jscrambler / CCG CAA CLUB GROUP

CAA Group Protects Millions of Motorists with Jscrambler Application Shielding

CASE STUDY

“Protecting our JavaScript was a requirement from day one in order to safeguard proprietary system designs that in turn protect the lives of millions of motorists.”

Jay Woo
President & CEO at CAA Group

Overview

About CAA Group

Founded in 1903, the Canadian Automobile Association (CAA) Group's mission is to protect motorists on Canada's vast network of roadways and highways.
Protecting millions of motorists, the emergency rescue teams receive between 3,200 to 5,500 emergency rescue calls per day.

Technology To The Rescue

Due to the finite number of resources, the organization developed **proprietary machine-learning algorithms** that enable the rescue teams to proactively manage their resources by pre-positioning rescue vehicles at the right location at the right time. The source code that controls these machine-learning algorithms is extremely sensitive, hence the need for extensive protection.

Summary

CHALLENGES

- Prevent reverse engineering
- Prevent code tampering
- Protect proprietary algorithms
- Prevent disruption of emergency rescues through malicious code alteration

SOLUTION

Jscrambler Code Integrity:

- Polymorphic JavaScript obfuscation
- Code hardening
- Self-defensive capabilities to stop reverse engineering and tampering attempts

RESULTS

- Smooth implementation
- 100% fit with tech stack and development/build pipelines
- Mitigating tampering and reverse engineering attempts at runtime
- Successfully retaining control over intellectual property
- Zero security breaches since the implementation

CHALLENGES

Over the last decade, we have witnessed a fundamental shift in how **technology enables organizations** to provide better services with decreased time to market.

Web technologies have been one of the main drivers behind this push. The rapid growth of the **JavaScript** ecosystem has allowed organizations to **quickly develop web, mobile and desktop apps** with a lower total investment.

With over a century's worth of service to the Canadian automotive community, CAA Group has established itself as one of the most trusted brands in Canada. Understanding the value of technology, the organization is using a **web-based tech stack** (JavaScript, Node.js) to develop and maintain an application that **tracks and monitors the location of all breakdowns**. This information is used by dispatchers to deploy roadside assistance in the shortest possible timeframe.

Today, **trust is interconnected with security**, especially in high-stakes scenarios such as providing emergency roadside service that **saves lives**.

To maximize the organization's ability to respond to stranded motorists, CAA Group developed **proprietary machine-learning algorithms**. These are crucial to ensure that rescue vehicles are properly positioned to assist anyone in need. Protecting these algorithms is key to ensuring that the organization continues to exceed customer expectations.

Finally, there's the significant risk of **code tampering**—CAA Group needed to ensure that malicious actors couldn't modify the source code. Failing to do so would compromise the organization's ability to respond to assistance requests and ultimately **affect how many lives could be saved**.

*"If the code was left unprotected, it could be **maliciously altered** and directly **affect the decisions** made by rescue dispatchers and controllers."*

Jay Woo
President & CEO at CAA Group

Solution

While searching for a security solution to meet the organization's specific needs, CAA Group came across several options. However, most current JavaScript obfuscation/ protection solutions (both free and commercial) fail to provide the multi-layered level of security required for a defense-in-depth strategy. During this prospecting stage, CAA Group **identified Jscrambler as the clear leader** in this space and as the right choice to protect its code.

The organization's main challenges were reducing the risk of IP theft and malicious code modification, which meant being able to **prevent any type of reverse engineering and tampering attempts**.

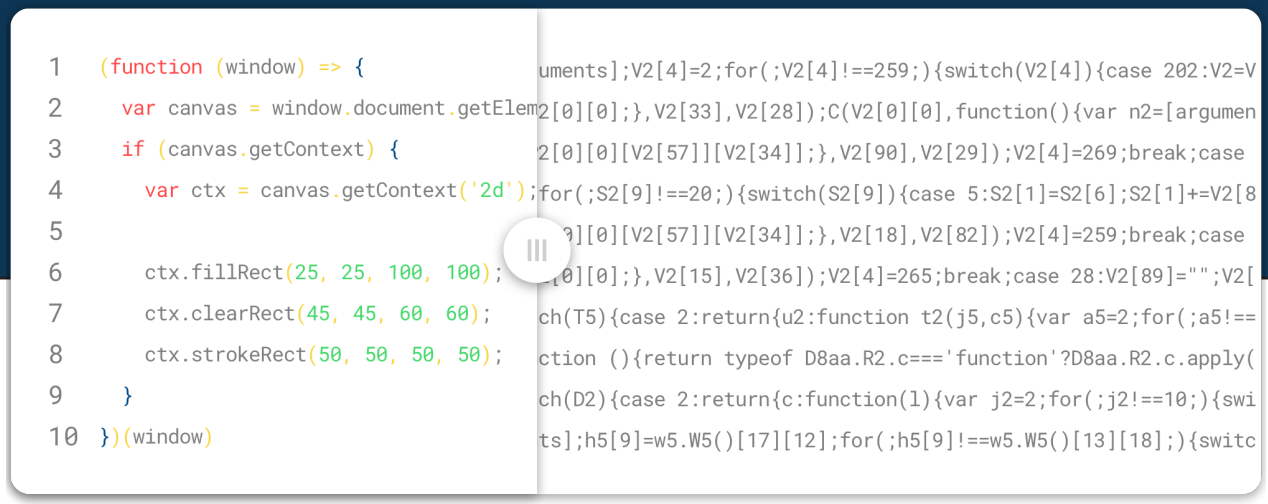
> *"We evaluated 3 other solutions and **Jscrambler was the most effective.**"*

Jay Woo
President & CEO at CAA Group

The solution to these challenges was a combination of two of Jscrambler's main protective layers: **JavaScript Obfuscation** and **Runtime Protection**.

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.

Solution



```
1  (function (window) => {
2    var canvas = window.document.getElem
3    if (canvas.getContext) {
4      var ctx = canvas.getContext('2d');
5
6      ctx.fillRect(25, 25, 100, 100);
7      ctx.clearRect(45, 45, 60, 60);
8      ctx.strokeRect(50, 50, 50, 50);
9    }
10 })(window)
```

```
uments];V2[4]=2;for(;V2[4]!==259;){switch(V2[4]){case 202:V2=V
2[0][0];},V2[33],V2[28]);C(V2[0][0],function(){var n2=[argumen
2[0][0][V2[57]][V2[34]];},V2[90],V2[29]);V2[4]=269;break;case
for(;S2[9]!==20;){switch(S2[9]){case 5:S2[1]=S2[6];S2[1]+=V2[8
9][0][V2[57]][V2[34]];},V2[18],V2[82]);V2[4]=259;break;case
[0][0];},V2[15],V2[36]);V2[4]=265;break;case 28:V2[89]="";V2[
ch(T5){case 2:return{u2:function t2(j5,c5){var a5=2;for(;a5!==
ction (){return typeof D8aa.R2.c==='function'?D8aa.R2.c.apply(
ch(D2){case 2:return{c:function(l){var j2=2;for(;j2!==10;){swi
ts];h5[9]=w5.W5()[17][12];for(;h5[9]!==w5.W5()[13][18];){switc
```

Original **Obfuscated**

> *"In Jscrambler we found **turn-key source code protection** with command-line and web interface options in addition to code obfuscation that **does not introduce performance degradation** in production."*

Jay Woo
President & CEO at CAA Group

While obfuscation provides a good level of protection against IP theft and reverse engineering, CAA Group wanted to go a step further and greatly elevate the cost for attackers targeting its proprietary and critical algorithms.

As such, they implemented Jscrambler **Self-Defending**, a runtime protection layer that adds **integrity checks** and other defenses to **prevent source code debugging and tampering**. If attackers try to debug the protected source code or experiment with it at runtime (dynamic analysis), the application immediately **triggers a security response** to thwart the attack. These responses are **highly customizable** and include breaking the app, redirecting the attacker, clearing the cookies, sending a security alert to CAA Group's security team, and calling a custom function.

With these two protective layers in place, CAA Group greatly **reduced the attack surface of its application** to any attackers looking to tamper with critical algorithms or any competitors wanting to access or retrieve proprietary logic.

> *"Kudos to Jscrambler for making source code security so **efficient**."*

Jay Woo
President & CEO at CAA Group

Results

Given the tech stack and processes already in place, CAA Group needed to ensure that they could implement a code protection solution that fit these processes and didn't result in any overhead.

This is precisely what the organization achieved with Jscrambler. The implementation happened with no hiccups, thanks to **extensive documentation** and **dedicated support** from Jscrambler's team of JavaScript and Application Security experts.

> *"Both the email and chat support channels were **outstanding**. Responses were consistently addressed within a few minutes."*

Jay Woo
President & CEO at CAA Group

Using both the Jscrambler web app and CLI, and thanks to **dedicated integrations with all the main JavaScript frameworks**, CAA Group successfully integrated Jscrambler's source code protection into the build process of the application.

Results

*"We saw **100% alignment** with our tech stack and our development/build pipelines."*

Jay Woo
President & CEO at CAA Group

This smooth implementation ensured that all of CAA Group's security challenges were addressed quickly and effectively. The layered security approach of **JavaScript Obfuscation** and **Runtime Protection** is successfully preventing static and dynamic code analysis, as well as any attacks that target the source code of the protected application.

And when it comes to putting this into numbers, the feedback from CAA Group's security team leaves no doubts:

*"Jscrambler has been **100% effective** and we have not had any security breach within the source code because of Jscrambler."*

Looking at the future, and with expectations that CAA Group will keep growing and developing cutting-edge technologies, the protection from **Jscrambler will support the organization in its mission** to rescue several millions of motorists on Canadian roads.

*"We have used Jscrambler since 2017 and foresee using this system for a long time into the future because Jscrambler continually releases **new security capabilities** that stay ahead of new security threats."*

Jay Woo
President & CEO at CAA Group

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**

Gartner®

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.