Relativity | Calder7 Spotlight

Building Trust (and Secure Software) at Relativity

Natalya Krecker

Contents

Executive Summary

The decision to place your private data in Relativity should not be made on a leap of faith. It should be sealed with a contract of trust. When it comes to the privacy of sensitive information, we know trust isn't given; it's earned.

To gain your trust, we're giving you an insider's look at how we secure our data at Relativity— specifically through our Secure Software Development Lifecycle.

How exactly do we run this lifecycle? The task doesn't lie solely with our army of engineers. There's another department working behind the scenes, focused on maximizing the highest standards of security and providing guidance and expertise to minimize risk and prevent vulnerabilities.

In this article, we'll discuss how Calder7's application security team assists Relativity's engineering department in building not only secure software, but our customers' trust.

Application Security

Our application security team (App-Sec) assists Relativity's engineers in three crucial areas: **Guidance**, **Verification**, and **Threat Modeling**. In the next few paragraphs, we'll explore each process in depth.

Guidance

First and foremost, App-Sec provides security guidance to our engineers and continually verifies that this guidance is being followed. We educate Relativity's engineering teams on security best practices for developers, provide standard security requirements for development projects, and are always available to answer their questions.

To help deliver this guidance, we automatically enroll all team members working in departments that support RelativityOne into our **Security Champion Program**. Product managers, quality assurance (QA) engineers, and even executive assistants are enrolled. This is to ensure everyone can internalize and support our security processes. Other enrolled departments include: engineering, internal technology, service delivery, product management, and security.

The Security Champion Program was meticulously designed to extend the reach of our App-Sec team by deputizing engineers with the knowledge and authority to make security-related decisions. The first level of the program includes a curriculum that teaches crucial security processes. For example, part of the training teaches engineers the policies for accessing data in RelativityOne, which state that they need the RelativityOne customer's explicit permission and approval to address security concerns.

The final level of our Security Champion Program is focused on providing teams security-related training that aligns to their current role. For example, Relativity's QA engineers use exploratory testing to identify functional defects and learn Calder7's threat modeling process to define and address risks in any given system. By the end of the program, QA engineers know how to use those threat modeling techniques during the exploratory testing phase of the software development cycle.

Another source of guidance provided by App-Sec is the **Secure by Design** initiative. This provides engineers with security requirements before software development begins and throughout the project planning phase. While we find that most teams plan to implement many requirements from their Champions knowledge, the Secure by Design initiative provides them with extra insurance.

The requirements originate from a variety of sources including our ISO 27001 and FedRAMP standard operating procedures, as well as the best practices expected by our architect and network teams. Examples of these requirements include static analysis tooling onboarding and inputting appropriate security events into Splunk (a logging and monitoring platform). Requirements are treated as a checklist, and completed requirements are verified as part of our release approval process.

Finally, we keep an open line of communication between App-Sec and our engineers. For example, if an engineer is unclear on any aspect of our Secure by Design process or has additional security questions, they can simply contact our team for additional guidance.

Verification

Another area where App-Sec ensures the security of our software is through the verification process. This is performed primarily via code reviews, participating in the Change Approval Board (CAB), and supporting external penetration testing efforts.

App-Sec performs a **code review** as part of the Secure by Design process or whenever engineers identify a need related to specific security requirements. Examples of these requirements include authentication, authorization, cryptography, or the introduction of new front-end components. For easy access, we host a detailed description of each subject and requirement on an internal documentation page available to all of our engineers.

The **Change Approval Board** is a group of Relativians who assess, authorize, and schedule changes as part of our change control process. By participating in the CAB, App-Sec has a voice in the release process and can ensure Relativity's change approval process is secure.

App-Sec also engages external vendors to perform **penetration testing** on our web application and Azure infrastructure for RelativityOne. Penetration tests are used to test the security of a system, software, network, or facility. By conducting these tests regularly, we can assess how well our defenses hold up to an attack.

Threat Modeling

Finally, to bridge the gap between guidance and verification, App-Sec continuously performs **threat modeling** sessions on Relativity's highest-risk applications. Threat modeling is the process of defining the risks in any given system so those risks can be properly addressed.

To prioritize an application for threat modeling, **all applications are scored based on risk** and implementation details.

Risk Factors:

- Audience
- Data the application has access to
- Data the application will display to the customer

Implementation Details:

- Authentication
- Authorization
- Cryptography

If needed, the findings of these sessions may turn into **vulnerability investigations**.

Vulnerability investigations are born from threat modeling sessions and other additional sources. Each vulnerability investigation is scored based on the worst-case scenario, assuming the threat is real, and prioritized for investigation. The investigation may result in filing that vulnerability and assigning it to the responsible team.

What Can We Secure Next?

This report is merely a broad overview of our Secure Software Development Lifecycle. We hope you now have a better understanding of how we secure our software. We wouldn't expect to earn your trust, however, by simply laying out our current platforms. Security is a changing field that's constantly adapting to an evolving landscape, so we want to stress that App-Sec is continually innovating new ideas to make our software even more secure.

Soon, AppSec will be taking its security requirements public so Relativity's third-party developers can follow the same guidance as Relativity's developers.

Ultimately, we want to earn the opportunity to hold your data, and you can trust that we'll do everything at our disposal to keep it secure.

About the Author

Natalya Krecker joined Relativity in 2013 as an engineer on the engineering platform team. After probing the CISO for advice on how to learn more about security, she was asked to join the team. In her current role as manager of security engineering, she leads the Calder7 application security team (AppSec). She assists Relativity's engineers in three crucial areas: guidance, verification, and threat modeling. Natalya holds a Masters in Computer Science from DePaul University in addition to CISSP and CCSP certifications. Fun fact: Natalya has made a career of breaking things.

About Relativity Trust

Thousands of organizations trust Relativity with their most sensitive data. We take every precaution to protect that data in a secure, performant system—as dependable as flipping a switch or turning on the tap.

Our internal security team, Calder7, includes cybersecurity, product security, compliance, and risk specialists with a simple mission: anticipate threats and stay ahead of the adversaries. Learn more about Calder7.

Relativity®

231 South LaSalle Street | 8th Floor
Chicago, Illinois 60604
+1 (312) 263-1177 | relativity.com