Creating and Maintaining Trust

Using Open Source Software

Open source software provides many benefits that IT and manufacturing organizations are trying to leverage—from faster time to market, adaptability and cost-effective solutions to a more collaborative development environment. However, using open source creates a responsibility to manage the associated risks surrounding security, license compliance and quality.

"Open source software has definitely changed the world. It powers tens of millions of devices, and today companies that aren't normally thought of as software companies are indeed software companies," Michael Lelchuk, manager of professional services at Revenera, said in a webinar. "There is [also] a learning curve around open source, its management, and the importance of not only getting involved, but also staying involved with the open source community."

Lelchuk went on to report that when his company Revenera performs audits of its customers' codebases, it finds 50 to 80% —if not more—are made up of open source. The company has also found that these companies are not properly tracking or monitoring the open source software in their codebases.

Open Source is the Modern Way to Build Software

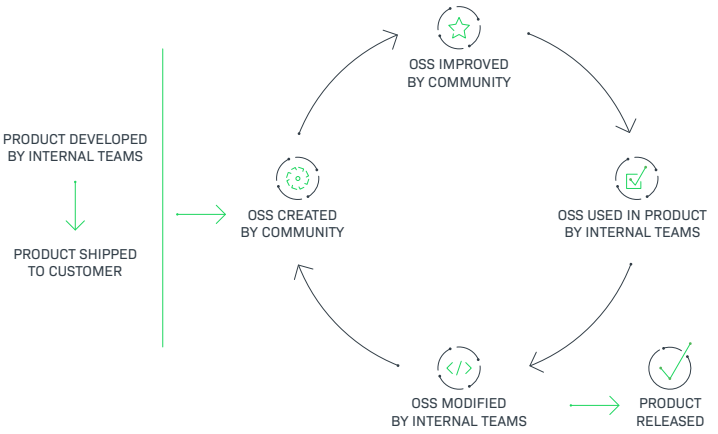

Figure 1. Typical cycle of open source use.

Two percent of the issues the company finds are issues that were initially disclosed before the audit and there is one issue detected for every 32,873 lines of code. "What this shows is really a lack of knowledge with understanding the composition of [the] company's code, and most likely companies are taking on an increased level of risk," said Lelchuk.

Because of these issues, Lelchuk believes license compliance is more important than ever, but it can be complicated to know where to get started.

Mark Gisi, director of the open source program office at Wind River Systems, explained that there are a couple of technologies that can help with this. For instance, the Software Package Data Exchange (SPDX) format provides a detailed analysis of the licensing of a software component. Then, there is OpenChain, which identifies key requirements for a quality open source compliance program. Both of these technologies promote the idea of creating a detailed, accurate Bill of Materials (BOM), which according to Lelchuk is "an assessment of what is in your code, what components you depend on, how they're being used, whether they're being distributed [and] the requisite security information.

"Producing a comprehensive Bill of Materials is perhaps one of the most important actions for development teams to take," Lelchuk added. In addition, Software Composition Analysis—the process of automating the view into open source software use for the purpose of risk management, security and license compliance—is a key component because it provides complete visibility into the open source inventory.

Gisi explained when Wind River was looking to acquire another company they didn't want to inherit any software from the target company without knowing what was in the code. They were able to work with Revenera who received the software from the target under an NDA to perform a forensic analysis of the source code. Revenera delivered the Bill of Materials to Wind River which reported on each component and its risk. "That was great because we were able to conduct an open source due diligence assessment without being exposed to the target's intellectual property," Gisi said in the webinar.

Figure 2. Bill of Materials produced from FlexNet Code Insight

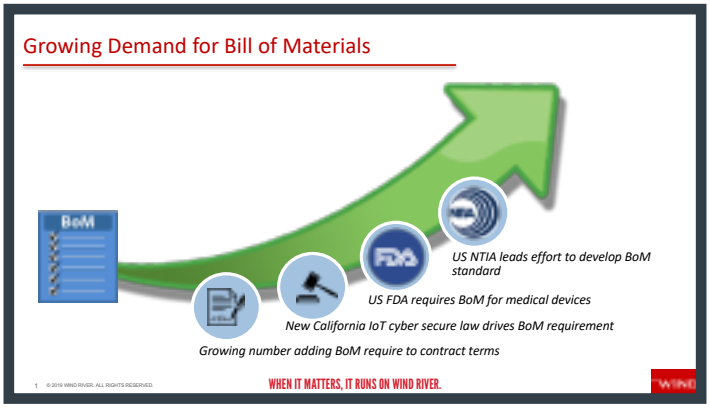

Figure 3. Increase in industry regulations driving demand for BOMs

There are two challenges when it comes to BOMs, which Gisi predicts will be smoothed out over time. First, Gisi explained that open source software has been around for over 20 years and all indications point to the fact that it's not going anywhere. Therefore, not only do companies need to produce a BOM, they also have to maintain it over time. Secondly, not everyone produces a quality BOM, and that can impact everyone that follows them in the supply chain. Gisi believes that we will soon have a standard for BOM creation which will make it easier to consume BOMs from other organizations.

"It is important in today's open source environment to be able to construct a detailed Bill of Materials. It's important for ongoing open source management success," said Lelchuk. "Everything starts by having a clear understanding of where and how you're using that open source software."

Revenera provides the enabling technology to take products to market fast, unlock the value of your IP and accelerate revenue growth—from the edge to the cloud. **www.revenera.com**