CLOUDFLARE

Product Brief

# Cloudflare Page Shield

Keep ecommerce and business safe from Magecart, client-side attacks targeting end-users

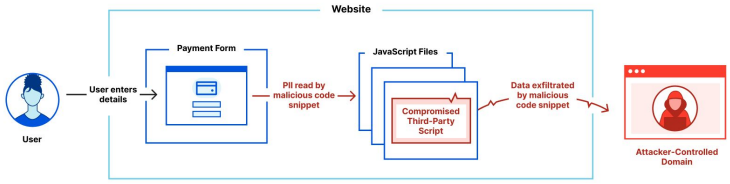
## Rising client-side attacks

### 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. Attackers have successfully exploited 3rd party scripts to exfiltrate sensitive user data to attacker-controlled domains. Multiple high-profile examples of these “Magecart” attacks have resulted in considerable brand damage and, in some cases, substantial GDPR fines.

Many companies have not formally tracked dependencies and are blind to what is on their site. Some organizations have used Content Security Policies (CSPs) to control what loads in a web visitor’s browser. However, CSPs are challenging to maintain and keep updated. They cannot detect if a permitted dependency has been compromised even when properly managed.




### 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.

### Meet PCI 4.0 client-side security requirements

The latest update to PCI DSS 4.0 sets out best practices to tackle supply chain attacks. Page Shield will help you meet these requirements without any additional effort.

### Visibility

Get complete visibility into 3rd party scripts on sites by continuously monitoring active scripts, changes to scripts, and the connections they make.

### Detection

Detect malicious behavior on your end-users’ browsers using threat intelligence and machine learning.

### Prevention & Mitigation

Receive custom notifications - newly detected scripts, scripts loaded from unknown domains, new scripts considered malicious, or code changes in your existing scripts.

# Features that let you take control of third-party scripts

| Page Shield | |
|---|---|
| **Script monitor** | Displays information about scripts detected in your domain's pages. |
| **Connection monitor** | Displays information about connections made by the scripts in your domain's pages. |
| **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. |
| **Malicious script detection** | Detects malicious scripts in your pages using threat intelligence and machine learning. |
| **Code change detection** | Detects any changes in the scripts loaded on your pages. |
| **Positive script blocking** | Enforce a positive security model to ensure only allowed scripts are loaded by the browser. |
| **Alerts** | Get instant alerts to stop malicious behavior. |


## Why would you select Page Shield?

- Get more control over third-party JavaScript
- Prevent attacks against your end-users
- Overcome the limitations of CSP
- Meet PCI 4.0 client-side security requirements

In a nutshell, you can effortlessly identify and mitigate supply chain attacks in the context of web applications.

## Cloudflare Leadership

Organizations gain a more effective application security posture with the Cloudflare global network as their enterprise security perimeter. The Cloudflare application security portfolio has received numerous accolades for its strength and breadth. Gartner named Cloudflare a leader in the **2022 Gartner® Magic Quadrant™ for Web Application and API Protection (WAAP)**. Gartner also named the Cloudflare WAF a 2022 Customer's Choice. Frost & Sullivan recognized Cloudflare as an Innovation Leader in the 2020 Global Holistic Web Protection while IDC and Forrester named the company a 2021 DDoS leader.