jscrambler

How Jscrambler helps dotConnect deliver secure banking apps

dotConnect

Jscrambler successfully protects and secures the source code of the banking applications.

About dotConnect

dotConnect is a fintech with the vision to empower financial institutions to provide their clients with a platform that delivers an exceptional digital banking experience. Via cloud-native solution architecture that is built for scale and resilience, dotConnect allows banks to accelerate their digital transformation and automation journeys. This enables these banks to provide a modern, customer-focused digital experience, reduce operational service requirements, and achieve low and predictable operational costs while also guaranteeing flexible integration with new and legacy banking systems using a decoupled approach.

Headquarters
Birmingham, UK

Use cases
Anti-Tampering,
Data Exfiltration Prevention

Industry
Business Services

With Jscrambler since 2019

Challenge

Today, 73% of all consumer interactions with banks are done digitally. And when it comes to banking, security is a prime directive. When asked about the most important attributes when choosing a bank, 82% of consumers say "ensures my transactions are safe/secure". Being aware of how security is one of the key drivers in the ongoing banking digitalization, dotConnect wanted to ensure that they were developing secure banking apps. This meant covering every inch of the attack surface.

> **"When you have a financial product out in the public domain, you're a prime target for attackers."**
> Mohamed Gamil, CEO & Founder of dotConnect

When it comes to web and hybrid mobile banking apps, one key security challenge is protecting the JavaScript code, which can be targeted by reverse-engineering, tampering, and injection attempts. This layer of protection is especially important to reduce exposure to data exfiltration and transaction fraud, which can originate from client-side attack vectors.

Solution

The answer to dotConnect's challenges in terms of source code protection was the cutting-edge technology provided by Jscrambler. Both founders had previously used Jscrambler in a previous solution within the banking sector a few years ago. So, when embarking on this new venture, they re-visited the market to compare vendors and found that Jscrambler was still the market-leading solution in this sector, thus it was the obvious choice. Because dotConnect had to **ensure maximum protection of the JavaScript source code**, its team decided to combine two of Jscrambler's most effective client-side security layers: JavaScript Obfuscation and Self-Defending.

> **"Jscrambler allows for easy configuration as well as a security setup with different levels of evolving protection."**
> Mohamed Gamil, CEO & Founder of dotConnect

Jscrambler's polymorphic JavaScript Obfuscation includes several different techniques that transform the original source code into a new version that is extremely hard to understand and reverse-engineer while keeping its original functionality. Included in this layer is Jscrambler's Code Hardening feature, which provides up-to-date protection against all reverse-engineering tools and techniques.

> **"The protection layer that Jscrambler provides is very, very difficult to interpret, break or bypass."**
> Mohamed Gamil, CEO & Founder of dotConnect

On top of this advanced obfuscation, dotConnect uses Jscrambler 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 the protected banking app at runtime, the app will immediately break. Likewise, if an attacker tries to modify the code to dynamically understand its logic at runtime, the application will break to stop the attack. This **advanced runtime protection** reduces the attack surface to data exfiltration attacks, by making it much harder for attackers to understand how the software works and plan/ automate these attacks.

Top Jscrambler features and capabilities for dotConnect

Polymorphic JavaScript obfuscation | **Self-Defending** | **Code Hardening**

Results

dotConnect successfully applied Jscrambler during the development and delivery of digital banking solutions for several fast-growing banking organizations in the UK. The development team had no issues integrating Jscrambler into the CI build process, thanks to detailed documentation and support from Jscrambler.

> **"The integration into our build pipelines was simple, hence all our apps are protected and deployed with minimal configuration. It's a very comfortable security layer."**
> Azure DevOps Engineer, dotConnect Development Team

Jscrambler directly helps dotConnect increase compliance with the **application security standards outlined by OWASP**. Specifically, the Mobile Top 10 Security Risks guide advises the use of obfuscation technology and runtime protection to prevent reverse engineering and code tampering. Jscrambler also ensures dotConnect satisfies the **PSD2 mobile app security criteria**. Namely, adopting security measures to mitigate risk from compromised mobile devices and cloning countermeasures (replication protection).

One of the key requirements of dotConnect was ensuring that they would pass their clients' and their own strict penetration testing rounds. Jscrambler helped them achieve that by passing 5 different penetration testing rounds with excellent feedback.

> **"Since integrating Jscrambler, we have consistently passed strict penetration testing and delivered secure mobile banking apps to our clients."**
> Mohamed Gamil, CEO & Founder of dotConnect

> **"Jscrambler is a key component that bolsters our security layer, thus assuring us at dotConnect that we deliver secure and trusted solutions to our clients and their customers."**
> Saj Shahid, CXO & Founder of dotConnect

For dotConnect, the road ahead looks extremely promising. With customer satisfaction at an all-time high, the company is growing fast and onboarding new banking clients, always assured that Jscrambler will provide top-notch client-side protection.

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