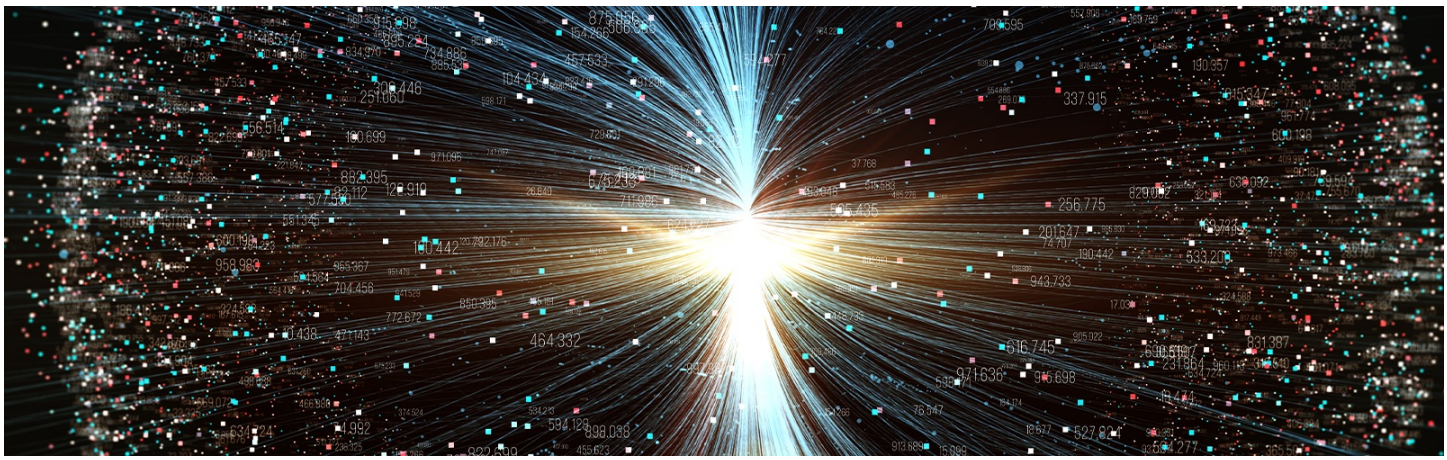
Synopsys Launches New Offering for Comprehensive Software Supply Chain Security



Black Duck Supply Chain Edition addresses vulnerabilities, license conflicts, and malicious code across open source and commercial dependencies as well as AI-generated code.

SUNNYVALE, Calif., April 9, 2024 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today announced the availability of Black Duck® Supply Chain Edition, a new software composition analysis (SCA) offering that enables organizations to mitigate upstream risk in their software supply chains. Black Duck Supply Chain Edition combines multiple open source detection technologies, automated third-party software bill of materials (SBOM) analysis, and malware detection to provide a comprehensive view of software risks inherited from open source, third-party, and AI-generated code. Development and security teams can track their dependencies across the entire application lifecycle to identify and resolve security vulnerabilities, malicious packages, and license violations and conflicts.

Supply Chain Edition builds on the market-leading capabilities of Black Duck and delivers a full range of supply chain security capabilities to teams responsible for building secure, compliant applications.

"With the rise in software supply chain attacks targeting vulnerable or maliciously altered open source and third-party components, it's critical for organizations to understand and thoroughly scrutinize the composition of their software portfolios," said Jason Schmitt, general manager of the Synopsys Software Integrity Group. "This requires constant vigilance over the patchwork of software dependencies that get pulled in from a variety of sources, including open source components downloaded from public repositories, commercial software packages purchased from vendors, code generated from AI coding assistants, and the containers and IT infrastructure used to deploy applications. It also requires the ability to detect and generate actionable insights for a wide range of risk factors such as known vulnerabilities, exposed secrets, and malicious code. Black Duck Supply Chain Edition combines a suite of best-in-class capabilities to streamline these requirements and attest to the results in standardized or customized SBOM formats."

Key features of Black Duck Supply Chain include:

- **Multiple open source detection technologies.** Accurately identify open source components across any programming language using the most comprehensive combination of software analysis technologies, including package dependency, CodePrint™, snippet, binary, and container analysis.
- **Third-party SBOM import and analysis.** Import SBOMs from third-party software suppliers and automatically catalogue the open source, commercial, and custom components contained in them.
- **Malware detection** (leveraging technology from ReversingLabs)**.** Perform post-build analyses to detect the presence of malware, such as suspicious files, potentially unwanted applications, protest-ware, and suspicious file structures.
- **Risk identification and mitigation.** Continuously monitor for open source vulnerabilities, exposed secrets, malware, and malicious packages in both the SBOMs you generate as well as those you import.
- **IP risk and license compliance management.** Automatically identify software licenses associated with your dependencies and receive guidance on obligations or conflicts with how the application is licensed, deployed, and distributed. Analyze AI-generated code to identify hidden open source snippets that may be subject to copyright or license obligations.

- **Industry standard SBOMs.** Export SBOMs containing all open source, custom, and commercial dependencies, in SPDX or CycloneDX formats, to align with customer, industry, or regulatory requirements. Leverage out of the box templates to meet the appropriate level of sharing detail specified by your downstream customers.

Black Duck Supply Chain Edition will be generally available on April 25 and showcased May 6-9 at the RSA Conference in San Francisco at the Synopsys Software Integrity Group booth, #1027.

For more information, visit our website or read the detailed blog post.

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

About Synopsys
Catalyzing the era of pervasive intelligence, Synopsys, Inc. (Nasdaq: SNPS) delivers trusted and comprehensive silicon to systems design solutions, from electronic design automation to silicon IP and system verification and validation. We partner closely with semiconductor and systems customers across a wide range of industries to maximize their R&D capability and productivity, powering innovation today that ignites the ingenuity of tomorrow. Learn more at www.synopsys.com.

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

SOURCE Synopsys, Inc.