

Black Duck Launches Signal Agentic Fix: Vulnerability Remediation at the Speed of AI-Driven Attacks

Newest Signal AI agent fixes software and supply chain vulnerabilities at machine speed while ensuring developers maintain control of what changes go into their code

BURLINGTON, Mass., Oct. 27, 2026 /PRNewswire/ -- [Black Duck®](#), the leader in application security for the AI era, today announced [Signal Agentic Fix](#), the newest agent in Black Duck Signal™. Signal is a collection of AI agents built to minimize the human workflow bottlenecks that prevent teams from securing their software fast enough to keep pace with the dramatic, AI-driven increase in vulnerabilities and exploits. Signal Agentic Fix combines Black Duck's market-leading deterministic static analysis (SAST) and software composition analysis (SCA) engines with AI-driven triage, fix generation and validation, and submits every change for human review before it is merged.

Signal Agentic Fix counters two pressures intensified by the rapid adoption of AI across software development. The first is a growing backlog of vulnerabilities, driven by the surge in AI-generated code, the higher vulnerability rates in that code, and a flood of new supply chain CVEs. The second is a collapsing time to exploit: attackers use AI to chain and weaponize vulnerabilities in hours, while human-led remediation is still measured in days or even weeks.

"The differentiator is not that AI can write a fix; it's whether you can trust it," said Dipto Chakravarty, Chief Product & Technology Officer at Black Duck. "A harness that pairs deterministic static and software composition analysis with AI-powered triage, fix generation, and validation, plus human-defined guardrails and approval gates is what makes agentic remediation something enterprises can actually trust and deploy."

Closing the loop: scan, triage, fix, validate, submit

Signal Agentic Fix automates the end-to-end remediation workflow that would otherwise be constrained by a team's available headcount and expertise:

- **Scan:** Uses Black Duck's deterministic SAST and SCA engines to identify defects in proprietary code and open source dependencies at scale – reliably and cost-effectively.
- **Triage:** Applies AI to assess severity, reachability and exploitability, filtering out false positives and prioritizing the issues that present the greatest risk.
- **Fix:** Generates code fixes for SAST findings using AI, and dependency upgrade fixes for SCA findings using remediation guidance from Black Duck Security Advisories, informed by ContextAI™.
- **Validate:** Re-scans the fixed code and, optionally, runs customer-defined compliance checks and functional tests to confirm that fixes introduce no new defects or vulnerabilities.
- **Submit:** Routes every change to a human for review and approval, either through the developer's AI coding agent or as a pull request in the team's source control system. Developers remain in complete control of

what goes into their code.

The result is higher remediation throughput and a sharply reduced window of exposure between the discovery of a vulnerability and the delivery of a validated fix.

Two ways to deploy: with AI coding agents, or in the DevOps pipeline

Signal Agentic Fix for Coding Agents: works as a security collaborator alongside the developer and their AI coding agent, such as Claude Code. It initiates SAST and SCA scans on new or existing code, triages and prioritizes findings, and reports issues and fix guidance back to the coding agent, which implements the fix. Signal Agentic Fix then re-scans to validate the result. Because the fix is delegated to the coding agent, it is governed by the same hooks and skills the team already uses for code generation, and the developer approves or rejects each change before it is applied.

Signal Agentic Fix for DevOps Pipelines: integrates with existing SCM and CI workflows, triggering the same remediation loop on events such as commits and builds, or on demand through a user interface. Fixes are generated using a configured LLM, validated, and submitted as an SCM pull request for team review and approval before merging.

Built-in guardrails keep teams in control

Organizations using Signal Agentic Fix do not have to choose between machine-speed remediation and the governance required in regulated and safety-critical industries:

- **Configurable remediation rules** define what the agent is allowed or required to fix, and how, at the project or organization level.
- **Configurable validation rules** let teams supply coding and compliance standards, additional context and test suites that every generated fix must satisfy.
- **Human-in-the-loop approval** ensures no change reaches the codebase without explicit developer or team sign-off.

Built on proven Black Duck technology

Unlike solutions that rely on AI alone, Signal Agentic Fix brings together market-leading Black Duck capabilities into a single agentic harness purpose-built for fast, reliable and validated remediation:

- The same deterministic SAST and SCA engines that power Black Duck Polaris®, Coverity® and Black Duck SCA, delivering the speed and economics required for enterprise scale.
- AI SAST Triage and AI SCA Reachability Analysis, introduced earlier this year, which prioritize findings by severity and exploitability and identify reachable open source vulnerabilities across any programming language.
- AI Fix Pull Requests, also introduced earlier this year, which generate and submit fixes for SAST and SCA issues.

- ContextAI, with more than 20 years of curated application security context that improves the accuracy and reliability of LLM-based analysis and remediation.

Availability

Signal Agentic Fix for Claude Code is available in Early Access today, with additional coding agent and DevOps pipeline integrations across Polaris, Coverity and Black Duck SCA delivering in the coming weeks.

For more information, visit our [website](#), read our [blog post](#), or register for one of our upcoming webinars in [North America](#), [EMEA](#), [APAC](#).

About Black Duck

Black Duck® is application security for the AI era. Our approach is hybrid by design. Deterministic analysis delivers verifiable results and serves as the system of record for governance, while AI-powered reasoning prioritizes what's exploitable and agentic remediation fixes it at machine speed — so your team ships as fast as AI writes code, without inheriting the risk that comes with it. Trusted by thousands of organizations in many of the world's most demanding industries, including aerospace, defense, automotive, semiconductor, and healthcare, and backed by more than 20 years of human-verified vulnerability intelligence. Learn more at blackduck.com.

SOURCE Black Duck Software

For further information: Mark Van Elderen, Black Duck, 650.793.7450, mvanelde@blackduck.com

<https://news.blackduck.com/2026-10-27-Black-Duck-Launches-Signal-Agentic-Fix-Vulnerability-Remediation-at-the-Speed-of-AI-Driven-Attacks>