IDC MarketScape

IDC MarketScape: Worldwide Application Security Posture Management 2025 Vendor Assessment

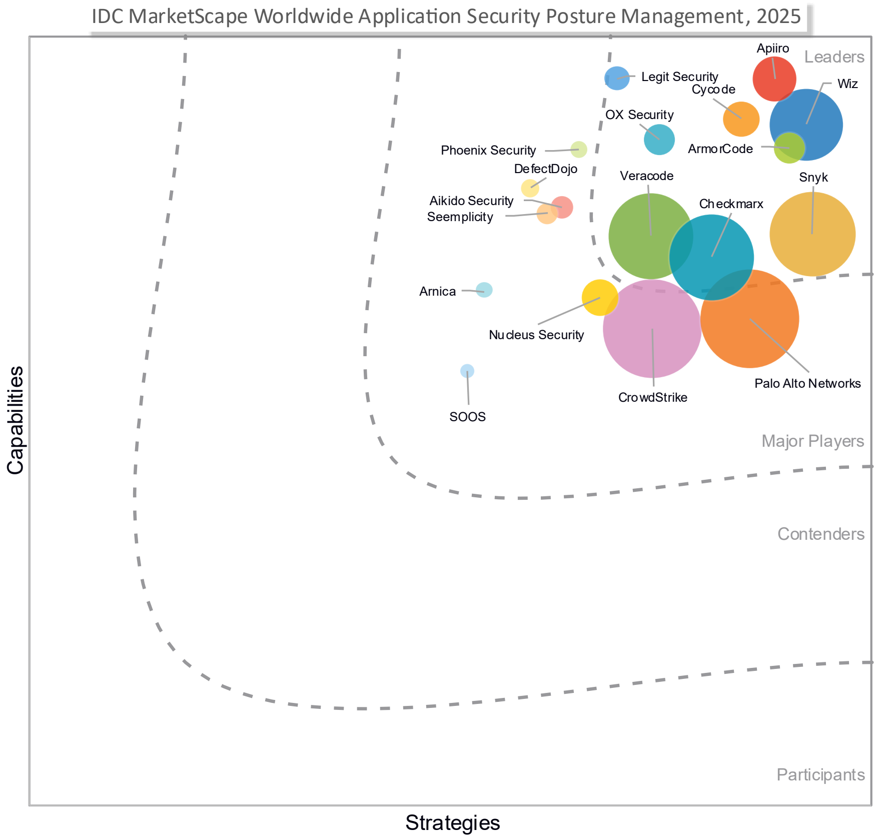
Katie Norton

THIS EXCERPT FEATURES VERACODE AS A LEADER

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Application Security Posture Management Vendor Assessment



Source: IDC, 2025

September 2025, IDC #US53001925e

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

ABOUT THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Application Security Posture Management 2025 Vendor Assessment (Doc # US53001925).

IDC OPINION

Application security posture management (ASPM) has emerged as a critical application security category in response to profound shifts in the cybersecurity landscape and the operational realities faced by modern development organizations. It evolved from the limitations of traditional application security testing (AST) and orchestration tools, expanding beyond code-level scanning to unify visibility, prioritization, and remediation across the entire software development life cycle (SDLC).

The urgency for ASPM adoption is being accelerated by several converging forces that are reshaping both the threat landscape and organizational security priorities:

- **Overwhelming vulnerability volumes and alert fatigue:** Organizations are contending with unprecedented volumes of vulnerabilities across their environments, often numbering in the hundreds of thousands or more. The constant influx of new findings from multiple security tools creates operational strain and desensitizes teams, making it harder to identify and act on truly critical issues in a timely manner.
- **Expanding attack surface from modern architecture:** The shift to microservices, ephemeral workloads, cloud-hosted CI/CD pipelines, and extensive use of open source components has greatly increased both the number and complexity of potential entry points for application attacks. This distributed and dynamic environment complicates security monitoring and demands a unified view of risk across code, infrastructure, and runtime.
- **Ineffectiveness of legacy vulnerability prioritization methods:** Traditional prioritization approaches, such as relying solely on Common Vulnerability Scoring System (CVSS) base scores, often fail to direct attention to the most pressing threats. This gap between risk scoring and real-world exploitability has led organizations to seek solutions that incorporate multiple contextual factors, such as exploitation likelihood, reachability, and business impact, to focus efforts where they matter most.

- **Lack of end-to-end visibility across the software life cycle:** Many organizations struggle to trace vulnerabilities from the point of introduction in code through to their deployment in production. This lack of linkage between development and runtime environments creates uncertainty around ownership, slows remediation, and increases the likelihood that exploitable issues remain unaddressed.
- **Fragmented visibility and disconnected security data:** Many application security tools scan at a single stage of the SDLC, such as code analysis during development or monitoring in production. Operating in isolation, these tools create data silos with little or no connection between findings, making it difficult to trace vulnerabilities from code to runtime, assign clear ownership, and coordinate remediation.
- **Security and development misalignment:** A core challenge in scaling DevSecOps is the persistent tension between security teams, which identify vulnerabilities, and development teams, which own the code. Findings are often handed off without clear ownership, actionable context, or understanding of operational impact, leading to delays, rework, and frustration. Developers can be pulled away from feature delivery by a constant stream of low-fidelity issues, while security teams struggle to gain traction on remediation.
- **Persistent cybersecurity skills and resource shortages:** The ongoing lack of skilled security personnel and limited internal resources make it increasingly difficult for organizations to keep pace with growing vulnerability backlogs and expanding security responsibilities. This capacity gap forces teams to make trade-offs in coverage, prioritization, and remediation speed.
- **Risks introduced by AI-driven development and AI-enabled applications:** Generative AI tools and AI coding assistants are accelerating software delivery but also increasing the likelihood of introducing insecure code. At the same time, organizations are embedding AI models and large language models (LLMs) directly into applications, creating new attack vectors such as model manipulation, prompt injection, and unintended data exposure. Attackers are likewise using AI to discover and chain vulnerabilities more quickly, raising the stakes for proactive detection and risk management.

The ASPM market itself is marked by rapid evolution and vendor convergence. Since the market formed, solutions have generally fallen into two categories:

- Platforms that incorporate native scanning capabilities
- "Aggregator" platforms that integrate findings from multiple existing security tools

However, increasingly, vendors are expanding beyond these distinctions to combine both approaches, responding to customer demand for comprehensive coverage and broader security posture management.

Adjacent markets, including AST, cloud-native application protection platforms (CNAPPs), DevOps platforms, and vulnerability/exposure management, are increasingly intersecting with ASPM. This convergence is blurring traditional category boundaries, intensifying competition, and making vendor positioning more complex for buyers. It also raises the bar for integration, breadth of coverage, and depth of analytics, as customers seek platforms that can consolidate capabilities, reduce tool sprawl, and provide a unified view of application security posture.

The pace of vendor innovation, the blurring of boundaries with adjacent markets, and the diversity of approaches make it challenging for buyers to determine which solutions best align with their needs. As such, this research is a timely response, providing an independent, structured evaluation of ASPM vendors to help create clarity that enables buyers to evaluate fit against their technical environments and identify vendor partners that can address both current requirements and long-term application security goals.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

To be included in this IDC MarketScape, vendors must have generated more than $1 million in revenue in 2024, with revenue derived from North America and at least one additional region, and have more than 25 customers actively using their ASPM platform in production. Vendors must also demonstrate that their platform meets at least seven of the following ASPM functional capabilities:

- Integrates with or offers proprietary or open source application security testing tools to identify security issues
- Aggregates, correlates, and normalizes security issues
- Connects or traces security issues from source code to runtime
- Applies risk-based prioritization using multiple contextual factors
- Determines root cause of security issues
- Enables security issue remediation via guidance, workflows, and/or automation
- Maintains a SDLC asset inventory or other software supply chain security functionality
- Generates open source inventories or software bills of materials
- Enables compliance monitoring, checks, or reporting
- Security supports policy management and enforcement

ADVICE FOR TECHNOLOGY BUYERS

- **Map your tooling and assess program maturity:** Start by inventorying your existing application security, DevOps, and cloud tools, noting where you already have strong coverage and where gaps remain. Evaluate the maturity of your AppSec program, including available resources, processes, and developer engagement. A clear understanding of your current environment and capabilities will help guide requirements definition and ensure investment is focused where it delivers the most impact.
- **Clarify your primary ASPM objectives:** Define what you most need from an ASPM investment, whether that is consolidating and contextualizing findings, improving risk-based prioritization, enabling code-to-cloud visibility, or strengthening remediation workflows. Being explicit about your goals will help narrow the field of vendors, guide how you assess capabilities, and ensure the selected solution aligns with your organization's priorities and long-term application security strategy.
- **Evaluate risk scoring methodology:** Understand how each vendor prioritizes security issues, and which contextual factors are incorporated, such as exploitability, reachability, business criticality, and threat intelligence. Determine whether the scoring approach aligns with your organization's risk management practices and supports the level of customization you require.
- **Assess remediation efficiency and effectiveness:** Evaluate how the platform enables the remediation of security issues, including how ownership is assigned and the clarity and actionability of provided context. Assess how well the workflows align with your current practices and whether they can also improve the speed, consistency, or efficiency of remediation. Remediation is a critical — and sometimes overlooked — component of ASPM, as making a prioritized list of issues only goes so far without the ability to drive timely and effective resolution.
- **Determine reporting and analytics needs:** Clarify the audiences you need to serve and the types of insights they require, then validate that the platform can deliver those views and reliably export data with the right access controls and freshness. In customer references for this research, reporting and analytics emerged as the most consistently cited area for improvement across platforms, making it important to investigate early in the selection process.
- **Investigate vendor road map and convergence strategy:** Given the pace of ASPM market evolution, assess whether the vendor has a clear vision for integrating adjacent capabilities such as cloud security, asset vulnerability management, software supply chain security, and compliance. Evaluate how planned AI capabilities, including generative AI and autonomous agents, will be applied to areas like prioritization, remediation, and workflow automation, and

whether they align not only with your organization's security policies and governance requirements but also with your broader AI road map.

VENDOR SUMMARY PROFILE

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

Veracode

Veracode is positioned in the Leaders category for the 2025 IDC MarketScape for worldwide application security posture management.

Founded in 2006 by Chris Wysopal and Christien Rioux, Veracode is a privately held application security company headquartered in Burlington, Massachusetts. In 2022, it was acquired for $2.5 billion by an investor group including TA Associates, Crosspoint Capital, and the British Columbia Investment Management Corporation. The company appointed Brian Roche as CEO in April 2024 to lead its next phase of growth.

Veracode Risk Manager (VRM) is the company's ASPM solution, launched following the April 2024 acquisition of Longbow Security. VRM aggregates findings from more than 50 sources across code, cloud, infrastructure, and security systems, with a Universal Connector extending coverage to less common or on-premises tools. Ingested data is normalized, enriched with asset and business context, and correlated to surface prioritized issues along with targeted remediation recommendations for efficient risk reduction.

To complement VRM's risk management capabilities, Veracode offers Veracode Fix, an AI-assisted remediation tool based on technology acquired through Jaroona in 2022. Granted a U.S. patent in 2025, Veracode Fix combines proprietary AI with expert-curated patterns to generate secure code fixes across 11 programming languages. It integrates into common development workflows, including IDEs, CLIs, and CI/CD pipelines, to support just-in-time remediation. When used alongside VRM, it helps accelerate issue resolution by automating fixes and reducing manual remediation effort.

Veracode publishes the annual *State of Software Security* (SoSS) report, now in its 15th edition, drawing on data from more than 126 million scans across nearly 1.3 million unique applications. The 2025 edition highlights trends in flaw prevalence, remediation speed, and security debt, reinforcing the importance of centralized visibility, contextual risk prioritization, and scalable remediation workflows. Findings include that half of all organizations have accrued critical security debt and that the average time to remediate flaws has increased by 47% over the past five years — challenges directly addressed by ASPM platforms such as VRM.

Customers report improved security posture after adopting VRM, citing better prioritization of risks, fewer misconfigurations in production, and clearer visibility into application security data. Users highlight strengths in data normalization, risk correlation, and remediation tracking, as well as satisfaction with deployment experience and customer support.

Strengths

- **Risk reduction optimized for remediation efficiency:** VRM's remediation model centers on the concept of "Best Next Actions," which are contextual recommendations designed to reduce the most risk with the least effort. The platform uses a scoring model that highlights issue urgency, derived from asset context, exposure, and business criticality. Combined with built-in root cause analysis and ownership attribution, this model enables organizations to focus on the most impactful remediation steps.
- **Open ingestion strategy beyond native scanning:** While Veracode began providing application security testing, VRM reflects a deliberate shift toward an application risk management platform by enabling ingestion of findings across the broader security ecosystem. This model allows organizations to consolidate risk data from both Veracode and third-party tools without being constrained to a single scanning source. This flexibility is especially valuable for teams looking to scale ASPM practices without reengineering existing security workflows or limiting visibility to one vendor's toolset.
- **Contextual dashboards with repo-to-runtime traceability:** VRM offers interactive, persona-aware dashboards that enable users to drill down into specific findings, with reusable filters to segment risk by application, environment, or compliance scope. A repo-to-runtime view maps findings back to source repositories, IaC templates, and pipelines, helping teams identify which components contribute most to production risk, while an Application Security Heatmap highlights high-risk applications and links them to responsible teams.

Challenges

- VRM's current prioritization and correlation models are rule and context based, with limited AI/ML integration beyond Veracode Fix. Features such as AI-driven risk scoring, false-positive detection, and automated issue grouping are not yet embedded in the core platform, which may become more important as organizations seek greater scale and precision in ASPM.

- While VRM offers streamlined dashboards and filters, it lacks advanced querying capabilities such as a built-in query language or natural language search. The absence of rich architectural or exploit-chain visualizations may limit some organizations' ability to explore complex relationships across the SDLC in a highly interactive way.

Consider Veracode When

Veracode is a strong fit for organizations seeking a mature, widely adopted application security platform that combines native testing with flexible ingestion of external security, infrastructure, and cloud data.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

Application security posture management (ASPM) is a continuous, contextual, and risk-based approach to managing application-layer security across the entire software development life cycle (SDLC), from code creation through deployment and operation.

ASPM platforms consolidate, correlate, and enrich data from a range of potential sources such as application security scanners (SAST, DAST, IAST, SCA, API security, container scanning), software composition and supply chain tools, code and artifact repositories, version control systems, build and CI/CD systems, cloud and on-premises infrastructure, runtime and detection-and-response telemetry, identity and access management systems, data security tools, and AI-enabled application elements. ASPM solutions construct a unified application architecture and risk model, mapping an application's components and the interdependencies of those components, along with the software supply chain that contributed to the application's creation and the risks associated with it.

Leveraging this model, ASPM dynamically prioritizes vulnerabilities based on contextual factors such as exploitability, reachability, business impact, and real-time threat intelligence, ensuring remediation efforts focus on the most critical issues. ASPM integrates directly with developer workflows, ticketing and alerting systems, and security orchestration tools to streamline remediation through automation, guidance, and, where applicable, auto-remediation. ASPM also enforces consistent security policies and orchestrates security tools across the SDLC to prevent vulnerable code from progressing unchecked. By continuously managing application security risks, ASPM strengthens overall security posture, improves operational efficiency, and supports compliance adherence.

LEARN MORE

Related Research

- *IDC TechBrief: Application Security Posture Management* (IDC#US51624024, forthcoming)
- *Worldwide Application Vulnerability Management Market Shares, 2024: Market Shake-Ups, Evolving Platforms, and Rising Expectations in the Age of AI* (IDC #US52831925, June 2025)

- *Worldwide Application Vulnerability Management Forecast, 2025–2029* (IDC #US52832325, June 2025)
- *DevSecOps and Software Supply Chain Security Survey, 2024: DevSecOps Adoption, Application Vulnerability Management, and GenAI* (IDC #US51139424, October 2024)

Synopsis

This IDC study evaluates 18 vendors in the worldwide application security posture management (ASPM) market. It provides a detailed assessment of each vendor's strengths, challenges, and approach to managing application-layer risk across the full software life cycle. This research followed the IDC MarketScape methodology, incorporating in-depth vendor briefings and surveys, along with customer reference interviews to present a comprehensive view of the ASPM landscape and market trends shaping platform selection.

"The ASPM market has become increasingly crowded as the number of vendors continues to grow. While this affirms its place as a defined category, the diversity of capabilities, origins, and design philosophies has created significant complexity for buyers," said Katie Norton, research manager for DevSecOps and Software Supply Chain Security at IDC. "This inaugural evaluation brings clarity to that landscape, offering a side-by-side view of the platforms and their strengths and challenges to help organizations identify the solutions best aligned to their strategic priorities."

ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com

Copyright and Trademark Notice