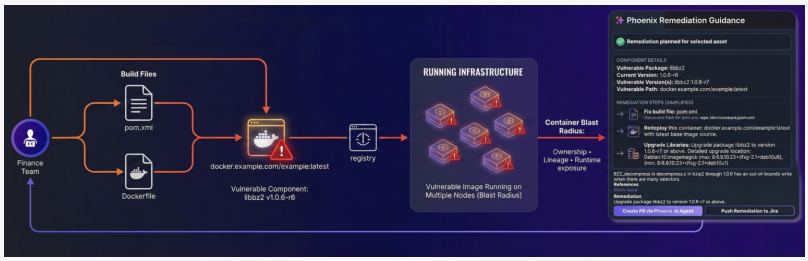
Phoenix Security Launches AI-Powered Remediation Engine Surgical Container to Code Fixes Without Deploying software

Actionable ASM and ASPM platform delivers AI container vulnerability remediation with 91% reduction of false positives



Phoenix Security Container Remediation

NEW YORK, NY, UNITED STATES, March 10, 2026 /EINPresswire.com/ -- Actionable ASM and ASPM platform delivers agentless container vulnerability remediation in line with CTEM principle, correlating base image lineage to build files — reducing SCA container noise by up to 91% and resolving critical findings with one click

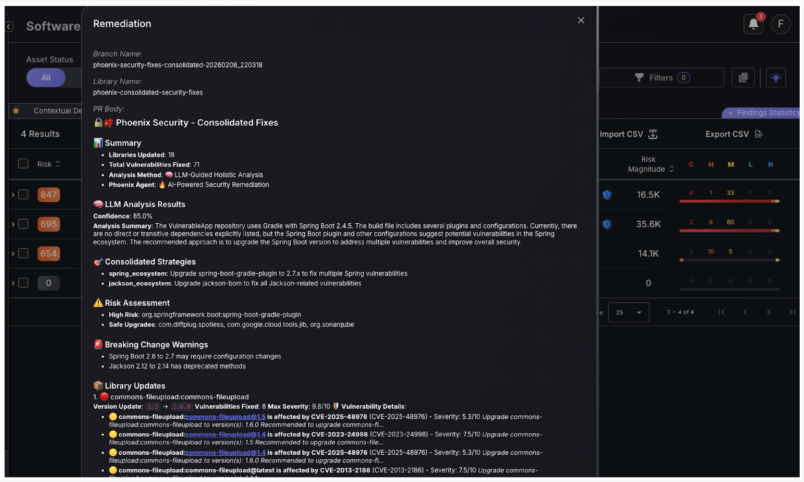
> Engineers don't have time to look at 300 vulnerabilities. They have time to look at one remedy. The era of the security team pushing vulnerability is over. Phoenix Security gives you this power"
>
> *Francesco Cipollone CEO & Co-Founder Phoenix Security*

Phoenix Security, the Actionable Attack Surface Management (ASM) platform following CTEM methodologies, today announced the general availability of its AI-powered Remediation Engine — a purpose-built capability that takes vulnerability management from alert reporting to agentic fix delivery. The release closes the loop on the full code-to-cloud security lifecycle: identifying what is reachable, correlating container findings to their source build files, and generating surgical remediation paths that engineers and AI agents can act on immediately — without requiring any container-side agent deployment.

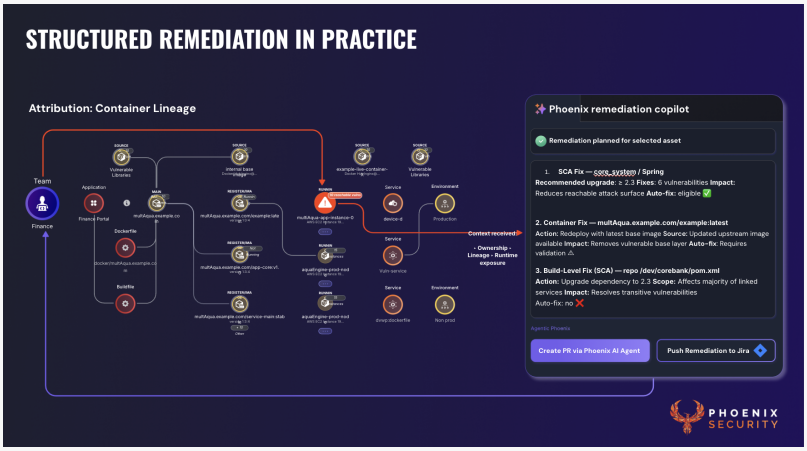
The Remediation Engine addresses one of the hardest unsolved problems in vulnerability management: knowing not just what is vulnerable, but exactly what to fix, in which file, by which team — without drowning engineers in noise or burning tokens on context-blind LLM calls.

Proven Outcomes Across Production Environments
98% container vulnerability reduction -ClearBank
96–99% critical reduction - ClearBank

94% container vulnerability reduction - Bazaarvoice
78% container vulnerability reduction - AD-Tech client
91% total noise reduction



SCA remediating Auto PR



Code to Container Remediation ASPM

From Alert Overload to a Single Actionable Remedy
Security teams and engineers operate in environments where scanners surface hundreds of container vulnerabilities per application — many flagged as critical, most irrelevant to what is actually running. The standard response is to hand that list to an AI agent and hope for the best. The result: wrong library versions upgraded, non-running containers patched, build pipelines broken, and security budgets consumed by LLM token costs with no reduction in real exposure.
Phoenix Security's Remediation Engine changes the calculus. Before a single fix is proposed, the platform traces each vulnerability through a full lineage graph: from the running container, back through the registry image, to the base image or build file where the issue originates. Only then does the platform generate a remedy — the minimum version increment that closes the most findings, mapped to the correct file, owned by the correct team.

Agentless Container Remediation: No Deployment Tax
Deploying security agents inside containers creates real operational friction — increased image size, modified runtime behavior, pipeline complexity, and compliance review overhead. Phoenix Security eliminates that entirely.
The Remediation Engine performs full container-to-build-file correlation without touching the running environment. It:
Maps each container image to its base image and originating build file (Dockerfile or build manifest)
Identifies whether the vulnerability lives in the base image layer or in application-layer dependencies within the container
Determines whether the container is active and externally reachable before assigning remediation priority
Proposes fixes at the correct layer — base image upgrade, build file patch, or SCA library update

— with breaking-change analysis included
Teams receive a single, ranked list of remedies. Not a vulnerability list. Not a scanner export. A fixed path.

AI Fix: Precision Remediation for Code and Container
Phoenix Security's agentic Remediator takes that remedy list and delivers executable fixes — directly to GitHub or the team's ticketing workflow. One click opens a pull request with the precise version increment, change rationale, and impact scope. No broad context windows. No speculative upgrades. No token waste.

The agent chain operates in three stages:
Researcher — maps vulnerabilities to threat actors, active exploit campaigns, MITRE ATT&CK techniques, and exploit typologies, enabling shift-left prioritization grounded in real threat intelligence
Analyzer — performs code-to-cloud reachability analysis, correlates container lineage, and scores each vulnerability against the 4D risk formula (exploitability + business criticality + deployment context + reachability)
Remediator — generates the minimum-viable fix, validates against breaking changes, and delivers a GitHub PR or Jira ticket with full traceability
Humans stay in control throughout. Engineers review, approve, and merge. Every fix is traceable to the source finding. AI accelerates the path — it does not replace the decision.

Gartner ASM ASPM Voice of the customer Phoenix Security

Threat Intelligence Already in Production: The Researcher Agent

Customers across fintech, retail, and ad-tech are already using Phoenix's Researcher agent to map their vulnerability backlog to active threat campaigns. Where traditional ASPM platforms surface a CVE score, Phoenix surfaces the attack chain — which threat actor groups are exploiting this library, which attack typology applies, and which findings in the backlog represent active exposure rather than theoretical risk.

This intelligence feeds directly into the Remediation Engine. Findings tied to active exploit campaigns are prioritized higher. Remediations are batched to close the highest-impact exposure chains first — not just the highest CVSS score.

Executive Perspective

“Engineers don’t have time to look at 300 vulnerabilities. They have time to look at one remedy. Phoenix gives them exactly that—the single fix that closes the most risk, at the right layer, in the right file, for the right team. We built the Researcher to map the threat. We built the Analyzer to find the reachable risk. And we built the Remediator to close it—surgically, without destroying your pipeline or your budget.”

— Francesco Cipollone, CEO & Co-Founder, Phoenix Security

Customer Results: Reduction at Scale

ClearBank — Fintech

98% reduction in container vulnerabilities; critical findings reduced to single digits

96–99% reduction in critical-severity container exposure

Millions saved in remediation costs; 4 hours per week reclaimed per engineer

“Phoenix helped us move from noise to precision. We now focus on what truly matters — and fix faster than ever before.”

— Neil Reed, Principal AppSec Engineer, ClearBank

Bazaarvoice — Retail Commerce

94% reduction in container vulnerabilities; one team reached zero criticals within one month

40% reduction in high-risk findings within two weeks of deployment

“We didn’t just improve visibility — we eliminated criticals. Phoenix made that operationally possible in days, not months.”

— Nate Sanders, Senior Manager, Security Engineering & Operations, Bazaarvoice

Ad-Tech client

78% reduction in active container vulnerabilities

82.4% reduction in SCA-to-container noise

“Phoenix gave us the missing bridge between code and cloud. The visibility is deep, the actions are clear — and the results speak for themselves.”

Availability

The Phoenix Security Remediation Engine is available now to all Phoenix Security customers. One-click GitHub PR generation, Jira integration, and Remediation Campaign workflows are included at no additional tier. Existing customers can access the Remedies view directly within the Phoenix platform dashboard.

Organizations evaluating ASPM, CTEM, or vulnerability remediation consolidation can request a live demonstration at phoenix.security/demo.

About Phoenix Security
Phoenix Security is the Actionable ASPM platform that correlates vulnerabilities from code to cloud and delivers prioritized, team-attributed remediation — not reports. Its 4D risk formula combines exploitability, business criticality, deployment context, and reachability to surface findings that represent real risk, not theoretical exposure. The platform's AI agent chain — Researcher, Analyzer, Remediator — maps threat actor methodologies, traces container lineage to build files, and delivers pull-request-ready fixes without deploying agents inside running containers. Customers, including ClearBank, Bazaarvoice, and clients across ad-tech and retail, have used Phoenix to reduce container vulnerability exposure by up to 98%, save millions in engineering time, and scale their security programs without scaling headcount.

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