Cloudflare Page Shield

Secure your web application supply chain and protect end-users from client-side attacks.

Rising client-side attacks

Blind spots created by third-party dependencies

For great web experiences, companies enhance website functionality with capabilities like chatbots or analytics obtained from other (3rd party) companies or developers. Attackers look to compromise these 3rd party dependencies to steal the private data end-users enter into a site, deliver malware, carry out crypto mining, or perform subsequent attacks.

Identify and mitigate supply chain attacks

Page Shield protects websites' end-users from client-side attacks that target vulnerable JavaScript dependencies. Page Shield receives information directly from the browser about what JavaScript files and modules are being loaded, conducts analyses to detect malicious scripts, gives you visibility on all active scripts, outbound connections, and alerts you whenever a JavaScript file is showing malicious behavior.

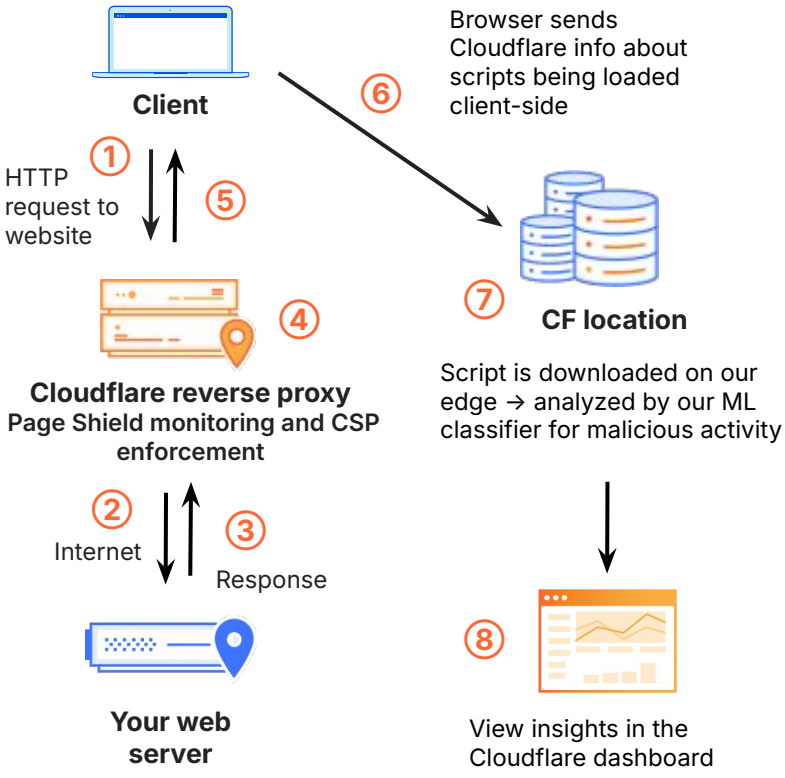

Figure 1: Cloudflare Page Shield architecture and traffic flow

Intelligent attack prevention

Get complete visibility into your web app supply chain and mitigate supply chain attacks by continuously monitoring active scripts, changes to scripts, and the connections they make.

Automatic threat alerts

Get instant notifications when new scripts are detected, marked as malicious, or loaded from unknown domains.

Meet compliance requirements

Reduce third-party vendor risk and address client-side requirements of regulations like GDPR, PCI DSS 4.0, and more. Page Shield will help you meet these requirements without any additional effort.

Features that let you take control of your web application supply chain and secure your end-users' browser environments

Page Shield	
Script monitor	Displays information about the third party scripts loaded in your domain's pages.
Connection monitor	Displays information about connections made by the scripts in your domain's pages.
Cookie monitor	Displays information about cookies detected in HTTP traffic.
Page attribution	Allows you to find on which page a script first appeared and view a list of the latest occurrences of the script in your pages.
New resources alerts and new domain alerts	Configure and customize notifications about newly detected scripts or scripts loaded from unknown domains.
Malicious script detection and alerting	Detects malicious scripts in your pages using threat intelligence and machine learning.
Code change detection and alerting	Detects any changes to the scripts and connections loaded on your pages. Alerts can be configured to send more or less frequently.
Malicious connection detection and alerting	Detects if a script makes a connection to a malicious domain, such as a command-and-control domain or cloud storage indicating data exfiltration.
Policies	Policies define the resources allowed on your applications through Content Security Policy (CSP) directives. Policies can log violations and enforce a positive security model defining an allowlist of resources, and blocking resources not included in the policies.

Ready to see Page Shield in action? Sign up for our free Client-Side Risk Assessment today.