SYNOPSYS®

Ensuring standards compliance and reducing license risk with Synopsys

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.

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.

“With Synopsys Coverity and Black Duck solutions, we were able to achieve our safety and quality standard certifications.”

—Ori Leibovich,
DevOps and Real-Time Development Manager

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.

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