SYNOPSYS®

Blue Yonder:

Extending a Secure SDLC to Remediate Open Source Security Issues

BlueYonder

Company Overview

With over $1 billion in annual revenue, Blue Yonder has been the world's leading supply chain provider for the past 30 years. Blue Yonder enables companies to improve their ability to plan, execute, and deliver by better predicting and shaping demand, fulfilling more intelligently and quickly, and improving customer experiences and loyalty. More than 4,000 global customers use Blue Yonder's unmatched end-to-end solutions portfolio to shorten their supply chains, increase speed of execution, and profitably deliver to their customers.

The challenge: If a vulnerability can't be found, it can't be patched

As with many organizations in the business of building software, Blue Yonder's portfolio of 100+ applications contains a mix of custom-built codebases and commercial and open source components. Analysts such as Forrester and Gartner note that over 90% of IT organizations use open source software for mission-critical workloads and that open source components often compose up to 90% of some applications.

While the number of vulnerabilities in open source is small compared to proprietary software, over 7,000 open source vulnerabilities were discovered in 2018 alone. Over 50,000 have emerged over the past two decades. Of the codebases reviewed by the Synopsys Black Duck Audit Services team in 2018, 60% contained at least one open source vulnerability. Over 40% contained high-risk vulnerabilities, and 68% contained components with license conflicts.

From a license compliance perspective, whether an open source license is one of the most popular licenses or a one-off variant, unless an organization is aware of the rights, obligations, and restrictions of using a specific open source component, they can't be sure whether they comply with those obligations. Noncompliant organizations could theoretically lose rights to their proprietary code or call into question the ownership of their IP.

From a security standpoint, all software, be it proprietary or open source, has weaknesses that may become security vulnerabilities. Only a handful of open source vulnerabilities—such as those infamously affecting Apache Struts or OpenSSL—are ever likely to be widely exploited. But when such an exploit occurs, the need for open source security management becomes front-page news—as it did with the Equifax data security breach of 2017.

A report by the U.S. Senate Permanent Subcommittee on Investigations noted that Equifax's lack of a complete software inventory was a major contributing factor to its massive security breach. "Equifax lacked a comprehensive IT asset inventory—meaning it lacked a complete understanding of the assets it owned," the report states. "This made it difficult, if not impossible, for Equifax to know if vulnerabilities existed on its networks. If a vulnerability cannot be found, it cannot be patched."

"We needed a solution to ensure we were tracking and managing open source and commercial components as part of our overall software security initiative."

Many companies don't formally manage their developers' use of open source, and few can produce an accurate, up-to-date inventory (also known as a bill of materials, or BOM) of open source components, licenses, versions, and patch status. In consequence, these organizations open themselves and their customers to risk.

"Our open source management prior to Black Duck was done primarily through spreadsheets, developer honesty, and with our providing basic guidance on using permissive rather than viral licenses," says John Vrankovich, Principal Architect at Blue Yonder.

"We have over a hundred products, with each of those products themselves having hundreds to thousands of different open source components. A decade ago, we had had little concept of identifying and understanding open source security vulnerabilities in our BOM. The move to Black Duck was to address our not knowing about open source security issues. We recognized that we needed a solution to ensure we were tracking and managing open source and commercial components as part of our overall software security initiative."

The solution: Black Duck software composition analysis

Blue Yonder first implemented Black Duck Code Center in 2015. Code Center provides Blue Yonder with software component selection, approval, and tracking of open source and other third-party software components. The goal was to automate Blue Yonder's Technical Review Committee's (TRC) review process from architectural through security and commercial review to final executive review across all Blue Yonder products and release gateways.

Blue Yonder added Black Duck software composition analysis (formerly known as Black Duck Hub) in 2017. Synopsys' Black Duck SCA is a comprehensive solution for managing security, license compliance, and code quality risks that come from the use of open source in applications and containers, enabling organizations to control open source usage across the software supply chain and throughout the application life cycle. Black Duck enables Blue Yonder to set and enforce open source use and security policies, automate policy enforcement with DevOps integrations, and prioritize and track remediation activities.

"All of our core products are using Code Center," says Meghan Caudill, project manager for third-party product compliance at Blue Yonder. "About three years ago, we began to use Black Duck SCA when building the CI/CD process for our Blue Yonder Luminate product line, newly developed, SaaS-native products. Our goal is full migration to Black Duck SCA by the beginning of 2020."

"We're now able to ensure that none of our products are released with open source license risks or security issues."

The results: A broad open source compliance strategy

"With the Black Duck tools we were able to write a broad open source compliance strategy that addressed our requirements and priorities," says John Vrankovich. "We're now able to ensure that none of our products are released with open source license risks or security issues. We're able to ensure that any issues we discover are tracked and remediated. We can ensure that all license obligations are being met, and that only approved open source components are used in our products. The bottom line is that we know what we're using, we know the licenses we're using, we know the versions we're using, and we know any security issues and component patch status."

"Black Duck provides a fully automated process for approval of open source and third-party components in our product. We have an accurate bill of materials for every product—a bill of materials that we can use for release management and during any type of merger and acquisition (M&A) process that might pop up. We know that the BOM is accurate, and we have a much better feel for the security stature of the product because of that."

The Black Duck integration with Jira allows Blue Yonder to fully extend its secure SDLC to the identification and remediation of open source security issues. "We have a single security project in Jira," says John Vrankovich. "All security issues—no matter if they're identified in Black Duck, if they're identified by a customer, if they are identified by dynamic testing, static testing, static security analysis or pen testing—go into the same security project in Jira."

"In Jira we manage a workflow for resolving identified issues. The issue is pushed to the specific application team for resolution. Security engineers review those issues and approve them for remediation. And during the release process—the gateways for releasing our software—that Jira information is utilized as a report to make sure that the release management team knows that all critical and high security issues have been addressed before they are allowed to ship."

"If you're a modern software development organization, you're basically following CI/CD processes and using CI/CD tools. Black Duck automatically hooks into those tools. The overhead for its use is very low. Both from a cost-of-goods perspective and a manual versus automated perspective the cost is lower."

The Synopsys difference

Synopsys Software Integrity Group provides integrated solutions that transform the way development teams build and deliver software, accelerating innovation while addressing business risk. Our industry-leading portfolio of software security products and services is the most comprehensive in the world and interoperates with third-party and open source tools, allowing organizations to leverage existing investments to build the security program that's best for them. Only Synopsys offers everything you need to build trust in your software.

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

Synopsys, Inc.
690 E Middlefield Road
Mountain View, CA 94043 USA

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