Theia & Jscrambler: **Protecting FinTech React Native Apps**

CASE STUDY

> *As a FinTech, we take security incredibly seriously, and that includes client-side runtime protection.* ***Today, we always ship new products with secure client-side logic as default.***

Dr. James Andrew Butler | Chief Technology Officer at Theia

Overview

About Theia

Theia is an award-winning Hong Kong-based **FinTech company** founded in 2018, developing technologies that empower retail consumers and Small-to-Medium Enterprises to take control of their finances, better manage risk, and seamlessly make payments around the world.

Theia offers corporate Visa cards, global payments solutions, and sophisticated business intelligence tools. Theia Corporate Visa cards are programmable with rules to enforce expense policies and provide peace of mind, whilst empowering employees with perks and privileges. Theia BI visualises every aspect of the state of the company, from high-level overviews of balances, payables, and receivables to deep-dive analytics showing every payment, who it was made by, and why. It integrates data from all of a company's accounting systems, bank accounts, corporate cards in order to build a complete view of the business.

Theia also proudly developed ReadyFX, in collaboration with a leading Airline and major financial institutions. ReadyFX provides real-time, automated cash and electronic currency conversion, banknote authentication, remittance, hedging, and risk management services for global businesses. ReadyFX services are available via the mobile application, and using Smart Kiosks located across Hong Kong, including at HK International Airport.

Summary

CHALLENGES

- Preventing reverse engineering
- Preventing code tampering
- Preventing intellectual property theft
- Obfuscating private API functionality

SOLUTION

Jscrambler Code Integrity:

- Polymorphic JavaScript obfuscation
- Code hardening and runtime protection
- Code locks for additional IP protection
- Self-defensive capabilities to stop tampering and debugging attempts

RESULTS

- One-day deployment
- Seamless integration with React Native and GitLab
- Mitigating tampering and reverse engineering attempts at runtime
- Successfully retaining control over intellectual property

CHALLENGES

When it comes to the financial industry, there is no doubt that security is a prime concern. This is especially true for Theia's case, as the company develops client-side SDK solutions in collaboration with banks.

Their bespoke integrations allow banks to **directly authenticate** with their customers through the Theia application stack. With such high-stake innovations, it is vital that Theia **can protect them from competitors** and any other malicious actors looking to profit off their solutions.

Since Theia is also providing financial trading services through the more recently launched ReadyFx app, the company must address additional risks. One key risk is end-users trying to find ways to take advantage of the system and, for example, obtain better market prices. As such, it is crucial that Theia is able to **restrict the way in which users can interact with their APIs.**

> *There are a lot of important considerations when implementing **business logic that directly touches banking rails.***
>
> **James Hale** | Chief Product Officer

Aware of all the security challenges they needed to face, Theia knew they needed a foolproof solution. The key challenge that the solution needed to address was **protecting their code**, which could potentially be targeted through reverse-engineering and tampering attempts, and protecting their intellectual property, which was white-labeled to third-party clients.

Plus, the required solution also had to be compatible with their cross-platform framework (React Native) used in both of their apps.

Solution

The solution to Theia’s challenges was the cutting-edge technology provided by Jscrambler. And since they needed to ensure **maximum protection of their source code**, they leveraged Jscrambler’s **JavaScript Obfuscation** with powerful **Code Locks** and the **Self-Defending** client-side security layers.

> *We evaluated several solutions for our obfuscation needs but we felt that Jscrambler’s code protection and tamper-proofing technologies were* ***the most advanced available****.*
>
> **Dr. James Andrew Butler** | Chief Technology Officer

Jscrambler’s polymorphic JavaScript Obfuscation applies several different techniques that transform the original source code into a new version that is **extremely hard to understand and reverse-engineer** while still keeping its original functionality. This was extremely important to address Theia’s challenges. Also included in this security layer is Jscrambler’s **Code Hardening** feature, which provides up-to-date protection against all reverse-engineering tools and techniques, making it an extremely resilient solution, unlike any other obfuscation technology available today.

Another key technique to elevate Theia protection against reverse-engineering, tampering, and intellectual property theft attempts was Jscrambler’s **Code Locks**. This feature includes a variety of locks that can be implemented in the source code, namely, domain locks, browser locks, OS locks and date locks. Since Theia supplies white-labeled solutions, gaining control over these applications’ allowed execution environments helped **reduce the attack surface** while bringing **additional business value**.

Solution

> *Code locks enable us to **retain control of our intellectual property when providing white-labeled solutions to third-party clients**, for example by restricting deployment based on domain names and IP addresses.*
>
> **Dr. James Andrew Butler** | Chief Technology Officer

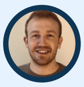
On top of these advanced obfuscation techniques, Theia also benefited from **Jscrambler's Self-Defending**, a security layer that adds integrity checks and other **runtime defenses** that prevent attackers from debugging or tampering with the code. As such, if anyone tries to debug Theia's protected apps at runtime, the apps will immediately break.

Moreover, if an attacker tries to modify the code to dynamically understand its logic at runtime, the application will also break to stop the attack. This advanced runtime protection further reduces the apps' attack surface, **by making it much harder for attackers to understand, plan and automate attacks**.

Results

The solution was successfully delivered with no implementation issues. Thanks to dedicated support from Jscrambler's team of JavaScript and Application Security experts, Theia solved all queries quickly.

> *It was very easy to get started with Jscrambler, thanks to the web interface for managing protections. We were **able to implement** using the PoC demo **in just one day**.*
>
> **James Hale** | Chief Product Officer



Results

Taking advantage of the dedicated integration between Jscrambler and React Native, triggering Jscrambler's code protection during the React Native build process was a seamless experience.

And since Theia is using GitLab to manage its CI/CD pipelines, they also leveraged the integration between Jscrambler and GitLab, which fit perfectly with their tech stack. As a result, every new build of any of Theia's apps is seamlessly protected as part of the CI workflow.

Jscrambler's thorough obfuscation and runtime solution **successfully addressed Theia's concerns** by providing the needed code protection against reverse-engineering and tampering attempts, as well as against potential intellectual property theft attacks.

The assessment from the company's security experts was conclusive: **Jscrambler became a key piece for Theia's defense-in-depth approach**.

> ***Our security specialists were satisfied*** *by the results of using obfuscation and tamper-proof tech in our frontend. It's an* ***important addition to our standard SAST-based approach*** *to securing our platform.*
>
> **James Hale** | Chief Product Officer

Contact Us

If you want to know more about how Jscrambler can help you secure your web and mobile applications, don't hesitate to contact us

hello@jscrambler.com

+1 **650 999 0010**

Jscrambler is the leader in Client-Side Application Security

Recognized in Gartner's **Market Guide for Online Fraud Detection**

and in Gartner's **Market Guide for In-App Protection**

Trusted by the Fortune 500 and major companies in Finance, Broadcasting, Software Development, E-Commerce, and Healthcare.