Black Duck Newsroom

DevSecOps Study Finds that Nearly Half of Organizations Consciously Deploy Vulnerable Applications Due to Time Pressures

Study conducted by analyst firm ESG explores security trends and challenges emerging in modern application development

Disclaimer: The Synopsys Software Integrity Group is now Black Duck®. Click here to learn more.

MOUNTAIN VIEW, Calif., Aug. 6, 2020 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today released the "Modern Application Development Security" eBook. Based on a survey of cybersecurity and application development professionals conducted by Enterprise Strategy Group (ESG), the eBook highlights the extent to which security teams understand modern development and deployment practices, and where security controls are required to lower risk. The study finds that nearly half (48%) of survey respondents consciously push vulnerable code to production due to time pressures. The study also identifies that integrations complementing high velocity application development are most important, according to 43% of respondents, to improving application security programs.

Download a free copy of the "Modern Application Development Security" eBook.

"DevSecOps has moved security front and center in the world of modern development; however, security and development teams are driven by different metrics, making objective alignment challenging," said Dave Gruber, Senior ESG Analyst. "This is further exacerbated by the fact that most security teams lack an understanding of modern application development practices. The move to microservices-driven architectures and the use of containers and serverless architectures has shifted the dynamics of how developers build, test, and deploy code."

Synopsys commissioned ESG, a leading IT analyst and research organization, to document insights into the dynamics between development teams and cybersecurity teams with respect to the deployment and management of application security solutions. ESG surveyed 378 qualified cybersecurity professionals with insight into and responsibility for security application development technologies, and application development professionals involved with securing development tools and processes. The survey respondents work at organizations in multiple industry verticals including manufacturing, financial services, construction/engineering, and business services, among others throughout the United States and Canada.

"The key insights identified within this study underscore the fact that organizations need to address application security holistically throughout the development life cycle," said Patrick Carey, Director of Product Marketing for the Synopsys Software Integrity Group. "Of the organizations consciously pushing vulnerable code into production, 45% do so because the vulnerabilities identified were discovered too late in the cycle to resolve them in time. This reaffirms the importance of shifting security left in the development process, enabling development teams with ongoing training as well as tooling solutions that complement their current processes so that they may code securely without negatively impacting their velocity."

Key insights from the study include:

- **Most organizations believe their application security program is effective, though many still push vulnerable applications into production.** Sixty-nine percent of survey respondents rate the efficacy of their current program as an 8 or higher on a scale of 0 to 10 (with 10 being the most effective). However, as nearly half of organizations consciously push vulnerable code on a regular basis, most have experienced production application exploits involving OWASP Top 10 vulnerabilities in the past 12 months.
- **DevOps integration is a critical element for improvement.** More than one-quarter of respondents say that their current application security tools add friction and slow down development cycles, while 23% identify poor integration with development/DevOps tools as a common challenge. Additionally, 26% of respondents note a difficulty with or lack of integration between different application security vendor tools as a common application security challenge.
- **Developers play an important role in application security, but they lack the skills and training.** Nearly one-third (29%) of respondents express that developers within their organization lack the knowledge to mitigate issues identified by their current application security tools. Furthermore only 17% say that their developers utilize just-in-time training available within their security tools and just 29% are required to participate in training at least once per quarter.
- **Organizations are planning to increase application security spending.** More than half (51%) of respondents report plans for significant increases in application security spending over the next 12 months. Forty-four percent plan to target application security investments toward cloud.
- **AppSec tool proliferation is driving many organizations to invest in consolidation.** Many organizations are struggling to integrate and manage the number of tools in place, often leading to a reduction in the effectiveness of their security program while also directing an inordinate amount of resources to manage them. With 70% utilizing more than ten tools, complexity becomes a key issue, and as a result, more than a third are focusing investments on consolidation.

To learn more, download a copy of the "Modern Application Development Security" eBook, register for our September webinar, or read our new blog post highlighting the survey's findings.

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 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.

Editorial Contact:
Liz Samet
Synopsys, Inc.
703-657-4218
elizabeth.samet@synopsys.com

SOURCE Synopsys, Inc.

---

https://news.blackduck.com/2020-08-06-DevSecOps-Study-Finds-that-Nearly-Half-of-Organizations-Consciously-Deploy-Vulnerable-Applications-Due-to-Time-Pressures