

# COUPONFOLLOW

## PerimeterX Case Study

### PROBLEM

CouponFollow's efforts to find and index high-value coupon codes through various channels including social media had struck a chord with users, which led to the company quickly becoming a category leader. Over the years as CouponFollow grew in size and reach, so too did the number of competitors who wished to replicate their success. In an effort to poach traffic, some competitors began using web scrapers to steal coupon data. These copycat companies would lift codes and copy directly from CouponFollow and repost it to their own website, which had a negative impact on CouponFollow's search engine ranking and significantly diluted the company's overall value.

To study the scope and source of the scraping problem, CouponFollow created a honeypot system in May, 2017 that featured fake codes on their site. These dummy coupons, which appeared to be associated with leading brands, were only visible to data scrapers—not real, human users. Within days, the fake codes had proliferated across dozens of competing coupon aggregation sites and now appeared on thousands of web pages dedicated to retail brands. What's more, the dummy coupons appeared with identical web copy, or spun copy that had been manipulated using content spinning techniques.

### CUSTOMER

With an increasing number of retailers offering deals and discounts, consumers have become inundated with promotions—both in their inboxes and social media feeds. As a result, shoppers often feel overwhelmed and ultimately miss out on valuable savings. **CouponFollow** provides a simple solution by indexing the most relevant and valuable coupon codes across tens of thousands of e-commerce websites, saving users time and money. These coupons are surfaced in real-time on their website and through their browser extension, Cently, which pulls from CouponFollow's proprietary database and applies codes automatically at checkout.

---

“Knowing these thin-content, low-quality, copycat coupon sites exist and can even rank on the first page of Google is deeply troubling for us as well as the retailer brands,” says CouponFollow founder Marc Mezzacca. “We exhaust considerable time and resources to aggregate the latest coupon information, and yet search engines will sometimes treat these fraudulent sites as equal sources of coupon data.”

## SOLUTION

---

As the CouponFollow team struggled to contain the situation internally, they contacted PerimeterX to help stop the scraper from harvesting content and preventing ongoing theft. Mezzacca learned about PerimeterX Bot Defender and how it uses machine learning and behavioral analysis to identify and block scraper bots without impacting overall user experience.

The PerimeterX solution easily integrates into the infrastructure. A JavaScript code—called a PX Sensor—is added to the required served web pages, which collects behavioral information on the users. The requests are then inspected by the enforcer, that is integrated in the Fastly CDN and provides scraper-blocking-as-a-service. PerimeterX Bot Defender behavioral fingerprinting provides real-time threat detection and evaluation of the sensor data, knowing what typical activity looks like to determine with great accuracy when activity is not associated with a human, as well if there is malicious activity even when a human is present. This improves blocking accuracy and decreases false positives over time

## RESULTS

---

CouponFollow implemented the PerimeterX Bot Defender in July of 2017 and began immediately blocking predatory bots. The implementation was smooth and took less than one week to roll out across all CouponFollow properties, due to the seamless integration the solution has with Fastly.

---

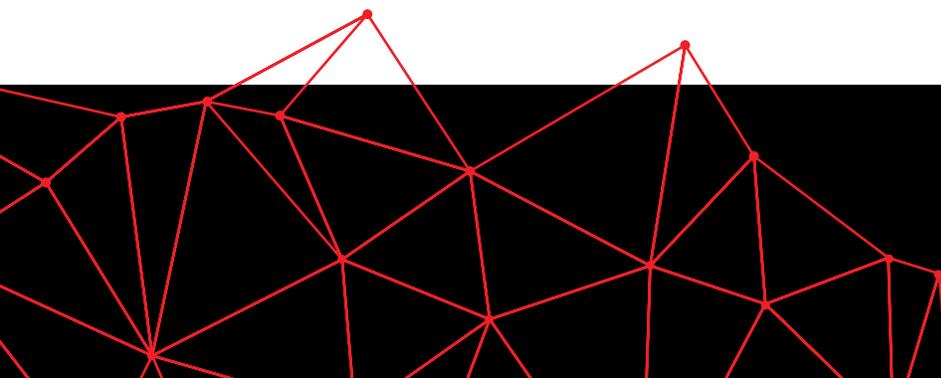
“By leveraging the PerimeterX partnership with Fastly—a CDN provider to CouponFollow—we were able to block scraping attacks at the edge, so our users’ load times wouldn’t be affected and could maintain piece of mind that the solution would scale,” notes Mezzacca.

By the middle of August 2017, PerimeterX had identified and blocked 4 million malicious pageviews that likely contributed to the ongoing attacks. To assess the effectiveness of the PerimeterX product, CouponFollow implemented a second honeypot test, placing a new batch of fake coupon codes on their site to attract scrapers.

After examining server logs and site analytics, CouponFollow determined that PerimeterX was blocking more than 98% of all attempts to scrape codes and content. This resulted in a dramatic decline in the appearance of identical content in Google search results and gave CouponFollow confidence their proprietary database was being protected.

---

“PerimeterX gave us the protection we desperately needed from malicious bots stealing our content and undermining our business,” says Mezzacca. “They were able to do this with virtually zero impact to our current users and without forcing us to make any large changes to our technology infrastructure. PerimeterX has been amazing to work with and we’re extremely happy with the results!”



perimeterx

[www.perimeterx.com](http://www.perimeterx.com)

[info@perimeterx.com](mailto:info@perimeterx.com)