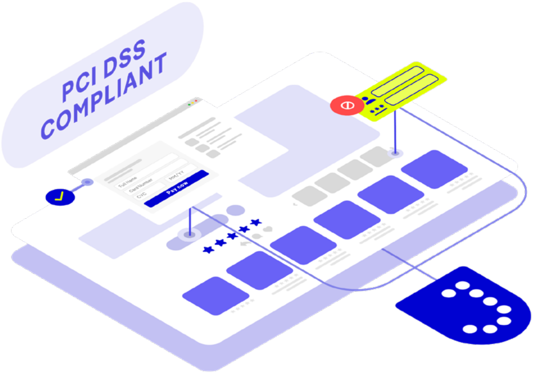
jscrambler

Jscrambler's PCI DSS Module

Achieve simple and scalable PCI DSS v4 compliance by authorizing, protecting, and monitoring payment page scripts while reducing script authorizations by 40%.



Fast-track your compliance and protect your website against clients-side risks such as web skimming attacks and data leakage

Authorize & Protect (6.4.3)

Jscrambler enables the discovery, authorization, business justification, and the integrity of all scripts to comply with requirement 6.4.3.

Detect & Alert (11.6.1)

Jscrambler detects and alerts on tampering, unauthorized modifications, and malicious behaviors to comply with requirement 11.6.1.

Control script behavior

Jscrambler allows you to easily generate assessment-ready compliance reports built for QSAs.

Key business benefits

Flexible Hybrid Architecture

Achieve quick and easy compliance with agentless or agent-based architecture with zero impact on website performance.

Streamlined Script Management

Our bulk approval feature is ideal for scaling, significantly reducing the time required to approve vendors across multiple payment pages and allowing your team to focus on critical tasks.

Delegated Compliance

Take advantage of Jsvrambler's deep expertise on PCI DSS requirements 6.4.3 and 11.6.1. Our team handles the bulk of the compliance work, reducing the need for additional in-house resources.

Powerful suite of features to achieve easy and scalable compliance with PCI DSS v4

Flexible Hybrid Architecture

Jscrambler offers deployment flexibility where you can go agentless or agent-based across each of your payment pages. The integration is super fast, allowing you to bring as many pages into compliance as needed. All the data goes back to the same dashboard. There’s no lock-in, and you can switch deployment methods back and forth as your risk appetite changes.

Script Inventory, Integrity Assurance and Justification (PCI DSS v4 6.4.3)

Maintains a real-time inventory of all scripts running on payment pages, along with justifications for their necessity and compliance status, helping organizations to keep track of and justify the use of each vendor script as required by PCI DSS v4. Jscrambler implements methods to confirm each script is authorized, aligning with the requirement to verify script legitimacy.

Script and Header Change and Tamper Detection Alerts (PCI DSS v4 11.6.1)

Jscrambler sends alerts on unauthorized modifications to HTTP headers, ensuring data transmission security. Jscrambler monitors the content of payment pages as received by the consumer’s browser, alerting to any unauthorized modifications, thereby preserving the integrity of the payment process.

Automated Workflow Integrations

Alerts can be configured to be sent automatically by email, through the SIEM dashboard, via Jira, or a dedicated Slack channel. These integration options can be configured through the dashboard, and the customer can ask for any other tool to be added through support.

Assessment-Ready Reports

Jscrambler provides a detailed assessment report detailing all vendors, scripts, and authorizations, simplifying the audit process for your QSA. This report will support you during internal and external audits.

Delegated Compliance

With Delegated Compliance, the Jscrambler experts manage the script authorization workflows for you. The service is comprised of 3 main parts: script management & justification, policy & procedures management, and annual assessment/SAQ guidance. Jscrambler offers unparalleled flexibility, allowing you to customize and select only the Delegated Compliance components you need to meet your goals.

Advanced Skimming Detection & Analysis

Jscrambler leverages advanced static code analysis techniques to thoroughly examine and identify potential threats associated with skimming attacks. The end result provides a comprehensive assessment of whether skimming activity is present on the website.

Skimming Prevention & Behavior Blocking

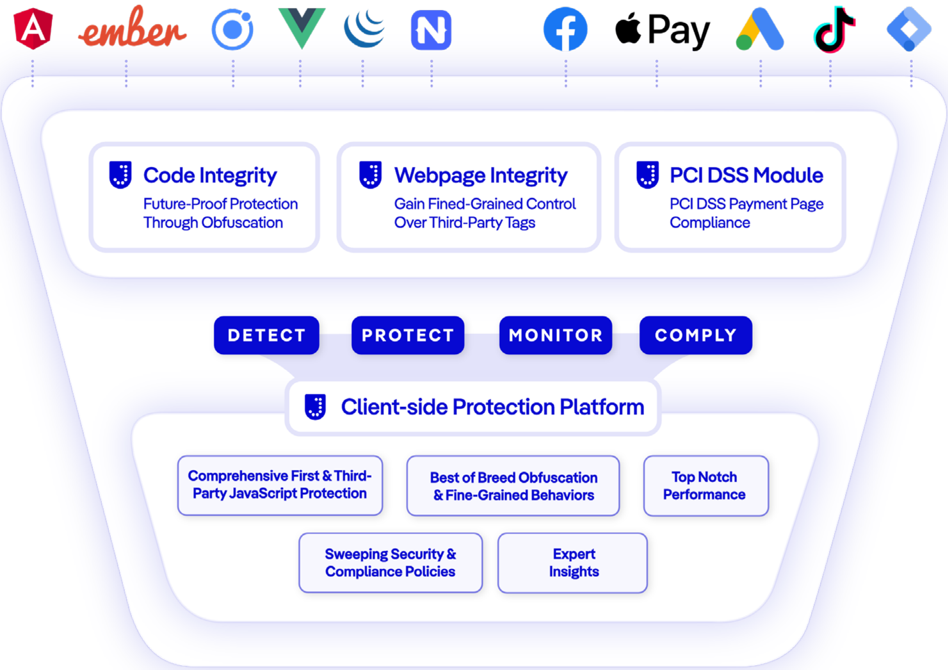
Jscrambler offers a suite of powerful features that offer granular control and block malicious script behaviors while maintaining full functionality. Data fencing features are critical to controlling exactly which scripts can read and access data, and keeping malicious actors from stealing sensitive information that users enter into forms. With Iframe Control, Jscrambler allows you to easily manage which vendors or scripts are permitted to create or manage iframes on your website.

Our clients vouch for us

> "We wanted to not only formally become PCI DSS-compliant but to have proper tools to track changes and control them. We prefer to rely on specific partners to do a specific job and be the best at what they do. At some point, I started to look for guys who could specifically address PCI DSS v4 requirements. And this is how I stumbled upon Jscrambler. With Jscrambler, I have one less thing to worry about and that is a big win".

Andrei Rebrov, CTO & Co-Founder at Scentbird

Jscrambler is the most comprehensive solution for client-side protection


ember
Pay
Code Integrity
Future-Proof Protection Through Obfuscation
Webpage Integrity
Gain Fined-Grained Control Over Third-Party Tags
PCI DSS Module
PCI DSS Payment Page Compliance
DETECT
PROTECT
MONITOR
COMPLY
Client-side Protection Platform
Comprehensive First & Third-Party JavaScript Protection
Best of Breed Obfuscation & Fine-Grained Behaviors
Top Notch Performance
Sweeping Security & Compliance Policies
Expert Insights

CYBER SECURITY EXCELLENCE AWARDS WINNER 2023

50 Technology Fast 50 2023 PORTUGAL Deloitte.

Gartner HYPE CYCLE FOR APPLICATION SECURITY 2024

BIG INNOVATION 2024

Highest User Adoption FALL 2024

Want to see Jscrambler's PCI DSS solution in action and effortlessly comply with PCI DSS?

Book a demo >