TALA

RETAIL USE CASE

How a family-owned business stopped Magecart and restored customer trust

When this online retailer wanted to enhance customer protection while improving user experience, they worked with Tala to deliver both.

BACKGROUND

When your business is "Large enough to be competitive, but small enough to ensure that every customer is significant," customer service and support are front and center. When this California-based, family-owned retailer began to receive customer complaints regarding stolen payment information, they knew they had to act quickly to resolve the issue and restore customer loyalty and trust.

> **"Our customers have always mattered the most to us and Tala ensured that our customers' sensitive information was protected at all times. This was the most critical component for establishing trust and customer loyalty."**

THE CHALLENGES

- Magecart and other client-side attacks
- Customer journey hijacking and session re-directs
- Rapid implementation and ease of use
- Protection from zero-day threats
- No performance impact

RETAIL USE CASE

THE NEED FOR SPEED

Following a preliminary investigation into the customer complaints, the retailer identified the possibility that a card-skimming script had been injected onto its website.

With the increasing prevalence of Magecart-style attacks, the retailer suspected that the code running on its website had been compromised - and knew they had to act urgently. They had to secure their website as quickly and efficiently as possible. They also wanted to eliminate the incidence of adware, malicious ads and session redirects on their website, to ensure customer retention and prevent revenue loss caused by customer journey hijacking attempts.

CHOOSING THE RIGHT SOLUTION

The retailer understood the gravity of the threats posed by Magecart-style attacks, as well those that degrade user experience. They wanted to secure their website and learn how they could prevent these threats. They were looking to deploy effective security measures quickly. Having identified the issue, they wanted to move quickly to implement preventative measures and evaluate vendors as quickly as possible to choose the best solution.

When evaluating solutions to stop magecart, secure its website and preserve customer experience, the retailer had key criteria:

- **Reliable, comprehensive defense from security threats:** Because they were looking for enterprise-grade protection against zero-day threats, detection or monitoring-only solutions were eliminated in the early stages. The retailer wanted to make sure that the website was protected against all kinds of evolving cyber threats, not just Magecart. They wanted to rely on proven, expert approaches to solving this problem rather than proprietary methods that could involve incorporating external code in their website.
- **Quick integration and deployment:** The solution needed to be up and running in a short time. Deploying a JavaScript-based solution would mean significant time and resources spent evaluating the external JavaScript and determining its impact on the website. Tala's certified Cloudflare integration module stood out, as it ensured that defense was up and running in minutes, without any burden on internal infrastructure.
- **Ease of ongoing management:** The retailer was looking for a quick, hands-off way to address threats. As a large chunk of the business was conducted online, website performance was paramount; they concluded that, due to their lack of impact on performance, CSP and other W3C standards represented the best approach. The website was also updated periodically, so they were looking for a solution that would update these policies in real time, based on ongoing monitoring of threats and anomalies. As they had a small IT team, they wanted to set and forget these security controls and be alerted only when necessary.

TALA

RETAIL USE CASE

BENEFITS AND BUSINESS IMPACT

Conversion rate uplift: Two months into deployment, the website saw a 5% increase in conversion rate. This was made possible by preserving the online user experience through prevention of malware, adware, malicious browser extensions and other forms of customer journey disruption. Tala made sure that customers stayed on the path to purchase and the user experience was always working as intended.

Revenue uplift and ROI: The conversion rate uplift translated to an 18% increase in revenue. The average order value also increased by about 6% and the retailer observed immediate returns on the deployment.

Safe and secure customer transactions: After deploying Tala, the retailer noticed an immediate dip in customer issues like malicious ads,and alerts on customer credit card information being used on unauthorized websites. Once in Block Mode, Tala identified and prevented numerous attacks reliably. The retailer was relieved that they had won back the most important component of their business: customer trust.

Continuous monitoring and alerting of threats: In addition to protection, continuous monitoring of web applications provided valuable, real-time insights into changes taking place in the application, enabling a proactive approach to monitoring JavaScript vulnerabilities.

Website performance: Website performance was preserved and online experience was protected. Tala's Cloudflare-certified module was optimized for preserving performance, and provided wide coverage with virtually no impact to performance metrics like Time-to-First-Byte and page load time as measured by the retailer's performance teams.

> **"The benefits were significant and immediate - we saw a tremendous uptick in conversion and a revenue boost that wouldn't have been possible without Tala."**