Black Duck Newsroom

Black Duck Research Highlights Growing Security Debt as Development Teams Accelerate with AI

Companies are achieving unprecedented deployment frequencies while security practices lag behind, creating significant risk

BURLINGTON, Mass., Oct. 8, 2025 /PRNewswire/ -- Black Duck® Software, Inc. ("Black Duck"), a leading global provider of application security solutions, today released the "Balancing AI Usage and Risk in 2025: The Global State of DevSecOps" report. The report provides actionable recommendations for both executive leaders and hands-on practitioners, emphasizing the need for robust AI governance frameworks, rationalization of the application security testing toolchain, and investment in developer-centric security tools.

Development teams are releasing code at an unprecedented speed, but security practices aren't keeping pace. Black Duck's research reveals that nearly 60% of respondents report deploying code daily or more frequently. But manual security practices can cause substantial challenges as AI-enabled development pipelines transform the very foundations of DevSecOps.

The comprehensive survey of over 1,000 global software and security professionals conducted in July and August 2025 highlights several critical challenges facing DevSecOps teams today:

- **Security lags behind development**: Despite rapid deployment frequencies, 46% of companies still rely on manual processes to get new code into the security testing queue, leading to incomplete coverage, greater friction with development teams, and growing security debt.
- **Tool sprawl crisis**: Over 71% of respondents report that a significant portion of their security alerts are "noise"—false positives or duplicate findings from different tools, destroying the ROI of security investments.
- **Speed vs. security dilemma**: An overwhelming 81% of professionals say that application security testing slows down development and delivery, creating tension between development and security teams.
- **AI is a double-edged sword**: AI is perceived as both a powerful tool for improving security and a significant new source of complex risks. While 63% believe AI helps write more-secure code, 57% agree it introduces novel security risks.
- **The need for workflow integration**: The top priority for improving application security testing is "better development workflow integration," chosen by 27% of respondents, indicating the need to shift toward embedding security seamlessly into developer workflows.

"The findings paint a clear picture: the old ways of doing application security aren't working, and speed without integrated security creates risk for companies," said Jason Schmitt, CEO of Black Duck. "To navigate this new world, development teams must shift from a reactive, tool-centric model to a proactive, platform-based strategy that integrates security directly into developer workflows to achieve true scale application security."

To learn more, download a copy of the "Balancing AI Usage and Risk in 2025: The Global State of DevSecOps" report, read our detailed blog post, or access the on-demand expert-led webinar.

About Black Duck

Black Duck® meets the board-level risks of modern software with True Scale Application Security, ensuring

uncompromised trust in software for the regulated, AI-powered world. Only Black Duck solutions free organizations from tradeoffs between speed, accuracy, and compliance at scale while eliminating security, regulatory, and licensing risks. Whether in the cloud or on premises, Black Duck is the only choice for securing mission-critical software everywhere code happens. With Black Duck, security leaders can make smarter decisions and unleash business innovation with confidence. Learn more at www.blackduck.com.

SOURCE Black Duck Software

For further information: Liz Samet, Black Duck, 336.414.6753, esamet@blackduck.com

---

https://news.blackduck.com/2025-10-08-Black-Duck-Research-Highlights-Growing-Security-Debt-as-Development-Teams-Accelerate-with-AI