feroot gusto

Case Study

Feroot Security Inspector Customer Success Story

Securing the Client Side to Proactively Manage Cyber Risk

Who

Gusto

Industry

Computer Software

Number of Employees

2000+

The Customer

Gusto's mission is to create a world where work empowers a better life. By making the most complicated business tasks simple and personal, Gusto is reimagining payroll, benefits, and HR for modern companies. Gusto serves over 200,000 companies nationwide and has offices in San Francisco, New York City, Denver, and Canada.

The Challenge

To Gusto, keeping customer data secure is paramount. From its well-defined corporate security strategy and dedicated public webpage, Gusto views itself as a data custodian that is entrusted with, rather than entitled to, customer data.

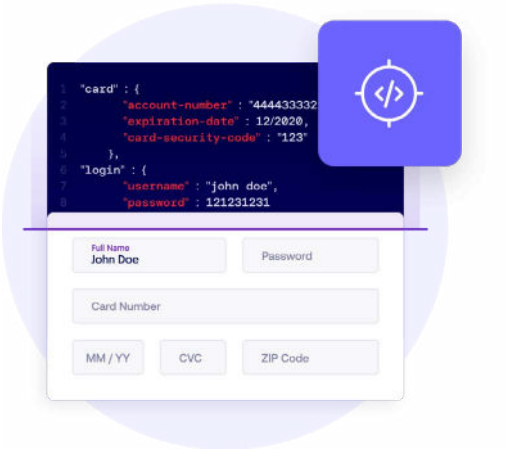
Ever since its inception, Gusto has continuously improved and enhanced its ability to detect and defend the business and its customers from cyber threats. Being a cloud-first organization with an ecosystem of web applications and web pages to protect, Frederick "Flee" Lee, Gusto's Chief Security Officer, and his team expanded their security strategy beyond traditional server-side security practices to enhance client-side security practices.

> "A day doesn't go by that you don't hear about a new JavaScript-based attack on a company's website or web application. We're seeing attackers pivoting from traditional server-side attacks to client-side attacks. To protect our business from server-side threats, we needed to enhance our client-side security capabilities to stay ahead of the threat."
>
> - Frederick "Flee" Lee, Chief Security Officer

With e-skimming, formjacking, JavaScript injection, and Magecart-like attacks on the rise, Flee and his team learned that they needed a new way to gain even fuller visibility of their cyber risk across their websites and web applications. They needed to have a technology that could provide them with a full inventory of all first- and third-party scripts, an even clearer understanding of vulnerabilities impacting the client-side, and immediate alerts to cross-border data transfer and potential data exfiltration.

The Goal

Flee empowered Karlotcha Hoa, Gusto Security Engineer, to determine how to enhance their **visibility into all of the scripts that make up their front-end web applications.** Karlotcha outlined what capabilities a client-side security technology needed to have, in order for them to be able to successfully protect their client-side JavaScript web applications. They included the ability to:



- Automatically generate end-to-end visibility of all front-end assets and the code used to build them, in order to manage JavaScript inventory and version control.
- Prioritize client-side errors and vulnerabilities based on severity and exploitability.
- Create a workflow based on meaningful and actionable security insights between application security and development teams to streamline front-end security operations.
- Conduct geo-based scans to ensure digital customer journeys adhere to regional compliance and privacy regulations.

The Choice

Karlotcha evaluated Feroot Security Inspector and ran an in-depth proof of concept (POC). The goal of the POC was to use Inspector to operationalize their client-side security capabilities, determine if the technology could uncover known unknown threats, and become the 'glue' that united the security and the front-end product development team for successful collaboration.

The Goals for Feroot Security Inspector:

- Identify and manage their web asset and JavaScript code inventory to reveal their client-side attack surface.
- Ensure that their web applications are assembled in the user browser as expected.
- Gain visibility by continuously testing and reporting on client-side web assets, to detect and remove threats and vulnerabilities (such as JavaScript injection attacks).
- Align the application security and front-end product development teams.

The Outcomes

After a thorough evaluation of Inspector's features and functionality, Karlotcha and Flee chose Feroot Inspector for Gusto to secure their client-side web applications. **Inspector was quickly provisioned to gain end-to-end visibility of the make up of their web applications, detect JavaScript vulnerabilities and threats, automate client-side security tasks, and integrate Feroot with existing security technologies and processes.** Inspector enabled Gusto to:

- Gain a greater overview of their client-side attack surface, by building an inventory of all first- and third-party scripts used to build their web applications.
- Reduce cyber risk by enhancing front-end threat detection and mitigation capabilities.
- Uncover unauthorized trackers on web applications and remove them to ensure customer security.
- Enact client-side security testing processes to maintain continuous web application security.
- Integrate client-side security workflows to operationalize client-side security, thereby reducing application security to front-end development issue resolution latency.
- Complement data privacy and data security projects with client-side data transfer alerting and protection.

Karlotcha Hoa
Security Engineer

"We needed greater visibility over our web applications to ensure they were loading the way we needed and expected them to in the users' browser. **With Feroot we have the ability to continuously scan our websites and make repairs as necessary.**

The best part of Feroot Inspector is that it is not intrusive. It's a plug and play solution that is easy to maintain. We use Inspector to look at our web apps, and it tells us everything we need to know to keep them secure. It's easy to use, and integrating it with our technology stack and workflows was quick and seamless."

Frederick "Flee" Lee
Chief Security Officer

"Now that we have Inspector integrated into our security operations, we are happier with our front-end security posture. We are even more confident that we are able to find issues in our web applications quickly and fix them. We believe we have a solid solution in place to keep our eyes on our front end.

In my role, I want to reduce as much cyber risk as possible. We needed a better way to find client-side threats and address them on our front-end. **With Inspector we have enhanced our ability to manage cyber risk and keep our customers safe at point of interaction."**

feroot

About Feroot
Feroot Security believes that customers should be able to do business securely with any company online, without risk or compromise. Feroot secures client-side web applications so businesses can deliver flawless digital user experiences to their customers. Leading brands trust Feroot to protect their client-side attack surface. Visit www.feroot.com.

Contact Us
sales@feroot.com | www.feroot.com