

MeDirect protects its source code with Jscrambler



Code Integrity's multi-layer protection greatly reduced the attack surface of MeDirect's banking application, making it much harder for potential attackers to understand the logic behind the app.

About MeDirect

MeDirect is a pan-European digital banking company founded in 2004 and a Malta's third-largest banking group regarding total assets. MeDirect focuses on WealthTech and specialized mortgage lending. It offers different tools and services to help customers manage their money from over 850 funds, 400 ETFs, and 3,000 stocks. MeDirect has over 106,000 customers and is expanding globally. Their vision is to provide a convenient way for people to manage and control their finances.

Headquarters
Malta

Use cases
IP Protection,

Reverse engineering prevention

Industry
WealthTech

With Jscrambler since 2022

Challenge

MeDirect was concerned about users accessing their code built with NativeScript. This represented a security risk as their source code could easily be reverse-engineered. MeDirect tried some obfuscation techniques to hide its code but quickly understood that it wasn't enough to ensure its security.

When choosing the best solution to protect their web application, MeDirect prioritized the ease of integration and the effectiveness of JavaScript protection. MeDirect was also worried about impacting the performance of their application - they wanted to guarantee that the new security solution would not have any performance impact.

Solution

MeDirect focused on the benefits of polymorphic JavaScript Obfuscation, which transforms source code into a new version that is extremely hard to understand and reverse engineer while keeping its original functionality. This security layer also includes Jscrambler's Code Hardening feature, which provides up-to-date protection against all reverse-engineering tools and techniques. MeDirect's team conducted several tests to check the threat resistance level and security effectiveness, including Penetration Tests, Vulnerability Scanning, and Code Reviews. This set of mechanisms was used to measure the ability of the code to resist different types of threats, such as code injection, data theft, and unauthorized access.



Top Jscrambler features and capabilities for MeDirect

Polymorphic
JavaScript
obfuscation

Code hardening and
self-defensive capabilities
against tampering attempts

Minimal impact on
performance and file
size optimization

Results

MeDirect's team encountered no issues when implementing Jscrambler. They started with the base mobile template first and integrated Code Integrity in minutes as it slid easily into their CI/CD pipeline. MeDirect had an extensive checklist of critical needs that Jscrambler managed to satisfy by providing in-depth protection of their app source code.

“Jscrambler fulfilled the entire checklist of the application security worries we had.”

Chris Portelli, Chief Technology Officer at MeDirect

MeDirect also registered no impact regarding their application performance. MeDirect's Version 5.0.0 on Android, which had two major introductions, verified a download size improvement of **42%**. The first introduction was Jscrambler's Code Integrity, the second was an upgrade from NativeScript 7 to 8. When checking the actual bundle size difference on the same version, MeDirect's team confirmed that the reduction in the JavaScript file size was around **44%**.

MeDirect's team started with the basic obfuscation template but quickly realized the additional value the solution could provide. They now have complete control over how to deploy the features to ensure in-depth protection of their app source code.

About Jscrambler

Jscrambler is the leader in Client-Side Protection and Compliance. Jscrambler is the first to merge advanced polymorphic JavaScript obfuscation with fine-grained third-party tag protection in a unified Client-Side Protection and Compliance Platform. Jscrambler's integrated solution ensures a robust defense against current and emerging client-side cyber threats, data leaks, misconfigurations, and IP theft, empowering software development and digital teams to securely innovate online with JavaScript. Jscrambler's technology is trusted by the Fortune 500 and thousands of companies globally.

If you want to know more about how Jscrambler can help you prevent client-side attacks, don't hesitate to contact us.
hello@jscrambler.com | +1 650 999 0010