source DEFENSE

# The Hidden Risk in Your Digital Supply Chain

## Understanding the Security and Compliance Gap that Could Cost You Millions

# INTRODUCTION

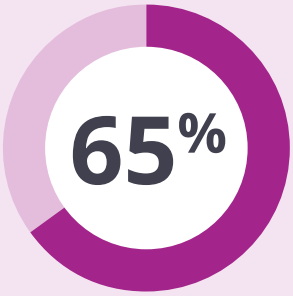
Change is nothing new to an industry literally built on creating new trends. Yet, the fundamental changes being seen in retail since the pandemic began are setting a pace unlike anything we've experienced in the past. From the dramatic shift to online shopping to the broadening adoption of curbside pickup, the retail industry may never be the same.

Driving much of the change is the massive move to e-commerce, which has grown two to five times faster than before the pandemic. In the U.S., year-over-year growth of e-commerce as a share of total retail sales was 3.3 times as much as pre-pandemic levels.[1] With continued double-digit growth in e-commerce, forecasts point to U.S. sales being on track to exceed $1 trillion for the first time in 2022.[2]

While this is good news indeed for brands, marketplaces, and other online retail venues, it's also fueling an entirely different trend: the growth in client-side cyberattacks driven through retail web applications. The result is massive data theft, including customer personally identifiable information (PII) and financial data such as credit card information. These attacks are putting retailers at risk of dramatic material losses in the form of security response costs, ongoing credit monitoring for impacted clients, and fines from compliance regimes.

Cybercriminals are cashing in on the success of e-commerce by attacking the soft retail underbelly, namely the website as it exists within a visitor's web browser, sometimes called the front end or client side of a web application. Client-side attacks — including digital skimming, formjacking, clickjacking, ad injection, content defacement, and others — represent some of the biggest security and compliance threats today for retailers. It's no wonder that industry analyst group Gartner believes that web application client-side protection will become a mainstream focus by 2023.

1. "How E-Commerce Share of Retail Soared Across the Globe," McKinsey & Company, March 2021
2. "Insider Intelligence's Retail Trends to Watch in 2022," Suzy Davidkhanian, Blake Droesch, and Andrew Lipsman, Insider Intelligence, December 2021




## Nearly two-thirds of consumers would churn if there was a data breach

65% of e-commerce shoppers say that "experiencing even a single data security breach would prompt them to leave a merchant for good."

**Source:** "Report: 65 Pct of Consumers Would Abandon Merchant After eCommerce Data Breach," PYMNTS.com, May 2021

# THE COMPLEXITY OF TODAY'S DIGITAL SUPPLY CHAIN

As a retailer, you can control first-party risk through governance and the defenses you put in place against attacks. Your organization can control second-party risk (your customers) by encrypting their sensitive data. The problem your company and other retailers face today is how can you mitigate the growing third-party (and fourth-party, and so on) risk in the e-commerce digital supply chain?

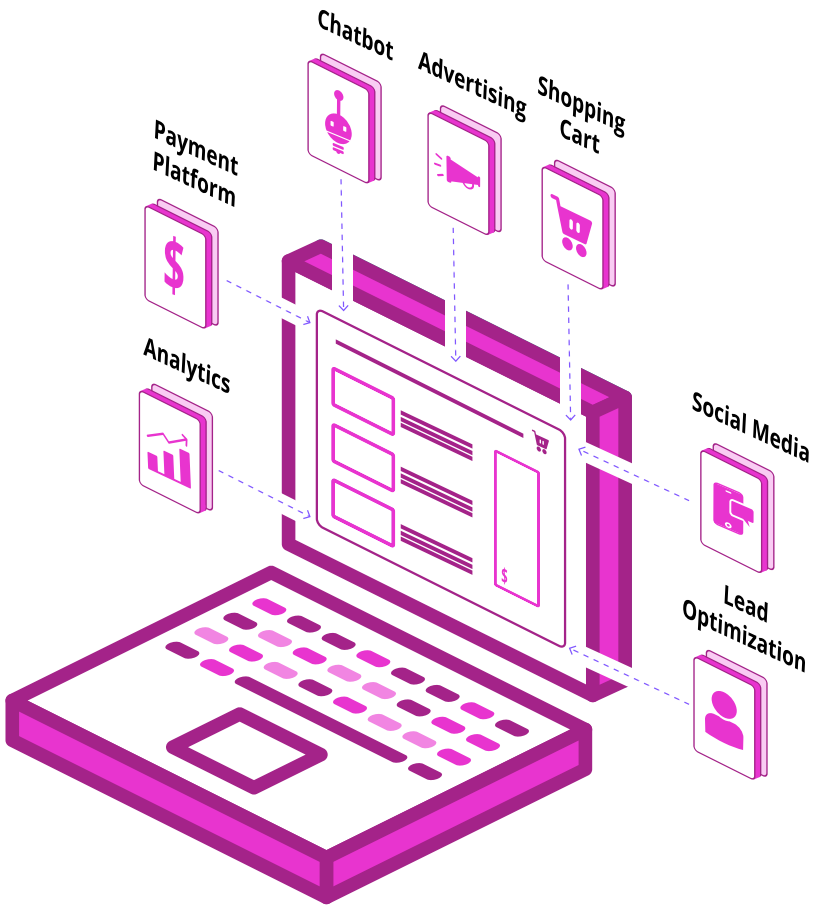
Let's start by looking at why supply chain risk is such a serious threat. As consumer expectations have grown, so has the mandate to deliver a rich customer experience that attracts and retains consumers as they increase their time spent shopping online.

The only way for the vast majority of retailers to keep pace with the digital expectations of consumers is to embrace a wide variety of third-party functionality that enhances and extends the user experience — such as payment platforms and services, chatbots, social media, analytics, and more. At the same time, third-party functionality that is critical to attract shoppers and drive conversions — including ads, trackers, and other marketing services — are also critical for e-commerce companies to deploy as part of the front end of their web applications.

All of which means that the average web application has a significant amount of code being sourced from third and fourth parties outside of the control of the retailer. In fact, based on internal Source Defense analysis, retail web applications include up to two dozen third or fourth-party plug-ins on average.

That's not all, third-party scripts often source additional content and functionality from fourth parties, further extending the web application's supply chain. These services all reside and operate outside of your security team's control because they are loaded from third-party and fourth-party servers directly to your customers' browsers, creating a major security risk.

**Figure 1. Digital Supply Chain for E-Commerce**



# THE PRICE OF UNDERESTIMATING THIRD-PARTY RISK

Thousands of retailers have been compromised by hackers in the past several years alone. Formjacking — a client-side web application attack — was responsible for more than half of retail breaches in the retail sector in 2020.[3] Since 2017, 150 million payment cards were detected as being compromised via Magecart attacks, with cybercriminals attempting to monetize the cards on the dark web for an estimated total of $37 billion.[4]

To understand what can happen if you don't address your company's digital supply chain risk, just consider the following public examples of attacks:

- More than 500 ecommerce sites running the Adobe Magento 1 system were infected with a credit card skimmer as a result of a Magecart attack discovered in January 2022.[5]
- Macy's was hit with a lawsuit over a client-side web application data breach and the company's stock price took a 10% hit following the breach being made public.[6]
- Neiman Marcus notified 4.6 million online customers in 2021 that their personal and financial information stored in their online accounts was exposed in 2020.[7]
- Segway's ecommerce store was compromised with a credit-card skimmer in January 2022, exposing card data from victims in the U.S., Australia, Canada, UK, and Germany.[8]
- Savory Spice disclosed a three-year Magecart attack that took place from April 2018 to March 2021. It took the company five months after the discovery of the attack to remedy the issue.[9]

3. "2021 Application Protection Report: Of Ransom and Redemption," Sander Vinberg, Raymond Pompon, Shahnawaz Backer, F5 Labs, May 2021
4. "Rising Magecart Attacks Place Victims in Jeopardy," Christopher Thomas, About-Fraud, October 2021
5. "Wave of MageCart Attacks Target Hundreds of Outdated Magento Sites, Bill Toulas, BleepingComputer, February 2022
6. "Macy's Hit With Malware Attack, Customer Data Stolen," Paul Ausick, 24/7 Wall St., November 2019
7. "Neiman Marcus Data Breach Exposes Personal Info of 4.6M Customers," Aaron Nicodemus, *Compliance Week*, October 2021
8. "Segway Hit by Magecart Attack Hiding in a Favicon," Tara Seals, Threatpost, January 2022
9. "Summer of Magecart," Source Defense, September 2021

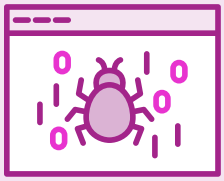
These companies certainly aren't alone in the level of risk or potential impact of this type of attack. Nearly every website (97.9% of all websites)[10] in the world today are susceptible because protection of client-side web applications is just now coming to the forefront of cybersecurity priorities.

Compliance fines represent one of the potentially significant costs that organizations face when client-side attacks or mistakes occur. Ticketmaster UK was fined $1.6 million under the General Data Protection Rule (GDPR) for a data breach stemming from third-party JavaScript code on its payment page, affecting nine million European customers.[11] British Airways agreed to pay a reduced fine of $26 million for GDPR violations that resulted from a Magecart attack.[12]

A data breach or leakage can also incur other direct costs such as legal fees, settlements of lawsuits, damages, forensic investigation, audit, and remediation. Indirect, but not insignificant, costs include brand reputation loss, customer churn, product delays, and downtime — all of which can impact revenue, company valuation, stock price, and shareholder value.

Today the average cost of a data breach is $4.24 million, up from $3.86 million in 2020. More than one-third of the costs (38%) are lost business, including customer turnover, lost revenue due to system downtime, and the cost of acquiring new business due to diminished reputation. The loss of customer personally identifiable information (PII) results in an average cost of $180 per lost or stolen record.[13]

10. "Usage Statistics of JavaScript as Client-Side Programming Language on Websites," W3Techs, February 2022
11. "Ticketmaster UK Fined $1.6M under GDPR for 2018 Data Breach," Aaron Nicodemus, *Compliance Week*, November 2020
12. "British Airways' GDPR Fine Dramatically Reduced," Doug Olenick, *Bank Info Security*, October 2020
13. "Cost of a Data Breach Report 2021," Ponemon Institute and IBM Security, July 2021



## Magecart massively expands its scope

In November 2021, the National Cyber Security Centre (NCSC) announced that 4,151 retailers had been compromised by hackers attempting to steal customers' payment information and other personal data via client-side vulnerabilities on checkout pages.

In 2020, cybercriminals used the same techniques to compromise an estimated 2,800 retailers, injecting malicious code to steal the payment details of tens of thousands of customers. The attack is considered the work of Magecart, which is a specific group of attackers who exploit the client-side attack surface and target the Magento e-commerce platform in particular. Client-side attacks, however, are not limited to one type of website platform or technology.

**Sources:** "Hackers Used This Software Flaw to Steal Credit Card Details From Thousands of Online Retailers," Danny Palmer, ZDNet, November 2021
"Cardbleed: 3% of Magento Install Base Hacked," Sensec, September 2020

# THE JAVASCRIPT VULNERABILITY THAT MAKES THESE ATTACKS POSSIBLE

Unlike exploitation of a newly discovered flaw, cybercriminals are taking advantage of a long-known security hole in JavaScript that gives all scripts — regardless of the source — the same level of control on the client side. This means that any JavaScript, including third-party code, has full access and authorship capabilities, which enables access to any and all data in forms, such as customers' personal and financial information.

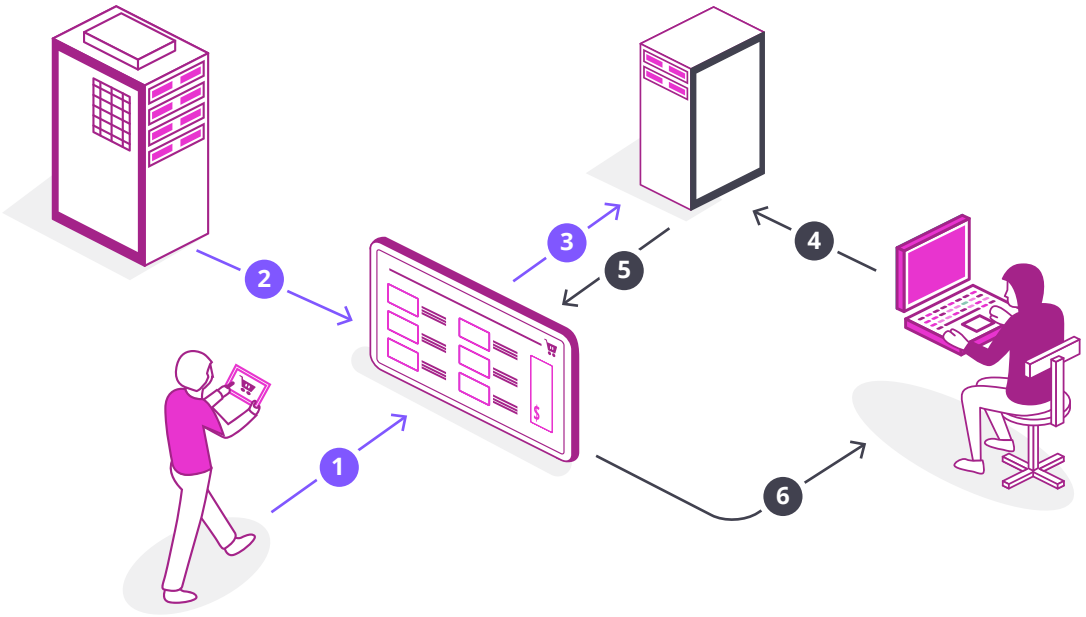
Here's how cybercriminals take advantage of this:

- Content is served and enriched: Web application logic — a combination of the retailer's application code and the integration of third-party content and functionality — is loaded and runs on the client side in the browser, beyond the protection of server-side security. The code is dynamically downloaded from a remote server, which means that it bypasses the traditional security infrastructure, including the retailer's firewalls and web application firewalls (WAFs).

- All scripts have the same level of control: Third-party and fourth-party scripts have the identical level of control as the retailer's own script. Every script on the page, no matter its origin, has access and authorship capability, meaning it can change the webpage, access all information on it (including forms), and can even record keystrokes and save them.

- The vulnerability is easily exploited: No component of traditional security programs can prevent client-side attacks perpetrated via JavaScript. All it takes is for the third-party vendor to be hacked and have its code changed or an internal developer to integrate malicious code, whether accidentally or intentionally. Retailers have limited means to dynamically detect the change and no means using server-side security solutions to prevent it from exfiltrating data or executing other malicious activity from the customer's browser.

**Figure 2. Client-Side Web Application Attack**




1. A customer visits your ecommerce website.
2. Content is presented in the customer's browser from your corporate web server.
3. The content is enriched with third-party JavaScript.
4. An attacker compromises the third-party server.
5. Malicious content is served to your customer's browser.
6. The attack is successful. Customer data is exfiltrated, putting company revenue and brand integrity at risk.

# WHY CURRENT SECURITY MEASURES AREN'T ENOUGH

Traditional server-side security doesn't address these JavaScript risks because client-side scripts operate completely outside of the security capabilities an organization deploys to secure the server side of their web applications.

Other security measures that may already be in place fall short as well. Application security validation testing or dynamic application security testing are not designed to test every use case or operate dynamically, nor can they test the code residing on a third-party or fourth-party remote server. They are also not capable of providing real-time scanning of all web traffic across the entire user population.

Likewise, using content security policy (CSP) and/or subresource integrity (SRI) features are not enough to protect client-side web applications from today's threats. While CSP and SRI can be powerful tools for website protection and data management, they have significant limitations that impact the ability for website owners to use these measures effectively against client-side threats.

Because it's difficult or impossible with existing security tools to detect these attacks, the majority aren't discovered for weeks or months, increasing the scope of damage and mitigation costs significantly.

## Billions of threats are lurking unseen

**1.2 BILLION** policy violations were detected by Source Defense per month in 2021 from retail deployments — and this represents only a small percentage of all retail web applications.

# HOW RETAILERS CAN PROTECT CLIENT-SIDE WEB APPLICATIONS

With adversaries increasingly focused on the client side, retailers must give equal attention to reducing the large material risk inherent in the JavaScript attack vector.

The best place to start is to gain a deeper understanding of your company's digital supply chain. Your security team can quickly assess how much exposure your company has on its consumer-facing site by discovering the answers to these questions:

- How many vendors are plugged into your company's consumer-facing site?
- What purpose does each serve?
- Are the plugins required on highly sensitive pages?
- Does their code give them read/write access to forms?

The next step is to deploy a solution specifically designed to provide client-side web application protection using a prevention-first approach versus only a detect-and-alert approach. With most security teams already overworked, understaffed, and drowning in alerts, solving the client-side problem can't add more burden for the security team. Solutions relying on a detect-and-alert approach flag potentially malicious activity and ask the team to investigate and respond to what can be thousands of false positives.

Instead, your company needs a solution that prevents the problem from the start, doesn't impact site performance, and requires little to no human oversight to work.

# DETECT, PROTECT, AND PREVENT CLIENT-SIDE ATTACKS WITH SOURCE DEFENSE

As the leader in web application client-side protection, Source Defense delivers what many might believe to be a unicorn in cybersecurity – a solution that is simple to deploy, has a management burden of a mere few hours per month, and adds no additional burden on already overburdened security teams. Source Defense is a prevention-first technology that stops the threat of client-side attacks without the need for alerts and investigation by security staff.  Source Defense already secures nearly one billion transactions and prevents nearly two billion compliance policy violations per month for some of the world's largest companies. The Source Defense patented Website Client-Side Security Platform offers the most comprehensive solution to detect website skimming, formjacking, and supply chain attacks and stop them before they affect your website or your customers.

Source Defense uses real-time, client-side sandboxing and permissions-based isolation and reflection to protect your company and your customers' data and prevent successful data exfiltration or leakage by:

- Isolating and monitoring JavaScript execution in an end user's browser, in real time, as the user interacts with your web page
- Using real-time JavaScript sandboxing to restrict the access that each script has to a web page as well as control that script's behavior
- Allowing or restricting access to different parts of the page and the data that they contain
- Monitoring and managing the flow of data from the page to other places
- Enforcing security controls

“

As far as things that are easy wins in information security, as few as they are, Source Defense VICE is a gem. From onboarding to normalized operations, the Source Defense team moves quickly and efficiently to protect customer sites. Customers have a clear and simple dashboard to utilize although you won’t have much reason to logon. The Source Defense team is constantly monitoring and adapting the system to provide you with the best security service. The lack of alerts to you from Source Defense is a testament to the efficiency of the ML and the Source Defense human intelligence team. Learn a new way to spend your nights and weekends — relaxing. So easy, works so well, unconscionable for an information security professional to not have Source Defense VICE in place.”

**— A multibillion-dollar global sports equipment and entertainment company**

## CONCLUSION

No retail brand wants to make headlines because of a data breach, especially with e-commerce playing an increasingly large role in profitability and growth. That’s why client-side attacks on retail web applications should be high on your list of security and compliance threats your organization needs to address immediately.

To protect your business and your clients from becoming the next victims, turn to a solution that prevents client-side attacks from being successful. Source Defense offers the only purpose-built, patented technology for real-time protection against risks and threats originating in JavaScript.

To learn more, visit
https://sourcedefense.com/request-a-demo/

To see how your website stacks up against threats and understand your risk, request a free risk report by visiting
https://sourcedefense.com/check-your-exposure/

source
DEFENSE

## About Source Defense

Source Defense is a security, compliance and performance optimization platform for any website that collects sensitive data or is transaction oriented. As the market leader in web application client-side protection, Source Defense addresses a ubiquitous gap in the management of 3rd party digital supply chain risk with a zero-trust model that extends security beyond the network to the edge/client-side. The Source Defense Platform provides real-time threat detection, protection and prevention of vulnerabilities originating in JavaScript, and currently protects leading organizations in the financial, healthcare, hospitality, and retail markets from the threat of JavaScript based attacks such as Magecart, digital skimming, credential harvesting and click-jacking. Source Defense secures nearly one billion transactions and prevents nearly two billion compliance policy violations per quarter.