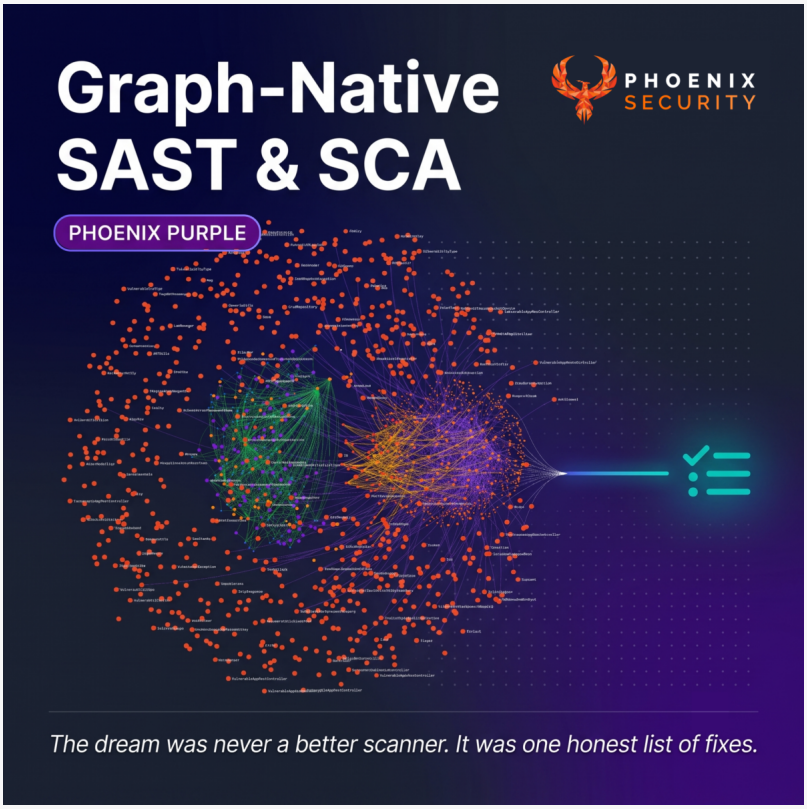
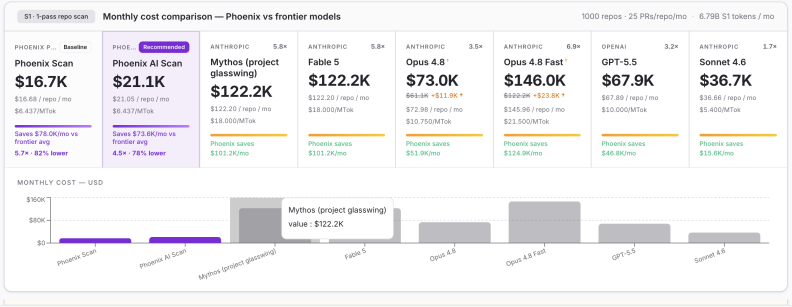
Remediation or Vulnerabilities Phoenix Purple adds Graph-Native SAST and SCA - One-Click Assessment and Remediation

Deterministic scanning correlated on a knowledge graph turns thousands of isolated findings into a single ranked remediation plan



Phoenix Security ASPM AST, Security Scan, Agentic, AI



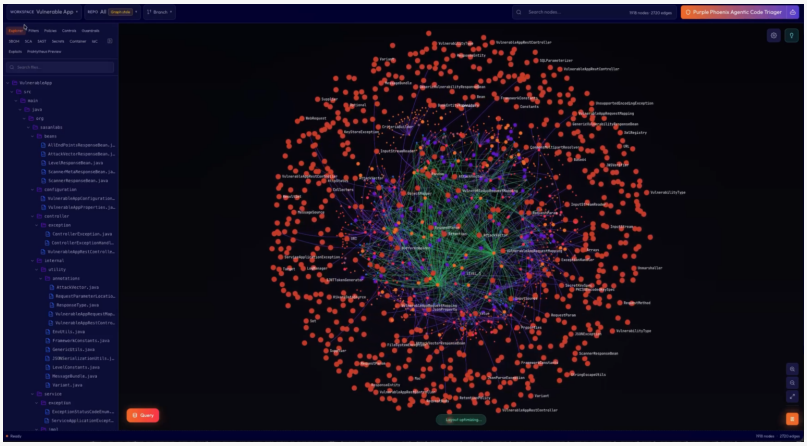
Cost of Remediaiton and Cost of Scan

LONDON, UNITED KINGDOM, July 28, 2026 /EINPresswire.com/ -- Phoenix Security today launched graph-native SAST and SCA in Phoenix Purple, its agentic code analysis platform, adding one-click assessment and one-click remediation that convert fragmented scanner output into a single, ranked, actionable remediation plan. The release merges traditional deterministic, rule-based scanning with knowledge-graph correlation — so security and engineering teams can see not just what is vulnerable, but which findings are reachable, how they chain into real exploit paths, and whether each fix is a breaking change before it ships.

Application security teams have run static and dependency scanners for years and arrived at the same outcome: a long, flat list of findings with no shared context. Static analysis runs in one pass, dependency analysis in another, each blind to the other. The result is thousands of findings and no reliable way to know which ones

matter. In an environment where the interval between disclosure and exploitation is now measured in hours, that lack of context carries real operational cost.

Phoenix Purple addresses the gap by running deterministic SAST and SCA against a continuously rebuilt knowledge graph that correlates every finding across code and dependencies.



Phoenix Purple KNGraph Agentic Code Scanner

What is available

Graph-native SAST. Static code analysis runs against the knowledge graph rather than file by file. Because the graph resolves call paths, taint flow, and entry points, analysis follows the reachable path through the code instead of matching a pattern in isolation. Teams select the ruleset appropriate to their language.

> My engineering team never asked me about correlation or deduplication, or whether a finding was one CWE or another. They asked which issues to fix, Phoenix Purple answers with a single ranked plan”
>
> *Francesco Cipolone*

SCA with reachability and four scan modes. Software composition analysis is summarized per library, with associated CVEs and affected code surfaced against each dependency. Reachability analysis identifies which vulnerable libraries are actually reachable in running code and deprioritizes those that are not. Four scan modes — quick, full, smart, and deep — let teams choose analysis depth, with quick and full serving as the everyday defaults.

Chainability map. Phoenix correlates findings across code and libraries and ranks them by complexity, chainability, and exploitability, showing which combinations of vulnerabilities can be used together to deliver an attack — for example, whether a remote code execution can lead into a buffer overflow and chain into a working exploit.

One-click assessment. A single action evaluates whether a finding is real, whether it is reachable, and whether it can be chained into an active exploit, returning an exploitability ranking and a breaking-change verdict across clear tiers: simple to execute, potentially breaking, definitely breaking, or unknown.

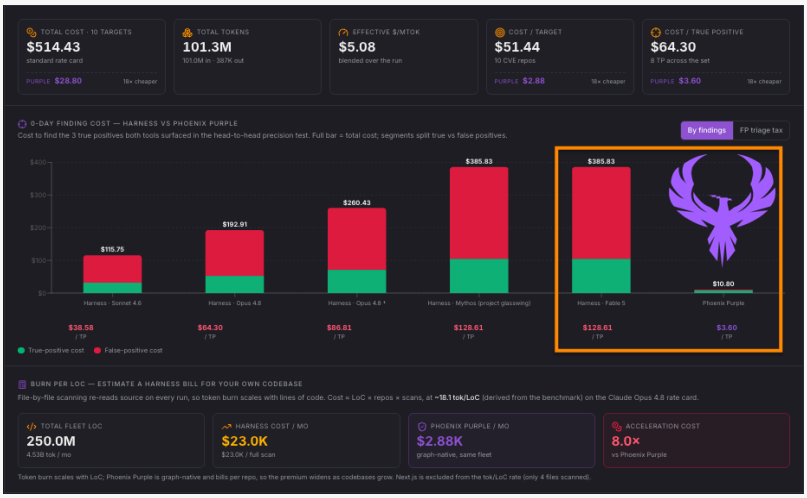
One-click remediation. Remediation produces a plan rather than a ticket: Phoenix determines affected files, bundles related fixes, identifies available compensating controls, and delivers the fix as a pull request with the reasoning included. Fixes are broken down by simplicity so teams can schedule them by effort, and breaking changes are held for human approval. Nothing

merges without review.

Every capability runs on a continuously rebuilt knowledge graph, keeping token consumption to a minimum: the model navigates the graph to reason rather than re-reading the codebase to reconstruct context on each run. Modeled cost comparisons are available at ai-scan-cost.phoenix.security.
Executive perspective

Availability
Graph-native SAST and SCA, with reachability, the chainability map, one-click assessment, and one-click remediation, are available in general availability in Phoenix Purple. Additional capabilities are shipping through the Phoenix Purple launch campaign over the following weeks. The control framework white paper will be released at black hat. Cost modeling is available at .

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



Phoenix Purple Token Saving Cost