CLOUDFLARE

SOLUTION BRIEF

Complimentary PCI 4 Client-Side Risk Assessment

Cloudflare Page Shield for advanced web app supply chain security

PCI DSS 4 and client-side security

Cloudflare Page Shield is a security and compliance solution built to address one of the most pressing threats to web applications and web visitors: web application supply chain compromise.

Attackers can modify the code of JavaScript components used on websites through various means, such as stolen account credentials or the exploitation of zero-day or unpatched vulnerabilities. Once they gain privileged access, attackers can launch downstream attacks on every website using the compromised JavaScript code.

New mandates from PCI DSS 4.0, effective March 2025, require organizations with payment pages to monitor scripts for attacks and protect their end users from browser supply chain compromise (requirements 6.4.3 and 11.6.1).

Did you know?

According to new research from Cloudflare, enterprise organizations have an average of 47 third-party scripts in their websites—a significant attack surface for supply chain compromise.

With a Page Shield PCI DSS 4 client-side risk assessment, you'll gain access to customized, real-time insights on:

- **Where** third party scripts and connections have been added to your websites.
- **What** specific threats are evading your defenses.
- **Which** third-party components have been compromised by malicious activity, potentially endangering your end users' devices and data.
- **How** your current posture measures up against PCI 4.0 client-side requirements (6.4.3 and 11.6.1).
- **How** to quickly address client-side security gaps and meet compliance requirements.

How it works

The best way to assess the effectiveness of security products is by using real-world data from your own websites. Page Shield's cloud-native service runs as a reverse proxy, gathering information directly from the browser. This allows you to get up and running in minutes without deploying any hardware or software.

- Set up in minutes, with no impact on website performance or your end users.
- Our assessment typically runs for 2 to 7 days, but you can see insights on third-party scripts and connections immediately after deployment.
- At the conclusion of the assessment, the Cloudflare team will provide a detailed, custom analysis. You can also access your dashboard at any time during the assessment.
- Additionally, your Cloudflare account team will alert you in real time to any supply chain compromises or active attack incidents during the assessment.

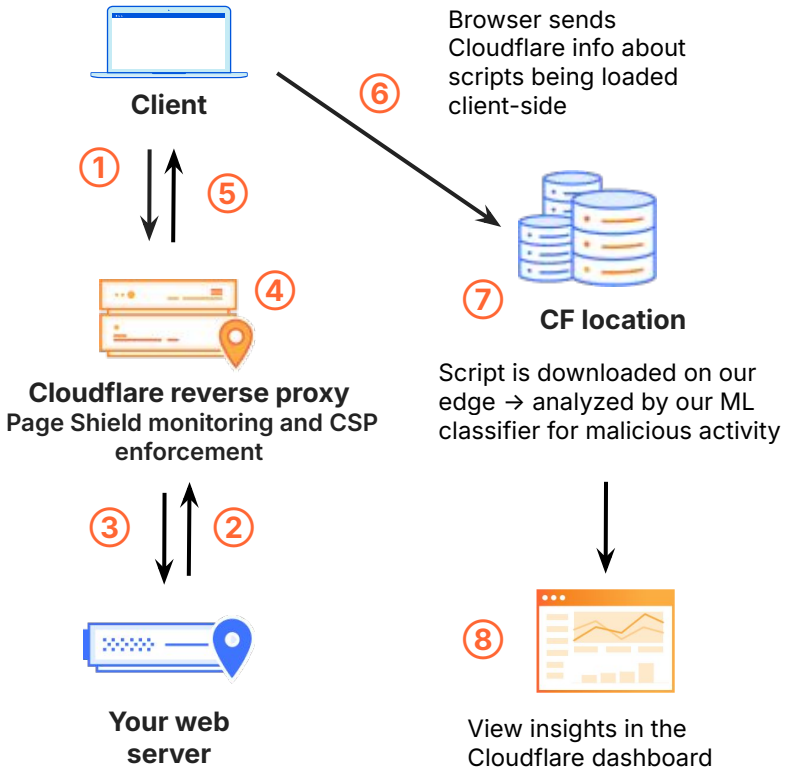

Figure 1: Cloudflare Page Shield architecture

Sample results from assessment

Inventory of active scripts			
Malicious	**Script**	**Host**	**Last Seen on Page**
⚠	https://example.com/papel/scripts/analytics.js	bt4al.example.com	/
⚠	https://example.com/0001.js	bt4al.example.com	/
	https://www.jsdeliver.com/package/npm/dog.js	bt4al.example.com	/pageshieldforcecsp.html
	https://bt4al.example.com/cdn-cgi/bm/cv/669835187/api.js	bt4al.example.com	/

Figure 2: A table representation of Page Shield's script monitoring

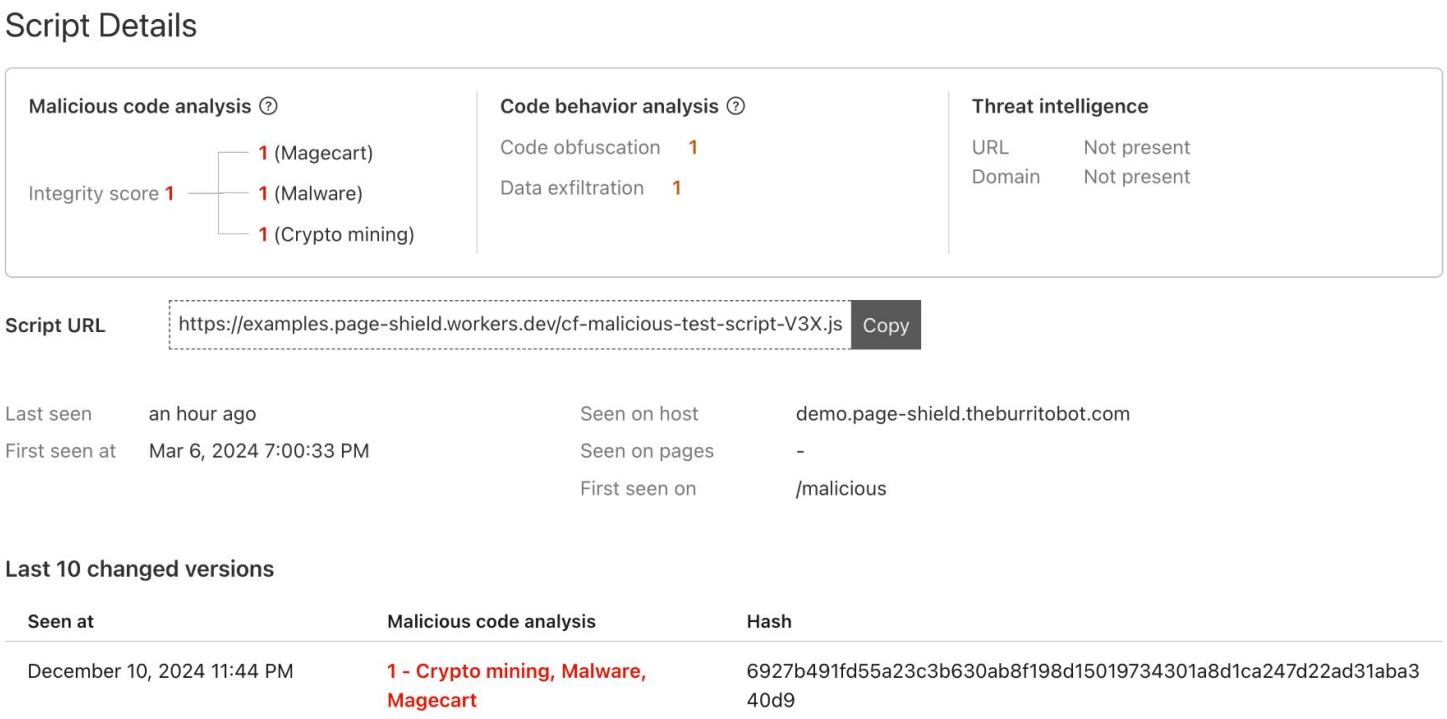

Figure 3: An example of the information provided to you when we find malicious activity in a script

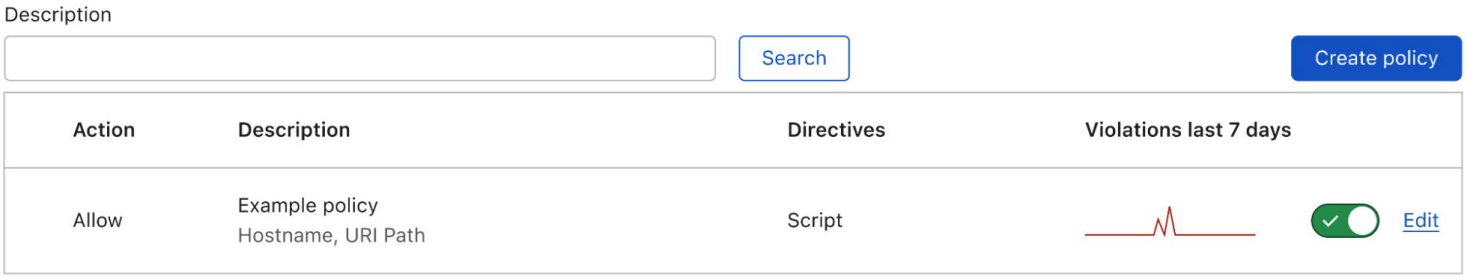

Figure 4: Enforce a positive security model with content security policies (CSPs) and view violations

Get started with a free PCI 4 client-side risk assessment today.