Cloudflare Page Shield

Client-Side Script Monitoring + PCI DSS 4.0

Enterprise Sales Training • Brandon Crowe

What Is Page Shield?

- Monitors every third-party script, connection, and cookie running in your visitors' browsers
- Detects malicious scripts using ML-based scoring — Magecart, skimmers, data exfiltration
- Uses Content-Security-Policy-Report-Only headers to see what's loading without breaking anything
- Tracks three categories: Scripts, Connections, and Cookies
- Alerts when a known-good script changes behavior or a new unknown script appears
- PCI DSS 4.0 requirement for anyone processing payments on their website

Why Page Shield Matters (The Business Case)

- API Shield protects your server-side APIs. Page Shield protects the client-side browser environment.
- Modern websites load dozens of third-party scripts — analytics, chat widgets, payment forms, A/B testing
- If ANY of those vendors gets compromised, the malicious code runs in YOUR customers' browsers
- Magecart attacks have hit British Airways, Ticketmaster, Newegg — millions of credit cards stolen
- You can't firewall JavaScript running in someone's browser. Page Shield is the only way to monitor it.
- PCI DSS 4.0 (Section 6.4.3) requires monitoring of payment page scripts — compliance deadline has passed

How It Works

1. Enable monitoring — Cloudflare injects a CSP-Report-Only header on your responses

2. Browsers report back — every script, connection, and cookie is reported to Cloudflare

3. ML scoring — Cloudflare analyzes each script for malicious patterns (data exfiltration, DOM manipulation, keylogging)

4. Dashboard visibility — see every resource loading on your site, scored and categorized

5. Alerts — get notified when a script changes, a new script appears, or a malicious pattern is detected

What Page Shield Monitors

Category	What It Tracks	Why It Matters
Scripts	Every external JS file loaded in the browser	Compromised scripts can steal credentials, payment data, PII
Connections	Every outbound connection your page makes	Detects data exfiltration to unknown domains
Cookies	Every cookie set by scripts on your domain	Catches tracking cookies and session hijacking attempts

Real-World Use Cases

Healthcare — A hospital website loads a chat widget, analytics, and a payment form. Page Shield monitors all those third-party scripts. If the chat vendor gets compromised and starts exfiltrating data (Magecart-style), Page Shield detects the malicious behavior, scores it, and alerts you before patient data leaks. This is a PCI DSS 4.0 requirement for anyone processing payments.

E-Commerce / Retail — Online stores load payment processors (Stripe, Adyen), analytics (GA4), live chat, and recommendation engines. A compromised analytics script could silently skim credit card numbers from the checkout page. Page Shield catches it.

Financial Services — Banking portals, investment platforms, insurance quote forms. All load third-party scripts for functionality. Page Shield monitors for any script attempting to capture keystrokes or exfiltrate form data.

Government / Corrections — Visitor-facing portals that process commissary payments need PCI DSS 4.0 compliance. Script monitoring catches malicious JS that could skim payment info or exfiltrate PII from visitor portals.

Media & Publishing — News sites and content platforms load 20-40 third-party scripts (ad networks, analytics, social widgets). Any one of them could be compromised. Page Shield provides visibility across all of them.

API Shield vs. Page Shield — Complete Picture

	API Shield	Page Shield
Protects	Server-side APIs	Client-side browser
Threat model	Malformed requests, BOLA, abuse	Compromised scripts, skimmers, exfiltration

How it works	Schema validation at the edge	CSP monitoring + ML scoring
Compliance	API security best practices	PCI DSS 4.0 (6.4.3)
Key feature	Block bad requests before they reach your server	Detect malicious scripts before data leaks

What I Built — Page Shield on saltwaterbrc.com

- Page Shield continuous monitoring enabled on saltwaterbrc.com
- Monitors Scripts, Connections, and Cookies across all pages
- Current status: clean bill of health — no third-party scripts detected
- Site runs entirely on first-party Astro-generated code (ideal security posture)
- Combined with API Shield (18 endpoints, schema validation) and WAF Managed Rules
- Security Events already showing real attacks: bots probing /.env, /wp-config.php.bak

Sales Talking Points

- "API Shield protects your back end. Page Shield protects your front end. Together, that's full coverage."
- "If your site loads a payment form, you need Page Shield for PCI DSS 4.0 compliance. The deadline has passed."
- "You can't firewall JavaScript in someone's browser. Page Shield is the only way to see what's running."
- "Magecart hit British Airways for 380,000 credit cards. A single compromised script. Page Shield catches that."
- "My site shows a clean bill of health — zero third-party scripts. How many does yours load? Let's find out."

Technical Architecture

Visitor loads page > Cloudflare injects CSP-Report-Only header > Browser executes scripts > Browser reports all resources to Cloudflare > ML scores each script > Dashboard shows results + alerts

No agents to install. No code changes. No performance impact. Just enable it in the dashboard.

Built by Brandon Crowe • Enterprise Sales • Cloudflare