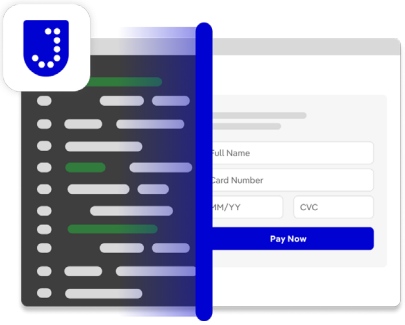
jscrambler

Jscrambler's Code Integrity

Protect your application's code with best-in-class first-party JavaScript obfuscation.



Protect your client-side assets and fortify your defense

Get advanced protection

Safeguard your web applications from malicious attacks with state-of-the-art obfuscation, environmental integrity checks, and dynamic runtime code protection.

Experience minimal impact on performance

Take advantage of comprehensive client-side protection with minimal impact on website or app performance. No compromises.

Seamlessly integrate

Code Integrity seamlessly blends into your current CI/CD processes, securing code integrity and maintaining customer trust. Setup time is just a few hours.

Key business benefits

Protect your Intellectual Property and your investment

Considerably reduce your attack surface by hardening JavaScript at runtime. Shield your exposed code and prevent reverse-engineering and zero-day exploits.

Accelerate release with CI/CD Support

Support first-party JavaScript obfuscation throughout the web application product lifecycle, seamlessly integrating it into the release process and the CI/CD pipeline.

Mitigate risks with total client-side visibility

Gain an extensive view into your client-side attack surface, receive notifications whenever your rules are violated, and make sure no risk stays unnoticed.

Powerful suite of features to help you excel at client-side protection

Polymorphic Code Obfuscation	Advanced obfuscation transformations with built-in resilience against all reverse engineering tools and techniques. Its polymorphism ensures that each new build has a completely different output.
Code Locks	Restrict where and how the code is being executed. Code Locks help to protect code by enforcing licenses, and preventing it from running outside of the set parameters, be it Browser, Date, Domain, or Operating System.
Automatic Configuration	Secure your app easily in under 3 minutes, without needing to configure it manually. Choose Automatic Configuration and apply code protection with just one click.
Anti-Tampering	Anti-Tampering protects your application against changing or modifying your code. The feature allows for the code to be repaired when that happens or for countermeasures to be deployed. Countermeasures can be specified (optionally) to be executed when someone tries to tamper with the code.
Countermeasures	Automatic reactions to thwart attacks, such as redirecting the attacker, getting a real-time notification, or calling a custom function.
Runtime Code Protection	Self-defensive capabilities that enable applications to detect and react in real time to any tampering, debugging, or poisoning attempts.
Anti-Debugging	Protect your application in runtime and thwart reverse engineering attempts with a powerful anti-debugging feature that detects debuggers in real-time and triggers countermeasures.
Anti Monkey Patching	Detects when your code is affected by malicious Monkey Patching, code poisoning, and changes in an eval function behavior.
Real-time Alerts	Immediately notice high-risk behaviors and gain real-time reaction capabilities, full application monitoring, and notifications.

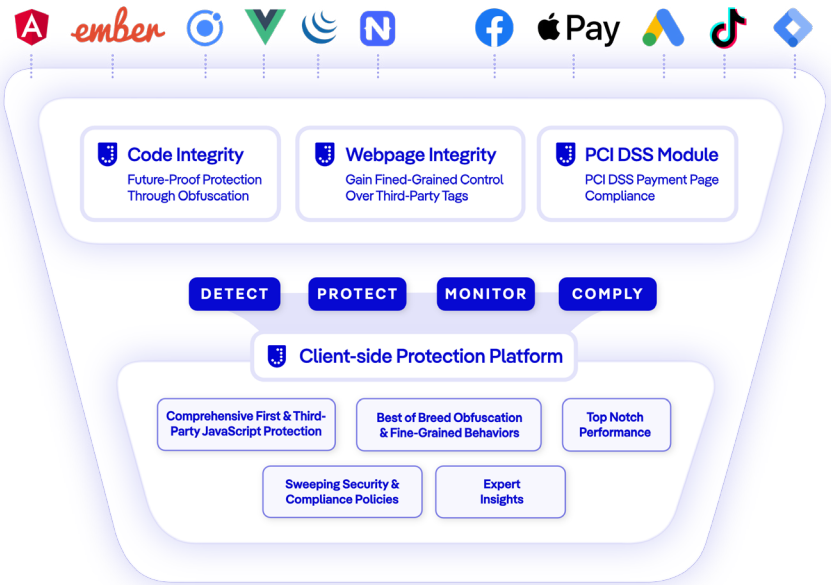
Full Compatibility

Code Integrity is the most compliant JavaScript protection solution in the market and works seamlessly with all major tech stacks, frameworks, and libraries.

Our clients vouch for us

"If I had to summarize the benefits of the Jscrambler product in one sentence, I would say it's state-of-the-art code protection and negligible performance impact."
Sven Hoffmann, CTO and Co-Founder at Powtoon

Jscrambler is the most comprehensive solution for client-side protection



Want to see Jscrambler's Code Integrity in action and start safeguarding your applications?

Book a demo