SYNOPSYS®

Calix

Releasing Secure Code That Meets Rigorous Standards

Company Overview

Calix builds platforms that connect the world. Founded in 1999 and based in San Jose, Calif., the company is a global provider of cloud and software platforms, systems, and services, with $480 million in annual revenue and an international customer base of more than 1,400 communications service providers.

The challenge: Release a high-quality, secure software codebase that meets rigorous standards

Just about every organization in business today, no matter what it sells, is also a software company.

That is true of Calix. To provide a quality product line of cloud and software platforms, systems, and services to major communications services providers, Calix builds and manages software—a combination of custom built, commercial, and open source—amounting to tens of millions of lines of code.

And software, no matter who builds it, is prone to vulnerabilities—more all the time since so much more software is being written. The National Vulnerabilities Database (NVD) reported 4,000–8,000 new vulnerabilities each year for a decade, but that number spiked to 14,645 in 2017, 16,511 in 2018, and 17,306 in 2019.

While open source software has fewer vulnerabilities than proprietary software, the Black Duck Audit Services team discovered more than 7,000 in 2018 alone.

Also, while open source is free, it comes with licensing requirements. If an organization knowingly or unknowingly fails to comply with the requirements of the components it is using, it could potentially lose the rights to its proprietary code or put the ownership of its IP at risk.

And while not all vulnerabilities will create catastrophic problems, they collectively expose an organization to a now-familiar list of risks: financial theft, corporate espionage, ransomware, the compromise of customers' sensitive data, and possible physical security breaches.

Like most tech companies, Calix was aware of those risks, but its security teams were also aware of how time consuming and expensive it was to analyze any part of its codebase manually, said Vivek Singh, director engineering, product engineering services at Calix.

"Specifically for the emergent systems, we could do a lot manually, but it would be very expensive," he said, adding that while the company had been using an open source scanning tool, it wasn't keeping current with newly discovered and reported vulnerabilities. "The updates were pretty slow," he said.

The solution: Synopsys application security testing tools

That's why Calix now uses multiple Synopsys software testing tools. They include:

- **Coverity**, a static application security testing (SAST) tool that offers precise, actionable remediation advice and context-specific eLearning to help developers fix defects fast. It also provides seamless integration into CI/CD pipelines with automated testing to maintain development velocity.
- **Black Duck**, a comprehensive software composition analysis (SCA) solution for managing security, license compliance, and code quality risks that come from the use of open source in applications and containers.
- **Defensics**, a comprehensive, versatile, automated black box fuzzer that enables organizations to discover and remediate security weaknesses in software efficiently and effectively.

Singh said Calix has been using Coverity for more than five years and brought in Black Duck and Defensics about two years ago.

"As soon as we spin a new stream for development for the next release, all of these processes, Coverity, Black Duck, Defensics—anything related to a scan process touching our codebase—automatically gets set up in our Bamboo CI engine. It is part of our daily build," he said.

"When we do a build—when a developer checks in the code—we have a centralized, mainline code repository, and this process starts on day one. All the reports are live and always current. It's very low manual touchpoints."

The results: Better software security faster

"Coverity solved all the problems for static analysis, along with providing a centralized database," Singh said. "It has a great reporting system, and for anybody from a program manager to product manager to development manager, the ability to manage all these things in a single place is key. While there are numerous static analysis tools on the market today, I would say Coverity is still best in class."

When it came to Black Duck, Singh said it was a triple win: faster, better, and cheaper. "It was a no-brainer," he said, pointing to automation as a huge improvement over the previous tool. "There is a lot of very clear reporting, it gives us a very crisp view into where we need to focus, so we don't need to have a senior architect sit and try to decode the whole report and figure out what issues we had in our codebase."

Defensics became part of the Calix software testing suite, Singh said, because "we were introducing new products to market and security was top of mind as we were venturing into new areas of the networking industry."

"We brought it in as a requirement more than because of any challenges we faced, because the new products—the new software we were going to develop—were very extensively in the area where we would have to look into fuzz testing protocol scans and things like that."

The bottom line, he said, is a deployment that delivers better software security faster.

"We click one button to set up a CI plan, and it pulls in everything from Black Duck, Defensics, Coverity, and our other security analysis tools, and they automatically get plugged in and start generating reports and scans, and if a bug needs to be fixed, it gets into our bug management system right away," he said.

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