Black Duck Newsroom

Black Duck Report Reveals Software Supply Chains Vulnerable as AI Adoption Outpaces Security

While 95% of surveyed organizations reported using AI tools in software development, only 24% have adopted comprehensive strategies to secure AI-generated code

BURLINGTON, Mass., Dec. 17, 2025 /PRNewswire/ -- Black Duck®, the leader in AI-powered application security, today announced the release of a new report, "Navigating Software Supply Chain Risk in a Rapid-Release World." The findings uncover a discrepancy between AI adoption and unprotected code, resulting in organizations having a widening risk gap.

The study, conducted by UserEvidence, is based on a survey of 540 software security leaders and practitioners. The report highlights a critical disconnect: while 95% of organizations are leveraging AI tools for software development, a mere 24% are implementing comprehensive intellectual property, license, security, and quality evaluations for AI-generated code. This oversight exposes the software supply chain to potentially severe and unaddressed risks.

Key Findings from the Report Include:

- **AI Adoption Outpaces Security:** Most organizations are embracing AI in development, yet robust security protocols for AI-generated code are largely absent, creating new attack vectors. Although 76% of respondents check AI code for security risks, only 24% perform IP, license, security, and quality evaluations for AI-generated code.

- **Dependency Management is Key to Preparedness:** Organizations highly effective at tracking and managing open source dependencies are significantly more prepared (85%) to secure open source software compared to the overall average (57%).

- **Automation Drives Faster Remediation:** Of the respondents that perform automatic continuous monitoring, 60% report remediating critical software vulnerabilities within a day. In contrast, only 45% of the full respondent pool say they remediate critical software vulnerabilities within a day showing that organizations that haven't implemented automatic continuous monitoring are at a clear disadvantage for protecting the software supply chain.

- **SBOM Validation Enhances Third-Party Security**: Validating Software Bills of Materials (SBOMs) from external suppliers dramatically improves an organization's ability to evaluate third-party software and respond to critical vulnerabilities. Of the respondents that prioritize SBOM validation, 63% of those that always validate SBOMs say they're highly prepared to evaluate third-party software; and 59% typically respond to critical software vulnerabilities within one day.

- **Compliance Controls Boost Efficiency:** Organizations with more compliance controls in place demonstrate greater efficiency in remediating critical software vulnerabilities. Of the respondents that use at least three compliance controls, 49% remediate critical vulnerabilities within a day. This percentage jumps to

54% for the respondents that use at least four compliance controls. Additionally, 35% of respondents cite interpreting and operationalizing complex regulatory requirements as their biggest challenge.

"We're in a new era of rapid software innovation, fueled by AI, but these findings reveal a critical challenge: security isn't keeping pace," said Jason Schmitt, CEO at Black Duck. "It's imperative that organizations prioritize robust security frameworks, with a sharp focus on AI-generated code and meticulous dependency management, to build truly resilient software supply chains."

The report emphasizes that a resilient software supply chain extends beyond mere compliance, enabling organizations to proactively address vulnerabilities, minimize downtime, prevent data breaches, and ultimately improve developer productivity and increase development velocity.

For more information, download your copy of the "Navigating Software Supply Chain Risk in a Rapid-Release World" report and read our blog post.

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.

Correction:*Update to the report links in the first paragraph and paragraph above the boilerplate.*

SOURCE Black Duck Software

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

---

https://news.blackduck.com/2025-12-17-Black-Duck-Report-Reveals-Software-Supply-Chains-Vulnerable-as-AI-Adoption-Outpaces-Security