Gartner. Licensed for Distribution

Magic Quadrant for Application Security Testing

6 October 2025 - ID G00795930 - 49 min read

By Jason Gross, Mark Horvath, and 4 more

Artificial intelligence, modern application designs and increased software supply chain risks are expanding the AST market scope. Cybersecurity leaders can identify and manage risk within applications by integrating and automating AST throughout software life cycles.

Market Definition/Description

Gartner defines the application security testing (AST) market as consisting of providers of products that enable organizations to assess applications for the presence and management of risk. These products identify risk by evaluating source code, performing runtime tests and inspecting supply chain components. AST products can be integrated throughout development workflows for continuous assessment or be used to perform ad hoc evaluations. They enable organizations to manage application risks by providing an integrated set of capabilities for risk identification, prioritization and triage, policy evaluation and enforcement, and remediation assistance. Market offerings are available in on-premises, SaaS and hybrid delivery models.

Organizations leverage AST products to assess applications for the presence of security vulnerabilities and other risks (e.g., legal and operational) throughout their life cycle. These assessments are used to measure and manage the risks within individual applications, application components or groups of applications in the context of their business criticality and other key attributes (e.g., environment, sensitive data handling, etc.). AST products further enable organizations to evaluate software for compliance with internal policies as well as regulatory requirements established by governments or authoritative industry groups.

Mandatory Features

The minimum, mandatory features for products in this market include those essential for vulnerability identification, test result evaluation and management, supply chain risk identification and communication, and developer enablement.

- **Vulnerability identification:**
  - **Static AST (SAST):** Assesses, using a variety of analytical techniques, an application's source, bytecode or binary code for security vulnerabilities, typically during the programming and/or testing phases of the software development life cycle (SDLC).
  - **Software composition analysis (SCA):** Identifies third-party components, open-source or commercial, included in the development of an application. In addition to dependency details, provides information regarding known vulnerabilities, potential licensing concerns, operational risks, and malicious package identification.
- **Application security posture management:**
  - **Policy evaluation:** Evaluates assessment results and applications against predefined, or customer-defined criteria for the introduction, or acceptable duration of risk presence.
  - **Prioritization and triage:** Recommends and allows for the adjustment of remediation priorities based on publicly available and proprietary information related to scanned artifacts, scan findings and risk considerations.
  - **Posture and performance reporting:** Provides measurements at the application and application portfolio level to quantify and measure adherence to expectations for introducing and addressing risk.
- **Software supply chain security:**
  - **Software bill of materials (SBOM) life cycle management:** Supports the ingestion, creation, and sharing of SBOMs for the purposes of identifying and communicating an inventory of third-party components, commercial or open-source, contained within an application and the risks therein.
- **Developer enablement:**

- **Developer education:** Includes just-in-time training and/or remediation guidance for individual scan findings as well on-demand training material for secure software development.

Common Features

Common features are those appearing in the product compositions offered by most sellers. Products often contain an assortment of these capabilities from each category, whereas those from niche players (e.g., AST for embedded systems) or those who focus on a particular category may be more selective.

- **Vulnerability identification:**
  - **Dynamic AST (DAST):** Externally probes applications in their running (i.e., dynamic) state during the testing and operational phases of the SDLC. DAST simulates attacks against an application, appraises the application's reactions and identifies the presence of vulnerabilities.
  - **Interactive AST (IAST):** Instruments, via the injection of a software-based sensor, an application to be tested. When the application is run (e.g., during functional testing), the sensor monitors and records multiple aspects of application activity, such as data and control flow. The tool then analyzes the information gathered to identify vulnerabilities.
  - **Secrets detection:** Specialized testing capabilities for the identification of exposed secrets (e.g., credentials, tokens, API keys, etc.) within code, configuration files or other artifacts.
  - **API security testing:** Specialized testing capabilities, including support for protocols used by APIs, payload analysis and checks for vulnerabilities unique to APIs. The ability to discover APIs in both development and production environments, as well as the ability to ingest recorded traffic or API definitions to support the testing of an API are common features.
  - **Container security testing:** Examination of container images, or a fully instantiated container prior to deployment, for the presence of security issues. Container security tools typically address both configuration hardening and vulnerability assessment tasks. Tools may also scan for the presence of secrets, such as hard-coded credentials or authentication keys.

  - **Infrastructure-as-code (IaC) scanning:** Review of IaC directives supporting the dynamic creation, provisioning and configuration of software-defined compute (SDC), network and storage infrastructure.

- **Application security posture management:**

  - **Unified visibility and correlation:** Supports third-party tool assessment ingestion to include cloud and infrastructure vulnerabilities and misconfigurations, deduplication and correlation of findings.

  - **Security workflow orchestration:** Policy-based configuration and initiation of security tests, controls and workflows for risk detection and response throughout an application's life cycle.

- **Software supply chain security:**

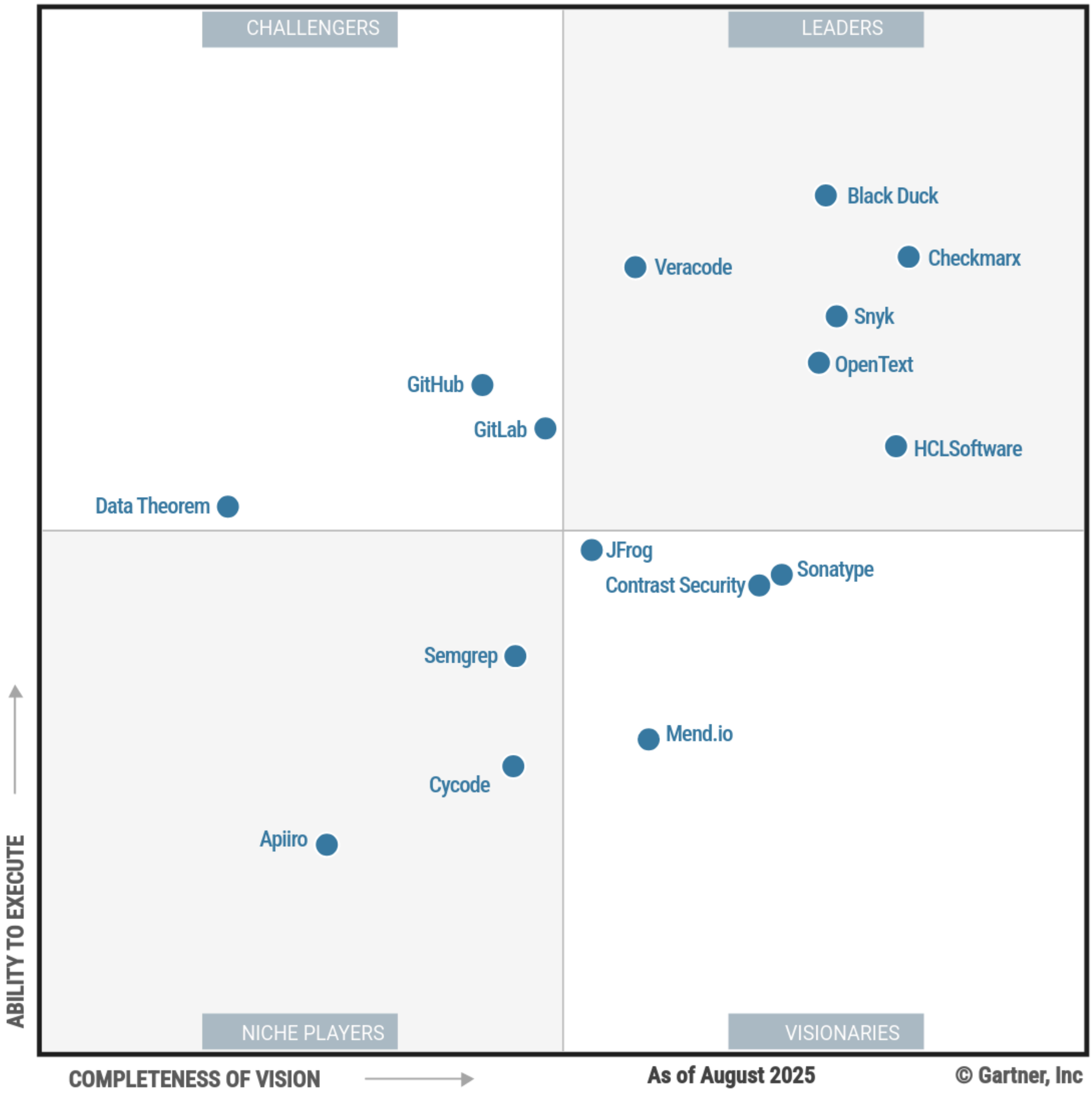
  - **Pipeline security:** Inventories and assesses security controls within development pipelines as well as the infrastructure and systems they both pull from and run from.

- **Developer enablement:**

  - **Secure coding assistants:** Resources that help developers, often through the use of AI, avoid the creation of insecure code or that provide suggestions for the automated remediation and/or mitigation of security bugs within existing code.

Magic Quadrant

Figure 1. Magic Quadrant for Application Security Testing



Vendor Strengths and Cautions

Apiiro

Apiiro is a Niche Player in this Magic Quadrant. It provides an Application Security Posture Management (ASPM) platform with AST capabilities for SAST, SCA, secrets detection, IaC scanning, API and pipeline security. The platform unifies, correlates and contextualizes risk across the software development life cycle by ingesting and deduplicating data from first- and third-party security scanners, including DAST, IAST and container security, as well as infrastructure and cloud security posture management solutions.

Apiiro integrates with enterprise systems for source code management (SCM), continuous integration/continuous delivery (CI/CD) and configuration management databases (CMDB), as well as ticketing platforms to embed security into the SDLC with closed-loop security workflows.

Headquartered in the U.S., Apiiro operates globally, serving organizations in North America, EMEA and Asia/Pacific (APAC).

Strengths

- **Risk-based prioritization**: Apiiro's Risk Graph aggregates findings from multiple sources and enhances them with business criticality, sensitive data presence and exploitability context to assign actionable risk scores.

- **Deep Code Analysis (DCA):** Apiiro's DCA technology continuously scans code repositories to build comprehensive inventories of applications and their architectures, including internal or external AI models and services.

- **SDLC integration:** Apiiro embeds security into development workflows by adding remediation guidance into pull request comments and tickets. DCA's material change detection triggers automated threat modeling by Apiiro's AI AppSec agent.

Cautions

- **Missing capabilities:** Apiiro's core solution does not include native DAST, IAST or container security scanning capabilities. Customers requiring these capabilities must obtain them from another provider, but can ingest their findings into Apiiro.

- UI complexity: Some Gartner Peer Insights reviews indicated difficulty with UI filters, the need to configure multiple policies for workflow automation and challenges with managing high volumes of data.

- **Customer support:** Support staff is heavily concentrated in North America, with limited presence and native language options in EMEA. This may present challenges for multinational organizations operating across diverse time zones and languages.

Black Duck

Black Duck is a Leader in this Magic Quadrant. It was established as an independent company in October 2024 when Synopsys sold its application security testing business to Clearlake Capital Group and Francisco Partners, which rebranded the company as Black

Duck. The company has retained its intellectual property, client base, sales teams and senior leadership, operating independently with minimal disruption to its offerings. Black Duck delivers a broad range of AST capabilities, including the Polaris SaaS platform, which provides integrated SAST, SCA, DAST and ASPM capabilities. Black Duck also offers dedicated solutions such as Coverity Static, Black Duck SCA, Seeker IAST and Software Risk Manager ASPM.

The company's portfolio includes two AI code security assistants: Code Sight, an included integrated development environment (IDE) plug-in for SAST and SCA; and Black Duck Assist, a SAST AI code assistant for remediation guidance, code fixes and a natural language interface.

Headquartered in the U.S., Black Duck offers its products globally and maintains a presence in North America, APAC and Europe.

Strengths

- **AI code security assistants:** Code Sight and Black Duck Assist receive strong reviews from developers and clients and show higher-than-median acceptance rates for automated remediation suggestions.

- **Application security posture management:** Black Duck's Software Risk Manager ASPM solution provides a comprehensive view of application risk, policy enforcement, result normalization and compliance management. SRM ingests results from both Black Duck and third-party tools.

- **Binary analysis:** Black Duck offers binary scanning, enabling detection of code snippets, partial libraries, containers and statically linked code that may be missed by manifest-based detection methods.

Cautions

- **Complexity and fit:** Black Duck's platform may be too complex or costly for small or midsize companies seeking only basic SCA or SAST functionality.

- **Software supply chain security:** Black Duck lacks support for detecting insecure pipeline configurations and vulnerable pipeline plug-ins, validating artifact integrity, and other risks within the development tool ecosystem.

- **Pricing:** Some customers report that Black Duck's pricing is complicated, which can be a barrier for smaller organizations and has been cited as a concern in pricing reviews.

Checkmarx

Checkmarx is a Leader in this Magic Quadrant, delivering a comprehensive suite of application security capabilities, including SAST, DAST, SCA, container security, API security and IaC security. These functions are available as stand-alone offerings and via the Checkmarx One platform, with most capabilities offered as SaaS or managed services.

Checkmarx emphasizes developer experience by integrating security into development workflows, providing prioritized and risk-based findings, and supporting developer training and security research. The portfolio includes autoremediation features and a recently launched ASPM solution designed for developer use.

Checkmarx is headquartered in the U.S., with a presence in North America, EMEA, APAC, and Latin America and South America.

Strengths

- **Application security posture management:** Checkmarx correlates and deduplicates findings from both its own tools and third-party sources, providing a unified view of risk and policy-driven workflows for streamlined security management.
- **Developer enablement:** Checkmarx's AI Security Champion provides context-aware remediation guidance and automated code fix recommendations directly within developer IDEs. The AI Code Security Assistant (ACSA) provides real-time secure coding support by monitoring and prompting secure code assistants for secure code.
- **Software supply chain security:** Checkmarx's Software Composition Analysis detects malicious and vulnerable open-source packages, including those for AI components. Its Repository Health solution identifies security misconfigurations in code repositories.

Cautions

- **Limited AI risk detection:** Checkmarx's AI risk detection is currently limited to known vulnerabilities in libraries used to build or integrate large language models (LLMs), and does not cover AI-specific issues like prompt injection or sensitive data disclosure. These capabilities are planned for release in 2026.
- **Missing capabilities:** Checkmarx does not offer IAST or mobile binary scanning, and its dynamic testing lacks support for native mobile clients.

- **Pricing and packaging:** Although an Essentials tier is available for smaller organizations, some customers report that Checkmarx's pricing and packaging can be difficult to understand, particularly due to additional costs for certain features or support options.

Contrast Security

Contrast Security is a Visionary in this Magic Quadrant, offering an application security platform that includes Contrast Scan (SAST), Contrast Software Composition Analysis (SCA) and Contrast Assess (IAST). In addition to Contrast Security's testing products, it offers Contrast Protect (runtime application self-protection) and Contrast Application Detection and Response (ADR) for runtime application security. Contrast One, the company's managed services offering, combines its security products with expert operational support.

Contrast Security is based in the U.S. and operates globally, with a presence in EMEA and APAC.

Strengths

- **Interactive application security testing:** Contrast Assess is one of the industry's most widely adopted IAST solutions, leveraging quality assurance or other forms of active testing (for example, DAST and load testing) to passively scan for security issues with minimal false positives.

- **Dynamic risk prioritization:** Contrast Score provides contextual risk ratings for individual findings and applications and are dynamically adjusted to reflect real-time risk. Scores are informed by Contrast Graph (a digital twin of the application built using runtime telemetry, application metadata and threat intelligence feeds), enabling teams to better prioritize remediation efforts.

- **Remediation automation:** Contrast AI SmartFix uses real-time context from Contrast Graph to generate application-specific vulnerability fixes, delivered through the Contrast MCP server for use with coding assistants like GitHub Copilot or as pull requests using GitHub Actions.

Cautions

- **Missing capabilities:** Contrast Security does not offer capabilities for DAST, secrets detection, container security, IaC scanning or security assessment of development infrastructure.

- **Limited ASPM:** While Contrast correlates its own findings, integrates with developer workflow tools and leverages runtime telemetry for risk-based prioritization, it does not ingest third-party findings, resulting in fragmented visibility into an application's overall risk posture.
- **Customer support:** Contrast Security offers 24/7 global customer support options. However, language support is relatively limited compared to other vendors. It covers North America, the U.K., the EU and APAC, with support for the English, French and Japanese languages.

Cycode

Cycode is a Niche Player in this Magic Quadrant, offering a unified application security platform that combines AST, software supply chain security (SSCS) and ASPM capabilities. The platform specializes in securing software development pipelines and providing unified visibility and correlation with ASPM.

Cycode leverages an in-house-developed multiagent AI framework for secrets detection, change impact analysis, natural language queries of its Risk Intelligence Graph (RIG), and remediation guidance and code-fix generation.

Cycode operates across North America, EMEA, APAC, and Latin America and South America.

Strengths

- **Pipeline security:** Cycode's Cimon product monitors pipeline executions to protect against supply chain attacks and automate SLSA attestations.
- **Posture management and reporting:** Cycode's ASPM capabilities include comprehensive dashboards for visibility, prioritization, remediation and compliance against frameworks such as CIS Benchmarks, SOC 2 Type II, ISO 27001 and NIST SSDF, using normalized risk scoring based on technical and business context.
- **Risk Intelligence Graph:** Cycode's hybrid data architecture maps relationships between code, assets, developers, pipelines and findings, enabling complex queries, risk correlation and real-time visibility across the entire SDLC.

Cautions

- **Missing capabilities:** Cycode offers DAST and API security only through partnerships with other providers, requiring clients to manage additional vendors for these functions.

- **Automated remediation gaps**: While Cycode provides AI-generated fixes, it lacks the ability to detect and prevent breaking changes for open-source software (OSS) library fixes and cannot recommend alternative libraries or automate license/operational risk remediation.

- **User experience:** Cycode's user interface and API can feel unintuitive, with some Gartner Peer Insights reviewers citing challenges in navigation and integration.

Data Theorem

Data Theorem is a Challenger in this Magic Quadrant, providing an application security platform that offers both AST and runtime protection capabilities for cloud-native, mobile and web applications. Its product suite includes Code Secure, Mobile Secure, API Secure, Web Secure and Cloud Secure.

The company serves a diverse client base, ranging from large enterprises to midsize organizations, with a significant presence in North America and growing adoption in APAC and Latin America and South America.

Strengths

- **Mobile and API security:** Mobile Secure provides comprehensive mobile app testing, including App Store Blocker Protection to help prevent app store rejection or removal. It also inventories back-end web services and APIs for testing with API Secure, which covers API-specific risks such as broken object-level access.

- **Reachability analysis:** Code Secure's SAST+ leverages DAST to validate the exploitability of static findings, while Code Canary confirms reachability and exploitability at runtime.

- **Single-page application (SPA) support:** Web Secure offers agentless dynamic runtime analysis for SPAs built on cloud-native and serverless architectures (Lambda) and provides a suite of hacker toolkits for testing critical applications.

Cautions

- **Software supply chain limitations:** Data Theorem lacks dedicated features for detecting security risks in development toolchains, verifying artifact integrity at each stage and evaluating the security of CI/CD pipelines. Data Theorem released new features to address this caution after the submission deadline for inclusion in this research.

- **Remediation automation:** Data Theorem does not offer automated remediation capabilities, requiring developers to manually implement recommended fixes rather than leveraging integrated, automated workflows such as those available in other platforms.

- **Pricing:** Some customers cite pricing as a concern, with cost being a top reason for not selecting Data Theorem as their AST provider.

GitHub

GitHub is a Challenger in this Magic Quadrant, offering AST capabilities through GitHub Advanced Security (GHAS). GHAS includes GitHub Code Security for built-in static analysis, AI-powered remediation with Copilot Autofix, advanced dependency scanning and proactive vulnerability management.

GitHub Secret Protection detects and prevents secret leaks in real time, blocking sensitive credentials from being pushed to repositories. The platform supports open-source, commercial and third-party integrations for DAST, API security, IaC scanning and container security.

GitHub, owned by Microsoft, is headquartered in the U.S. and operates worldwide, including North America, EMEA, APAC, and Latin America and South America.

Strengths

- **Developer-native integration:** GitHub's security offerings, including SAST, SCA and secret scanning, are natively integrated into its platform and developer workflow, surfacing alerts directly within pull requests for early triage and remediation.

- **AI-powered remediation**: Copilot Autofix, one of the most widely adopted AI code security assistants, leverages AI to suggest secure code fixes for vulnerabilities detected by CodeQL, providing actionable guidance directly within pull requests.

- **Developer enablement:** GitHub's integrated source code management and CI/CD tools embed security features — such as dependency review and secrets scanning — directly into pull requests and related workflows. This integration enhances the developer experience and promotes shift-left security by enabling earlier detection and remediation of vulnerabilities.

Cautions

- **Missing capabilities:** GitHub lacks proprietary solutions for DAST, IAST and comprehensive API and container security testing or discovery. Open-source vulnerability reachability analysis is also not currently available.
- **Limited AI risk detection**: GitHub's detection of AI-related risk is limited to AI-specific libraries installed using a supported package manager. It does not include testing for AI-specific vulnerabilities, such as prompt injection or sensitive information disclosure.
- **Limited mobile support:** GitHub offers mobile testing support with CodeQL (SAST) and Dependabot (SCA) for Swift (iOS) and Kotlin (Android), but it does not provide dynamic testing and does not include mobile-specific policy definition and evaluation.

GitLab

GitLab is a Challenger in this Magic Quadrant. GitLab provides AST capabilities as part of its broader DevSecOps platform. GitLab offers SAST, SCA, IaC scanning, container scanning, secrets scanning, DAST, dependency scanning, fuzz testing and posture management as part of its Ultimate tier of the platform.

GitLab operates and delivers its AST products and services across multiple global regions, including North America, EMEA, APAC, and Latin America and South America. In China, GitLab's services are offered through a distribution partner.

Strengths

- **Unified DevSecOps platform:** GitLab offers a comprehensive, AI-native DevSecOps platform that natively integrates a broad spectrum of security capabilities, including SAST, SCA, DAST, secrets detection, API security, fuzz testing, container scanning and IaC, directly into the software development life cycle.
- **Custom Compliance Frameworks:** In 2024, GitLab introduced Custom Compliance Frameworks. This feature allows compliance managers to tailor and automate specific compliance requirements (e.g., SOC 2, ISO 27001, NIST frameworks and the CIS GitLab Benchmark) to different codebases directly within the platform.
- **Software supply chain security:** GitLab has full visibility and traceability into the software delivery pipeline, from code commit to applications running in production.

Cautions

- **Limited DAST and IAST offerings:** GitLab's DAST does not integrate with popular test automation tools such as Selenium or Postman. Additionally, GitLab does not offer IAST capabilities.

- **Limited AI risk detection**: GitLab's detection of AI-related risk is limited to known vulnerabilities within libraries and SDKs used to interact with LLMs. It does not include testing for AI-specific vulnerabilities, such as prompt injection or sensitive information disclosure.

- **AST product packaging:** All AST offerings are now exclusively part of GitLab's Ultimate edition, requiring the adoption of GitLab for both CI/CD and SCM to use its AST solution.

HCLSoftware

HCLSoftware is a Leader in this Magic Quadrant. It offers SAST, DAST, SCA and IAST, as well as enterprise features such as IaC, secrets detection, API security and an AI code security assistant. AppScan integrates with modern DevSecOps workflows and leverages AI-driven analytics for improved detection and triage.

The platform has significantly expanded its Intelligent Findings Analytics (IFA) and Intelligent Coding Analytics (ICA) engines, enhancing accuracy and detection coverage for both code analysis and runtime testing.

HCLSoftware is headquartered in Noida, Uttar Pradesh, India and operates worldwide. Products are available globally, with strong penetration in North America, APAC, the U.K. and the EU, and are delivered through a mix of direct and indirect channels.

Strengths

- **ASPM advancements:** AppScan's ASPM features include improved dashboarding, correlation, customizable reporting and updated compliance policies, as well as integration with AppScan SSCS for software supply chain security through a partnership with OX Security.

- **AI-driven analytics:** The platform leverages IFA to reduce false positives and improve triage, and ICA to expand detection coverage, including dynamic understanding of unseen APIs. CodeSweep provides real-time IDE feedback and AI-powered autofix recommendations.

- **API security:** AppScan provides robust, multilayered API security, with AI-driven continuous discovery, including shadow and “zombie” APIs via eBPF inspection and dynamic testing to enhance visibility and protection.

Cautions

- **Business logic detection:** AppScan has limited capability for detecting API business logic vulnerabilities, often requiring third-party tools for certain use cases.
- **On-premises tooling:** HCLSoftware’s software composition analysis (SCA) and container security offerings were not available for on-premises deployments until the release of AppScan 360º v2.0 (September 2025).
- **Pricing and support:** Some customers cite pricing as a concern, especially for organizations with limited budgets or smaller teams. Customer support in some regions may not meet expectations for comprehensiveness.

JFrog

JFrog is a Visionary in this Magic Quadrant, offering a comprehensive software supply chain platform with capabilities spanning early-stage risk prevention to runtime protection. Its solutions include open-source package curation, SCA, secrets detection, SAST and security for containers, IaC, pipelines and runtime environments.

JFrog’s offerings are available as multitenant SaaS or on-premises deployments, including support for air-gapped environments. The platform emphasizes policy enforcement and artifact integrity throughout the software delivery life cycle.

JFrog is headquartered in the U.S. and serves customers throughout North America, EMEA and APAC.

Strengths

- **Policy enforcement and attestations:** JFrog evaluates and enforces policies throughout the SDLC and can generate cryptographically signed attestations (for example, SLSA and SBOM) for release builds to help meet regulatory and compliance requirements.
- **Software supply chain security:** The platform covers the entire SDLC, integrating tools such as JFrog Curation for preventive open-source risk protection and JFrog Xray (SCA) for detection within pipelines. JFrog Advanced Security extends supply chain protections to include scanning for secrets, contextual analysis and testing for IaC and pipeline risks.

- **Developer experience:** JFrog embeds security into developer workflows through IDE extensions, CLI tools, SCM integrations and partnerships with AI coding assistants such as GitHub Copilot, enabling early detection and rapid remediation of issues.

Cautions

- **Missing capabilities:** JFrog does not include native solutions for DAST, IAST, dedicated API security testing or comprehensive ASPM, requiring organizations to look elsewhere for these capabilities.

- **Product packaging:** Security features are bundled within the broader JFrog platform and are not available as stand-alone offerings, which may not suit organizations seeking best-of-breed or point solutions.

- **New product maturity:** JFrog's SAST and IaC scanning solutions are relatively new and less mature than those of established competitors in this Magic Quadrant, with some customer feedback citing limited customization options and user experience concerns.

Mend.io

Mend.io is a Visionary in this Magic Quadrant, delivering the Mend AppSec Platform with capabilities for static analysis, SCA, IaC testing and container security. The platform offers robust automated remediation for both SAST and SCA, enabling organizations to address security risks efficiently without slowing development.

Mend.io serves a diverse customer base across industries such as software, services, finance and telecommunications, and it competes globally with large vendors. The company is known for its simplified pricing model, making it easier for customers to access the full range of features.

Mend.io is headquartered in the U.S. and Israel, with operations in North America, EMEA, APAC, and Latin America and South America.

Strengths

- **AI risk detection:** Mend.io identifies and surfaces known risks related to internal and external AI components used by applications, as well as those specific to AI-enabled applications, such as misinformation and sensitive information disclosure. Mend AI Premium extends coverage to include automated red-teaming for conversational AI.

- **Triaging and prioritization:** The correlation engine analyzes findings across SAST, SCA, container and infrastructure scans, enabling organizations to resolve related vulnerabilities through a single remediation action.
- **Automated remediation:** Mend.io offers automated remediation capabilities for first-party code and third-party libraries through Mend SAST and Mend Renovate. The products deliver AI-powered fixes within developer IDEs or by generating pull requests.

Cautions

- **Partner-dependent coverage:** Mend.io does not provide native DAST and IAST, relying on OEM partners for these capabilities. Changes to partner agreements may require clients to manage additional tools and vendors.
- **Pricing:** Some prospects cite challenges with perceived value for cost, especially when comparing Mend.io to point solutions or repository vendors.
- **Limited IaC functionality:** While the platform supports IaC misconfiguration scanning, it lacks secrets detection and cannot identify configuration drift in production environments.

OpenText

OpenText is a Leader in this Magic Quadrant. Its Fortify portfolio delivers capabilities for SAST, DAST, SCA and IAST, as well as enterprise features such as IaC scanning, secrets detection and API security. ASPM capabilities are offered through the OpenText Application Security platform. Solutions are available for on-premises deployment, as SaaS offerings or through managed services.

The company is headquartered in Canada and operates globally, with dedicated sales and support for its products worldwide.

Strengths

- **Application security posture management:** OpenText provides a unified view for correlating, deduplicating and prioritizing findings across its product line, with risk scoring and policy-driven governance. The platform can also ingest findings from third-party commercial or open-source tools through parser plug-ins or APIs.
- **AI risk detection:** OpenText identifies and surfaces risks associated with AI components and services used within, or externally by, applications at runtime. Current capabilities

include detection of prompt injection, excessive information disclosure and insecure input handling, with policies configurable to block or flag risky components.

- **Flexible deployment:** OpenText offers one of the broadest portfolios in the industry, with broad language support and deployment options for on-premises, SaaS, private cloud and managed services.

Cautions

- **Limited remediation automation:** Automated remediation for SAST findings is mainly available through IDE plug-ins with varying language support. Pull request automation is supported for vulnerable open-source packages but does not detect breaking changes.
- **Missing capabilities:** OpenText does not offer dedicated container security testing with container registry integrations, nor detects security misconfigurations in development pipelines or source-code management systems. Additionally, secrets detection capabilities lack status validation.
- **Pricing complexity:** OpenText's broad deployment options and long market presence have resulted in a complex pricing model, which can complicate negotiations for buyers seeking the best licensing approach.

Semgrep

Semgrep is a Niche Player in this Magic Quadrant. Semgrep offers Semgrep Code (SAST, Semgrep Supply Chain (SCA) and Semgrep Secrets (secrets detection). The free, open-source Semgrep Community Edition (CE) provides a subset of Semgrep Code's capabilities. The Semgrep AppSec Platform is available as a hosted multi- or single-tenant SaaS solution or can be deployed on-premises. While scanning capabilities can be used in air-gapped environments, the web-based interface and APIs are not supported, requiring locally managed detection rules and off-platform access to security findings.

Semgrep operates directly on source code, enabling incremental code changes without requiring aggregation of the entire codebase. The platform supports semantic analysis, automatically applying user-written queries to semantically equivalent variations of matching code.

Semgrep is headquartered in the U.S. and operates globally. It serves clients in North America, EMEA, APAC, and Latin America and South America.

Strengths

- **Detection rule customization:** Semgrep allows users to create custom SAST rules with a flexible YAML-based syntax to detect specific code patterns or vulnerabilities and enforce coding standards.
- **AI-powered remediation assistance:** Semgrep Assistant leverages its “Memories” and AI to automate triage and provide custom, step-by-step remediation guidance based on Semgrep rules and code context. Additionally, the platform can integrate with AI-enabled coding tools such as Cursor to ensure secure code generation and enhance developer support.
- **Ecosystem and community:** Semgrep offers a large library of predefined and community-contributed rules that can be copied, modified or extended, enabling users to tailor detection to their specific needs.

Cautions

- **Missing capabilities:** Semgrep does not offer solutions for DAST, IAST, container security, dedicated API security testing or ASPM, requiring organizations to look elsewhere for these capabilities.
- **Supply chain security limitations:** Semgrep does not provide support for detecting insecure pipeline configurations, vulnerable pipeline plug-ins or development tool ecosystem risks.
- **UI and reporting:** Some users report challenges with the user interface and find exported reports lacking in presentation quality.

Snyk

Snyk is a Leader in this Magic Quadrant. Its AST offerings include Snyk Code (SAST), Snyk Open Source (SCA), Snyk Container, Snyk Infrastructure as Code, and Snyk API & Web.

In 2025, Snyk acquired Invariant Labs to advance its AI and machine learning security capabilities. The company also launched Snyk API & Web in 2025, delivering DAST as a fully integrated solution following the 2024 acquisition and incorporation of Probely’s DAST technology into the Snyk platform.

Snyk is headquartered in the U.S. and operates globally, with service and support staff in North America, Europe and APAC, and strong market penetration in North America.

Strengths

- **AI-powered remediation:** Snyk provides remediation suggestions and human-in-the-loop fix automation with rollback capabilities within IDEs, pull requests, the Snyk web UI and via CLI for SAST, IaC, SCA and container findings.
- **Developer enablement:** Synk integrates with developer tools throughout the SDLC, offering feedback, remediation guidance and automated remediation within IDEs, SCM workflows, CI/CD pipelines and ticketing systems.
- **AI risk detection:** Snyk identifies and surfaces known risks associated with open-source AI components used to build applications, and treats output from LLMs as untrusted inputs, ensuring added scrutiny during testing activities.

Cautions

- **Supply chain security limitations:** Snyk does not provide support for detecting insecure pipeline configurations, vulnerable pipeline plug-ins or development tool ecosystem risks.
- **Limited legacy language support:** The platform is focused on modern programming languages, with limited support for legacy languages, which may be a concern for organizations with older codebases.
- **Limited reporting customization:** Some users have noted that the platform's customization options are limited. Despite the new UI and reporting functions, reporting is still cited as a weak point by some customers, especially when customers have many projects or specific needs for customized metrics. Snyk announced early access, for Enterprise plan customers, to its tenant-level Snyk Analytics in July 2025, which introduced customizable dashboards.

Sonatype

Sonatype is a Visionary in this Magic Quadrant, with a strong focus on software supply chain security and early-stage risk prevention. Its platform includes SCA, binary/artifact scanning — including AI/LLM models — and container security. Sonatype offers SAST capabilities through an OEM partnership with OpenText.

Sonatype leverages curated open-source intelligence and AI-powered capabilities to provide automated policy enforcement and advanced remediation, including perimeter protection and malicious open-source component and AI/LLM model blocking via Repository Firewall.

Sonatype is headquartered in the U.S. and serves clients primarily in the U.S., U.K., EU, and APAC and Japan.

Strengths

- **Software supply chain security:** Sonatype integrates across the SDLC, offering core SCA, artifact and container scanning, and SAST via OpenText Fortify, with a focus on early risk prevention and supply chain security.
- **AI risk detection:** The platform uses heuristics, metadata and SBOM analysis to identify AI and LLM components, enabling policies to block or flag risks such as untrusted models, noncompliant datasets or unclear licenses.
- Policy-driven risk prioritization: Sonatype's policy engine applies business rules and metadata to prioritize findings, with the Sonatype Developer module factoring in fix complexity and reachability.

Cautions

- **Missing capabilities:** Sonatype does not offer native DAST, IAST or IaC, and its SAST is only available through its partnership with OpenText, which may require managing additional vendors.
- **ASPM solution:** The platform lacks a dedicated ASPM tool, though it uses available data from SSCS, open-source and SBOM features to inform risk decisions.
- **SAST transition:** Sonatype is moving away from its own SAST engine in favor of the OpenText partnership, narrowing its direct coverage in this area.

Veracode

Veracode is a Leader in this Magic Quadrant. Following its 2024 acquisition of Longbow Security Veracode has rebranded itself as an Application Risk Management (ARM) platform provider. Its platform, now called Veracode Risk Manager (VRM), introduces ASPM capabilities. Additionally, Veracode purchased technology from Phylum to enhance its software supply chain capabilities with malicious open-source package detection and an open-source package firewall.

Veracode continues to offer comprehensive AST capabilities, including SAST, DAST, SCA, container scanning and IaC scanning, penetration testing as a service, a package firewall, application security program management support and remediation consulting, as well as hands-on experiential and course-based security training for developers.

Headquartered in the U.S., Veracode provides its solution and services globally.

Strengths

- **Application security posture management:** VRM ingests security findings from third-party tools and deduplicates and correlates them with Veracode AST findings to provide a unified view of risk. Findings are enriched with runtime context, threat intelligence and business criticality to assign risk scores to facilitate prioritized remediation.

- **AI-powered remediation:** Veracode Fix provides human-in-the-loop remediation suggestions for SAST findings that developers can review and accept within IDEs, pull requests or in bulk via the CLI. Unlike many secure coding assistants, it was trained using Veracode's proprietary reference patches to avoid license and privacy risks.

- **Customer support:** Veracode provides 24/5 global service coverage and offers dedicated customer success managers and program management consulting for an additional fee. U.S. clients can also pay for additional U.S.-based staff options and FedRAMP support.

Cautions

- **SaaS-only offering:** Veracode offers a SaaS-only product, which limits adoption in markets where organizations are unwilling or unable to expose their code to the cloud. While Veracode offers the use of customer-managed encryption keys, this option may not fully address all customer concerns.

- **Limited secrets status detection**: Veracode can detect hardcoded secrets but cannot determine their status (for example, valid or revoked).

- **Limited AI risk detection:** Veracode does detect the inclusion of generative AI components and their associated risks, but it does not provide AI-specific risk detection, such as excessive information disclosure or prompt injection.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

- Apiiro
- Black Duck
- Cycode
- Data Theorem
- JFrog
- Semgrep

Dropped

- Onapsis previously appeared in the AST MQ, but was dropped due to the revised inclusion criteria and focus on AST platforms providing broad language support.
- Synopsys no longer appears due to the divestiture of its Software Integrity Group to Clearlake Capital Group and Francisco Partners, resulting in Black Duck being established as an independent company.

Inclusion and Exclusion Criteria

To qualify for inclusion, providers need to satisfy criteria as defined below.

Market Participation

Providers must satisfy all of the criteria below for inclusion in this research.

- Provide a dedicated AST solution that is generally available (GA) as of 1 January 2025.
- Satisfy each of the **technical capabilities relevant to Gartner clients**, listed below.

- Provide support for all **mandatory features** identified in the Market Definition.

Note: Products considered to be GA must be available on a price sheet/card for purchase by clients.

Market Performance

Providers must satisfy one of the criteria listed below for inclusion, in generally accepted accounting principles (GAAP):

- Have generated at least $100 million in annual revenue in calendar year 2024.

OR

- Have generated at least $55 million in annual revenue in calendar year 2024, with at least 20% coming from more than one geographic region.

  OR

- Have earned at least $10 million in annual revenue in calendar year 2024 and 100% year-over-year growth when compared to calendar year 2023.

Technical Capabilities Relevant to Gartner Clients

Provider solutions must satisfy all technical capabilities relevant to Gartner clients:

- Must support the ability to automate vulnerability identification tests from within developer workflows (e.g., pull/merge requests, CI/CD pipelines, etc.).
- SAST offerings must include the capability to identify security flaws within code written in common development languages (e.g., Java, Python, C#, PHP, JavaScript).
- SCA offerings must include the capability to identify OSS libraries that present risk in the form of vulnerabilities, undesirable licenses and malicious packages, and that are out-of-date.
- Must be able to ingest and generate SBOMs in commonly accepted formats (e.g., SPDX, CycloneDx, SWID).

Evaluation Criteria

These are the attributes on which vendors and their products are evaluated. Evaluation criteria and weighting indicate the specific characteristics and their relative importance that support the Gartner view of the market and that are used to comparatively evaluate providers in this research.

Ability to Execute

Product or Service: This criterion assesses the core goods and services that compete in and/or serve the defined market. This includes current product and service capabilities, quality, feature sets, skills, and more. These goods and services can be offered natively or through OEM agreements/partnerships, as defined in the Market Definition/Description section. This criterion specifically evaluates current core AST product/service capabilities, quality and accuracy, and feature sets. It also evaluates the efficacy and quality of ancillary capabilities and integration into the SDLC.

Overall Viability: Viability includes an assessment of the organization's overall financial health, as well as the financial and practical success of the business unit. It assesses the likelihood of the organization to continue to offer and invest in the product, as well as the product's position in the current portfolio. Specifically, we look at the vendor's focus on AST, its growth and estimated AST market share, and its customer base.

Sales Execution/Pricing: This criterion looks at the organization's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support and the overall effectiveness of the sales channel.

We look at capabilities such as support for proofs of concept and pricing options for both simple and complex use cases. The evaluation also takes into account feedback received from clients on their experiences with vendor sales support, pricing and negotiations.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customers' needs evolve and market dynamics change. This criterion also considers the provider's history of responsiveness to changing market demands.

Marketing Execution: This criterion assesses the clarity, quality, creativity and efficacy of programs designed to deliver the organization's message in order to influence the market, promote the brand, increase awareness of products and establish a positive identification in the minds of customers. This "mind share" can be driven by a combination of publicity, promotional activity, thought leadership, social media, referrals and sales activities. We evaluate elements such as the vendor’s reputation and credibility among security specialists.

Customer Experience: We look at the products and services and/or programs that enable customers to achieve anticipated results. Specifically, this includes quality supplier/buyer interactions, technical support and account support. It may also include ancillary tools, customer support programs, availability of user groups and service-level agreements (SLAs).

Operations: Vendor operations were not rated as part of this evaluation.

.

Ability to Execute Evaluation Criteria

Evaluation Criteria	*Weighting*
Product or Service	High
Overall Viability	High
Sales Execution/Pricing	Medium
Market Responsiveness/Record	Medium
Marketing Execution	Medium
Customer Experience	High
Operations	NotRated

Source: Gartner (October 2025)

Completeness of Vision

Market Understanding: This refers to the vendor’s ability to understand customer needs and translate them into products and services. Vendors that show a clear vision of their markets listen to and understand customers' demands, and they can shape or enhance market changes with their added vision.

Marketing Strategy: We look for clear, differentiated messaging that is consistently communicated internally and externalized through social media, advertising, customer programs and positioning statements. The visibility and credibility of the vendor's ability to meet the needs of an evolving market is also a consideration.

Sales Strategy: We look for a sound strategy for selling that uses the appropriate networks, including direct and indirect sales, marketing, service and communication. In addition, we look for partners that extend the scope and depth of market reach, expertise, technologies, services and the vendor's customer base. Specifically, we look at how a vendor reaches the market with its solution and sells it — for example, leveraging partners and resellers, security reports or web channels.

Offering (Product) Strategy: We look for an approach to product development and delivery that emphasizes market differentiation, functionality, methodology and features as they map to current and future requirements. Specifically, we look at the AST product and service offering, and how its extent and modularity can meet different customers' requirements and testing program maturity levels. We evaluate the vendor's ability to develop and deliver a solution that is differentiated from the competition in a way that uniquely addresses critical customer requirements. We also look at how offerings can integrate relevant non-AST functionality that can enhance the security of applications overall.

Business Model: Vendor business models were not rated as part of this evaluation.

Vertical/Industry Strategy: Vertical/industry strategies were not rated as part of this evaluation.

Innovation: We look for direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or preemptive purposes. Specifically, we assess how vendors innovate to address evolving client requirements to support testing for DevOps initiatives, API security testing, serverless and microservices architecture. We also evaluate the extent to which the vendor develops methods to make security testing more accurate. We evaluate innovations, not only in AST, but also in areas such as containers, training and integration with the developers' software development methodology.

Geographic Strategy: This criterion evaluates the vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside its "home" or native geography, directly or through partners, channels and subsidiaries, as appropriate for that geography and market. We evaluate the worldwide availability of, and support for, the offering, including local language support for tools, consoles and customer service.

Completeness of Vision Evaluation Criteria

Evaluation Criteria	*Weighting*
Market Understanding	High
Marketing Strategy	High
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	NotRated
Vertical/Industry Strategy	NotRated
Innovation	High
Geographic Strategy	High

Source: Gartner (October 2025)

Quadrant Descriptions

Leaders

Leaders in the AST market demonstrate breadth and depth of AST products and services. They typically provide mature, reputable SAST, DAST, IAST and SCA, and demonstrate vision through a clear, well-articulated path to support the growing needs of modern developers.

Leaders offer support for tools such as API testing, IaC, fuzzing, container support and cloud-native development support in their solutions. They also typically provide organizations with options for on-premises and AST-as-a-service delivery models for testing, as well as an enterprise-class reporting framework to support multiple users, groups and roles, ideally via a single management console. Leaders should be able to support the testing of mobile applications, identify risks related to the use of AI/LLMs, detect issues within software supply chains and provide application security posture management capabilities. They should exhibit strong execution in the core AST technologies they offer. Although they may excel in specific AST categories, Leaders should offer a complete platform with strong market presence, growth and client retention.

Challengers

Challengers in this Magic Quadrant are vendors that have executed consistently, often with strength in one or more particular technologies (e.g., SAST, SCA, DAST or IAST) or by focusing on a single delivery model (e.g., on AST as a service only). In addition, they have demonstrated that they can compete with the Leaders in their particular focus area and have demonstrated momentum in both the overall size and the growth of their customer base.

Visionaries

Visionaries in this Magic Quadrant are AST vendors with a strong vision that addresses the evolving needs of the market. Visionary vendors provide innovative capabilities to accommodate DevOps, containers, cloud-native development and similar emerging technologies. Visionaries may not execute as consistently as Leaders or Challengers.

Niche Players

Niche Players offer viable, dependable solutions that meet the needs of specific buyers. Sometimes referred to as specialists, Niche Players fare well when considered by buyers looking for “best of breed” or “best fit” to address a particular business or technical use case that matches the vendor’s focus. Niche Players may address subsets of the overall market. Enterprises tend to choose Niche Players when the focus is on a few important functions, or on specific vendor expertise, or when they have an established relationship with a particular vendor. Niche Players typically focus on a specific type of AST technology or delivery model, or on a specific geographic region.

Context

Since Gartner's first publication of the Magic Quadrant for Application Security Testing in 2013, the market has rapidly evolved alongside customer needs. Early AST solutions were designed for security teams to assess applications for risk just before deployment. However, as modern development practices and architectures emerged — including the adoption of AI — security teams struggled to keep pace, and existing tools failed to identify risks across the expanding attack surface.

In addition to AI accelerating the pace of software delivery, AI components embedded within applications introduce an entirely new and evolving class of vulnerabilities. In response, the market expanded to support modern architectures, automated testing within development workflows and created features designed to improve the developer experience.

This year's Magic Quadrant continues to emphasize the importance of identifying risk in both applications and the software supply chain, while expanding focus to include features that help organizations manage and remediate those risks. Gartner's research and client observations reveal several trends shaping this evolution, including the impact of AI on both the speed of development and the complexity of risk.

Artificial Intelligence: Accelerating Risk and Remediation

Generative AI is rapidly transforming software development. Gartner's Software Engineering Survey for 2025 reveals that roughly half of development teams now use generative AI tools, with nearly 70% of engineering leaders citing reduced time spent on engineering tasks as a key benefit. [1] With most clients reporting productivity gains of 10% to 15%, adoption is expected to accelerate.

AI, We Have a Problem

Generative AI coding assistants produce vulnerable code. In Gartner's 2025 AI in Software Engineering Survey, 66% of organizations using AI tools in the SDLC report little to no improvement in the security of their code. [2] A separate study by the Center for Security and Emerging Technology within Georgetown University found that 48% of AI-generated code contained vulnerabilities. [3] While modern AST tools can help detect these issues before code reaches production, the increased speed of code creation strains developer capacity for remediation. The rise of AI component reuse and AI-enabled applications also introduces new classes of risk.

AI, We Have a Solution

Vendors in the application security testing market are rapidly evolving their offerings to address the risks introduced by the inclusion of generative AI components and use of generative AI coding assistants. Beyond using AI to improve detection accuracy and risk prioritization, providers are investing in AI-powered remediation — ranging from enhanced guidance to fully automated fixes from AI code security assistants. The leading solutions are embedding these remediation capabilities directly into developer workflows, ensuring that addressing vulnerabilities is as seamless as detecting them.

As organizations increasingly build or integrate AI components, Gartner recommends that buyers look for solutions that:

- **Identify AI components:** Detect the inclusion of AI components, present known risks associated with them and support policies that govern their use.
- **Provide specialized AI testing:** Offer targeted testing and analysis capabilities to uncover vulnerabilities unique to AI-enabled applications.
- **Include remediation capabilities:** Automate first- and third-party code fixes with an AI code security assistant or provide highly contextualized and prescriptive remediation guidance.

Signal-to-Noise Challenge

As noted in the previous Magic Quadrant for Application Security Testing, "'shift left' has already been achieved." Capabilities for integrating and automating application security testing throughout the software development life cycle are now an expectation for AST products, not a differentiator. However, as organizations instrument source code management and CI/CD pipelines with risk detection controls, they are encountering a new challenge: an overwhelming volume of alerts.

Security teams struggle to accurately measure and prioritize risk reduction activities when faced with overlapping findings from multiple tools. Developers report frustration as productivity suffers from addressing findings that are not exploitable or have already been resolved.

Even organizations new to application security are wary of these pitfalls. Gartner recommends that buyers seek application security testing solutions that offer features for:

- **Application security posture management:** Capabilities to ingest and correlate signals from security tools across applications, software supply chains and runtime environments to calculate comprehensive risk scores and continuously monitor for new risk.
- **Developer enablement:** Automated remediation, deep integration into existing developer tools throughout the SDLC and actionable remediation advice.

Market Overview

Market Growth Remains Strong

The AST market is projected to reach $5.1 billion in 2025, continuing a trend of rapid expansion. End-user spending on AST tools hit nearly $3.4 billion in 2023, marking a 27% increase over 2021's total of $2.6 billion.

Drivers of Demand

This growth is fueled by rising regulatory and industry mandates, high-profile breaches linked to insecure code, vulnerable supply chains, accelerated development of new code and the expanding attack surface from modern architectures. Organizations are retooling to secure both legacy and cloud-native applications. The rapid adoption of AI is adding new risks, as leaders must now manage risks related to AI components and AI-enabled applications alongside the increased volume and velocity of AI-generated code.

Buyer Impacts: More Choice, Persistent Pricing

The focus on application security has brought more vendors into the market, especially those addressing software supply chain security and application security posture management. Incumbents are also expanding their offerings. While this gives buyers more options, strong demand has allowed vendors to sustain higher prices. Buyers can achieve discounts through negotiation, especially when consolidating vendors or if market growth slows.

A Dynamic Vendor Landscape

The AST market continues to see significant merger and acquisition (M&A) activity and portfolio expansion. Buyers should engage with existing providers to understand and influence product roadmaps when seeking solutions to fill capability gaps in their existing programs.

M&A activity since the last publication of this research has included the following:

- Cycode acquired Bearer in April 2024, enhancing its SAST and adding API discovery.
- GitLab acquired Oxeye in March 2024, improving SAST and introducing code-to-cloud traceability.
- JFrog purchased Qwak AI in July 2024 to add machine learning models to its supply chain platform.
- Mend.io acquired Atom Security in December 2023, extending reachability from code to runtime containers.
- Snyk expanded with Helios (January 2024), Probely (November 2024) and Invariant Labs (June 2025), introducing Snyk Runtime, Snyk API & Web and Snyk Guardrails.
- Veracode acquired Longbow Security in April 2024 for ASPM and Phylum in January 2025 for malicious package detection.

Additionally, Synopsys divested Black Duck in October 2024. Black Duck now operates independently.

⊕ Evidence

⊕ Evaluation Criteria Definitions

statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner's Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity." Gartner research may not be used as input into or for the training or development of generative artificial intelligence, machine learning, algorithms, software, or related technologies.