CASE STUDY

Fortune 500 Retailer - A Customer ROI Study

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

Introduction

Cequence Security is transforming application security with an award-winning AI-powered software platform that protects web, mobile and API-based applications against automated bot attacks and targeted vulnerability exploits. This document profiles a 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 activity).

The malicious bot activity impacted the Retailer in multiple ways

1. Customer Impact:
   - PII Theft
   - Reward Points Theft
   - Gift Card Theft
   - Password Reset
   - Account Lockout
2. 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 a F500 online retailer over the past year. Prior to deploying Cequence Security's solution, this retailer was made aware that a large number of its customer credentials were available in the cyber-crime underground. Based on this information, this retailer conducted a proof of concept (POC) with 4 different Bot Mitigation vendors. Cequence Security won the POC by a huge margin based on the internal scoring system that the customer developed for the POC. The customer purchased the Cequence platform, and it has been deployed at the retailer for more than a year.

Although there are several problem areas associated with malicious bot activity, this study is based on only on one use-case – Account Take Over (ATO) - due to the credential-checking attacks they were experience 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 Cost of Malicious Bots

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

1. **Cost of Compromised Accounts** – Several factors determine this number, and it may vary 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 cost and loss of business due to frozen accounts, add to the cost. Based on our discussion with this retail 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 and impact user experience. Companies deploy more infrastructure than required to compensate for the resources consumed by the malicious bot activity. Excessive infrastructure consists of hardware (servers, storage, 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)

Not Measurable Cost

Apart from measurable cost, malicious bot activity can harm a company in other ways. For example:

1. **Brand Impact** – Customers expect companies to have best security practices that protect their private data. Notifying customers of their account being breached is not the best experience. Customers have to go through several steps in order to recover their accounts. In the process they may lose personal and credit card information, which leads to more customer pain. This bad customer experience leads to brand damage and may result 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 and operations.

Summary

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

About Cequence Security

Cequence Security is a venture-backed cybersecurity software company founded in 2015 and based in Sunnyvale, CA. Its mission is to transform application security by consolidating multiple innovative security functions within an open, AI-powered software platform that protects customers web, mobile, and API-based applications – and supports today's cloud-native, container-based application architectures. The company is led by industry veterans that previously held leadership positions at Palo Alto Networks and Symantec. Customers include F500 organizations across multiple vertical markets, and the solution has earned multiple industry accolades, including 2018 Gartner Cool Vendor. Learn more at www.cequence.ai.