

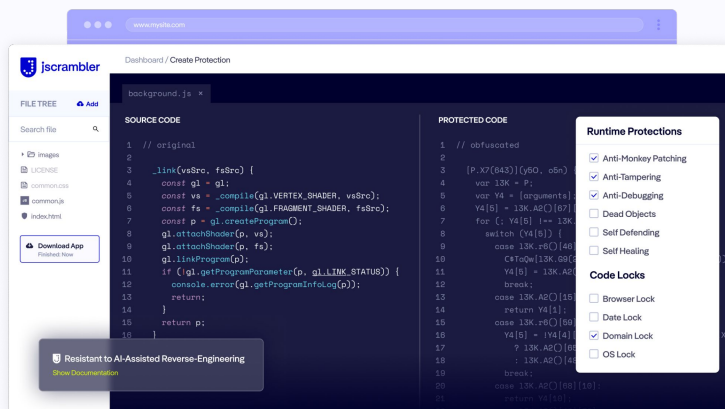
Jscrambler Code Integrity

Protect your client-side assets with Jscrambler Code Integrity, the market's leading code protection solution built for AI-assisted attacks.

Challenge



Modern applications execute inside the browser, delivering proprietary algorithms, validation logic, and workflows directly to end-user devices where anyone can inspect them. With direct access to your code, bad actors can reverse engineer algorithms, bypass licensing, manipulate workflows, automate fraud, and extract competitive intelligence. And traditional security can't help: backend controls, firewalls, and server-side protections stop at the browser's edge. Once your code executes client-side, it's beyond their reach.



KEY BENEFITS



Full compatibility
with all major JavaScript tech stacks, frameworks, and libraries



LLM-Resilient protection
through polymorphic code obfuscation



Seamless CI/CD integration
with setup time of just a few hours

Jscrambler Approach



By combining LLM-resilient obfuscation, runtime integrity checks, and tamper detection, Jscrambler's Code Integrity ensures your proprietary logic cannot be read, replicated, or manipulated whether by a manual attacker, an automated bot, or an AI-assisted reverse engineering tool. The result is a hardened application that protects your intellectual property, reduces fraud exposure, and strengthens your compliance posture across every environment it runs in.

"Thanks to Jscrambler, we've been able to keep our technology secure without any further incidents of code theft for over eight years. So it's safe to say that the product has a 100% success rate in our specific use case."

— Tim Akhmetvaleev, Head of Sales at FlippingBook

[Read the case study →](#)

Jscrambler Code Integrity

Protect Your Intellectual Property and Investment

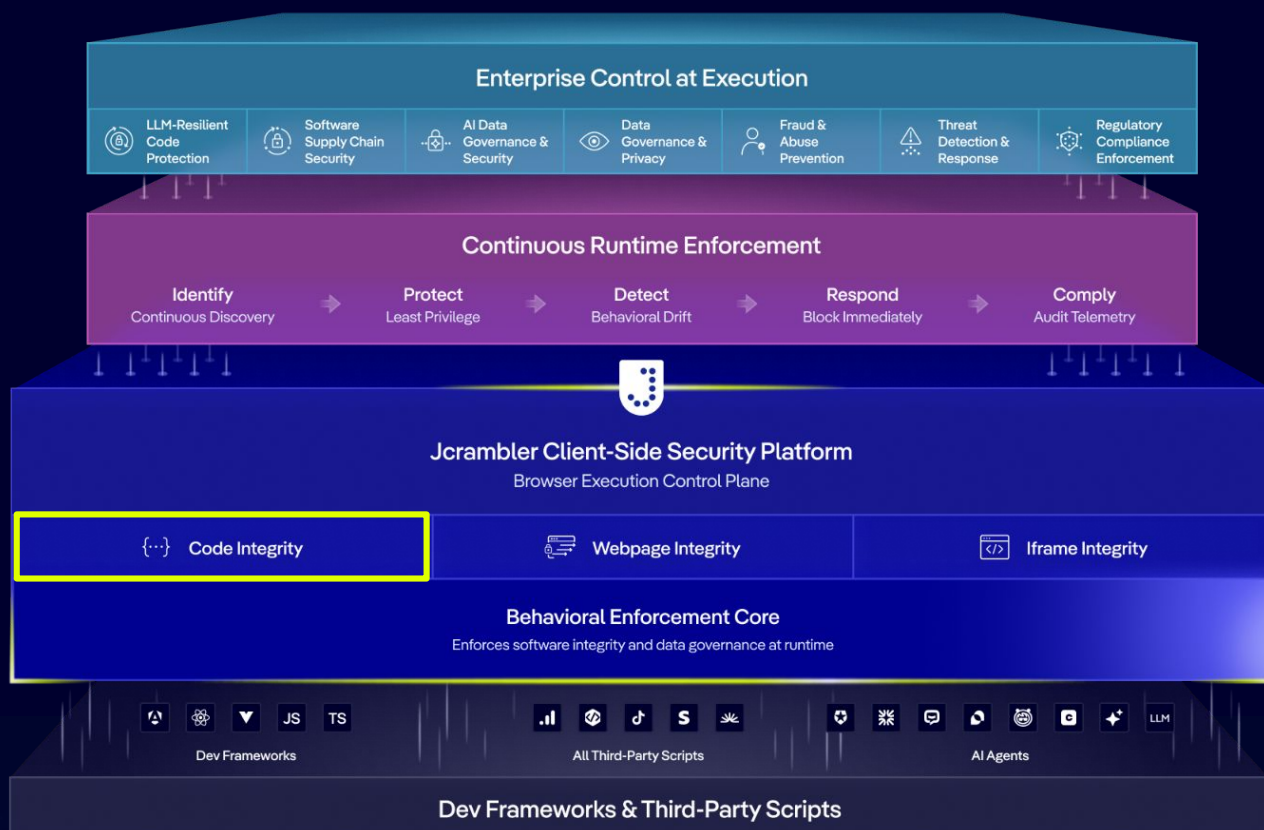
Prevent reverse engineering, zero-day exploits, and LLM-assisted code analysis. As AI tools lower the barrier to extract and replicate proprietary logic, resilience against automated comprehension is now a core security requirement.

Reduce Fraud and Automated Abuse

Protect authentication flows, pricing rules, and transaction logic from bots and manipulation. Code Integrity makes it dramatically harder to automate attacks against the client-side logic that drives your business-critical workflows.

Enforce Licensing and Regulatory Compliance

Ensure your code cannot be modified by attackers attempting to bypass licensing restrictions. Maintain compliance with GDPR, CCPA, NIST, and OWASP by building resilience directly into your application.



Go Beyond the Edge: Contact us today to enforce enterprise policies into the browser runtime.

[Jscrambler.com/contact-us](https://jscrambler.com/contact-us)