GlobalDots

Retailer Saves $500K/mo and Increases Revenue with Anti-Bot Innovation

Case Study

In collaboration with

SHAPE

Background

In an era which sees an uplift in every retailer's ecommerce share, website performance and security can make or break the business.

Cloud innovation leader and technology partner GlobalDots, joined forces with Anti-Fraud innovator Shape Security (part of F5) to deliver a holistic eCommerce security solution that boosts overall profitability; One that filters out bad bots and reduces operating costs, while delighting legitimate customers with a smooth, converting shopping experience.

The real big winners of eCommerce surge

2020 saw the largest year-over-year growth in eCommerce sales. Throughout this growth, fraudsters continued to develop sophisticated attacks to fill their pockets. One of the most devastating attack types is automated fraud: bots that mimic the actions of a real customer so they can bypass fraud prevention tools. These bots use fake identities to gain access into an eCommerce site allowing it to initiate fraudulent transactions like chargebacks, account takeovers, or gift card skimming.

This caused malicious bot traffic on retailer sites to skyrocket. Nowadays, it's not uncommon to see malicious bots comprising 99% of an eCommerce site's traffic.

So, what can be done to protect your store from online fraudsters while still maintaining an exceptional user experience for your real customers?

How Does Automated Online Fraud Occur?

Automated online fraud occurs at every step of the buying process. Upon entering a site, automated online fraud can begin through price scraping, stealing your content, or blocking inventory. Account creation is also susceptible to fake accounts associated with abuse of incentive programs.

Your login page is typically the most susceptible page to automated online fraud through credential stuffing and account theft. Once an account is stolen, the fraudster can utilize the stolen account's loyalty points. Alternatively, automated online fraud can occur in the form of gift card cracking where an online bot inputs random characters for redeeming gift cards. Even the checkout page is susceptible to scalping credit card information.

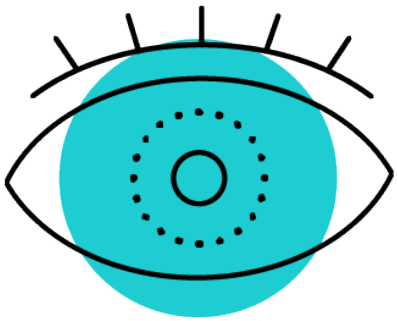
Business Implications of Automated Online Fraud

Each fraudulent transaction ends up costing the eCommerce business money in one way or another.

For example, most website hosting providers offer a set number of visitors or data in each plan, so an artificial increase in these numbers caused by malicious bots can force a business to upgrade its web hosting servers. Given that malicious bots can comprise up to 99% of an eCommerce site's traffic, a site may need a hosting plan that's x100 more than the volume of legitimate traffic. Now, just imagine how bot traffic may inflate your cloud and CDN costs.

On top of directly costing online retailers money, automated online fraud also results in a loss of existing and potential revenue. The security features you implement in order to prevent automated online fraud also impact your customers. These security features create a longer checkout process resulting in cart abandonment and churn. Overall, this worsens the customer experience, which is the reason 61% of consumers decide to switch to a competitor.

Fighting Automated Online Fraud with a Holistic Anti-Bot Solution



The standard defense approach using static rules is simply not enough to stop the vast majority of automated online fraud. These static rules typically look at the number of times a user has attempted to log in or set a point scoring system based on different actions to detect bots.

However, modern-day bots utilize a number of different technologies, such as VPNs, to completely avoid these common approaches to defending against automated online fraud. Even Captchas are not effective as nowadays bots have a higher rate of solving Captchas than humans do, as captchas can also cause difficulties for real customers.

So, what's the alternative?

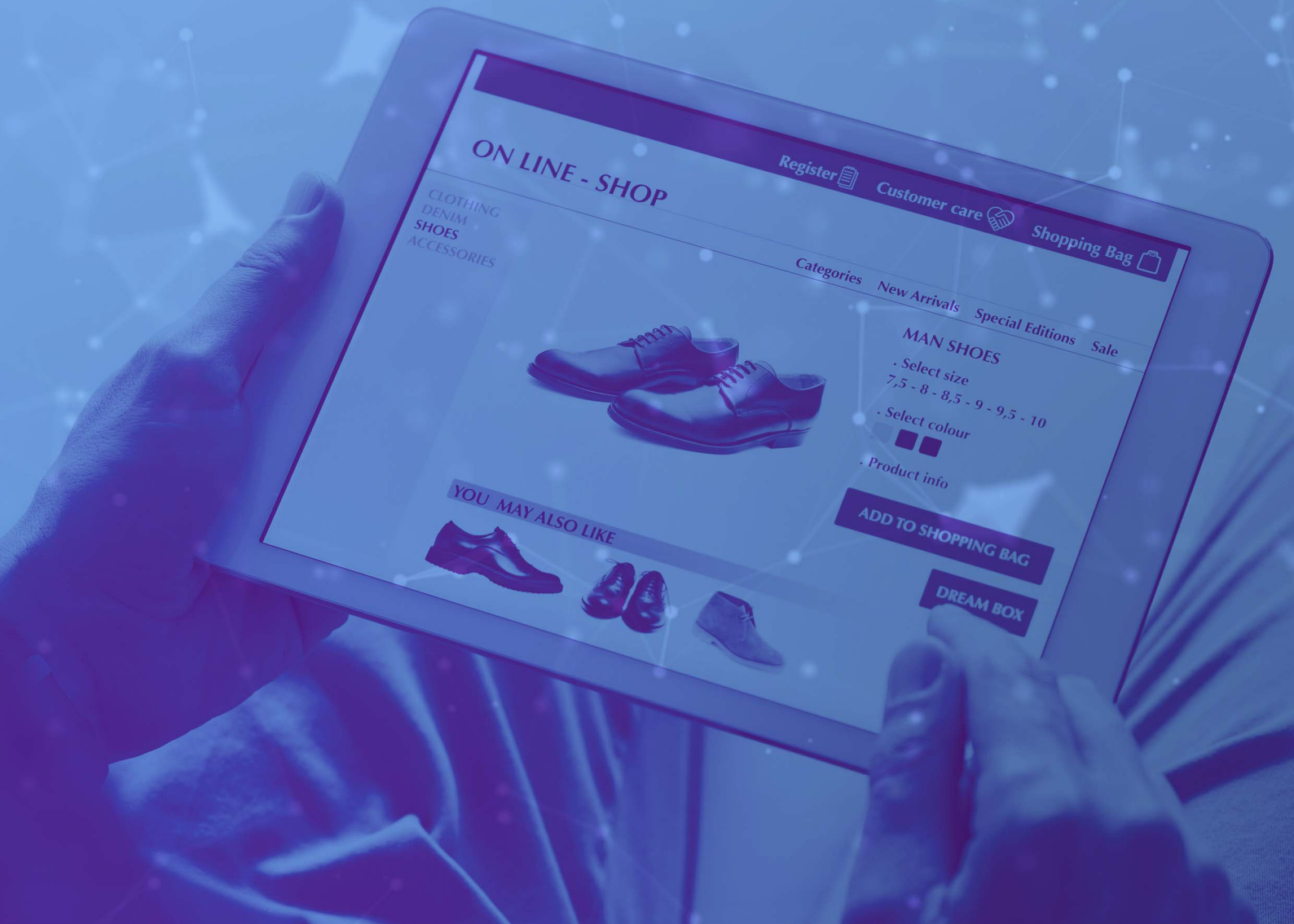
Modern anti-bot solutions provide a separate "experience" for real users and bots to completely avoid these potential drawbacks and stop automated online fraud in its tracks. Essentially, these solutions provide one "experience" for unknown users with strong security controls and a separate "experience" for legitimate users that removes these security controls. This allows you to provide your real customers with an excellent user experience without compromising your security against automated online fraud.

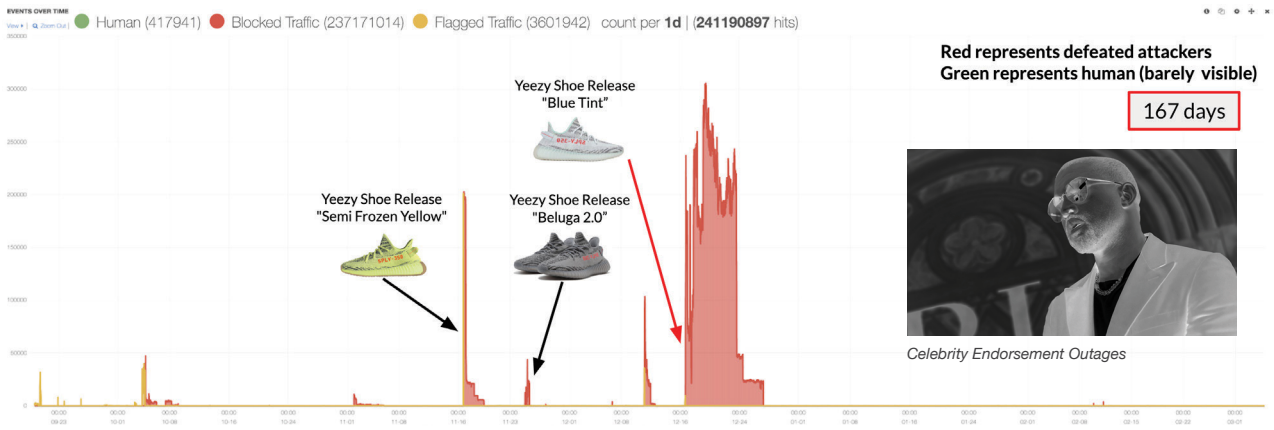
To determine whether a user is a real customer or a bad actor, a holistic anti-bot solution uses a type of funnel that gradually determines if a user is legitimate. It starts with detecting and removing known synthetic traffic based on a variety of parameters. Then, the users who pass the synthetic traffic check go through a different set of security measures to determine the likelihood of them committing fraudulent behavior. Finally, the user proves their identity confirming that they are who they say they are. All of these steps need to be an automated, scalable, and quick-learning process in order to remain up-to-date with modern fraud tactics.

Once a user passes these measures, they can access a different online experience without security controls for an optimal customer experience.

Retailer Solves Bot Spikes, Fixes Fraud, Friction and Fake

Case Study





250M Total POSTs

425K Human

249M Automated

99.8% Automated

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.

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.

Challenging Landscape

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

$500K SAVED
IN THE FIRST 30 DAYS

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
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.

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.

"CAPTCHAs simply do not work and cause higher bounce rates and cart abandonment."

All quotes are from the retailer's CIO

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 regio**n, but found that this led to too many false positives and, again, did not result in a significant reduction in fraud.

After having reviewed a few leading bot mitigators, the retailer zeroes in on Shape Security, which could proactively mitigate fraud without adding friction to the customer-experience journey.

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

"From day one we saw a nearly 100% drop in fraud from automation."

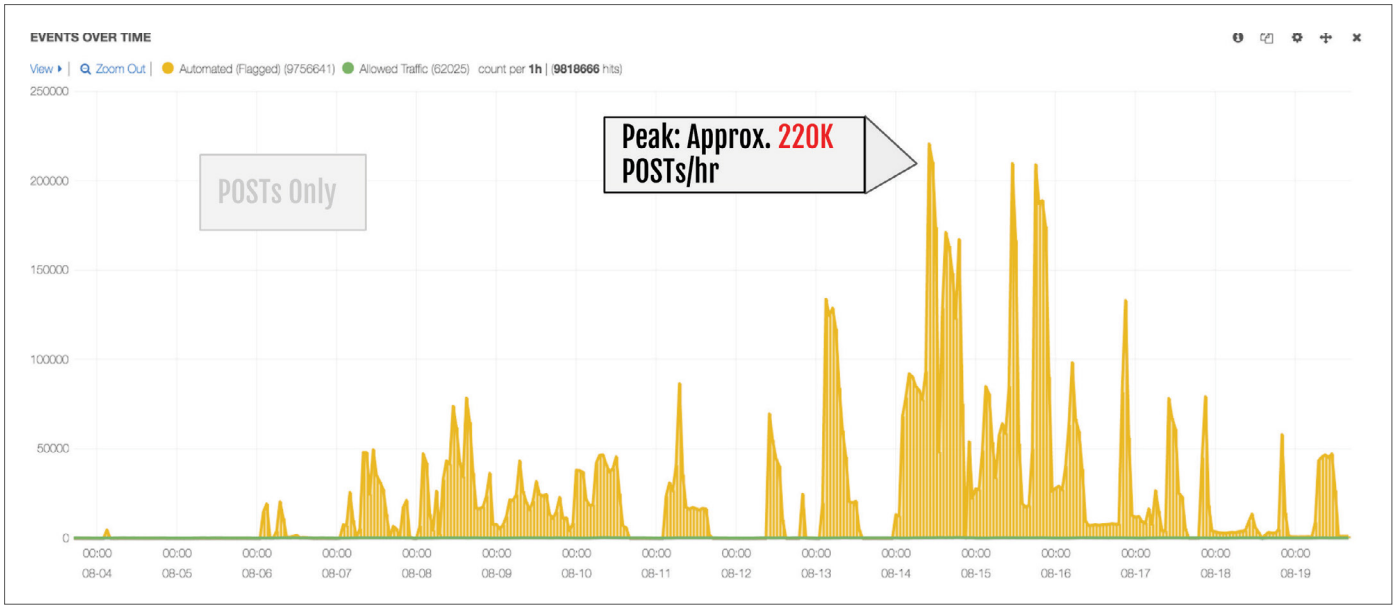
The Outcome

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. The most optimal defense with low false positives before is decided upon in collaboration with the client, before engaging in mitigation mode.

The observation mode 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, thousands of successful account-takeovers were recorded, 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.

After three weeks of observation, mitigation mode was switched on. 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.

"For the first time, we earned visibility into 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."



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, 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 TCO and revenue alike.**"

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.

Conclusion

Advanced anti-bot and anti-fraud solutions can simultaneously enhance an organization's security, increase profitability, and improve its reputation. The key is separating bot traffic from legitimate user traffic with the highest level of confidence, then introducing legitimate users with a frictionless shopping experience.

An anti-fraud solution that is implemented correctly should not even need any ongoing maintenance and support as it uses ML and security intelligence to adjust to new attack patterns.

Managed options also exist, which may fit very large or quickly-growing eCommerce retailers with a global user base.

The right option for your business depends on its unique profile, risk map, and growth plans. An impartial security partner with engineering capabilities, who can also implement and configure the optimal solution is, therefore, highly advised.

About GlobalDots

GlobalDots is a world leader in discovering and implementing cloud & web innovation. Over the last 17 years, GlobalDots enabled streamlining and smart growth in over 500 business customers, providing enterprise-grade Anti-Fraud & Website Security solutions.

Fusing an insatiable hunger for innovation with a diligent team of hands-on experts, we help our business customers maintain an up-to-date technology position in a quickly-changing world. Our seasoned engineers test & master each solution's capabilities, pros & cons, to advise your perfect fit and enable fast, smooth adoption. Service goes from precise configurations & team education to advanced professional services.

About SHAPE Security

Shape Security defends the world's largest enterprises from sophisticated cyberattacks and fraud. Shape customers include three of the Top 5 US banks, five of the Top 10 global airlines, three of the Top 5 global hotels and two of the Top 5 US government agencies. The company has raised $100M+ from Kleiner Perkins, Google Ventures, Eric Schmidt, and other leading investors to build an advanced web, mobile, artificial intelligence, and machine learning platform for global scale application defense.

The Shape platform, covered by 50 issued patents and 100+ additional patent applications, prevented over $1B in fraud in the last year. Shape was named by CNBC as one of the 50 most disruptive companies in the world. Today, the Shape Network defends 1.4 billion user accounts from account takeover and protects $1B of in-store mobile payments worldwide.

GlobalDots

Contact Us

for end-to-end adoption
of the latest bot mitigation solutions.

SHAPE