SYNOPSYS®

FINRA Improves Development Efficiencies, and Tightens Up Open Source Security

Company Overview

FINRA is not-for-profit organization dedicated to investor protection and market integrity. It regulates one critical part of the securities industry—brokerage firms doing business with the public in the United States. FINRA, overseen by the SEC, writes rules, examines for, and enforces compliance with FINRA rules and federal securities laws, registers broker-dealer personnel and offers them education and training, and informs the investing public. FINRA provides surveillance and other regulatory services for equities and options markets, as well as trade reporting and other industry utilities.

FINRA, the Financial Industry Regulatory Authority, is charged with ensuring fair financial markets for American investors. The nongovernmental regulator's mission is to safeguard the investing public against fraud and bad practices, and it pursues this mission by writing and enforcing regulations for all U.S. brokers and brokerage firms.

Every day, the regulator processes approximately 6 terabytes of data and information on a staggering 20 billion financial transactions to build a holistic picture of U.S. market trading. At any given time, FINRA's 500 software developers have between 100 and 130 apps under management—which translates to 100,000 builds, Kostas Gaitanos, senior director of development services at FINRA, explains.

Given these realities, it's no surprise that managing developers' use of open source code—and controlling the security implications of its use—has become more and more challenging for FINRA.

Homegrown solution increases administrative burdens

But as time went on, managing the homegrown workflow became almost a full-time job for FINRA lead systems engineer Marcela Carbo. "The reporting became an issue," Carbo says. "We realized it wasn't scalable, and we couldn't do effective tracking."

An investigation of other options led the regulator to a commercial database solution that enabled tracking of open source code during different stages of the workflow. This allowed FINRA to understand what code was coming in, but not where specific components were being used. The approval process also left much to be desired, Carbo explains.

"Our approval process boiled down to: as long as the dev team opened a ticket, then it moved forward," she says. "We had repos created for 'awaiting approval' 'approved,' etc... thus mapping the various repos to key workflow stages. As long as the dev team submitted a ticket, we felt we were following the approval policy. But we lacked a solution for what to do when components were rejected. We didn't have a complete picture of who was using what and where and how."

"When we built our business case for bringing in Black Duck, our internal information security group was a co-sponsor of the effort. This group now has a significantly easier way to determine which artifacts and versions are affected by any security vulnerability and which applications are impacted as a result. This capability did not exist before, so this is huge."

—Kostas Gaitanos, senior director of development services, FINRA

Gaitanos adds, "In this world we live in, you pick one open source artifact, and it comes with many dependencies. If you had 30 or more dependencies, you'd end up with the task of creating and managing 30 or more tickets. This increased the administrative burden on developers," he says. "Given the volume we were dealing with, we had to change the way we looked at this problem. We somehow had to shift our focus from reviewing 100% of artifacts introduced to our environment, to an exception-based review process. This way the vast majority of artifacts get vetted automatically by the process and only a select few get flagged, based on predefined conditions, to be reviewed by both our legal department and by technologists."

A new approach: Automating open source code management with Black Duck

To address these issues, FINRA turned to Artifactory Pro and Black Duck. Our OSS Logistics solutions enabled the organization to automate the management of open source code. It soon became apparent that this approach vastly improved scalability and saved time and effort through the elimination of manual tracking. Our solution also offered significantly improved visibility into code use, thanks to the creation of a continually updated open source bill of materials (BoM).

"Under the old system, everything had to be tracked up front as part of the process. Now, we track open source code usage on an exception basis only, because of the BoM," Gaitanos explains. "A human only gets involved in the event of an exception. This saves a lot of time." Carbo adds, "For us, the main thing is to get out of development's way. The old system really slowed down development, but with Black Duck, they don't have to worry about filling out spreadsheets. Plus the legal team would have to get involved to vet each usage, and they don't have to do this now. Changing a version doesn't prompt all this work."

Since the Black Duck solution was implemented, FINRA is saving three "person days" of work per app on average, Gaitanos says. The regulator's legal department has also seen its open source-related workload reduced by 75%, and it was able to abolish a technology review team that vetted open source license compliance under the old system.

Redesigning apps with volume in mind

Since FINRA's charter also includes providing training to brokers and brokerage houses, along with providing brokers with permits to trade in North American markets, much of the regulator's application development emphasis is on this type of high-stakes, high-volume work. This means that improving efficiencies in software development is extremely important to helping FINRA carry out its mission.

"When you have this kind of volume to process through, you end up redesigning apps with volume in mind," Gaitanos says. "Efficiency is critical. We've seen a huge savings not only from a human interaction and effort perspective, but in the way folks behave towards the process. The more hurdles you put in front of developers, the more likely it is they will work around you. We're taking hurdles out of their path and making things easier for them."

Going forward, Carbo says, the FINRA team expects to further simplify workflows, to make Black Duck even more user-friendly.

Open source security: Part of the Black Duck business case

In addition to streamlining development, FINRA has also seen an immediate impact on open source security—which it views as a great validation for Black Duck.

"When we built our business case for bringing in Black Duck, our internal information security group was a co-sponsor of the effort," Gaitanos says. "This group now has a significantly easier way to determine which artifacts and versions are affected by any security vulnerability and which applications are impacted as a result. This capability did not exist before, so this is huge."

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior.

For more information about the Synopsys Software Integrity Group, visit us online at www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com

©2019 Synopsys, Inc. All rights reserved. Synopsys is a trademark of Synopsys, Inc. in the United States and other countries. A list of Synopsys trademarks is available at www.synopsys.com/copyright.html. All other names mentioned herein are trademarks or registered trademarks of their respective owners. October 2019