



Full-Featured Webpage Threat Monitoring

Key Business Benefits

- **Gain complete visibility** over every threat to your client-side, regardless of the delivery mechanism.
- **Preserve your reputation**, by keeping your users protected when they submit sensitive information or perform transactions.
- **Safeguard revenue streams**, by ensuring that no client-side attacks are diverting your users or tricking them and damaging your conversion rate.
- **Ensure client-side compliance** with regulations such as PSD2.

Jscrambler detects any kind of client-side injection in real-time

User Interface Protection

Jscrambler provides continuous monitoring of unwanted changes to the user interface, guaranteeing that the user interface is always displayed as-designed.

DOM Monitoring

Real-time monitoring of the webpage, with real-time notifications for client-side threats such as code injections. Full protection against DOM tampering, including zero-day threats.

Customer Hijacking Prevention

Complete visibility and prevention of unwanted changes to the customer journey, including injected ads, popups, and other malicious content.

Supply Chain Attacks Mitigation

Full client-side protection against Supply Chain Attacks, with real-time detection and effective mitigation of compromised third-party scripts and code dependencies.

Trusted by the Fortune 500 and 43000+ companies and individuals globally.

+1 650 999 0010

contact@jscrambler.com

jscrambler.com



Supply Chain Attacks

Your third-party code suppliers don't have enterprise-grade security.

You must protect your client-side against supply chain attacks.

66%

Average web application code coming from third-party providers

1000+

Code dependencies in modern JavaScript applications

420K+

Credit cards stolen by Magecart Supply Chain Attacks in 2018

Browser Extensions As An Attack Vector

Malicious extensions are easy to publish and spread. They defeat most security layers, *including CSP*, and **can completely modify every aspect of your web application.**

500M+

Individuals using browser extensions

10%

Total submitted Chrome extensions classified as malware

71%

Chrome extensions that ask for full read/write permissions on all websites

Banking Trojans & Man-in-the-Browser Attacks

Trojans and MitB attacks are able to sniff out and modify transactions while they're happening in the browser, stealing credentials and funds from infected users' accounts.

1.8M+

Users infected by mobile banking trojans in 2018

50%

Increase in banking trojans in 2018 alone

\$550M+

In damages from MitB attacks since 2010

Trusted by the Fortune 500 and 43000+ companies and individuals globally.

+1 650 999 0010

contact@jsrambler.com

jsrambler.com