SYNOPSYS®

Íslandsbanki

Managing & Mitigating Open Source Vulnerabilities with Black Duck SCA

Company overview

An Icelandic bank with roots tracing back to 1884, Íslandsbanki offers consumer, private, and corporate banking services, mortgage loans, private equity, wealth management, credit cards, and other financial services to businesses and consumers.

The challenge: Managing open source in containers and applications

"We were initially looking for a software composition analysis (SCA) solution to actively monitor our container deployments for open source vulnerabilities," said Finnur Örn Guðmundsson, infrastructure architect at Íslandsbanki. "We felt we weren't managing the open source we were using in a consistent fashion, and monitoring it entailed a lot of manual labor on the part of our developers."

"When we dug more deeply into our needs, we also saw the potential benefit of SCA for our noncontainerized workloads. We wanted to have a tool to scan our packages in the CI/CD pipelines and to be able to stop deployments if there were serious vulnerabilities that might affect us and/or our customers. The development teams would then be able to fix those vulnerabilities during the development cycle. Having a single automated solution to manage the open source in both our containers and standard deployed applications was essential to minimize the workload on our developers."

Why software composition analysis?

Open source is the foundation for every application in every industry. In fact, the Synopsys 2021 "Open Source Security and Risk Analysis" (OSSRA) report found that 98% of audited codebases contained open source. But paralleling the popularity of open source is a growth in risk—specifically around open source licensing, code quality, and especially open source security. Eighty-four percent of the audited codebases examined in the OSSRA report were found to have at least one vulnerability, with an average of 158 vulnerabilities per codebase.

Manual tracking of open source is a Sisyphean task; organizations simply can't adequately track and manage the sheer amount of open source they use by spreadsheet anymore. Software composition analysis is an automated process that identifies security vulnerabilities, license compliance, and code quality issues that may arise from the use of open source in applications and containers.

The solution: Black Duck SCA with Black Duck Security Advisories

"We evaluated a few SCA solutions and did a proof of concept of the three final candidates," Guðmundsson continued. "Of the three, we found Black Duck® to be the best fit for our needs. At the time of our evaluation, Black Duck was the only solution we tested that was able to scan software whether packaged as containers or as standard deployments."

Guðmundsson cited Black Duck Security Advisories (BDSAs) as a key feature of Black Duck SCA. These advisories offer curated and prioritized security notifications reaching well beyond the standard information found in free feeds like the National Vulnerability Database. With thousands of exclusive listings curated by security experts, Black Duck Security Advisories provide timely vulnerability descriptions, severity scoring, and advanced, actionable remediation guidance.

"The BDSAs give us good insight into if a vulnerability might affect us or not, if it is being exploited in the wild, and what package versions fix the vulnerability," said Guðmundsson. "And Black Duck SCA It makes it easy to see which of our solutions are using the vulnerable package in question."

The results: A single tool to manage and mitigate open source vulnerabilities

Implemented in April 2021, Íslandsbanki has already seen positive results from Black Duck SCA. "Our CI/CD toolchain includes Azure DevOps, Visual Studio, Docker, and Kenna," said Guðmundsson. "We have six development teams testing 177 applications, and conduct Black Duck scans for every master branch build and pull request."

"Implementing Black Duck has given us a single tool to manage and mitigate vulnerabilities, allowing our development, operations, and security teams to see the status of our deployments," Guðmundsson concluded. "The product is easy and straightforward to use, and we'd recommend Black Duck to anyone looking into an SCA solution."

The Synopsys difference

Synopsys Software Integrity Group provides integrated solutions that transform the way development teams build and deliver software, accelerating innovation while addressing business risk. Our industry-leading portfolio of software security products and services is the most comprehensive in the world and interoperates with third-party and open source tools, allowing organizations to leverage existing investments to build the security program that's best for them. Only Synopsys offers everything you need to build trust in your software.

For more information about the Synopsys Software Integrity Group, visit us online at www.synopsys.com/software.

Synopsys, Inc.
690 E Middlefield Road
Mountain View, CA 94043 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com