Phoenix Security Recognized as a Major Player in IDC Marketskape for ASPM 2025

LONDON, UNITED KINGDOM, September 17, 2025 / EINPresswire.com/ -- Phoenix Security, the pioneer of actionable Application Security Posture Management (ASPM), today announced its recognition as a Major Player to Leader for IDC MarketScape: Worldwide ASPM 2025. This recognition highlights Phoenix Security's distinct market position, setting the benchmark for integrating AI agents, contextual intelligence, and remediation-focused workflows across the software development lifecycle — from code to container to cloud.

Ai agents Phoenix Security

ASPM Moves Center Stage

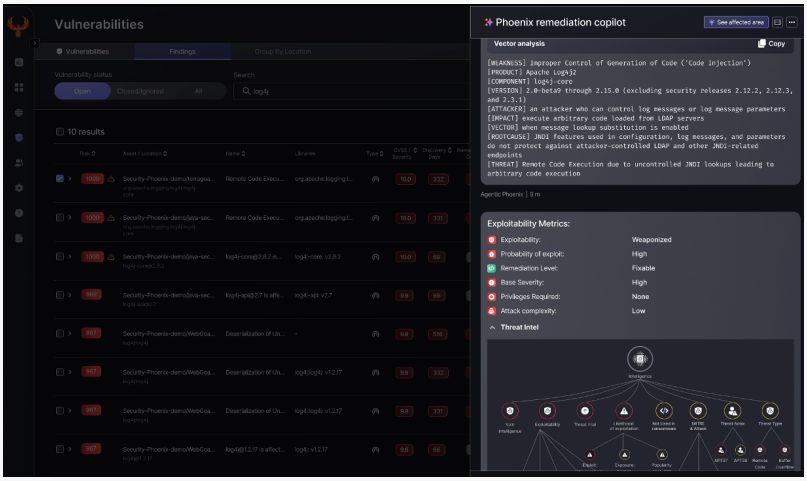
The IDC MarketScape underscores ASPM as the category that has matured out of necessity. Where traditional scanners and orchestration tools failed to scale, ASPM now delivers unified visibility, contextual prioritization, and remediation at scale. Legacy vendors have bolted on ASPM-like features through acquisition, but we believe Phoenix Security stands apart as a natively AI-driven, remediation-first ASPM platform, architected from day one to tackle ownership attribution, noise reduction, and actionable remediation.

The Escalating Challenge: Why ASPM Must Be Remediation-Centric

- Vulnerability Explosion: From just over 1,000 CVEs logged in 2000 to more than 220,000 in

2024, the growth shows no sign of slowing. By 2026, the annual number could approach one million.

- Flat Budgets, Stretched Ratios: While vulnerabilities grow at 35% year-over-year, security budgets rise just 6%, leaving teams outnumbered with ratios of 1:40 or worse.
- Only 1–10% Matter: Studies confirm only a fraction of vulnerabilities are exploitable or business-critical. Yet legacy tools flood teams with irrelevant alerts.



AI Agent Analyzer Phoenix Security

Phoenix Security built its platform to solve exactly this imbalance — cutting through the noise to deliver precision, attribution, and impact-aligned remediation.

Phoenix Security's Differentiator: The 4D Risk Model

Phoenix converts vulnerability overload into prioritized, actionable intelligence through its 4D Risk Model, which evaluates:

Ownership – assigns vulnerabilities directly to accountable teams.

Exposure – distinguishes internet-facing from internal assets

Business Impact – maps vulnerabilities to critical services and revenue drivers.

Threat Intelligence – integrates exploitability signals, KEV, and EPSS.

This framework reduces millions of findings to a surgical task list aligned to business risk.

AI Agents That Work With You, Not Against You

Phoenix Security rejects the hype of "AI-only" security. Instead, the company delivers AI agents designed to enhance, not replace, human decision-making:

- The Researcher – evaluates vulnerabilities using CTI, EPSS, and ransomware likelihood, mapping them against threat actors and attack typologies .
- The Analyzer – simulates attack paths, enriching findings with real-world exploit data and reachability analysis .
- The Remediator – automates ticket routing, generates tailored remediation playbooks, consolidates duplicates, and even proposes code or PR changes for developer approval.

Together, these agents have driven up to 90% reductions in mean time to remediate (MTTR) while freeing developers to focus on building products, not firefighting alerts.

Francesco Cipollone, Co-Founder and CEO of Phoenix Security, emphasized:

“With organizations struggling to remediate, it is fundamental to automate attribution and help teams focus on the remediation that has the most impact — and align this with business objectives.”

Integration: From Code to Container to Cloud

Phoenix Security’s ASPM provides agentic remediation campaigns, reachability analysis, and contextual deduplication to unify fragmented security signals:

- SCA Reachability Analysis: Filters out libraries unused at build time, cutting false positives before code ever ships .
- Container Reachability Analysis: Identifies exploitable libraries in runtime containers, eliminating up to 50% of non-fixable container vulnerabilities .
- Container Version Control: Ensures only secure, active container images are tracked, reducing runtime noise by up to 91% .
- One Backlog Attribution: Provides a single, team-specific backlog, mapping vulnerabilities directly to owners and fostering accountability .

These integrated features collapse silos across SAST, SCA, containers, and cloud, ensuring remediation occurs where it matters most.

Proof at Scale: Real-World Results

ClearBank – The UK’s first new clearing bank in over two centuries cut container vulnerabilities by 98%, reduced critical findings by 96%, and saved. The team scaled operations 10X with improved collaboration and precision with developers

Bazaarvoice – By embedding Phoenix into Backstage, Bazaarvoice slashed container vulnerabilities by 94%, automatically mapped 32K ownership rules, and the devops team registered the developers team, resolving all critical risks within the first month of engagement and adoption

Top 3 ad tech businesses – Leveraging code-to-cloud contextual deduplication, the Ad-tech reduced container
vulnerabilities by 78%, achieved an 82% drop in SCA-to-container noise, and improved clarity between developers and security.

These results prove that Phoenix doesn't just reduce noise — it redefines how organizations remediate vulnerabilities at scale.

The recognition of IDC strengthen ASPM belief

As Phoenix Security, we are honoured by this high recognition as a major player with one of the highest capabilities and at the border with Leadership

We believe in those principles that have provided us the recognition from names like Clearbank, Bazaarvoice, and more retail and finance sector clients

- Remediation focus: going beyond dashboards and SLAs to measurable business outcomes
- Threat-centric prioritization: correlating exploitability, reachability, and attacker behavior.
- Customer-driven innovation: rapidly developing features like remediation campaigns and one backlog in response to client needs.

Roadmap: Redefining Remediation for the Future

Phoenix Security is already extending ASPM into adjacent domains such as exposure management (CTEM) and CNAPP integration. Upcoming innovations include:

- Agentic Remediation Campaigns: systemic fixes applied across entire environments.
- Ownership as Code: embedding team attribution in CI/CD pipelines.
- Compliance Alignment: support for FedRAMP, SOC2, and NIS2.

Why Phoenix Security Matters Now

Attackers weaponize vulnerabilities in days; defenders often take months. Traditional vulnerability management can't close this gap. Phoenix Security provides:

- 98% less noise through contextual deduplication.
- Millions in developer time savings.
- Clear ownership mapped across code, containers, and cloud.
- AI agents that accelerate remediation while keeping humans in control.

IDC MarketScape vendor assessment model is designed to provide an overview of the competitive fitness of technology and service suppliers in a given market. The research utilizes a rigorous scoring methodology based on both qualitative and quantitative criteria that results in a single graphical illustration of each supplier's position within a given market. IDC MarketScape provides a clear framework in which the product and service offerings, capabilities and strategies, and current and future market success.

Phil Moroni

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