CEVA: DSP and AI Processors

Ensuring standards compliance and reducing license risk with Black Duck

Company overview

An industry frontrunner for over 20 years, CEVA is the leading licensor of wireless connectivity, smart sensing technologies, and cocreation solutions for a smarter, safer, and connected world. Many of the world's leading semiconductor system companies and OEMs create power-efficient, intelligent, secure, and connected devices using CEVA's IP for a range of markets, from mobile to consumer, automotive, robotics, industrial, aerospace and defense, and IoT. CEVA is committed to upholding its social responsibility and values of preservation and environmental consciousness.

To learn more about CEVA, click here.

The challenge: Enforcing coding standards and reducing license risk

For CEVA's DevOps/Real-Time Development Manager Ori Leibovich, the challenge was twofold: he needed more-effective enforcement of coding standards and a reduction of license-related risk. Prompted by CEVA's recent work on AI processors for system-on-chip (SoC) designs within the automotive industry, Leibovich saw that CEVA's security program needed to come into compliance with the industry's strict security and safety requirements. Furthering the challenge, Leibovich reported that "CEVA's software development [had] grown rapidly" in recent months, making an automated solution that could keep up with increasing development speeds especially critical.

With an already-mature security program in place, CEVA needed solutions that could fit seamlessly into existing development activities and tooling, and support current security efforts without slowing down or overcomplicating existing initiatives.

Leibovich's desire to meet automotive industry safety certifications led him to investigate a two-pronged upgrade to CEVA's security program: a robust static application security testing (SAST) and software composition analysis (SCA) tools.

The solution: Black Duck SCA and Coverity SAST

CEVA elected to adopt Black Duck® SCA and Coverity® Static Analysis into its existing development pipelines. Black Duck SCA's automated policy management makes it easy for teams to define policies for open source use, security risk, and license compliance up front, while automating enforcement across the entire software development life cycle (SDLC)—all with tools developers are already using. Coverity SAST, a fast, accurate, and highly scalable SAST solution, makes it easy for development and security teams to address security and quality defects early in the SDLC. They can effortlessly track and manage risk across their app portfolio and ensure compliance with security and coding standards.

"With Coverity SAST and Black Duck SCA, we were able to achieve our safety and quality standard certifications."

—Ori Leibovich,
DevOps and Real-Time Development Manager

Black Duck SCA

Leibovich noted that development on his team had "grown rapidly, so we decided that a tool for open source automatic detection [would be] crucial to avoid legal issues." CEVA deployed Black Duck in an environment that included approximately 400 developers and hundreds of thousands of lines of code, and began running weekly Black Duck scans. Black Duck's seamless integration into existing pipelines made it easy for CEVA to add it to existing security activities and set it to work identifying all the open source in its software. According to Leibovich, CEVA had found that this level of discovery was "not possible with other SCA tools" on the market.

Coverity SAST

Faced with industry standard ISO 26262 ASIL-B and quality/reliability standard ISO9001, CEVA needed to achieve very specific security requirements.

ASIL is a risk classification system defined by the ISO 26262 standard for the functional safety of road vehicles. This standard carries with it the expectation of "the absence of unreasonable risk," an expectation that extends down to the quality of the code within the applications that power a vehicle. Similarly, ISO9001 holds organizations to a high level of integrity and quality; orgs must be able to demonstrate their ability to consistently provide products that meet regulatory requirements. As a trusted industry leader, CEVA wanted to quickly ensure and demonstrate its ability to comply with all requirements and continue to deliver the highest-quality products and solutions, including processors, sensor hubs, digital signal processors, and more.

"After investigating several tools, we found out that the Coverity SAST [was] the easiest to integrate in our CI/CD process and to adopt for use with our internally developed compiler," Leibovich said. With Coverity SAST in place, CEVA could now comprehensively track and manage compliance through a wide range of security, quality, data protection, and safety standards.

The results: Effortless compliance and risk reduction

Effortless compliance with Coverity SAST

Complying with industry standards and regulations can be daunting, especially when finding and identifying code and ensuring its quality becomes progressively more difficult due to increasing development speeds. Knowing how to address violations after they are found can be even more daunting. Coverity makes it easy to filter identified issues by category, view trend reports, prioritize remediation of vulnerabilities based on criticality, and most importantly, manage policy compliance across teams and projects.

CEVA was able to quickly integrate Coverity SAST into its CI/CD processes, and then demonstrate that it was satisfying industry regulation requirements. Leibovich found that Coverity SAST "increased code quality and security," helped "find defects with a low false positive rate," and "enforced coding standards like MISRA C and AUTOSAR C++." Most importantly, Coverity SAST easily "integrated with [its] internally developed compiler," meaning existing development activities were uninterrupted and unhindered by the addition of a new solution.

Reduced risk with Black Duck SCA

Without a complete picture of the code within an application portfolio—specifically open source—an organization risks exposing itself to security, license compliance, and code quality risks. License compliance violations can result in costly litigation or compromise an organization's valuable intellectual property.

Black Duck SCA helped CEVA eliminate license compliance risk from its development environment. After investigating several tools, CEVA found that Black Duck SCA would be the easiest to integrate and the least disruptive to its thriving security program, while also delivering results right away. Leibovich said that Black Duck SCA "integrated open source identification and management within our SDLC" and helped "identify open source licenses in use"—all critical activities for minimizing risk associated with license noncompliance.

Black Duck helped CEVA bolster its security efforts and bring security into alignment with the quality of its solution offerings. And by increasing security and compliance efforts, CEVA has reinforced that customers can trust its products. Leibovich summarized the company's new-found security posture, stating that "CEVA can show that we are working according to safety protocols, and we have no issues with customers due to open source usage. We can show code is going through a static analysis tool and [we] therefore [have] better-quality software. And we can show that CEVA is working according to safety protocols."

Now, Coverity SAST and Black Duck SCA scans are initiated automatically within CEVA's development pipelines. They are providing detailed reports that developers and managers can use to ensure security and compliance, allowing teams to focus on what they do best—developing the industry-leading processor and platform IP solutions they are known for.

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.