The platform that found critical vulnerability in Anthropic Claude Code Phoenix Security - Purple an Agentic code scan

Graph-native platform integrates with AI coding agents and reports a modeled 10–33x reduction in token-scanning costs

HOW Phoenix Security KNGraph Launch - Cybersecurity AI security ASPM Vulnerability managment

LONDON, LONDON, UNITED KINGDOM, July 28, 2026 /EINPresswire.com/ -- Phoenix Security today announced the general availability of Phoenix Purple, an application security platform designed to analyze code produced by AI coding agents. According to the company, the platform integrates directly with AI coding assistants, uses graph-based code intelligence to reduce scanning token cost by a modeled factor of 10 to 33 times compared with file-by-file approaches, and delivers remediations as pull requests. The release extends Phoenix Orange, the company's existing Application Security Posture Management (ASPM) platform.

The launch addresses a shift in how software is written. AI coding agents now generate a significant share of new code and open pull requests at high volume, frequently introducing third-party dependencies that receive limited human review. Industry data indicates that the interval between vulnerability disclosure and active exploitation has narrowed to a matter of days, increasing pressure on security teams to identify and remediate issues earlier in the development process.

Token consumption has emerged as a practical constraint for organizations adopting AI-based security scanning. A number of open-source projects have appeared that use large language models to identify vulnerabilities, but the operational cost of running frontier models across

entire codebases has drawn scrutiny. Phoenix Security positions Phoenix Purple as an approach that reduces that cost by using a knowledge graph to direct analysis, so that the language model evaluates only the code paths identified as relevant rather than re-reading an entire repository on each scan.
Company statement

IDC Market Scape ASPM 2025

Platform capabilities
Integration with developer tools. The Purplephx integration supports Cursor, VS Code, Claude Code, and Windsurf. A GitHub application performs pull-request scanning without continuous-integration configuration, surfacing findings as inline comments that describe the issue, its relevance, and a proposed fix. A Model Context Protocol (MCP) server integration makes the knowledge graph queryable from the coding agent.
Graph-native scanning. The platform constructs a knowledge graph once, parsing seven programming languages and mapping call graphs, taint traces, entry points, and reachable paths, then navigates that graph on subsequent scans. In a scenario modeled by the company on a 1,000-repository fleet of 250,000 lines each, scanned monthly, graph-native scanning was calculated at $3.60 per confirmed vulnerability compared with $64.30 for a file-by-file approach on the same model, approximately 87 percent lower for equivalent findings. The company notes these figures are modeled and provides a public cost calculator.

> Back when I led security engineering, I wanted remediation for true positives delivered straight to engineers. Phoenix Purple makes that real, without breaking the token bank”
>
> *Francesco Cipollone*

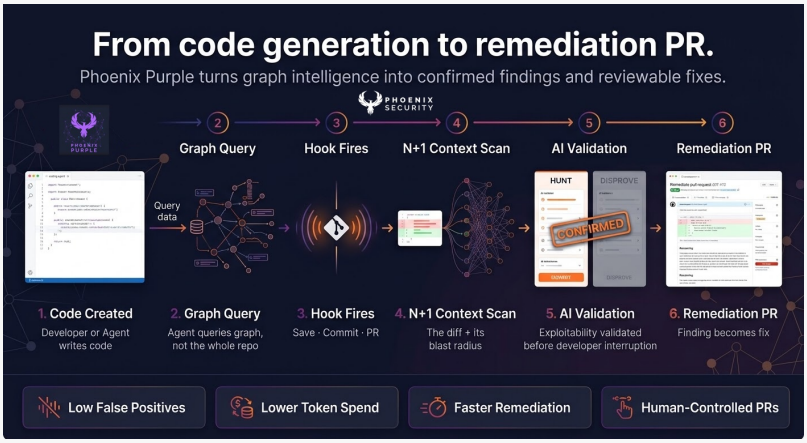
Pull-request and multi-repository analysis. Each pull-request change is analyzed against the graph, including call-graph neighbors affected by, but not directly modified in, the change — an approach the company describes as N+1 contextual analysis. Across multiple repositories, a vulnerability in a shared library is attributed to each repository that imports it, with reachability assessed per repository and findings routed to the owning team.

Remediation delivery. Findings are ranked using reachability, threat intelligence, fixability, ability to chain and combine into an exploit, weaponization signal, and business context. Confirmed

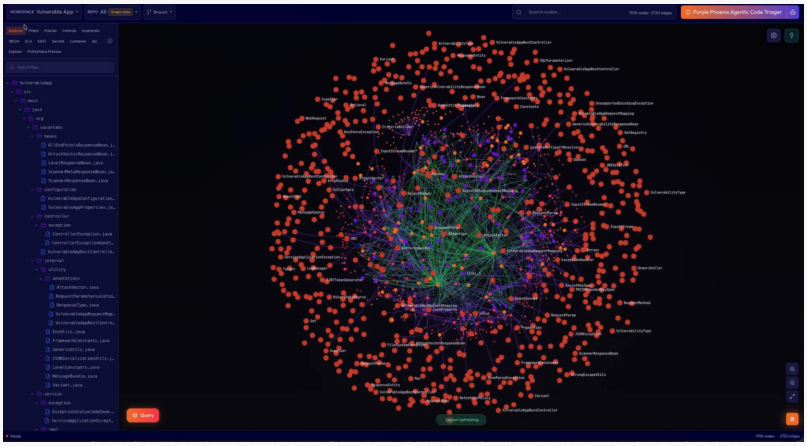
findings are delivered as pull requests containing threat context, with a risk tier that determines the review path. Changes classified as breaking or high-risk require explicit human approval before merging, and no change is merged automatically.
Relationship to existing platform

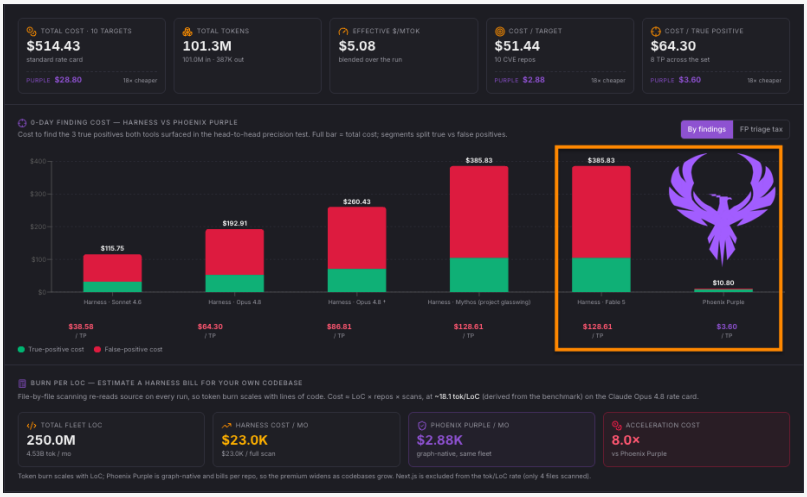
Phoenix Orange, the company's ASPM platform, aggregates findings from multiple scanners into a single queue, filters unreachable findings, attributes issues to owning teams, and connects code-level findings to the cloud services where the code runs. The company reports the platform is in production at ClearBank, Bazaarvoice, and Integral Ad Science (IAS). According to Phoenix Security, deployments have delivered a 98 percent reduction in container vulnerabilities at ClearBank, $6.3 million in developer time saved at Bazaarvoice, and a 78 percent reduction in active container vulnerabilities together with $1.95 million saved at IAS. Phoenix Purple extends this platform to the code-generation stage of the development lifecycle.

Phil Moroni
Phoenix Security
+1 919-594-8888
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
X



HOW Phoenix Security KNGraph Scanner Works - Cybersecurity AI security ASPM Vulnerability managment


Phoenix Purple KNGraph Agentic Code Scanner



Phoenix Purple Token Saving Cost