jscrambler

Web Banking Meets Client-Side Security

Key Business Benefits

Minimize exposure to data breaches, by protecting JavaScript code and gaining real-time visibility of client-side attacks.

Minimize exposure to losses from transaction fraud, by preventing banking trojan webinjects and other client-side exploits.

Increase compliance with regulations such as PSD2 by increasing client-side security and monitoring web pages in real-time.

Easily integrate with your SIEM to maximize your organization's ability to respond to threats in real-time.

Code Integrity protects the source code of your web banking platform

Enterprise-Grade Application Shielding

With Jscrambler's resilient obfuscation, environment checks and defenses against malicious modification/injection of code, attackers won't be able to reverse engineer, debug or tamper with your app's JavaScript and native code.

Best-in-class Runtime Protection

Give self-defending capabilities to your web banking platform, which will detect debugging/tampering attempts and trigger countermeasures like breaking the application.

Webpage Integrity secures your platform against malicious code

Full Client-Side Visibility

Monitor the behavior of each of your website's scripts in real-time, see the full details of each detection and receive warnings for critical security threats.

Webpage Threat Mitigation

Mitigate client-side attacks to your website in real-time regardless of the attack vector and keep your users safe at all times. Prevent web supply chain attacks, data leakage, banking trojan webinjects, adware and customer hijacking.

Gartner **2019** MARKET GUIDE FOR IN-APP PROTECTION

Gartner **2020** MARKET GUIDE FOR ONLINE FRAUD DETECTION

Trusted by the Fortune 500 and thousands of companies globally.

BBVA mibanco SAMSUNG verimatrix DRIVING TRUST intertrust

+1 650 999 0010 hello@jscrambler.com jscrambler.com