Black Duck Newsroom

Black Duck Signal Sets a New Standard for Securing AI-Generated Code

Powered by ContextAI, Signal delivers the only AI code security solution driven by over 20 years of collected security intelligence

BURLINGTON, Mass., March 23, 2026 /PRNewswire/ -- Black Duck®, the leader in AI-powered application security, today announced the general availability of Black Duck Signal™, an agentic AI application security solution purpose-built to secure AI-generated code in autonomous development workflows.

As agentic AI coding assistants increasingly design, code and deliver production software, organizations face a new class of application risk—created at unprecedented speed and scale. Black Duck Signal is designed to meet this shift head-on, delivering AI-native security that intelligently assesses risk, validates findings and automates remediation at AI speed.

Signal introduces a new model for application security: agentic AI augmented by decades of human-curated security context. Delivered as an agentic AI solution, Signal enlists a coordinated system of specialized AI security agents that draw on ContextAI™, Black Duck's application security model, to analyze code, assess impact and guide remediation actions in real time. By leveraging ContextAI, Signal delivers Black Duck's vast security expertise and experience as context to security decisions that solutions built solely on general purpose AI cannot provide.

"AI is no longer just accelerating development—it's actively authoring software," said Jason Schmitt, CEO of Black Duck. "Signal unlocks AI-driven development by removing risk and bringing intelligence, determinism and governance to that reality."

Security Built for a New Era of Software Development

Black Duck Signal integrates directly into the modern agentic software development life cycle, via model context protocol (MCP) and APIs that support AI coding assistants, IDEs and automated AI pipelines. It continuously analyzes code across languages, frameworks and architectures—identifying security defects early, eliminating the noise common with AST findings and intelligently working with AI coding assistants to fix issues with little to no developer action required.

Signal is designed to complement existing application security testing activities by natively supporting agentic AI workflows, where traditional application security testing tools may lack the agility, speed or contextual awareness required to keep pace with AI.

Agentic AI Security That Reasons, Validates and Acts

Signal is built on an agentic AI architecture that goes beyond single-model analysis. Multiple specialized agents and models work together to analyze vulnerabilities, validate exploitability, prioritize risk and recommend or apply fixes using human-like logic—delivering more reliable outcomes across the software development life cycle.

This approach enables Signal to actively address high-impact and complex vulnerabilities, including those based on business logic errors or in languages not supported by traditional AST tools. Signal also goes beyond simple

text matching of code patterns associated with other LLM-assisted security analysis tools by using multiple forms of component, signature, snippet and other analysis techniques to accurately match artifacts with security context in real-time.

ContextAI: The Model for Building Secure Software

At its core, Signal analysis is differentiated by its use of ContextAI, Black Duck's purpose-built application security model containing petabytes of human validated security intelligence. ContextAI provides deep, real-world context—grounded in decades of application security expertise—so Signal's agents can assess risk and remediation actions with higher accuracy and precision.

By combining LLM reasoning with ContextAI's security intelligence, Signal delivers higher-fidelity analysis and action than solutions built on generally trained AI models alone—reducing false positives and increasing confidence in automated security decisions.

Governance That Unlocks the True Potential of AI

AI is fundamentally transforming the way software is built. But as organizations seek to tap into the tremendous potential of AI, they can find that the load of managing security defects can dramatically limit their ability to realize the gains. Black Duck Signal unlocks this potential by enabling enterprises to govern AI-generated software responsibly and at AI scale, helping them move faster with AI while maintaining security, compliance and trust across the application life cycle.

Black Duck Signal is now generally available and will be showcased May 23–26 at the RSA Conference in San Francisco at the Black Duck booth, #1027 South Hall.

Watch the Black Duck Signal demo video to learn more about AI-driven security for modern development teams.

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/2026-03-23-Black-Duck-Signal-Sets-a-New-Standard-for-Securing-AI-Generated-Code