Overview
Most software developed today uses third-party or open source components, which often contain vulnerabilities susceptible to cyber attack. Applications in critical areas such as finance, healthcare, and national defense are an especially appealing target for hackers and cyber criminals. In addition, development organizations rarely identify or review third-party licenses, leaving their code susceptible to copyright issues. Our solution integrates Black Duck Binary Analysis results into the standard Coverity defect triage workflow to diagnose potentially expensive vulnerabilities and license issues associated with third-party components.

Black Duck Binary Analysis
Black Duck Binary Analysis is a binary and runtime code analysis platform that addresses the challenges of an increasingly complex and fragmented software supply chain. Black Duck Binary Analysis can scan practically any software or system, including desktop and mobile applications, embedded system firmware, and more. It quickly identifies third-party and open source components, known vulnerabilities, license types, and other potential risk issues.

Coverity Connect
Coverity Connect is a comprehensive, collaborative issue management interface that lets you see code status and health and evaluate and triage findings in a project. Metrics such as the number of new, fixed, and outstanding vulnerabilities provide defect trend data over time.

How the integration works
The integration works with either a Black Duck Binary Analysis cloud instance or an on-premises installation. A new Coverity Connect instance is provisioned (or an existing one reused), and the scripted solution is installed in the customer environment. It automates the process of uploading an application, monitoring the scan, extracting vulnerability and third-party licensing information, and importing the vulnerability information into Coverity Connect. The solution can be configured to scan each new version of an application automatically to reveal new vulnerabilities and whether old ones have been fixed.
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. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

For more information, go to www.synopsys.com/software.

©2019 Synopsys, Inc. All rights reserved. Synopsys is a trademark of Synopsys, Inc. in the United States and other countries. A list of Synopsys trademarks is available at www.synopsys.com/copyright.html. All other names mentioned herein are trademarks or registered trademarks of their respective owners.

01/30/19 ds-coverity-blackduck-binary.