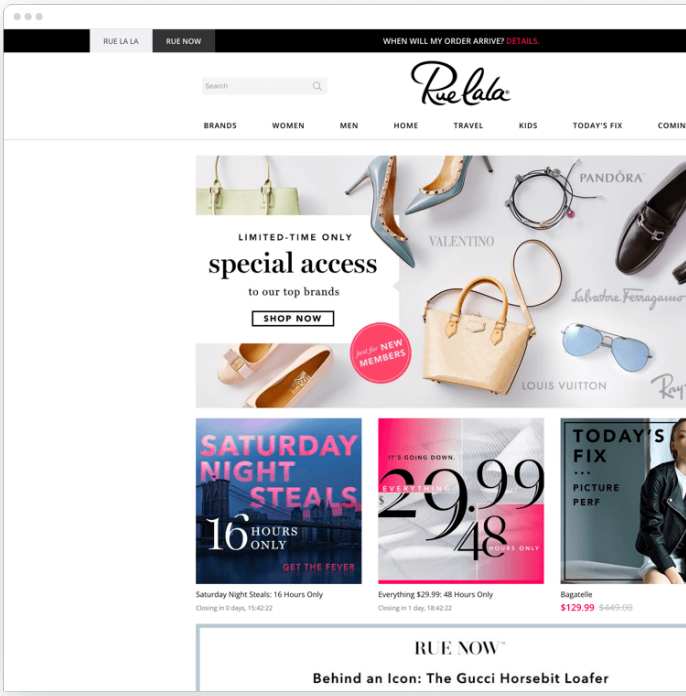
Creating blissful user shopping experiences.

How Castle and Rue La La partnered to prevent potential account takeovers, save engineering time, and create blissful user shopping experiences

INDUSTRY	LOCATION	EMPLOYEES
E-commerce	**Boston, MA**	**600+**



The Challenge

More than 16 million Members rely on Rue La La to deliver the best brands across a variety of categories such as fashion, beauty, home, travel, and more at even better prices. A key part of Rue's mission is putting its Members first, spanning everything from delivering strong user experiences to making shopping personal and protecting them from possible security threats.

Rue La La's security team has long been laser-focused on table stakes, like ensuring PCI compliance and implementing controls that protect Members. They've also put effective log aggregation and WAF in place to detect anomalous activity and general threat scenarios.

But as shopping moves online, so too have threats. And with overall data breaches on the rise, account takeovers (ATOs) are one of the fastest-growing threats to online businesses of every kind. In 2016, total account takeover losses reached $2.3 billion, according to a recent Javelin study.

This has big implications for any business trying to protect its users from malicious activity—nevermind simply providing a best-in-class user experience. Account takeovers have real costs for businesses, such as chargebacks, customer service calls, and any risks to their brand and public profile.

The Rue La La team spotted this broader trend early on, recognizing that with so much out of their hands—like people reusing passwords—the old approaches to protecting users needed to be re-evaluated.

> "For any e-commerce provider, potential fraudulent activity and cybercriminals are part of the reality of the industry now. Our Members entrust us with their business. So, our goal is to always be one step ahead of threats to protect our Members and our company," noted Director of Engineering Ken Pickering.

The Solution

Rue La La needed a solution that was specifically focused on ATO, put the user first, and cut down on manual work.

Rue La La was familiar with how to deal with routine fraud—and had effective tools in place to do so. But it was clear to the team's security experts that preventing account takeover requires a different approach than existing anti-fraud solutions provide.

They considered common instruments in place for ATO, like network controls, but they realized these tools would be too blunt. Such approaches often sweep up good users in their nets, which introduces both friction and frustration and eats into growth. Plus, malicious activity often still trickles through controls at the network level.

Given Rue La La's focus on its Members, they wanted a solution that would approach things holistically from the user perspective.

At Rue La La, security issues like account takeover prevention are in the domain of the engineering team. They knew they needed a solution that would let them automate the challenges of monitoring its millions of users for suspicious account activity—while letting the team focus on what it's best at.

Pickering was also drawn to Castle's use of machine learning. The better the self-learning risk model, the better user protections become. Best of all, because Castle is automated, they don't have to consistently monitor the integration.

The Result

Rue La La integrated Castle's SDKs right into login process and automating the password reset workflow in just a few hours.

Castle enabled Rue La La to continue to protect its millions of users from ATO attempts, but in a more streamlined manner and timeframe. Pickering said with Castle in place, overall user fraud is low, as are associated calls to customer service.

Best of all, with Castle in place, Rue La La didn't have to dedicate any additional resources to stop ATOs cold.

Rue La La set up the integration to rely on triggers, so the team doesn't really need to monitor the UI unless they need to investigate the impact of an attack—critical for a company with millions of shoppers.

"A successful integration is one that I don't have to sit on to use and that can alert us with a minimal amount of false positives," Pickering said. "That's what we have with Castle."

Now, Castle lets Rue La La take advantage of a next-gen heuristics and security policy that automates previously manual work. It also removes a lot of the burden of combing through logs to make sure there aren't unseen problems.

Most companies wouldn't know about an ATO problem until it's too late. Now, Rue La La doesn't have a problem, period. "Castle has been a great partner, and has made it possible for our security and engineering teams to continue to focus on innovation rather than potential ATO threats," Pickering said.