feroot quickbase

Case Study

Feroot Security Inspector Customer Success Story

Driving Customer Trust by Ensuring Security of the Client-side Digital Ecosystem

Who

Quickbase

Industry

Computer Software

Security Team Size

5

Number of Employees

550+

Customer Since

2020

The Customer

Quickbase is a computer software company that provides a no-code operational agility platform to its customers. The platform enables organizations to improve their operations through real time insights and automation across complex processes and disparate systems. Their goal is to help companies be more responsive to their customers by providing real-time visibility into workflows and operations.

The Challenge

The Quickbase security team prides itself in staying ahead of cyber threats and government regulations that might impact their customers. When the European Union started to discuss the General Data Privacy Regulations (GDPR), Michael Lemire, Quickbase Chief Security & Compliance Officer, realized that he and his team had a gap in their security program.

> **"We needed to wrap our arms around client-side security, both in our own code and the 3rd party scripts we load into our users' browsers when they visit our web properties.** We also needed to ensure we were maintaining compliance with increasingly stringent privacy regulations."
>
> - Michael Lemire, Chief Security & Compliance Officer.

He jumped to action to learn as much about client-side security as he could, and what he and his team could do to stay ahead of cyberthreats harmful to their customers and business. With third-party scripts leading to security breaches such as e-skimming, formjacking, and Magecart-like attacks increasingly in the news, Michael and his team decided that they needed to include client-side security as part of their security program.

The team needed clearer visibility across their company's marketing website and web services. Michael and his team began searching for a solution that could discover all of Quickbase's web assets and inventory scripts in use and provide the team with insights to quickly take corrective action if there was a security vulnerability or unauthorized script change.

The Goal

Michael and his team outlined what a client-side security program might entail and what they needed to accomplish for it to be effective:

Security Program Capabilities

- **Align and comply** with current and upcoming privacy regulations (e.g. GDPR).
- **Understand what data was being captured** from user input across all web assets.
- **Generate and continuously enumerate a full inventory** of web pages, tracking tools, advertising tools, cookies, scripts, and other critical information required to secure Quickbase's digital ecosystem.
- **Develop reports** on the full breadth of what Quickbase loads into user browsers on a continuous basis.

Program Execution & Team Capabilities

- **Build a strong relationship** with the marketing team to follow client-side security best practices and respond to client-side threats.
- **Understand how the marketing team uses web assets** to bring in new customers and serve existing clients.
- **Make sure the marketing team has the correct security protocols** in place to remove unnecessary scripts and protect customer information.
- **Establish client-side security** workflows and governance.

The Choice

Mike and Zach R., a Quickbase Security Engineer, evaluated the steps they would need to take to inventory and continuously scan their client-side assets. It quickly became apparent that they needed a technology that would automate the tedious and continuous efforts needed to stay abreast of third- or fourth-party code changes. Michael and Zach acquired Feroot Inspector because of the product's ability to:

- **Identify their web asset inventory** and reveal their client-side attack surface.
- **Audit and report** on the effectiveness of their security controls.
- **Continuously test their user-side web assets.**
- **Exceed privacy, risk, and compliance goals.**
- **Help mitigate client-side security issues.**

The Process

Zach took on the challenge to build Quickbase's client-side security program using Feroot Inspector as the platform for it. In close collaboration with Greg B., Manager of Software Engineering, Zach successfully executed the program to protect Quickbase's most valuable assets—it's customers. Zach and Greg followed a two-phase, client-side, security program implementation plan:

Phase 1: Deploy Inspector to Inventory and Clean-up Quickbase's Digital Ecosystem

- **Develop an end-to-end inventory** all website and web applications assets.
- **Enumerate all marketing trackers**, advertising tools, scripts, forms, and more.
- **Work with marketing** to clean up zombie scripts, unused scripts, remove unnecessary trackers, remove unused web pages, and reduce Quickbase's client-side attack surface.
- **Ensure marketing and security** are aware of what they are loading onto customer browsers and what digital assets

Phase 2: Establish Governance and Accountability

- **Assign a dedicated marketing operations person** to utilize Feroot Inspector to keep track of and continuously clean digital assets.
- **Develop and, if necessary, execute on an incident response** plan to quickly fix client-side security issues.
- **Enact processes and procedures** to habitually use Feroot Inspector to continuously scan Quickbase's digital assets, act on alerts, investigate alerts, and respond to issues effectively.

The Outcomes

As a result of Zach and Greg's fantastic teamwork, Quickbase now has a solid client-side security program in place. By continuously scanning their digital ecosystem, the Quickbase team has been able to:

- **Clean-up their digital ecosystem** by removing zombie scripts and unused web assets.
- **Have full visibility** across web assets.
- **Keep track of old pages and content** not utilized over time.
- **Quickly respond to client-side security threats** to eliminate cyber risk.
- **Deploy repeatable and automated client-side security workflows** using their Jira integration.
- **Have a constant overview** of their client-side attack surface.
- **Stay out of GDPR crosshairs** by complying with EU privacy regulations.
- **Collaborate effectively with the marketing team** using Inspector as their core tool.
- **Report on client-side governance**, risk and compliance.
- **Keep customer data safe** from client-side breaches.

"The beauty of Feroot Inspector is that it covers a clear and present attack vector. Over 5% of attacks come via supply chain and third-party scripts, and most security teams are blind to these with their current security tools. This particular attack vector is becoming more and more prominent. We're seeing more real-world client-side attacks coming. So, from a security perspective, it's in the news and it's real. From the privacy perspective, everyone is aware how important it is to align with privacy best practices and regulations.

We're on a mission to be the trusted low-code vendor in the industry. Our number one priority is to establish trust with our customers and ensure the security of our entire digital ecosystem. Feroot Security Inspector has provided us with an automated technology to uncover our client-side attack surface and protect it in real-time."

Michael Lemire
Chief Security & Compliance Officer

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