HOW A TOP RUNNING SHOE BRAND NEUTRALIZES THOUSANDS OF FAKE E-COMMERCE SHOPS BEFORE CUSTOMERS FALL VICTIM

AT A GLANCE

OBJECTIVE

- Combat a tenfold increase in fraudulent e-commerce shops
- Reduce time-to-takedown
- Achieve takedown cost-efficiency over UDRP

CHALLENGE

- Scams identified too late after consumers fell victim
- Escalating call volume as a result of fraud
- UDRP volume became cost-prohibitive

SOLUTION

- AI finding fake websites before traffic is directed to them
- Outsource takedowns to experienced response team
- Expert management of takedown queues

RESULTS

- Reduced customer fraud complaints by 93%
- Significant acceleration of time-to-takedown
- Hundreds of thousands of dollars in cost savings

CHALLENGE

A 100-year-old running apparel company popular among U.S. runners faced a surge in customer fraud complaints due to counterfeit online shops exploiting their brand. The fraudsters behind those shops lured consumers with too-good-to-be true discounts on shoes and apparel to steal payment information or conduct non-delivery fraud. The threat – growing from one impersonation attack per week to nearly 20 – resulted in lost sales, brand damage, and fraud complaints inundating their call center.

The company's initial approach to the problem, filing Uniform Domain-Name Dispute-Resolution Policy (UDRP) complaints, was too expensive, too slow, and ineffectual. The UDRP process was not only costly at $1,000 per filing (and $10,000 in some cases with overseas registrars), but also slow and failed to halt scams before customers fell victim, leading to negative perception of the brand and decreased customer satisfaction.

"A big part of the frustration was keeping track of all the sites. Are they up? Are they down? Do we have them in our possession?" a fraud analyst at the company said. "Then there's the waiting period. You file it. They look at it. There might be locks on the domain. You have to transfer it to your registrar from another registrar, and you can't transfer it out easily."

"UDRP is a huge hassle, ultimately not very effective, and very very expensive."

— Fraud Analyst
Top U.S. Running Footwear Brand

ALLURE SECURITY

SOLUTION

Reaching a record-breaking week of nearly 100 customer complaints about fraudulent online shops, the brand recognized they could no longer suffer the continued degradation of their online reputation, and their existing process was unsustainable. With this urgency in mind, they decided they needed to proactively address the issue head-on.

Wanting to refocus internal staff on core competencies, they sought out external online brand protection expertise. After evaluating four vendors they chose Allure Security for its AI-powered online brand-protection-as-a-service. This included protecting their brand on social media to counter deceptive ads and posts that direct consumers to counterfeit e-commerce sites.

Allure Security's AI engine excels in detecting impersonations that evade others by automating the examination of virtually every new domain published on the Internet for potential brand impersonations.

Deployment is also near instantaneous thanks to the fact that no complex integrations or code changes are necessary. "Super easy implementation," the fraud analyst said.

In addition, unlike other solutions the team evaluated that flagged thousands of pages for manual review, Allure Security's AI engine employs computer vision and natural language processing to automate the task, significantly reducing false positives.

The fraud analyst and team also particularly valued Allure Security's multi-pronged approach to response. "What drew us to Allure Security was the way you tackled the issue," he said. "It wasn't just about taking the website down, it was working with Google and Microsoft and others to get blocks and warnings in place."

"Allure Security is far better than anything we tried in the past. It's more effective and faster at takedowns and especially at finding sites before they're up and running and have traffic going to them."

RESULTS

Once the team implemented Allure Security, customer complaints about counterfeit e-commerce shops plummeted 93 percent. The fraud analyst and his team presented this substantial decrease in call volume to management – a clear indication that fewer customers were falling victim. Management also appreciated the quantification of more fake sites identified, blocklisted, and taken down faster than ever before.

When asked how he would describe Allure Security's impact on his company's operations to peers, the fraud analyst responded: "We ran into the fraud issue, and what we were doing didn't work. Allure Security came in and very easily took a lot of this work off of our plate and reduced the number of complaints about imposter websites from our customers that were getting scammed."