source DEFENSE

eBook

Protecting the Digital Checkout Lane

[Understanding the Web Security Gap that Puts Brand Trust at Risk]

[01] Brand Experience and the Online Customer Journey are Everything

Security and Privacy are Core to the Brand Experience

Online shoppers want a dynamic experience that establishes a connection with your brand. To provide an increasingly engaging online experience, you rely on an ever-expanding digital partner supply chain third parties plugged into your eCommerce site — which power rich content, multimedia, reviews, social connections, chat, personalization software, analytics, retargeting, and potentially even the checkout.

While your digital supply chain is critical to the online experience, it's this same supply chain that also puts your customers at risk. **This is because they load code that you don't own, manage or control in every customer web session**. This code is dynamic and changes when your partners needs it to — the security and behavior of this code isn't governed by your people, and they could never keep up even if it were. With some of the biggest companies experiencing up to **4,300 changes** in partner code every year, this is a tremendous gap in both data privacy and security.

This opens up the potential for data leakage — where a partner might be capturing information without your knowledge, violating privacy mandates such as GDPR, CCPA, and the Virginia Act. It also opens the door for data theft, which results in credit card fraud and identity theft.

This theft is called **"Digital Skimming"** or **"eSkimming"** and it is on the rise. In fact, a new payment card fraud report shows as many as 10,000 unique eCommerce sites were infected by Magecart e-skimmers in 2022*. Consumers say they will walk away from brands that don't protect them from these types of attacks.

* Source https://www.recordedfuture.com/annual-payment-fraud-intelligence-report-2022

You need to approach cybersecurity with the same diligence as physical security. You know how important the security of your brick-and-mortar stores is, you've invested into in-store security cameras, maybe security guards, loss prevention personnel, and well-lit parking areas to protect your customers from being pickpocketed. You go to great lengths to make sure there aren't card skimmers on your point-of-sale systems. However, when it comes to your online shoppers, they face the risk of skimming every time they fill out a form on your site.

You've done so much work to build your brand and create a great online experience, yet in this area of cybersecurity, you're flying blind. The good news is that there is a way to seal the door between cyber attackers and your customer **data with Source Defense.**

80%

of modern website code isn't written or controlled by the retailers themselves

82%

of consumers impacted by cyberattacks suffered major life consequences

78%

of consumers think twice about doing business with a retailer after a breach

[02] An Ongoing Problem That's Gone Too Far

The Industry Is Starting to Fight Back

Here's the reality: Digital Skimming/ eSkimming attacks aren't new and they're never going to go away — not even the biggest companies are safe from it:

BRITISH AIRWAYS

British Airways had 380,000 consumers impacted by an attack.

ticketmaster

Ticketmaster had 40,000 consumers impacted.

Forbes

A Magecart attack forced Forbes Magazine to temporarily shut down its website.

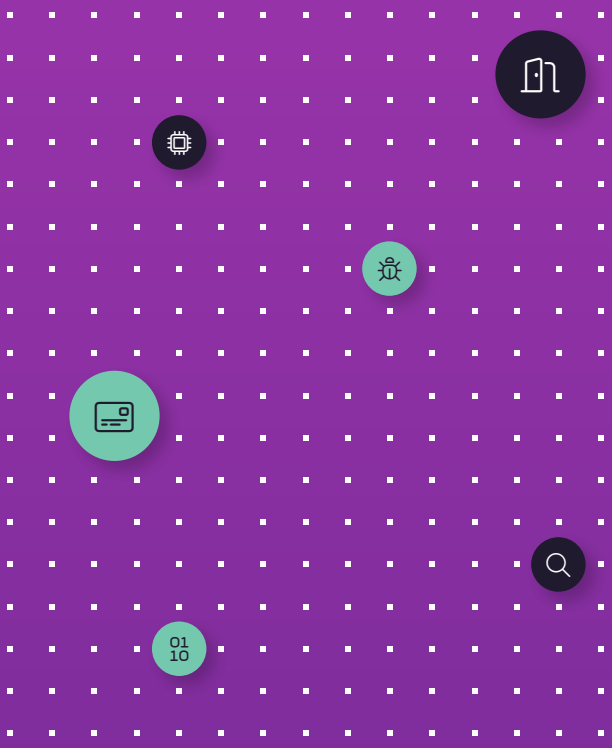
The issue is that there's a toxic equation of high profit for criminals with a low barrier of entry. Cybercriminals can easily access exploit kits for just a couple thousand dollars and operate with the knowledge that the vast majority of retailers aren't prepared to defend.

These attacks are typically ongoing and can have a long-lasting impact on your customers. Because so few companies have yet to address this security gap, some of the most high-profile digital skimming attacks have gone unnoticed from **6 months to 2 years.**

As **93 percent of the world's websites rely on third and fourth parties**, the industry is finally waking up to the severity of the issue and is starting to warn retailers to do something about it. Visa recently warned that **75 percent of VISA breach investigations involve digital skimming and third-party integrations on websites**. In light of this, there are an increasing number of data privacy and data security requirements calling for protection against these attacks — like the recent changes to PCI DSS recommendations for digital skimming protections.

93%

of the world's websites rely on third and fourth parties



However, even while the industry is starting to get it right, you might not be acting quickly enough to catch data leaks or breaches before they happen, which can wreak financial havoc on your business.

For example, a retailer doing $50m in online sales might process upwards of 349,000 transactions per year.

Therefore, constant exposure exists for hundreds of thousands of its customers, and it can't wait to address the problem when it is both severe, real, ongoing, and most importantly, EASY to address.

[03] Even the Best Websites are at Risk

Get a Handle on Your Exposure and Close the Gaps

According to Source Defense's 2022 State of the Industry Report, there are an average of 15 third and fourth-party scripts on any given website. The capabilities we see in most partner code can result in data privacy violations and make it very easy for an attacker to piggyback on for data theft. In fact, it's never been easier for cyber attackers to figure out what partners any retailer is working with. And with the ease of targeting retailers based on this data, attacks are easy to conduct in either targeted or broad fashion.

95%

of all purchases will be through eCommerce by 2040 according to analysts*

By the year 2040, analysts estimate that 95% of all purchases will be through eCommerce.* With this rapid increase in transactions, there's an equal increase in vulnerable consumer data. Unfortunately, many companies aren't prepared to effectively address the threat of rising cyber-attacks.

A siloed company is an unprepared company. When all departments (e.g., digital, marketing, security, compliance, etc) are working together, they can properly identify the vulnerable points in their supply chain.

* Source: https://www.nasdaq.com/articles/uk-online-shopping-and-e-commerce-statistics-2017-2017-03-14

[4 STEPS]

to Getting a Handle on Your Supply Chain Security

1	Conduct a risk review of your website 
2	Begin an inventory of all your supply chain partners and either justify or decomission them 
3	Establish an ongoing conversation about your digital skimming risk 
4	Evaluate solutions and prioritize investment in security 

[04] Protecting Your Consumers is Protecting Your Brand

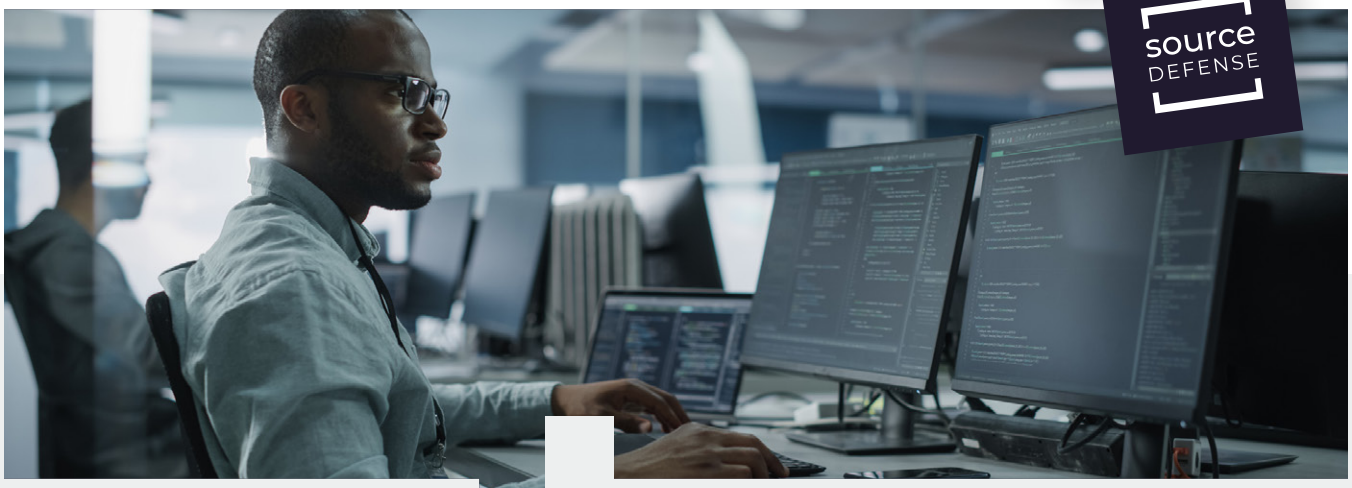
An Easy, Rapid, and Cost-Effective Solution to Minimize Risk

Source Defense can help you quickly gain visibility into this risk and mitigate any problems — preserving the customer experience and eliminating the risk of data leakage and data theft. We are experts in helping retailers prevent digital skimming, Magecart, formjacking, risky Javascript libraries, and open-source risks.

With our patented technology designed with simplicity in mind, we'll help you solve this complex problem without adding strain to your already strained security operation. You'll gain complete visibility into your website partner ecosystem — allowing you to know what script is running and what it is doing.

Our platform ensures that your website is compliant with data privacy mandates and secure from digital skimming attacks.

We have a hassle-free, hands-off, no-expertise-required solution to the problem. Usually, implementation is done in just two weeks and costs less than a penny per transaction for assured customer protection.



[CASE STUDY]

Protecting a Global eCommerce Business Against Digital Attacks

Problem

A critical threat to customer data and brand reputation

News about Digital Skimming attacks like Magecart and formjacking affecting online retailers underscored the urgent need for a solution to protect both the company and its customers. Protecting customers' personally identifiable information (PII) and credit card data were top priorities. Additionally, the company wanted to find a solution that was not just reactive, relying on detection and after-the-fact remediation, but preventive, ensuring that malicious behavior was stopped before it could harm customers.

Solution

A seamless and automated level of data protection

The company recognized that eSkimming and other JavaScript attack vectors were not going away. As a result, the security team tested the Source Defense security platform by placing sample scripts on their website to see if the application would work during the proof-of-concept process. The Source Defense platform successfully met the security team's requirements for a robust, proactive solution to combat this unique form of attack while simultaneously ensuring site performance and user experience remained optimal.

- **No infrastructure changes required:** The Source Defense platform fits seamlessly into the company's existing security stack to combat sophisticated eSkimming/Magecart and formjacking attacks.
- **Accurate and automatic prevention:** With its patented preventative technology, Source Defense was a complete solution with the ability to combat the growing sophistication of such attacks without requiring constant reconfiguration and maintenance.
- **Comprehensive coverage:** Source Defense provided a complete and automated solution for detecting malicious activity from third-party scripts that could unknowingly leave the company's web properties vulnerable to compromise.

Results

Digital data, safe and sound

The company and their respective subsidiaries safeguarded their website from attacks leveraging Source Defense.

- **Ongoing protection without additional overhead**: Source Defense's comprehensive and automated approach enabled the company to stay on top of potential third-party script threats.
- **Reduced risk of digital skimming attacks:** Source Defense helped the company save significant resources by automating the prevention of eSkimming, Magecart, formjacking, and other JavaScript attacks. The company reduced resources by detecting and blocking vulnerabilities where scripts could hijack customer data and jeopardize the customer experience.
- **Brand reputation protected**: Source Defense provided brand and reputation security by eliminating costly threats and safeguarding their visitors' personal details, payment information, and online shopping experience.

> **In working with Source Defense, the proof of concept was smooth and easy to follow as well as a seamless implementation process. Our confidence in the Source Defense team was proven very early on in our relationship and we feel our websites and more importantly, the security of our customers' data are in very good hands.**
>
> Director of Global Information Security

[05] Close the Gap as Soon as Possible

Act Now or Act Soon — But Act Nevertheless!

Your digital supply chain could be putting you and your customers at risk - for both data leakage and the threat of eSkimming/Digital Skimming attacks. So let's get started.

Source Defense is offering free risk reports and access to our platform demo to get up and running quickly.

Schedule a Demo

Chat with a security expert

Learn More

Want to learn more about the risks of Digital Skimming and how to address them?

- Retail Data Breaches: What comes next? Understanding the aftermath of a digital skimming attack
- Canada's largest alcohol retailer hit by Magecart attack
- Magecart e-skimmer attacks targeted thousands of eCommerce sites in 2022
- What happens to a customer after a data breach?
- Data Security: Your ultimate duty to your online customer
- All about eSkimming Attacks