Blue Yonder:

Extending a Secure SDLC to Remediate Open Source Security Issues

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

The solution: Black Duck software composition analysis

Blue Yonder first implemented Black Duck Code Center in 2015. Code Center provides Blue Yonder w

Blue Yonder added Black Duck software composition analysis (formerly known as Black Duck Hub) in 2

“All of our core products are using Code Center,” says Meghan Caudill, project manager for third-party

Many co

“Our open source management