

## Web Application Security

Protect your site against web skimming attacks



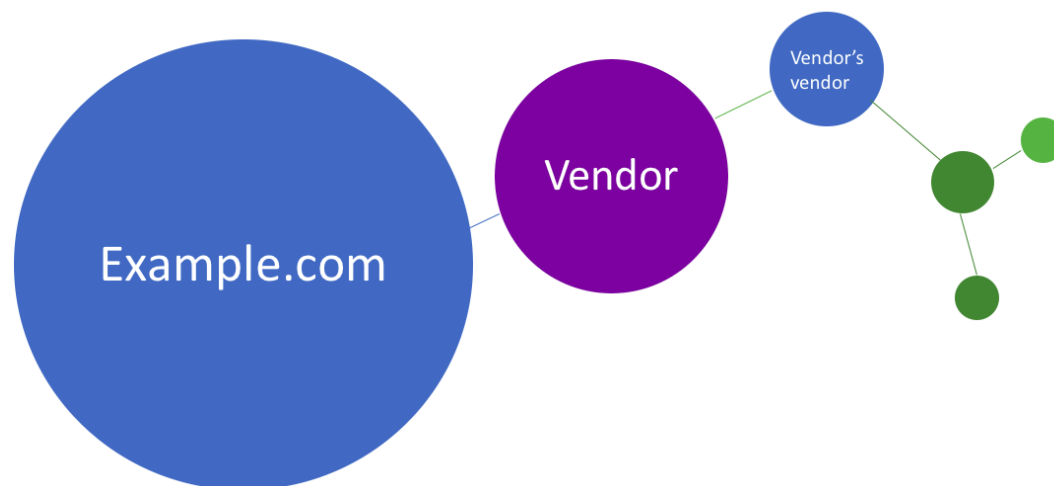
# Protect your site against web skimming attacks



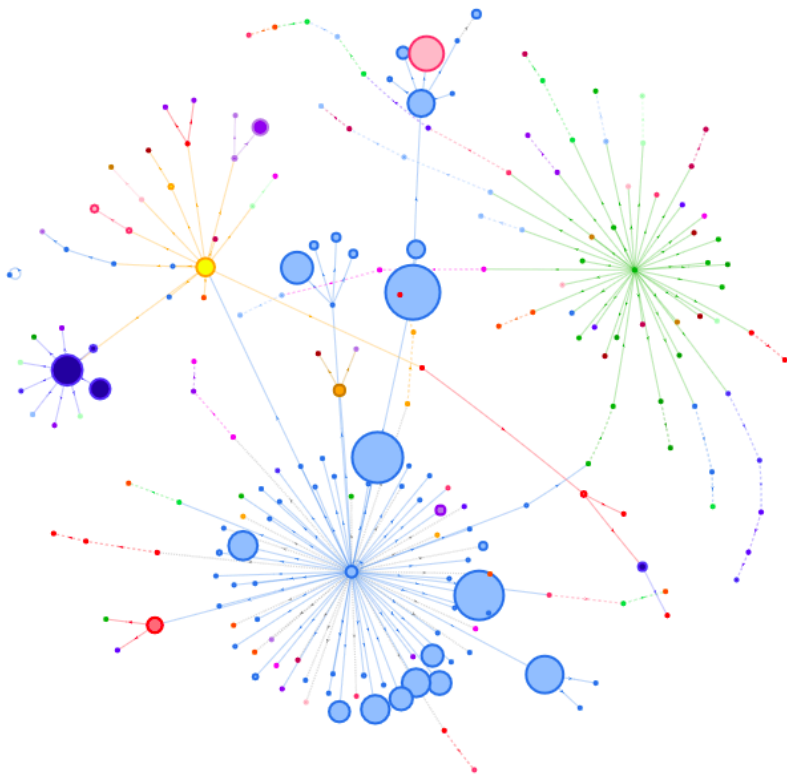
Detect attackers trying to steal data via first or third-party scripts that you use on your site. Client-Side Protection & Compliance identifies suspicious and malicious script behaviors, and helps you take action to protect your site and visitors. You don't need to deliver your content on Akamai's Intelligent Platform to use Client-Side Protection & Compliance. Apply detections to any website, no matter where you host it.

## Magecart and other data hijack threats

All contemporary websites run with a constellation of third-parties we depend on to provide vital features like marketing automation, animations, web experience personalization, advertising, analytics, and other widgets that enrich your site's user experience and inform your business. These third-party vendors do so via code they run on your site. That magic code in turn, relies on your vendor's vendors who run their own code, which is also connected to your website, and so on.



If you look at an actual working website, the network is extensive:



*Blue dots represent requests the original site controls. All other nodes are third parties that connect to the original web site, with direct access to its users through the chain.*

This setup creates a large attack surface for your website, which you can't control or track. You may trust your vendors, but you wouldn't know if they or any of their solution providers are compromised.

## The threat

The code that your third-party vendors run on your site, is separate from your code and your server, so traditional WAF protections aren't part of the mix. More urgently, their code is in contact with your user and can listen in on user entries and send that data wherever it wants.

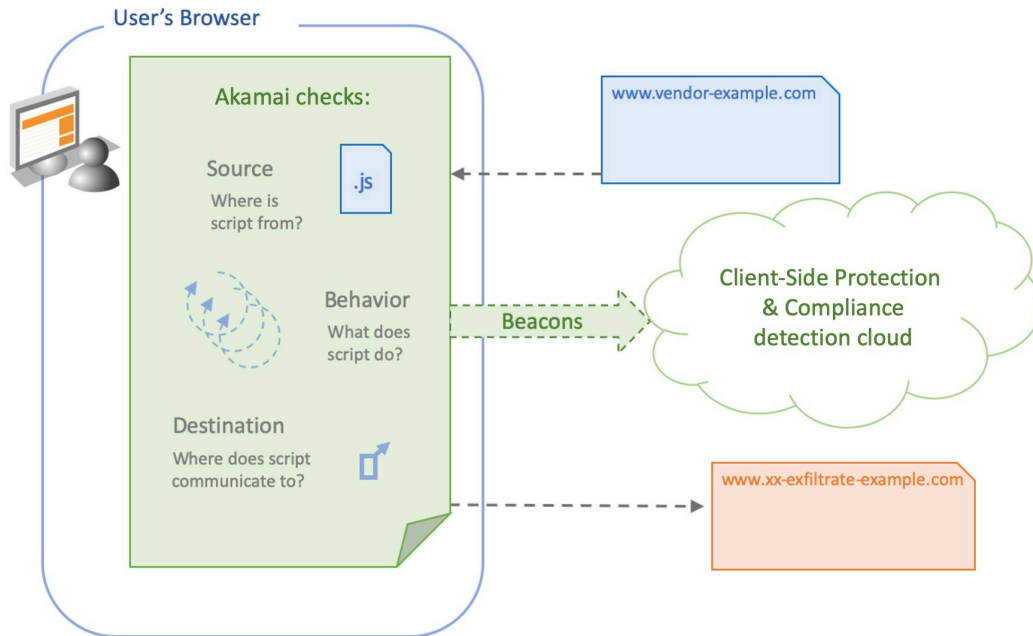
If a bad actor gains entry to the chain, it's not much different from card skimmers in the physical world who insert their bogus device on a bank machine and wait for users to interact directly with that skimmer, while the bank knows nothing about it and can't protect the user.

When attackers get access via third-party code, they can do nefarious things like copy the payment data every user enters in the shopping cart, intercept your users' credential entries, or deface your site.

## How detections work

Client-Side Protection & Compliance constantly analyzes user interaction with your website to identify suspicious and malicious script behavior, potential vulnerabilities, and any script activities that violate policies you define. It lets you manage JavaScript-based threats without degrading the user experience or slowing application development.

When users visit your site, the solution monitors activity in their browser, collecting data on JavaScript activity. It tracks the source of scripts (usually your site's vendors, whom you pay to run scripts on your site), the behavior those scripts execute, and any destination those scripts are sending data to.



Client-Side Protection & Compliance collects JavaScript activity data from an user's web browser and sends that back to our servers on a beacon. A beacon is an HTTPS request (initiated before a user moves to the next page) that includes data, either as HTTP headers, body, or as part of the request's query string.

## Compliance

To help you comply with the new client-side JavaScript security requirements in [PCI DSS \(version 4.0\)](#)<sup>1</sup> which the [Payment Card Industry Data Security Standard](#)<sup>2</sup> introduced in March 2022, we've added a robust feature set to safeguard payment data in the web browser.


Client-Side Protection & Compliance automatically tracks and inventories scripts on payment pages, ensuring their integrity and authorization. Your security team can easily justify the purpose of scripts that are executing on payment pages, with predefined justifications and automated rules.

The solution also monitors for changes in HTTP headers and payment page protections to defend against page tampering. A comprehensive dashboard and dedicated PCI alerts make it easy to rapidly respond to compliance-related events and provide auditing evidence.

## The solution

Akamai can help you protect your site, even from these hidden threats. Our Client-Side Protection & Compliance detects activity that could be stealing user data, or otherwise interfering with the user experience. You can track and investigate these events to rapidly understand and act on the threat.

After you set up your Client-Side Protection & Compliance configuration (for details on setup, read the full [online help](#)<sup>3</sup> you can apply it in a security policy. **Client-Side Protection & Compliance** appears as an additional protection type alongside your others like **IP/Geo Controls**, **DoS Protection**, and so on. The security policy, its match target, and additional injection criteria you set all determine where the system injects special detection JavaScript on your site.

 Make sure the protection configuration you want to apply is active on production before you try to apply it in a security policy.

1. Create or edit a security policy (Or, for most Web Application Protector users, just open your security configuration).
2. On the left side of the screen, under **Protections**, click **Client-Side Protection & Compliance**.
3. If this protection is off, turn it **On**.
4. Select the **Client-Side Protection & Compliance Configuration** you want to apply.  
Only those active in production appear as choices.
5. Scope protections.  
The match target of the security policy you're working in, sets the scope of protections. Within that, you can:

- Set a percentage of end-user page views that experience Client-Side Protection & Compliance JavaScript injection on a page. When you first start using these protections, you can set a small percentage then track results. Then work your way up to 100%. Client-Side Protection & Compliance injects JavaScript detection randomly on HTML pages that comprise the percent of your site you entered.
- Specify specific pages or paths where you want to always inject or never inject. For example, you may want to always inject detection on sensitive form pages where users enter data, but never inject but never inject on your Accelerated Mobile Page (AMP) pages.

6. Turn injection on or off for individual requests.

You can enable or disable detection for specific requests in order to conduct unit testing. You do so by inserting a query string parameter as part of the request. You'll find these values in **Test Parameters** and can use them override other Injection Criteria settings. To:

- Enable detections, include the parameter name and value you see under **Force Injection**.
- Disable detection, include the parameter name and value you see under **Disable Injection**.

7. Click **Save**.

To learn how to monitor suspicious script activity and take action on incidents, read the [Client-Side Protection & Compliance Online Help](#) <sup>Ⓐ</sup> (login required).

Updated 4 months ago

← Prevent account abuse

Protect your brand →

Did this page help you?   **Yes**   **No**

🌐 Select Language ▼

[Legal & privacy](#)

[Cookie settings](#)

[Akamai Status](#)

[Community](#)

[Training](#)

[Control Center](#)

[Cloud Manager](#)

© 2025

Akamai  
Technologies