

F5 Distributed Cloud Client-Side Defense: Prevent Skimming and Formjacking

Like credit card skimming in the physical world, cybercriminals have developed attacks to take ownership of legitimate websites and install digital skimming to steal credit card numbers, social security numbers, national identity numbers, names, addresses, login credentials, and other personally identifiable information.



KEY BENEFITS

Protect customer privacy

Monitor client-side code for malicious JavaScript that compromises customer privacy.

Stop account takeovers

Prevent criminals from stealing session identifiers, security tokens, and credentials.

Reduce compliance violations

Ensure your organization is taking all necessary measures to safeguard personal data.

THE TOOLS NOW IN THEIR
ARSENAL-FIREWALLS,
WAFS, BOT DEFENSES,
AND SIEMS-ENFORCE
A SECURITY BOUNDARY
AT THE PERIMETER YET
EXPOSE CUSTOMERS IN THE
PRECISE LOCATION WHERE
THEY INTERACT WITH YOUR
BUSINESS: THE BROWSER.

Chief information security officers (CISOs) face a client-side security gap that puts their customers' privacy and financial well-being at risk. With Magecart-like criminal attacks against websites causing massive breaches, government fines, and loss of customer confidence, the challenge of keeping customers safe online needs urgent attention.

In this attack vector, criminals take over third-party JavaScript files in what is known as a supply-chain attack and exploit the compromised scripts to read customer data and exfiltrate it to attacker-controlled domains. The criminal organization Magecart made this form of attack infamous in 2015 with several high-profile attacks against well-known brands in air travel, ticketing, and retail. These attacks compromised and exploited the Magento shopping cart platform used widely in eCommerce. Since 2015 the attacks have expanded across a wide variety of targets. By 2020 there had been over 2 million Magecart attacks that cost businesses an estimated \$1 billion in 2019 alone.

F5 Labs has identified client-side attacks as a top cause of security breaches. For its 2021 Application Protection Report, F5 Labs found that formjacking payment cards remains one of the most common types of attacks and was responsible for 61% of web attacks.³

Unfortunately, CISOs have lacked the means to ensure effective web security. The tools now in their arsenal—firewalls, WAFs, bot defenses, and SIEM systems—enforce a tight security boundary at the perimeter, where web traffic enters the data center. Yet those tools expose customers in the precise location where they interact with your business: the browser.

Criminals see the value to be stolen, they see that enterprises are not monitoring the browser, and they've discovered myriad ways to inject malicious code and exfiltrate customer data.

CISOs seeking to solve these threats face an ever-present challenge: the dynamic and complex nature of modern web architectures. Today's applications depend on dozens of JavaScript source files from many different domains, each with long supply chains of dependencies, each changing frequently, and many beyond the control of the enterprise. Attackers need only compromise a single file in the JavaScript supply chain to gain complete control over a web application, which enables them to take over accounts, steal financial information, and make off with customers' personal data.

With this level of threat, CISOs need an eye on the browser just as they have an eye on HTTP traffic entering their data center. F5® Distributed Cloud Client-Side Defense—an innovative, new technology driven by rich client-side signal collection and machine learning—gives CISOs the visibility they need to close the client-side security gap.

Client-Side Monitoring, Detection, and Mitigation

Distributed Cloud Client-Side Defense has two core components that establish its efficacy: JavaScript that captures signals and a machine learning analysis service that processes those signals.

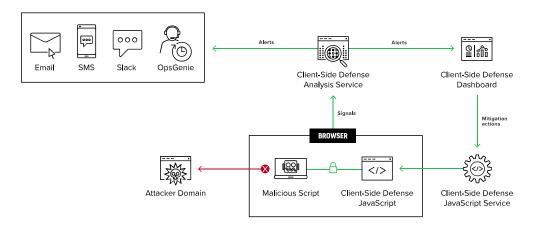


Figure 1: Continuous monitoring, alerts, and one-click mitigation.

F5's JavaScript signal collection has capabilities that make it uniquely effective at detecting malicious JavaScript active in a web application. The Client-Side Defense JavaScript is lightweight and highly performant. It executes in short bursts, freeing the JavaScript thread to ensure a responsive user experience.

This JavaScript is highly obfuscated with an industry-leading JavaScript virtual machine and randomized opcodes, ensuring that attackers can't reverse engineer the code to learn how they're being observed. The virtual machine compresses and obfuscates the signals collected before they're delivered to the analysis service. Without these critical protections, criminals would quickly discover ways to bypass security monitoring.

The Client-Side Defense JavaScript transmits signal data to F5's cloud analysis service, where advanced machine learning algorithms uncover suspicious data exfiltration patterns. When criminal exfiltration is discovered, Client-Side Defense provides alerts via emails, SMS, Slack, Opsgenie, and the Software as a Service (SaaS) console, where with one click the enterprise can block exfiltration to attacker-controlled domains.

These components of the Client-Side Defense system work together to provide continuous and comprehensive protection against JavaScript supply chain attacks. This high level of protection is essential for modern web applications, which are complex and ever changing.

KEY FEATURES

Continuously monitor for threats

Immediately catch attacks by continuously monitoring for malicious JavaScript across your websites.

Get timely alerts

Receive actionable alerts through your preferred channel: email, SMS, Slack, Opsgenie, or the SaaS console.

Alleviate data theft with one click

Stop data exfiltration with the click of a button.

Conclusion

Increasingly, customers and governments demand that organizations take every reasonable measure to protect privacy. Yet the complex and dynamic nature of modern web applications makes it extremely difficult to defend against Magecart-like attacks that put customer data at risk.

To defend against JavaScript supply chain attacks, enterprises require monitoring in the browser, rich signal collection, and advanced machine learning to provide continuous and comprehensive protection.

Distributed Cloud Client-Side Defense provides continuous monitoring in the browser. Know when attackers strike. Mitigate immediately. Protect customer privacy.

Get started today. Contact an expert at sales@f5.com to arrange a free trial.



¹ Jonathan Reed, Magecart Attacks Continue to 'Skim' Software Supply Chains, Security Intelligence (January 21, 2022), found at https://securityintelligence.com/articles/magecart-software-supply-chain/

Ophir Ashkenazi, Magecart Primer: 5 Things Every CFO Should Know, FEI Daily (March 9, 2020), found at https://www.financialexecutives.org/FEI-Daily/March-2020/Magecart-Primer-5-Things-Every-CFO-Should-Know.aspx

³ F5, Inc., 2021 Application Protection Report, found at https://www.f5.com/content/dam/f5-labs-v2/article/pdfs/F5-Labs-2021-Application-Protection-Report-24AUG21.pdf