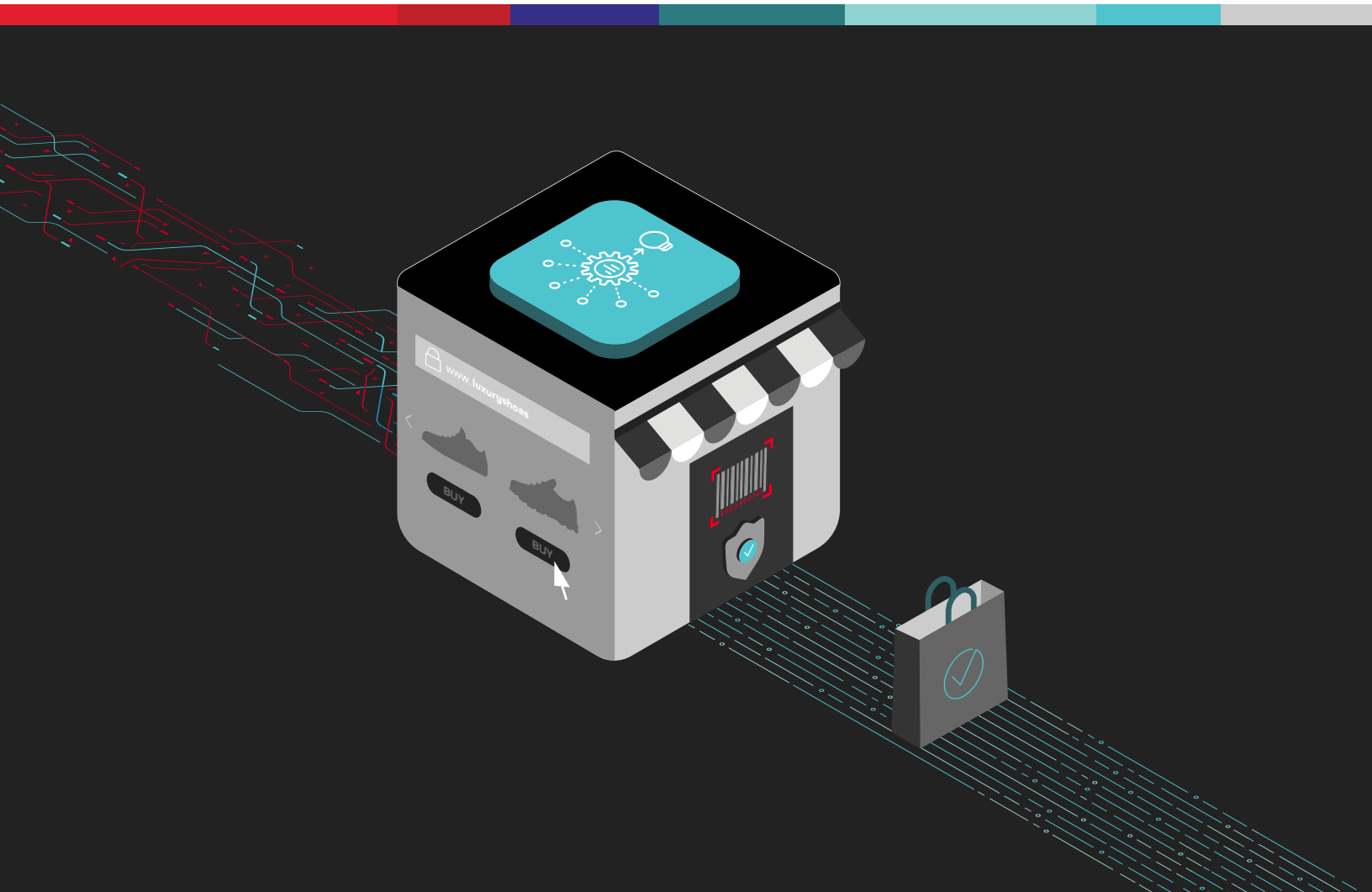
CASE STUDY

Retailer Solves Shoe-Bot Spikes, Fixes Fraud, Friction and Fake



CHALLENGING LANDSCAPE:
THE 5 PAIN POINTS

- Fraud and chargebacks
- BOPIS theft
- Shoe scalpers
- Server outages
- Gift card cracking

The Customer

A North American chain of department stores has a robust brand that stands for luxury, legacy, and customer satisfaction. They operate stores in North America and numerous outlets in Asia Pacific.

The retailer's bedrock belief is in innovating to improve customer experience, both in-store and online. They strive to provide a friction-free shopping experience with easy login, hassle-free gift cards, and stored payment information. They pioneered "buy online, pickup in-store" (BOPIS).

One of the retailer's flagship promotions is the fanfare surrounding its release of limited-edition sneakers from marquee brands with a-list celebrity endorsements.

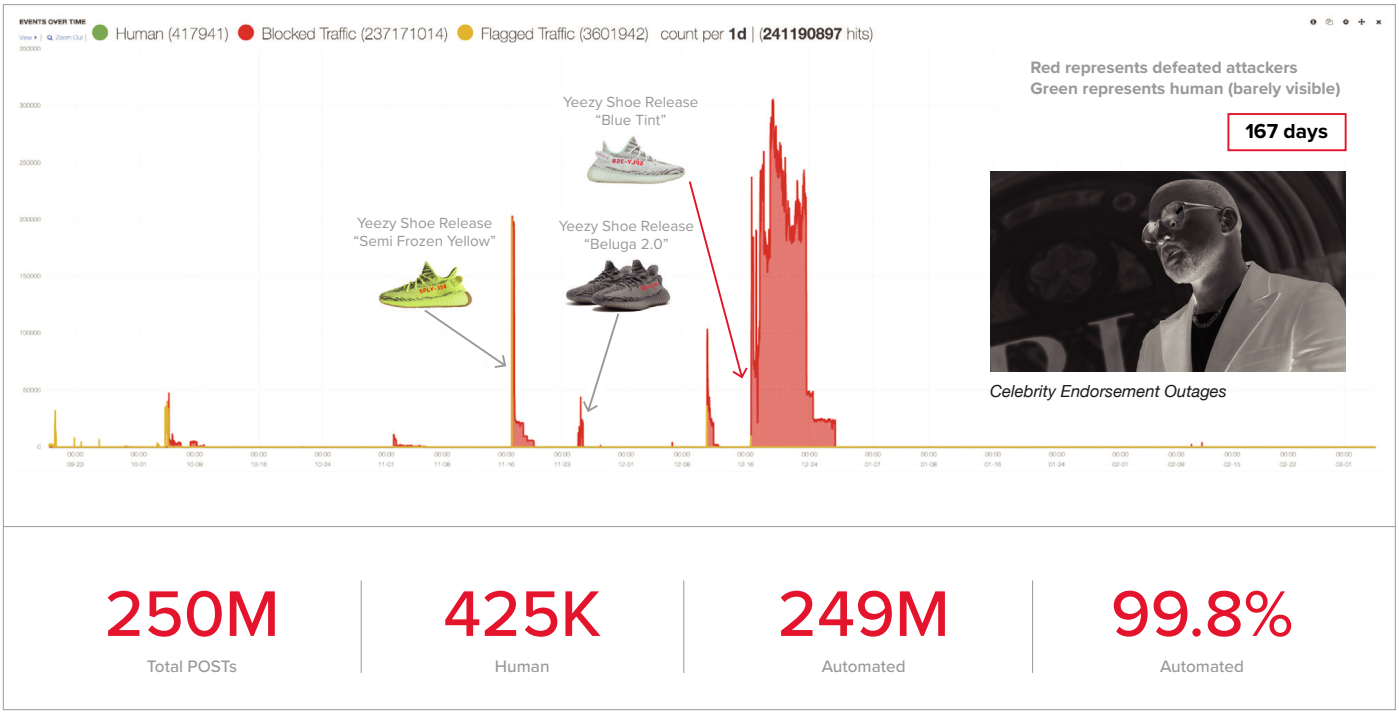


Figure 1: Attack traffic

$500K SAVED IN THE FIRST 30 DAYS

The Challenge: Fraud vs Friction

The retailer's dedication to a friction-free shopping experience opened the doors to rapacious automation attackers, resulting in five pain points for the company's IT and loss departments.

CHALLENGE 1: FRAUD AND CHARGEBACKS

Attackers launched credential-stuffing campaigns against the retailer, using logins from credential spills to perform account-takeovers (ATO) and plugging in stored payment information to buy and ship expensive luxury items. The retailer was paying twice: once to the attacker, and again to the customer with the chargeback. Even worse was the loss of customer trust.

CHALLENGE 2: BOPIS FRAUD

Attackers also targeted the retailer's BOPIS system. After they bought items online using stored payment data from compromised accounts, a mule would shuffle up to retrieve the merchandise in-store before the fraudulent charges were noticed by victimized customers.

CHALLENGE 3: SHOE-BOT SCALPERS

The retailer periodically featured special promotions around limited-edition athletic footwear. The shoe supply was restricted to only a few hundred pairs. Consumers were excited to buy these on "drop day," but automated shoe-bots were snapping up the entire inventory within seconds of the release, causing high bounce rates and frustration among real human users.

CHALLENGE 4: SHOE-INDUCED SERVER OUTAGES

The shoe-bots hammered the retailer's online store relentlessly during the campaign. The retailer knew that most of the traffic polling their shoe sale was automated, but they could not tell the difference between human and bot. The flood of automated queries led to severe disruption, indicated by high numbers of internal server errors. This impacted the conversion of all other products, not just the footwear.

CHALLENGE 5: GIFT CARD CRACKING

Fraudsters were testing millions of 16-digit gift card number combinations to find cards that had been purchased but not yet used. When the attackers cracked a card, they would suck out the value, either through combining balances or buying merchandise.

"CAPTCHAS SIMPLY DO NOT WORK AND CAUSE HIGHER BOUNCE RATES AND CART ABANDONMENT."
-CIO of retailer

The Decision

The retailer first tried to combat the attackers by implementing traditional countermeasures. They added a CAPTCHA during their checkout process, but the result was the opposite of what they were looking for. The CAPTCHA did not reduce fraud at any significant level, and the additional user experience friction led to high shopping-cart abandonment rates among real human users.

The retailer also tried blocking by IP address, but the attackers quickly adapted using proxies to get around the blocks (proxies for this purpose cost only $2 per 1,000 IPs). Managing the blacklists became a full-time job for the retailer's IT staff, leaving them no time to do their actual jobs. Finally, the retailer tried to block by geographic region, but found that this led to too many false positives and, again, did not result in a significant reduction in fraud.

THE RETAILER NEEDED A SOLUTION THAT HAD THE FOLLOWING CHARACTERISTICS:

- Maintain convenience (stored payment)
- Had 0% additional user-experience friction
- Had low false-positive rates

The retailer turned to Shape Security, which could proactively mitigate fraud without adding friction to the customer-experience journey.

The Outcome

There are two stages to a Shape deployment: observation and mitigation. In observation mode, Shape analyzes incoming requests and learns the retailer's traffic profile to create a tailored defense. Shape and the client collaborate on the most optimal defense with low false positives before Shape goes into mitigation mode.

"FROM DAY ONE, WHEN SHAPE WENT INTO BLOCKING MODE, WE SAW A NEARLY 100% DROP IN FRAUD FROM AUTOMATION."
-CIO of retailer

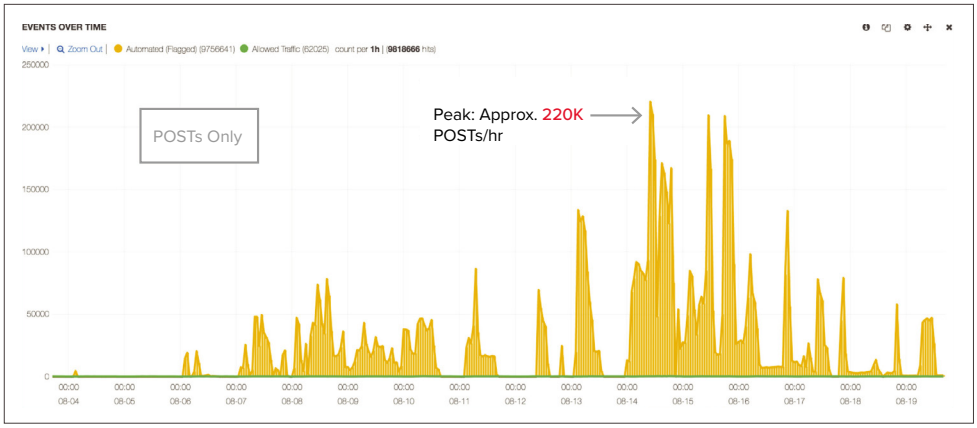
Shape confirmed the retailer's suspicion that the lion's share of web traffic was automation. During shoe promotions, automation comprised an astonishing 99.8% of page requests. Bots also made up 98.5% of visitors to their gift card-balance page. Overall, the automation of page requests for the web property was 97%.

During observation mode, Shape recorded thousands of successful account-takeovers, projecting an annual rate of more than 50,000 ATO per year. The attackers' credential-stuffing campaigns were peaking at more than 250,000 requests per hour.

"SHAPE PROVIDED US, FOR THE FIRST TIME, VISIBILITY THESE WERE FAKE CUSTOMERS. FAKE PEOPLE. 99 TIMES OUT OF 100, IF SOMEONE WAS TRYING TO CHECK THE BALANCE OF A GIFT CARD, IT WAS AN ATTACKER."
-CIO of retailer

After three weeks of observation, Shape and the retailer went live with mitigation. The results were immediate. In the following 30-day period, the retailer saved over $500,000 in fraud that would have been lost due to account-takeovers and gift card cracking.

The attackers twice attempted to retool around Shape's defenses. Because Shape tracks marauders using hundreds of client signals, they were automatically found and blocked again. In the words of the retailer: "While customers are loyal, fraudsters are not; once we stopped them, they went away".



With automation attackers repelled by Shape, the origin servers saw only the human visitors—a mere 1% of the previous load. By reducing 99% of traffic, Shape lifted “a huge burden off our infrastructure, which had a direct positive impact to revenue.”

Internal server errors went away and real customers could once again buy limited-edition athletic footwear. The retailer was delighted to pull CAPTCHAs from every part of their site, removing user friction and restoring the smooth customer-experience journey.

Freedom to Innovate

Finally, and perhaps most significantly, after “seeing how effective Shape was in preventing all types of fraud, from account-takeovers to gift card cracking,” the retailer was able to free up staff to focus on their customers, offering interactive experiences and promotions and getting back to their bedrock belief in innovation.

To learn more, contact your Shape Security or F5 representative, or visit shapesecurity.com or f5.com.