Synopsys Advances Application Security Testing for Developers with Rapid Scan

New Rapid Scan Capabilities in Coverity SAST and Black Duck SCA Help Development Teams Secure Cloud-native Applications as Fast as They Write Them

MOUNTAIN VIEW, Calif., July 27, 2021 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today announced the availability of new Rapid Scan capabilities within the company's Coverity static application security testing (SAST) and Black Duck software composition analysis (SCA) solutions. The Rapid Scan features provide fast, lightweight vulnerability detection for both proprietary and open source code. Rapid Scan is optimized for the early stages of development, particularly for cloud-native applications and infrastructure-as-code (IaC).

While comprehensive and thorough security testing is critical to managing risk in the later stages of the software development lifecycle (SDLC), it is often too time- and resource-intensive to perform full scans at every incremental step in the early stages of the SDLC. Rapid Scan complements conventional application security testing activities by enabling development teams to perform fast SAST and SCA scans at every code check-in or early-stage build without slowing them down. It allows developers to shift left efficiently and prevents security issues from propagating into the later stages of the SDLC.

"One of the hallmarks of modern software development is breaking down large processes into smaller, more manageable tasks that can performed rapidly and concurrently in a distributed fashion," said Jason Schmitt, general manager of the Synopsys Software Integrity Group. "For organizations embracing DevSecOps, application security testing needs to follow suit. With Rapid Scan, Coverity and Black Duck users can run quick preventative scans to detect and eliminate surface-level vulnerabilities as their developers write and commit code, and they can use the same solutions to run deep scans later in the SDLC prior to deploying their applications."

The new capabilities include:

Coverity Rapid Scan. The new Rapid Scan capabilities of Coverity SAST provide fast security analysis of proprietary code at the developer's desktop and in continuous integration (CI) pipelines such as GitLab and GitHub Actions. Coverity Rapid Scan is optimized for cloud-native applications built on infrastructure-as-code frameworks such as Kubernetes, Terraform, and CloudFormation, and microservices such as GraphQL, Kafka, and Postman. Rapid Scan can quickly detect many of the most common security weaknesses, as well as problematic misconfiguration flaws and API misuses.

Black Duck Rapid Scan. The Rapid Scan capabilities of Black Duck SCA allows developers and release managers to perform fast dependency analysis to determine if any of the open source components in their application violate their organization's security and license policies prior to merging code into release branches. Black Duck Rapid Scan is optimized for speed and efficiency by providing developers with early insight into dependency risk and by deferring resource-intensive SCA activities such as multi-factor open source detection and generating a complete software bill of materials to later stages of the SDLC.

Intelligent Orchestration and Rapid Scan. The Coverity and Black Duck Rapid Scan capabilities can be used in conjunction with Synopsys' Intelligent Orchestration solution to automatically trigger fast SAST and SCA scans based on events in the continuous integration (CI) pipeline. Intelligent Orchestration, which enables DevOps teams to run the right security tests at the right time, can leverage Rapid Scan at early stages in the pipeline when speed and efficiency are critical, and it can run full Coverity and Black Duck scans at later stages in the pipeline when validating the quality and security of applications prior to deployment.

To learn more about Rapid Scan for Coverity and Black Duck, read the blog post.

About the Synopsys Software Integrity Group

Synopsys Software Integrity Group 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. Learn more at www.synopsys.com/software.

About Synopsys

Synopsys, Inc. (Nasdaq: SNPS) is the Silicon to Software™ partner for innovative companies developing the electronic products and software applications we rely on every day. As an S&P 500 company, Synopsys has a long history of being a

global leader in electronic design automation (EDA) and semiconductor IP and offers the industry's broadest portfolio of application security testing tools and services. Whether you're a system-on-chip (SoC) designer creating advanced semiconductors, or a software developer writing more secure, high-quality code, Synopsys has the solutions needed to deliver innovative products. Learn more at www.synopsys.com.

Editorial Contact:
Mark Van Elderen
Synopsys, Inc.
650-793-7450
mark.vanelderen@synopsys.com

SOURCE Synopsys, Inc.