Black Duck Newsroom

AI Coding Hits 97% Enterprise Adoption; New Black Duck Study Shows Governance Is the ROI Multiplier

Survey findings reveal organizations that fail to operationalize AI across the entire SDLC will fall short of expected productivity gains

BURLINGTON, Mass., June 9, 2026 /PRNewswire/ -- Black Duck®, the leader in AI-powered application security, today released *The State of AI-Powered Software Development* report revealing that while AI coding tools consistently improve productivity, they also introduce bottlenecks elsewhere in the SDLC, particularly around security, code review, and governance.

A survey of 800+ enterprise software engineers and DevOps professionals was conducted in partnership with independent research firm UserEvidence. The findings uncover that software development is at an inflection point: AI coding assistants have achieved near-total adoption (97%) and deliver measurable productivity gains but widening governance deficits and accelerating security risks are emerging as the defining operational challenges of AI-powered development.

Key findings include:

The Governance Gap Is the Industry's Most Urgent Problem. If there is a single finding that defines the current state of AI-powered development, it is that organizations have raced to adopt AI coding tools, but governance processes have not kept pace.

Two-thirds of developers (68%) say it is extremely important to have a clear, automated system for tracking AI-generated code and measuring its impact for debugging, security, and accountability. Yet fewer than one-third of teams (30%) have full governance in place for AI coding assistant adoption and oversight.

The ROI case for closing this gap is compelling: teams with full governance in place are 55% more likely to report a major improvement in efficiency. Governance, in other words, is not a compliance checkbox, it is a direct ROI multiplier.

Efficiency Gains Mask Growing Operational Risk. AI coding assistants deliver measurable results: 92% of development teams report improved productivity and release velocity, with 58% citing a major improvement. Developers reclaim an average of eight hours per week, and more than half of respondents (53%) have grown total code volume by over 25%.

But the gains carry a cost. Nearly 90% of teams encounter issues with AI-generated code, with bottlenecks emerging in manual review (52%), security testing (51%), and code rework (48%). Rather than reducing overall effort, AI shifts it, redistributing workload from code creation to validation, testing, and remediation stages of the pipeline.

Security Concerns Are Rising in Lockstep with AI Usage. Nearly two-thirds of development teams (64%) express moderate or extreme concern about AI coding assistants introducing security defects or vulnerabilities. Those with the highest level of concern tend to be among the heaviest AI users, with 51% of this subgroup relying

on AI coding assistants for most new development.

As code generation accelerates and code volume scales, the attack surface expands, and manual security processes are failing to keep pace.

Human Oversight Is Still Essential. Industry response to this challenge is already taking shape. An overwhelming 86% of respondents believe an AI agent or model should evaluate AI-generated code. More specifically, 56% would prefer a dedicated AI security agent separate from the code-generation tool itself, while 30% believe the same AI model that generated the code should also review it for security issues. Even so, 84% of developers prefer to keep a human in the loop via pull requests or real-time IDE suggestions, preserving human oversight as a critical check in the AI-assisted SDLC.

The Developer Role Isn't Disappearing, It's Evolving. As AI takes on a greater share of code production, the nature of developer work is shifting. Respondents anticipate that developers will spend significantly more time in three key areas: reviewing and validating AI-generated code (29%), complex architecture and system design (29%), and security verification and risk management (23%).

This shift signals the next step toward a fully agentic SDLC, one where AI autonomously performs application security testing that adapts to threats at machine speed.

"AI coding assistants have permanently changed the economics of software development, and the productivity numbers make that undeniable," said Jason Schmitt, CEO at Black Duck. "But the data also clearly shows that speed without governance is a liability, not an advantage. As AI-generated code volume and expectations increase, the winners with AI are the ones building automated security and governance guardrails that scale alongside their development velocity."

About the Research

Black Duck partnered with independent research firm UserEvidence to survey 831 enterprise software engineers and DevOps professionals at organizations with 500+ employees. The study was conducted in March 2026 across a range of industries, with a majority representing technology and SaaS organizations.

To learn more, download *The State of AI-Powered Software Development*.

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: LizSamet, Black Duck, 336.414.6753, esamet@blackduck.com

https://news.blackduck.com/2026-06-09-AI-Coding-Hits-97-Enterprise-Adoption-New-Black-Duck-Study-Shows-Governance-Is-the-ROI-Multiplier?cmp=pr-sig