Synopsys Enhances Its Software Integrity Platform to Address Evolving Needs of Organizations Building Security and Quality into their Software

Latest Product Updates Expand Coverage for New Programming Languages and MISRA Compliance, Improve Integration Capabilities and Increase Flexibility

MOUNTAIN VIEW, Calif., July 13, 2017 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today announced key updates to its Software Integrity Platform that are designed to help companies build security and quality into their software while reducing time-to-market. In the era of digital transformation, building secure and reliable software is challenged by the rapid, complex and diverse nature of development cycles. The latest updates to the Synopsys Software Integrity Platform address these challenges with expanded support for new programming languages, full coverage for the Motor Industry Software Reliability Association (MISRA) guidelines, improved automation and integration capabilities, and increased flexibility.

According to a recent Forrester Research report, "Applications are increasingly the face of interaction between companies and their customers; this includes customer-facing applications, differentiating mobile apps, Internet-of-things (IoT) device interfaces, and streamlined back-end processes. Meanwhile, application security technologies continue to evolve based on new developer methodologies, new attack vectors, new application types, and new business needs."[1]

"The latest enhancements to the Synopsys Software Integrity Platform help organizations address the rapid pace of change when developing and securing their software," said Andreas Kuehlmann, senior vice president and general manager for the Synopsys Software Integrity Group. "By expanding our coverage to include new programming languages and standards compliance, and ensuring our solutions integrate with a diverse ecosystem of development tools, we enable our platform to be adaptable to a wide range of customer needs. Synopsys is positioned to guide organizations along their software integrity journey as the industry landscape evolves."

The new updates to the Synopsys Software Integrity Platform include a wide range of enhancements and features:

Expanded coverage: Organizations are expanding their software portfolios, resulting in the adoption of new programming languages, frameworks, and open source software components, while they are simultaneously navigating security, quality and compliance requirements. Empowering organizations to improve the security and quality of their broadening software portfolios, Synopsys continues to expand the coverage of its Software Integrity Platform.

- Programming languages and analysis checkers – The latest platform updates introduce Coverity® Static Analysis support for the Swift programming language, improved Protecode™ Software Composition Analysis support for open-source components written in Ruby programming language, and new eLearning courses for secure programming techniques in Android, iOS, and JavaScript. Synopsys has also expanded its static analysis offerings to detect a wider range of security and quality defects across all supported programming languages including Java and JavaScript.
- Industry standards – Synopsys' Static Analysis tool now provides full coverage for MISRA, a series of software development guidelines used by the automotive and other safety-critical industries to promote the safety and security of embedded systems. With this update, the Synopsys' Software Integrity Platform now supports all statically verifiable rules in MISRA C 2004, MISRA C++ 2008, and MISRA C 2012.

Integration and automation: With the emergence of trends such as DevOps and continuous integration/continuous deployment (CI/CD), organizations are shifting toward more rapid and iterative development methodologies. To keep pace, software security testing efforts need to leverage automation and integrate with development tool chains and workflows. Synopsys continues to introduce news ways to automate the security and quality testing process, integrating it seamlessly with other development tools and workflows.

- Synopsys updated its static analysis integration with CI/CD tools like Jenkins, as well as current versions of popular integrated development environments (IDEs), including Eclipse 4.7, Microsoft Visual Studio 2017, and IntelliJ IDEA. Integrating static analysis into development tools allows organizations to test early and often without disrupting their workflows or leaving their development environments.
- Synopsys updated its software composition analysis solution to automate the confirmation of identified open-source software components, which accelerates adoption and time-to-value.
- For its Managed Services for application security testing (AST), Synopsys added additional API

enhancements to assist clients with automation of assessments. Organizations can manage their applications via the API, as well as export results and schedule assessments.

Flexibility: When it comes to making software secure, every organization has unique requirements and challenges that go beyond the confines of traditional out-of-the-box security solutions. Synopsys is committed to making its Software Integrity Platform flexible and customizable, giving companies the freedom to tailor the existing solutions to address new or special needs.

- In this latest update, Synopsys introduced a Defensics® Fuzz Testing Software Development Kit (SDK) for building custom fuzz testing tools that detect critical security vulnerabilities in software applications and embedded devices. The SDK is built on the underlying technology of the industry leading Defensics Fuzz Testing tool, which was used to discover the infamous Heartbleed vulnerability. The Synopsys Fuzz Testing SDK is a powerful framework that provides companies the flexibility to test proprietary, niche or previously unsupported communication protocols and file formats.
- Synopsys also added more flexibility to its eLearning solution, the self-paced security training component of its Software Integrity Platform. It has modularized the courses into bite-sized, consumable and mobile responsive modules, providing developers with focused training around a wide array of evolving technology stacks.
- Synopsys added workflow enhancements to its Managed Services for application security testing to increase customer self-service and flexibility. Tests can now be removed from the queue and rescheduled quickly and easily. A new commenting feature was also introduced to the Managed Services workflow, providing a single location for customers and Synopsys consultants to communicate, ask questions, and provide updates. These updates enable Synopsys' Managed Services offering to be more responsive to organizations' changing needs, ultimately improving service utilization and value delivered.

About the Synopsys Software Integrity Platform

Synopsys offers the most comprehensive solution for building integrity —security and quality— into the software development lifecycle and supply chain. The Software Integrity Platform unites leading testing technologies, automated analysis, and experts to create a robust portfolio of products and services. This portfolio enables companies to develop personalized programs for detecting and remediating defects and vulnerabilities early in the development process, minimizing risk and maximizing productivity. Synopsys, a recognized leader in Application Security Testing (AST), is uniquely positioned to adapt and apply best practices to new technologies and trends such as IoT, DevOps, CI/CD, and the Cloud. For more information, go to 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 the world's 15th largest software company, Synopsys has a long history of being a global leader in electronic design automation (EDA) and semiconductor IP and is also growing its leadership in software security and quality solutions. Whether you're a system-on-chip (SoC) designer creating advanced semiconductors, or a software developer writing applications that require the highest security and quality, Synopsys has the solutions needed to deliver innovative, high-quality, secure products. Learn more at www.synopsys.com.

1. "TechRadar™: Application Security, Q3 2017", Forrester Research, Inc., July 6, 2017

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

Simone Souza
Synopsys, Inc.
650-584-6454
simone@synopsys.com

SOURCE Synopsys, Inc.