jscrambler

Bionano increases compliance with regulations using Jscrambler

bionano™

Jscrambler provided Bionano with the most resilient JavaScript protection, satisfied the needs from regulation requirements for code protection, and protected the intellectual property of the company's technology.

About Bionano

Bionano is a biotechnology company that specializes in genome mapping and analysis and can enable researchers and clinicians to reveal answers to challenging questions in biology and medicine. Bionano's mission is to transform the way the world sees the genome through optical genome mapping (OGM) solutions, diagnostic services, and software. Bionano also offers an industry-leading, platform-agnostic genome analysis software solution, and nucleic acid extraction and purification solutions using proprietary isotachophoresis (ITP) technology.

Headquarters
San Diego, USA

Use cases
Compliance with regulations, IP theft prevention

Industry
Biotechnology, Health Diagnostics

With Jscrambler since 2019

Challenge

Each time Bionano engages in an enterprise-level clinical environment, they are subjected to a rigorous security audit. By interacting with many security organizations globally, they gained an in-depth understanding of what these security organizations expected.

Bionano chose Node.js as their visualization platform as it facilitated reaching the widest audience of users (macOS, PC, and Linux). It also provided an extensive array of visualization tools such as D3js, ThreeJS, and ChartJS that allow the creation of rich interactive genomic maps for customers to explore. Bionano software is free to encourage the use of Saphyr-generated data. Anyone can download and start their own Bionano Access Server. Bionano needed a way to protect their downloaded client and server-side JavaScript logic to satisfy multiple security regulations.

Solution

The Bionano system itself is designed not to hold protected private information (PPI), so the company did not face significant liability to be concerned with. However, as an extra precaution and to be as compliant as possible, the company understood the need for JavaScript code protection.

In search of the optimal solution, Bionano tested some JavaScript obfuscation solutions but found out that these could be easily reversed or debugged. Jscrambler was the only solution that passed all their tests and which they were not able to reverse.

“Jscrambler was the only product we found that could not be cracked.”

Scott Way, Director of High-Performance Computing and Genome Visualization at Bionano

This implementation of Jscrambler was greatly derived from the need to comply with several different regulatory requirements. In the specific case of Bionano, the regulations that apply to their clinical customers vary depending on their local principalities. Some regulations like ISO 27001 and 27002 specifically require source code protections while others have more general data protection and/or encryption requirements.

Jscrambler does not solve all of Bionano’s security concerns, but it provides what the company needs to protect the source code enough to satisfy all regulations in that regard. Then, there’s also the matter of protecting intellectual property. Bionano’s system provides comprehensive genomic variation data for review.

“We needed our Node.js application protected to satisfy multiple data protection regulations in customer clinical environments. Jscrambler did that for us and it was easy to incorporate into our tech landscape.”

Scott Way, Director of High-Performance Computing and Genome Visualization at Bionano

Their software does this in an elegant way that may seem straightforward—but, under the covers, a lot of sophisticated work has been done. Jscrambler goes beyond data protection to protect the company’s investment in its technology.

Top Jscrambler features and capabilities for Bionano

- Resilient JavaScript obfuscation
- Built-in protection against reverse-engineering tools
- Anti-tampering and anti-debugging capabilities

Results

Thanks to the source code protection provided by Jscrambler, Bionano now obfuscates its code and is capable of preventing debugging. This allows them to satisfy the security concerns of their clinical customers and continue using the platform that gave them the best value.

> **"Beyond providing data protections, Jscrambler protects the investment made in our technology. This also makes our clinical customers more comfortable when installing our system since they are ingrained with data protection policies."**
>
> 
>
> Scott Way, Director of High-Performance Computing and Genome Visualization at Bionano

As for the implementation of Jscrambler itself, Bionano simply had to add the Jscrambler product to their DevOps scripts and as a result, Jscrambler was able to deploy obfuscated code internally and in their installation files within a day.

The company uses Ansible to deploy software internally and to automate installation builds and was also able to incorporate the Jscrambler CLI into their automation scripts easily. And even though their product is fairly complex and probably larger than most Node.js projects, Bionano only ran into some file count limitations but was able to solve them quickly with Jscrambler's support.

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