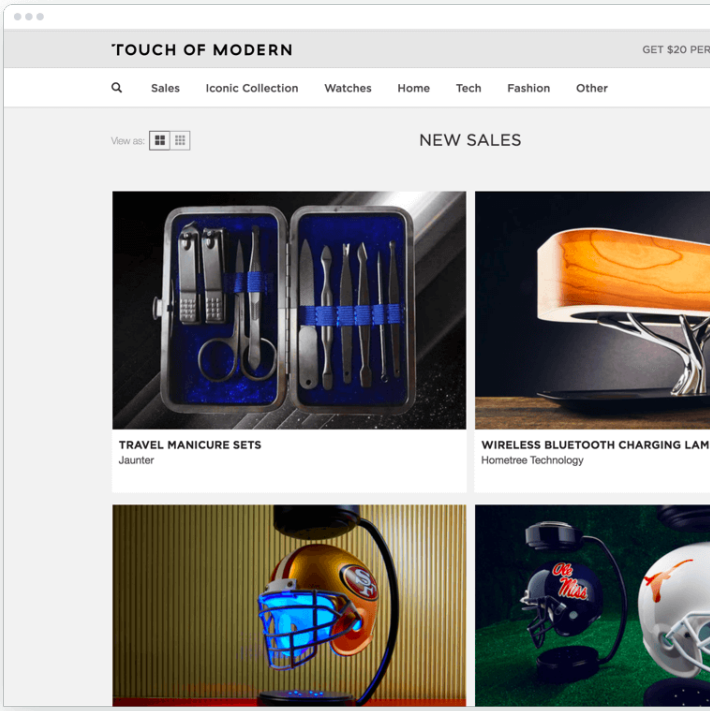
TOUCH OF MODERN

Protecting users and deterring hackers once and for all

How Touch of Modern turned to Castle to protect its users and deter hackers once and for all.

INDUSTRY	LOCATION	EMPLOYEES
E-commerce	**San Francsco, CA**	**125**



The Challenge

Back in 2012, Touch of Modern went from an idea to launch in about three weeks. Since then, the company hasn't stopped growing: It reached its first million dollars in revenue in just three months, and grew by more than 100% annually in its first few years in business. Now, it's booking well over a hundred million dollars in revenue every year.

That philosophy of rapid iteration—and staying out of its users way—is now embedded in Touch of Modern's DNA. From the beginning, they wanted to cater to the average user. And when it comes to security, they wanted to ensure that they weren't blocking legitimate users out of their accounts.

But the security landscape started shifting, when a series of high-profile breaches including LinkedIn, Yahoo, and others, meant that more and more user accounts were vulnerable. They started seeing more and more brute-force attacks, as hackers were trying those password lists on their site.

The first thing they did, says co-founder and CTO Steven Ou, was to implement Cloudflare to protect against general attacks and malicious activity. They also implemented Sift Science to deal with order fraud. That way, every time there was an ATO attack, the team would see the spike in attempts to the login endpoint, block, and mitigate them. They'd then pass a list of potentially affected accounts to their customer service team, who would ask the users to reset their passwords, while Sift would catch fraudulent transactions.

"As time went on, however, we started to see a significant increase in the attacks, and it was becoming much too burdensome to handle manually," Ou said. On an average day, for example, the dozen-person support team might handle a thousand tickets—but when an attack came in, there might be another thousand people to reach out to, doubling their daily workload. "We were also slow in responding because there was a delay in seeing the impact on our servers and actually identifying that an attack was happening." And there was some risk in waiting to catch abuse at the point of transaction, which could lead to chargebacks or erroneously shipped orders.

The Solution

Like the broader e-commerce industry, Touch of Modern started by focusing on fraud prevention.

"It seems like a natural evolution to focus upstream," Ou said. "There's no reason why we shouldn't be preventing an account takeover to begin with. If we can successfully prevent 100 percent of account takeovers, we greatly diminish the probability that we'll get a fraudulent order at all; it entirely eliminates one method of fraudulent orders."

Touch of Modern needed a solution that would scale with the pace of attacks, protect users, and stop ATOs at the login.

"At first, our main objective was just to know whether something happened in real time, so we could mitigate attacks quickly," Ou said. From there, Castle made it possible to actually automate account takeover prevention, by blocking malicious login attempts and notifying customers about resetting their password to resolve the incident. Ou integrated Castle himself, just as he was kicking the tires of the integration over the course of a few days.

The Result

Now, account takeover prevention is built in to the system, and automated so that no one even needs to look at it. "Customer service doesn't deal with this at all anymore; it's 100% off their plate," Ou said.

While he and the rest of the Touch of Modern team used to see reports come in of 100s or even 1000s of accounts getting compromised, in the three months since they rolled out the full Castle integration, Ou estimates he's seen less than a dozen accounts flagged as compromised.

> **"I think it's because Castle now straight-up blocks bad actors when they attempt to log in so the bad actor never gets a positive login response, which in previous attempts would get blocked later. I think that signals there's just nothing here to attempt."**

In other words, in addition to preventing attacks, Castle has also helped discourage future ones, by looking like zero success rate on that password list. Ou said it was difficult to even begin to quantify the benefit Castle has provided, on top of freeing up CS resources and blocking fraud earlier in the funnel.

"The benefit of Castle is that account takeover is a total non-issue now. We don't spend any resources thinking about it. We've been able to do everything else we'd choose to prioritize."