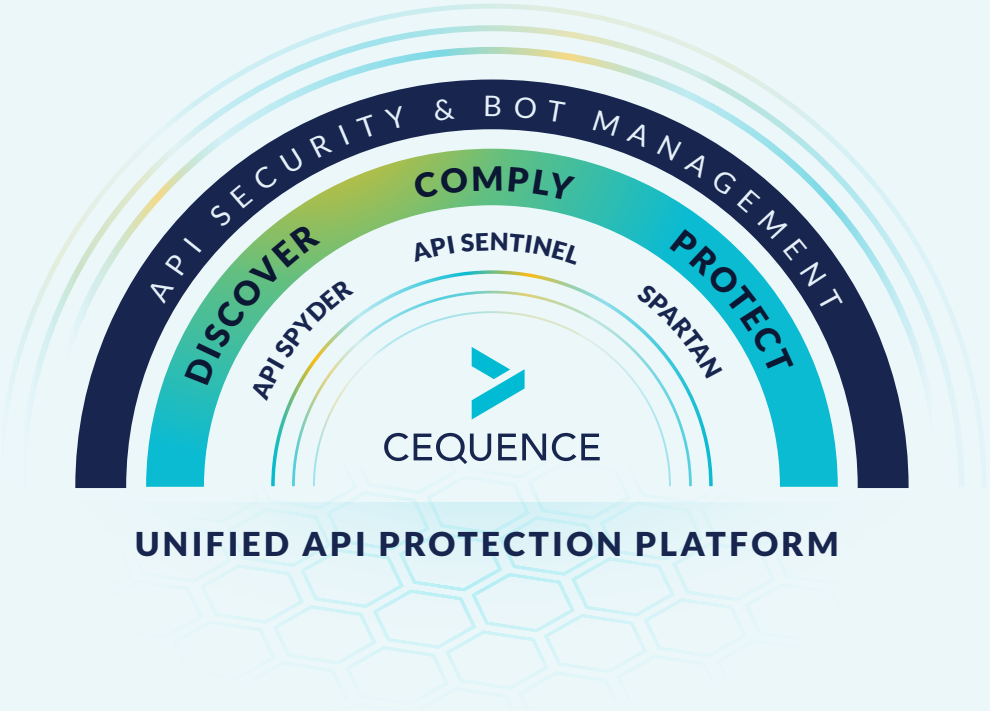
Cequence can be enabled to protect APIs and web applications in as little as 15 minutes and can immediately begin reducing the operational burden associated with preventing attacks that can result in fraud, data loss and business disruption. Alternatively, the modular architecture allows Cequence to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

Fraud Team Support

If an organization's team needs assistance, the Cequence 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 an extended team working side by side to prevent threats.

Cequence Fraud Prevention is Part of the Cequence Unified API Protection Platform

The Cequence **Unified API Protection platform** unites discovery, compliance, and protection across all internal, external, and third-party APIs to defend against attacks, targeted abuse, and fraud. Onboard APIs in minutes, without requiring any instrumentation, SDK, or JavaScript deployments. Cequence solutions scale to the most demanding government, Fortune and Global 500 organizations, securing more than 8 billion daily API calls and protecting more than 3 billion user accounts. The Cequence Unified API Protection platform also includes **API Spyder** for attack surface discovery, **API Sentinel** for API security posture management, and **Spartan** for bot management.



CEQUENCE

5201 Great America Pkwy, Suite 240, Santa Clara, CA 95054 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai