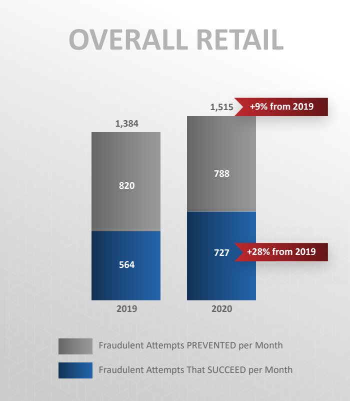
SOLUTION BRIEF

CEQUENCE® SECURITY

Stopping Automated Attacks Against Retailers

Retail environments are lucrative targets for cybercriminals (and competitors) to launch automated malicious attacks, including account takeovers, content scraping, and automated shopping. Executed against either the web or mobile application, or the supporting APIs directly, these attacks appear to be legitimate transactions, are difficult to defend against and if left unchecked can introduce significant business risks, including:

- **Financial and administrative losses** caused by awards points, gift cards, or product theft as a result of an ATO.
- **Lost sales** to competitors who scrape content, code, pricing, and images, then offer a lower price.
- **Damage to brand and customer loyalty** as a result of automated shopping bots, excluding legitimate buyers.

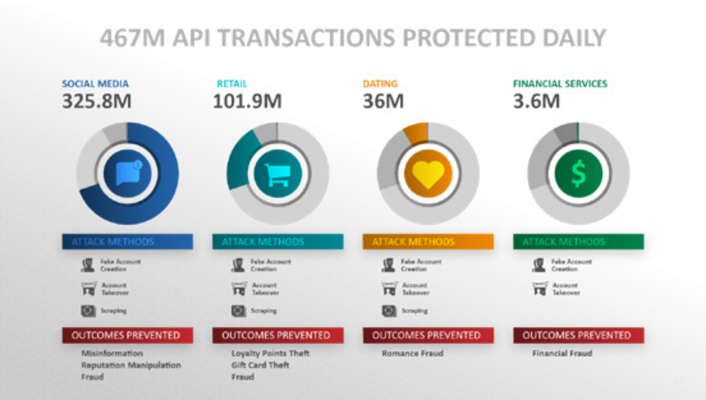


According to the 2020 Lexis Nexis True Cost of Retail Fraud, every $1.00 in retail fraud carries an actual cost of $3.34. As shown in the image from the same report, retail fraudulent transaction prevention efforts are successful a mere 52% of the time up 9% year over year. While a 9% improvement is encouraging, the statistics show that attackers are winning with a success rate of 48%, a 28% increase year-over-year. Retailers need to advance their bot prevention to keep up with the cybercriminals.

Limitations of Traditional Defenses

Many organizations turn to first-generation bot detection vendors to address automated attacks against their APIs with limited success due to their client-based (JavaScript and mobile SDKs) approach. These approaches introduce significant challenges to today's fast-moving retail environments, including:

- **Application deployment delays** caused by added application development, QA, and validation cycles.
- **User dissatisfaction** from slow webpage load times and forced mobile app upgrades.
- **Inconsistent protection for APIs** caused by the inability to inject a telemetry collecting agent into API traffic.
- **Lack of sustained efficacy** due to exposed client-side code that attackers can analyze and then evade.



Solution: The Cequence Application Security Platform

On a daily basis, the Cequence Application Security Platform with Bot Defense protects nearly half a billion API transactions across a range of industries including retail, which represents 22% of those transactions. Bot Defense is the only solution on the market that does not require the use of JavaScript or a mobile SDK to collect attack telemetry.

Bot Defense is based on CQAI, an ML-based analytics engine that enables retail organizations to automatically discover API, web, and mobile application endpoints and build an intuitive site map for visibility and policy-based protection. Then, using over 150 customizable automation indicators, CQAI determines the intent of each transaction request. If malicious activity is detected, organizations can use customizable Bot Defense mitigation policies using multiple response options such as blocking, rate-limiting, or deception. The agentless, ML-based approach can be deployed quickly and helps IT security and fraud teams achieve the following security objectives:

- **Prevent patterns of misuse** that can lead to fraud and user dissatisfaction.
- **Protect newly deployed APIs and web apps automatically** – no instrumentation required.
- **Unify protection across all application channels**, including web, mobile, and API.
- **Detect and prevent GET-based attacks** that are often missed by agent-based approaches.

Customer Spotlights

Stopping Loyalty Points Theft

Account Takeover

This retail customer was faced with extreme user dissatisfaction and financial losses due to loyalty points theft as a result of large scale account takeover attacks. The bad actors were able to evade the incumbent defenses using both validated credentials and automated toolkits with predefined attack configurations. With Cequence Bot Defense deployed across 20+ web and API endpoints, automated account takeovers have been reduced by 99% along with the associated costs of loyalty point theft.

Defending Against GET-based Scraping

Scraping Attack

A large European retail customer was fighting a loosing battle with high volume content scrapers who evaded their client-based protection mechanisms by performing the scraping attacks on APIs, using HTTP-get method, instead of a POST-method. This meant that the incumbent solution (JavaScript-based) prevention telemetry could not be collected, and the attacks succeeded. Cequence Bot Defense takes a different, agentless approach that can detect and mitigate the GET-based attack against APIs consistently and with a higher degree of efficacy than the competition.

Preventing Automated Shopping

Automated Shopping Bot

Automated shopping can be a double-edged sword. On one hand, the retailer is selling their goods, albeit to organizations that may then resell them for a higher price. On the other hand, loyal customers who want to purchase the products for their use are missing out, and possibly going to a competitor. For this retailer, Cequence Bot Defense quickly detected the automated activity and separated the malicious from legitimate using the trained ML models in CQAI. The customer was then able to implement the appropriate blocking or rate-limiting policies.

To learn more and to sign up for a 30-day free trial, please visit www.cequence.ai.

CEQUENCE® SECURITY