

Cryptsoft

Improving scan speeds while maintaining CI development velocity

CRYPTSOFT

Company overview

Australian security firm Cryptsoft offers software development tools for security system design, deployment, validation, and interoperability. Its products include the OASIS Key Management Interoperability Protocol (KMIP), OASIS Public Key Cryptography Standard #11 (PKCS#11), and smartcard solutions.

To learn more about Cryptsoft, click [here](#).

The challenge: Increase and improve security scans at the speed of DevOps

As organizations rapidly evolve their development practices into streamlined and agile [DevOps](#) methodologies, tools capable of adapting and keeping pace with development speeds and complexities are critical. Specifically, tools must seamlessly integrate into existing pipelines without “breaking the build” or decreasing development velocity.

Cryptsoft depends on accurate and efficient security scanning for the successful production of its industry-leading software products. So any security solutions that are incorporated into its software development life cycle ([SDLC](#)) pipelines must be capable of adequately maintaining development velocity.

Tim Hudson, CTO and company founder, said, “Our customers are some of the most well-known companies in the technology industry, and their combined expectations, and the critical nature of the software that we provide for key management systems and hardware security modules, means that we must use every possible tool that is available to improve code quality, security, and stability.” This high-stakes demand—along with ever-increasing development speeds—drove Cryptsoft to look for a static application security testing ([SAST](#)) solution that could keep up and scale to its DevOps needs.

Hudson said that it was his intent “to get in front of our customers who are performing intermittent scans of releases, and catch items before our customers see them.” This requirement necessitated a robust SAST tool capable of catching bugs sooner and without slowing down [CI](#) processes.

The solution: Black Duck application security testing tools

Cryptsoft adopted Black Duck [Coverity® SAST](#) solution to support development speeds and increase security and software quality.

Coverity is a fast, accurate, and highly scalable static analysis solution that helps development and security teams address security and quality defects early in the software development life cycle, track and manage risks across the application portfolio, and ensure compliance with security and coding standards.

“Coverity helps [us] see bugs in advance and address them, and also enables a much faster support response when a customer queries whether an item raised is an issue or a false positive,” Hudson said.

“Coverity continues to remain the most useful of the static code analysis tools, with its broad coverage and scanners. The false positive rate remains consistent despite the ever-increasing range of code checks that have been added. It is simply the best tool of its type in the market—still clearly ahead of its competitors,” he continued.

“Developing large systems without tools like Coverity is like playing Russian roulette—it just isn’t something you should contemplate. Coverity gives you confidence that you haven’t missed something in your manual review processes, and that equates to an easy decision to make on a simple value-for-money basis.”

—Tim Hudson, Cryptosoft, CTO

The results: Rapid accurate feedback, seamless integration

Cryptosoft expected that introducing the latest release into its build process would be relatively straightforward. Hudson said those expectations were exceeded. “When we integrated it into our build processes, [we] were classifying issues the same day we received the software,” he said. This ease of integration is a critical component of DevOps-compatible tools. Failure to seamlessly integrate into existing pipelines can derail development activities. With Coverity, Cryptosoft’s efforts were uninterrupted—it was up and running the same day.

In addition to its seamless integration, Coverity enabled Cryptosoft to get reliable results fast and early. “The ability for our developers to get immediate feedback from our continuous integration environment means that Coverity is simply part of the overall development process, rather than something that happens at the end of a development cycle. This enables us to determine and adjust any potentially problematic constructs during development, which reduces false positives even further. Static code analysis within all possible code paths helps significantly when detecting potential issues in harder-to-test contexts. And that does lead to overall more robust software that we can deliver to our customers,” Hudson said.

With the help of Coverity SAST, Cryptosoft’s security posture now matches the fortitude and reliability of its industry-leading security product offerings, solidifying its reputation as a proven and trusted security software leader.

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.

©2024 Black Duck Software, Inc. All rights reserved. Black Duck is a trademark of Black Duck Software, Inc. in the United States and other countries. All other names mentioned herein are trademarks or registered trademarks of their respective owners. September 2024