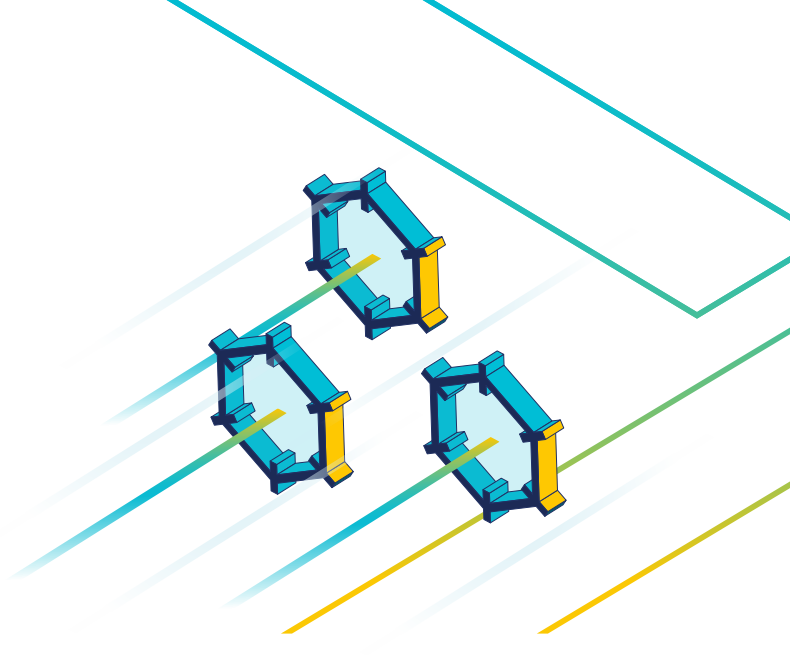
CEQUENCE

Case Study

Cequence Cuts Fraud Detection from Hours to Seconds



Incomplete Fraud Detection Took 3 Hours Too Long

One of the Largest Investment Firms in the World

The second largest investment firm in the world has over $7 trillion dollars in assets under management. It offers a wide variety of financial products to over 30 million retail investors that rely on this firm to manage their investment and retirement accounts. Their clients expect easy, secure, and uninterrupted access.

Key API Application That Powered Customer Access

The investment firm, in a highly competitive market, is expected to provide customers with opportunities to invest in a wide variety of financial investments, while ensuring they have secure and protected access to their online investment accounts. Due to their large asset size, they had become an attractive target for cybercriminals to initiate rolling cyberattack campaigns that aimed to gain unauthorized access to customer accounts. Once compromised, it allowed cybercriminals to exfiltrate money out of retail accounts for illegal financial gain.

Detecting account takeover (ATO) attacks had become a mission critical function whose responsibility was held within the fraud team. Every successful fraud attack on the investment firm's online retail accounts, eroded customer confidence, increased customer attrition, and damaged brand image.

Enormous Pressure on the Fraud Team

To prevent fraudulent transactions, the fraud team relied on identifying suspicious logins on their application programming interface (API) endpoints. The investment firm had an existing security tool, a post-forensic analysis product that they used to detect fraudulent transactions at each of their API endpoints. This solution was not working effectively since it took them up to 3 hours to identify if a fraudulent transaction had taken place. In addition, it still required an analyst to manually sift through thousands of transactions to surface potentially fraudulent transactions. This was extremely time-consuming and exhausting work that placed enormous pressure on the fraud team.

Cequence Detects All Fraud Traffic

The Cequence Unified API Protection (UAP) solution was introduced to the fraud team for faster identification of fraudulent activity that attempted to access their API application. In a matter of hours, Cequence assisted the investment company to configure security policies through API Spartan, a UAP component that enabled them to dramatically reduce the time it took to identify fraudulent activity.

Customer Profile

A worldwide investment firm with over $7 trillion dollars under management, serving over 30 million retail investors around the world.

Goals

- **Faster Fraud Detection** Enable faster fraud detection, reducing the amount of time required to detect fraud attacks.
- **Minimize Manual Analysis** Minimize the manual analysis work to detect fraud that was taking up to 3 hours a day.
- **Move to Proactive Security** Security team wanted to move away from constantly being in reactive mode to a more proactive security mode.

The Results

Cequence Helps to Reduce Fraud Detection Time, Saving Hours per Day

By deploying API Spartan, a component of the Cequence Unified API Protection (UAP) solution, they were able to now achieve their original business goals of reducing the amount of time and manual work required to detect malicious fraud attacks that targeted both their web and mobile applications.

They now were able to achieve the following:

- **Faster Fraud Detection:** Cequence was able to reduce fraud analysis time, shaving off hours of analysis time each day.
- **Automated Analysis:** By implementing Cequence, they eliminated hours a day of manual analysis that allowed them to focus on a narrow set of high probability fraud transactions.
- **Powerful Security Policy:** Cequence offered a powerful security policy language that allowed them to create custom security policies that could pinpoint targeted attacks.
- **Easy Deployment:** Unlike other fraud detection solutions, Cequence required no mobile SDK or JavaScript instrumentation to work since the required security intelligence is built into CQAI, Cequence's machine learning (ML) based technology which is used to analyze user behavior.

What They Achieved

- **Fraud Discovery Time:** With Cequence, their mean time to detect (MTTD) time was reduced from 3 hours to 30 seconds.
- **Detection Efficacy:** They were able to detect 100% of known fraud attacks which contrasted with their prior solution that required hours of manual work and was fraught with mistakes.
- **Analyst Productivity:** Their mean time to respond (MTTR) dramatically improved, enabling them to respond faster to a narrow set of high-probability fraudulent transactions, saving 4 hours a day.
- **Proactive Security:** The analysts moved from always being reactive to 100% proactive, enabling them to spend more time responding to attacks in a more productive manner.