Sonatype

Real World Experience: Media & Entertainment

Customer Results

- Developer-friendly open source governance
- Greater architectural consistency
- Reduced risk in using open source
- Time-consuming rework avoided

NEXUS LIFECYCLE USER

Open source governance now moves at the speed of Agile

Media & Entertainment

> "Typically we are seeing scans in under 30 seconds. If you decide you want to ban a component or change your policy with respect to open source licenses you can quickly re-evaluate. That's a very fast operation."

The Challenge

In the rush to get new releases to market, developers use open source components to save time. In fact, 90 percent of a typical application today is comprised of open source software. This world-renowned entertainment company experienced a "huge wake-up call" after a Sonatype report showed hundreds of thousands of component downloads from the Central Repository over 12 months.

"We were absolutely astounded by the volume of open source downloads," the Director of Architecture said. "And we realized that our centralized open source review team had processed less than 3 percent of the components being used. This was a wake up call for us." The review team was focused on license and technical review of open source components but had no visibility into security vulnerabilities. Without visibility into vulnerabilities, developers were re-using unvetted components, which perpetuated the problem. "We didn't want to get in the way of developers using open source," he said. "We just wanted to make sure they were doing it safely."

Why Sonatype?

The company chose Sonatype's products to bring its "Paving the Path to Compliance" program to life. The proactive program involves stakeholders across the organization—legal, development, enterprise architecture and security—and "makes it easy for developers to do the right thing," the director explained.

> “It’s proving to be very appealing to the developers. They are not getting hit with a hammer at the end of the development cycle or waiting forever for approvals.”

Nexus Lifecycle (formerly Component Lifecycle Management - CLM) plugs into the tools where developers access and use open source to build software—the IDE, Continuous Integration Servers and the Nexus repository manager that stores and organizes binary software components.

“That is fantastic because you can see the vulnerability information right in front of you in the tools you use everyday,” he said. Developers see known risks and get instant support in choosing safer versions. Not only does Nexus Lifecycle increase visibility into vulnerabilities, it also tracks usage and enforces policy throughout the SDLC.

Analysis of a build or at the integration stage takes less than 30 seconds so it doesn’t slow down development. And because Nexus Lifecycle’s knowledge base is continuously updated, even the newest security vulnerabilities, license risks and quality issues are identified in seconds.

Results

Open source governance is now “more carrot than stick.” Policy is centrally defined yet automated and available to developers in the tools they use everyday. This makes for governance that is scalable, fast and effective, enabling developers to meet tight schedules and avoid time-consuming rework to remove troublesome components later on.

“It’s proving to be very appealing to the developers,” the director said. “They are not getting hit with a hammer at the end of the development cycle or waiting forever for approvals.” Instead, from the start, developers are empowered to make the right decisions when choosing open source components so they can deliver software that’s compliant with policy, secure, and delivered on time and in budget.