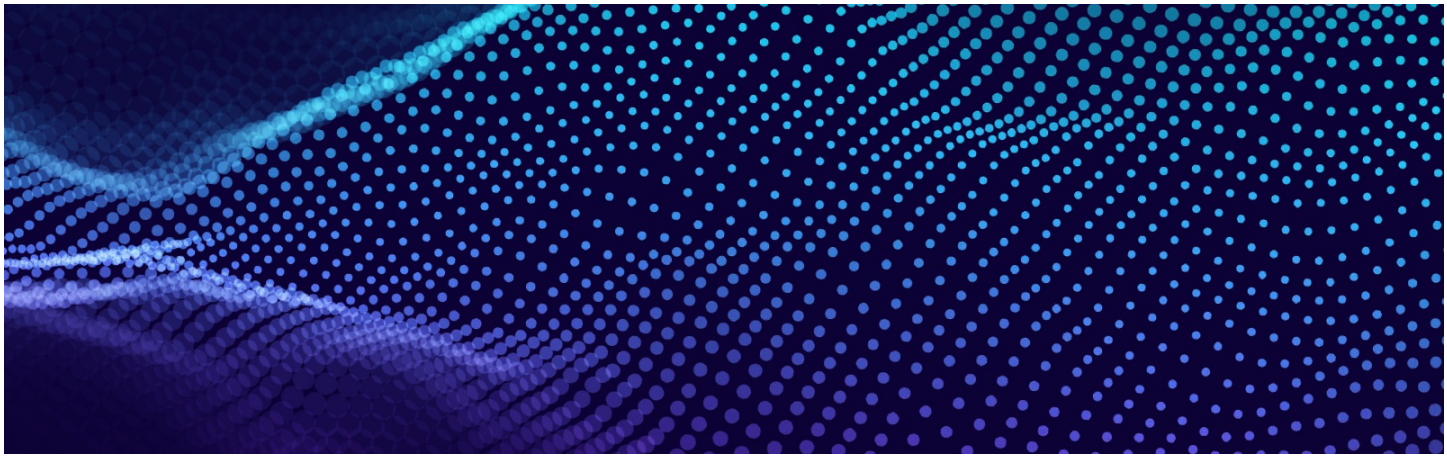
New Synopsys Research Reveals Vast Majority of Organizations Report DevOps Delays Due to Critical Security Issues



Over 80% of survey respondents indicated that a critical security issue in deployed software impacted their DevOps delivery schedule in the last year

SUNNYVALE, Calif., Oct. 10, 2023 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today announced the publication of its "Global State of DevSecOps 2023" report examining the strategies, tools, and practices impacting software security. The new report from the Synopsys Cybersecurity Research Center is based on a survey conducted by Censuswide polling more than 1,000 IT professionals across the world – including developers, application security professionals, DevOps engineers and CISOs, as well as experts in technology, cybersecurity, and software development.

Over 80% of survey respondents indicated that a critical security issue in deployed software impacted their DevOps delivery schedule in the last year. Implementing DevSecOps, a framework focused on embedding security testing throughout each phase of the software development life cycle (SDLC), is an established way to reduce the volume of critical vulnerabilities and exploitable security issues in production applications.

"While a vast majority [91%] of organizations have adopted some level of DevSecOps practices, they continue to face barriers effectively implementing its methods, especially at enterprise scale," said Jason Schmitt, general manager of the Synopsys Software Integrity Group. "Specifically, we're noticing that organizations across the globe are struggling with integrating and prioritizing the results from the multiple application security testing tools used by their teams. They also struggle to enforce security and compliance policies automatically through infrastructure-as-code, a practice that was cited most often by respondents as a key factor of their security program's overall success."

Key findings from the report include:

- **Most security professionals are already using AI –and even more are wary of its risks.** A majority (52%) of survey respondents noted that they are actively using AI to enhance their organization's software security measures. However, even more (76%) are "very or somewhat concerned" about potential errors or issues with AI-based cybersecurity solutions.

- **Remediation timelines for most organizations can span weeks.** Twenty-eight percent of respondents said their organizations take as long as three weeks to patch critical security risks/vulnerabilities in deployed applications. Another 20% said it can take up to a month, even as most exploits appear within days.

- **Application security testing tools are seen as useful to at least two-thirds of respondents.** When asked to gauge the usefulness of security tools and practices – including dynamic application security testing (DAST), interactive application security testing (IAST), static application security testing (SAST), and software composition analysis (SCA) – each tool included in the survey was regarded as useful by at least two-thirds of respondents. The report identifies SAST as the highest-regarded AST tool, with 72% indicating that they find it useful. That is closely followed by IAST (69%), SCA (68%), and DAST (67%).

- **Security testing responsibilities are equally shared between internal security and**

development/engineering teams. Software developers and engineers (45%) are just as likely to be tasked with performing security tests on their organization's business-critical applications and continuous improvement (CI) pipelines as internal security team members (46%). One-third (33%) of organizations are also enlisting external consultants to supplement the efforts of internal teams.

To learn more, download a copy of the "Global State of DevSecOps 2023" report 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
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:
Liz Samet
Synopsys, Inc.
336-414-6753
esamet@synopsys.com

SOURCE Synopsys, Inc.