CEQUENCE

Case Study

Fortune 500 Retailer – A Customer ROI Study

Cequence solution saves more than $1.7M in costs associated with bot attacks

Cequence Security is transforming API security with an award-winning AI-powered software platform that protects web, mobile, and API-based applications against bot attacks and targeted vulnerability exploits. This document profiles a Fortune 500 retail industry customer that deployed the Cequence platform and enjoyed not only strong application security, but also significant cost avoidance/savings by preventing bots from achieving their objectives (specifically, account takeover).

The malicious bot activity impacted the customer in numerous ways:

Customer Impact

- PII Theft
- Reward Points Theft
- Gift Card Theft
- Password Reset
- Account Lockout

Business Impact

- Increased Support Cost
- Fraud Related Loss
- Increased Load on Web, Application and Database Servers
- Brand Impact
- Customer Loyalty Impact

This ROI study is based on data collected at the online retailer over a year's time. Prior to deploying the Cequence solution, this retailer was made aware that a large number of its customer credentials were available in the cybercrime underground. Based on this information, the retailer conducted a proof of concept (POC) with 4 different bot management vendors. Cequence won the POC by a huge margin based on the internal scoring system that the customer developed for this trial. The customer subsequently purchased the Cequence platform, and has now been deployed for several years.

Although there are several problem areas associated with malicious bot activity, this study is based on a single use case of Account Take Over (ATO) due to the credential-checking attacks they were experiencing by malicious bots. ATO activity due to manual fraud was not considered as part of this analysis. Most enterprises deploy anti-fraud solutions to solve the manual fraud based ATOs.

Economic Costs of Malicious Bots

The economic costs of malicious bot activity can be categorized into two broad categories:

1. Cost of Compromised Accounts – Several factors are considered in this calculation, though it varies from company to company as well as industry to industry. In the retail space, if registered accounts have credit, cash, award balances, or automatic payment setup, the value per compromised account increases. Customer support costs and loss of business due to frozen accounts only add to the cost. Based on our engagement with this customer:

a. Cost of each compromised account was $50

b. Average number of accounts compromised per day = 1000

c. Eliminating duplicates, only 10% of the average accounts compromised per day are new and unique = 100

d. Percentage of customer base impacted per year based on 10,000,000 registered accounts = (100 x 365/10,000,000) % = 0.36%

e. Cost of compromised accounts per year = 365 x 100 x $50 = $1,825,000

2. Infrastructure Oversizing Cost – Excessive bot traffic causes applications to slow down, adversely impacting the user experience. Companies typically deploy more infrastructure than would otherwise be required to compensate for the resources consumed by the malicious bot activity. The additional infrastructure consists of hardware (servers, storage, and network components), network bandwidth, and hosting infrastructure. Based on the 60-95% range of bot traffic on the application, the excessive infrastructure cost was estimated to be $450,000.

The total annual cost is determined by combining the two categories above:

Compromised accounts	$1,825,000
Infrastructure oversizing	$450,000
TOTAL ANNUAL COST	**$2,275,000**

The cost avoidance/ROI delivered by Cequence Security is based on the following:

Cost of malicious bot attacks	$2,275,000
Investment in Cequence ASP	$500,000
RESULTS IN COST SAVINGS OF	**$1,775,000**

(a 455% payback in just two months)

Non-Measurable Costs

Apart from measurable costs, malicious bot activity harms organizations in other ways. For example:

1. Brand Impact – Customers expect companies to have best security practices that protect their personal and financial data. Notifying customers of their account being breached is not a positive experience, requiring customers to go through several steps in order to recover their accounts. In the process they may lose personal and credit card information, leading to additional pain. This poor customer experience causes brand damage and often results in significant customer loss.

2. Increased Staffing and Processes – Dealing with a continuous, high volume of compromised accounts forces companies to increase staffing in customer support, operations, security, legal, etc.

Summary

The Cequence Security deployment yielded a 4.55x return on investment for this retail customer, with a payback period of 2 months. Apart from the measurable ROI, the retailer's negative brand impact was reduced, customer experience was improved, and the customer service and support load was significantly reduced.

About Cequence Security

Cequence, a pioneer in API security and bot management, is the only solution that delivers Unified API Protection (UAP), uniting discovery, compliance, and protection across all internal and external APIs to defend against attacks, targeted abuse, and fraud. Requiring less than 15 minutes to onboard an API without requiring any instrumentation, SDK, or JavaScript integration, the flexible deployment model supports SaaS, on-premises, and hybrid installations. Cequence solutions scale to handle the most demanding Fortune and Global 2000 organizations, securing more than 8 billion daily API calls and protecting more than 3 billion user accounts. To learn more, visit **www.cequence.ai**.