Black Duck Newsroom

Black Duck Releases BSIMM16 Revealing AI and Regulatory Compliance Reshaping Application Security Processes

The industry's largest application security study shows organizations adapting to AI-generated code, government mandates, and evolving training methods

BURLINGTON, Mass., Feb. 4, 2026 /PRNewswire/ -- Black Duck®, the leader in AI-powered application security, today announced the release of BSIMM16, the 16th edition of the Building Security In Maturity Model (BSIMM), revealing how organizations worldwide are transforming their software security initiatives (SSIs) to manage risk introduced by AI adoption, increasing regulatory pressures, and the need for more agile security training approaches. For the first time in BSIMM's 16-year history, AI has overtaken all other forces in reshaping security priorities.

The comprehensive study is based on assessments of 111 organizations across multiple industry verticals including financial services, healthcare, technology, and independent software vendors (ISVs). The report provides unprecedented insights into real-world application security practices protecting approximately 91,200 applications developed by 223,700 developers.

The BSIMM16 study reveals several key trends and insights, including:

- **AI is now the defining challenge in application security.** Organizations are simultaneously securing AI-powered coding assistants and defending against AI-enabled attacks. BSIMM16 highlights three major shifts: a 10% rise in teams using attack intelligence to track emerging AI vulnerabilities; a 12% increase in using risk-ranking methods to determine where LLM-generated code is safe to deploy; and a 10% uptick in applying custom rules to automated code review tools to catch issues unique to AI-generated code.

- **Government regulations are accelerating major security investments.** Global mandates are pushing organizations to strengthen application security, with a sharp focus on software supply chain transparency and securing development environments. Nearly 30% more organizations are now producing SBOMs to meet transparency requirements. BSIMM16 also reports a 50%+ surge in automated verification of infrastructure security and more than 40% growth in streamlining responsible vulnerability disclosure—driven by the EU Cyber Resilience Act and evolving U.S. government demands.

- **Software supply chain security is rapidly rising in importance.** Organizations are expanding their focus beyond internally developed code to secure the entire software supply chain ecosystem. In addition to the significant increase in SBOM adoption for deployed software, BSIMM16 observes more than a 40% rise in establishing standardized technology stacks—clear signs that supply chain security is becoming a core priority.

- **Application security training is undergoing a major shift.** Traditional multi-day security courses are being replaced by just-in-time, bite-sized learning that fits modern development workflows and learner preferences. BSIMM16 reports a 29% increase in organizations delivering expertise through open collaboration channels, giving teams instant access to security guidance. Notably, after years of decline, traditional awareness

training is beginning to rebound.

"The real risk of AI-generated code isn't obvious breakage—it's the illusion of correctness. Code that looks polished and professional can still conceal serious security flaws," said Jason Schmitt, CEO of Black Duck. "We're witnessing a dangerous paradox: developers increasingly trust AI-produced code that lacks the security instincts of seasoned experts. That's why the surge in SBOM adoption reported in BSIMM16 is so critical, since it gives organizations the transparency to understand exactly what's in their software—whether written by humans, AI, or third parties—and the visibility to respond quickly when vulnerabilities surface. As regulatory mandates expand, SBOMs are moving beyond compliance—they're becoming foundational infrastructure for managing risk in an AI-driven development landscape."

Established in 2008, BSIMM is a maturity model that tracks the activities of software security professionals. It helps organizations plan, execute, and measure their software security initiatives. BSIMM data is collected through comprehensive interviews conducted during assessments by security professionals, after which the anonymized data is analyzed to identify trends in software security practices.

For the first time in its history, BSIMM16 introduces no changes to the framework structure, signaling the maturity and stability of application security practices across the industry.

To learn more, download the BSIMM16 report and read the detailed blog post.

Acknowledgements
Black Duck would like to thank Jamie Boote, Ben Hutchison, Mike Lyman, and Sam Schueller, authors of the BSIMM16. Additional thanks to the nearly 170 individuals who helped gather the data for the BSIMM data pool, along with the 111 executives from the SSIs we studied to create BSIMM16.

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/2026-02-04-Black-Duck-Releases-BSIMM16-Revealing-AI-and-Regulatory-Compliance-Reshaping-Application-Security-Processes