SYNOPSYS® Mi2 PARTNERING SUCCESS

CÔNG TY CỔ PHẦN TIN HỌC MI MI

Gartner® Magic Quadrant™ for Application Security

Magic Quadrant for Application Security Testing

17 May 2023

By Mark Horvath, Dale Gardner and 3 more.

Modern application design, the shift to the cloud and the accelerating adoption of DevSecOps are expanding the scope of the AST market. Security and risk management leaders can meet tighter deadlines and test more complex applications by integrating and automating AST in the software life cycle.

Market Definition/Description

This document was revised on 19 May 2023. For more information, see the Corrections page on gartner.com.

Gartner's view of the market is focused on transformational technologies or approaches delivering on the future needs of end users. It is not focused on the market as it is today.

Gartner defines the application security testing (AST) market as the buyers and sellers of products and services designed to analyze and test applications for security vulnerabilities. This market is highly dynamic and continues to experience rapid evolution in response to changing application architectures and enabling technologies.

In this analysis, and in vendor assessments, we continue to increase our focus on emerging technologies and approaches, as well as AST tools that address the new requirements they bring. Overall, the market comprises tools offering core testing capabilities — e.g., static, dynamic and interactive testing; software composition analysis (SCA); and various optional, specialized capabilities.

AST tools are offered either as software-as-a-service (SaaS)-based subscription offerings, or less often, as on-premises software. Many vendors offer both options. Core capabilities offer foundational testing functionality, with most organizations using one or more types, which include:

- Static AST (SAST): Analyzes 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): Used to identify open-source and, much less frequently, commercial components in use in an application. From this, known security vulnerabilities, potential licensing concerns and operational risks can be identified.

Optional capabilities provide more specialized forms of tests, and typically supplement core capabilities based on an organization's application portfolio or application security program maturity. They include:

- API testing: APIs have become an important part of modern applications (e.g., single-page or mobile applications), but traditional AST toolsets may not fully test them, leading to the requirement for specialized tools and capabilities. Typical functions include the ability to discover APIs in both development and production environments and test API source code, as well as the ability to ingest recorded traffic or API definitions to support the testing of a running API.
- Application security posture management (ASPM): ASPM continuously manages application risks through the detection, correlation and prioritization of security issues from across the SDLC, from development to deployment. They ingest data from multiple sources, then correlate and analyze their findings for easier interpretation, triage and remediation. They act as a management and orchestration layer for security tools, enabling controls and the enforcement of security policies. By providing a consolidated perspective of application security findings, ASPM tools facilitate the management and remediation of individual findings while offering a comprehensive view of security and risk status across an entire application or system.
- Container security: Container security scanning examines container images, or a fully instantiated container prior to deployment, for security issues. Container security tools focus on a variety of tasks, including configuration hardening and vulnerability assessment tasks. Tools also scan for the presence of secrets, such as hard-coded credentials or authentication keys. Container security scanning tools may operate as part of the application deployment process, or be integrated with container repositories, so security assessments can be performed as images are stored for future use.
- Developer enablement: Developer enablement tools and features support developers and members of the engineering team in their efforts to create secure code. These tools focus primarily on security training and vulnerability remediation guidance, either on a stand-alone basis or integrated into the development environment.
- Dynamic AST (DAST): DAST analyzes applications in their running (i.e., dynamic) state during the testing and operational phases. DAST simulates attacks against an application (typically web-enabled applications, but increasingly application programming interfaces [APIs] as well), analyzes the application's reactions and determines whether it is vulnerable.

- Fuzzing: Fuzz testing relies on providing random, malformed or unexpected input to a program to identify potential security vulnerabilities — e.g., application crashes or abnormal behavior, memory leaks or buffer overflows, or other results that leave the program in an indeterminate state. Fuzzing, sometimes called nondeterministic testing, can be used with most types of programs, although it is particularly useful for systems that rely on a significant amount of input processing (e.g., web applications and services, APIs).
- Infrastructure-as-code (IaC) testing: Gartner defines IaC as the creation, provisioning and configuration of software-defined compute (SDC), network and storage infrastructure as source code. IaC security testing tools help ensure conformance with common configuration hardening standards, identify security issues associated with specific operational environments, locate embedded secrets, and perform other tests supporting organization-specific standards and compliance requirements.
- Interactive AST (IAST): IAST tools initiate and equip a running application (e.g., via the Java Virtual Machine [JVM] or the .NET Common Language Runtime [CLR]) and examine its operation to identify vulnerabilities. Most IAST implementations are considered passive, in that they rely on other application testing to create activity that the IAST tools then evaluate.
- Mobile AST (MAST): This addresses the specialized requirements associated with testing mobile applications, such as those that run on devices using iOS, Android or another OS. These tools generally use traditional testing approaches (e.g., SAST and DAST) that have been optimized to support languages and frameworks that are commonly used to develop mobile and/or Internet of Things (IoT) applications. They also test for vulnerabilities and security issues unique to those environments.
- Software supply chain security (SSCS): Functions intended to identify and manage risks associated with software supply chains. They may include:
  - Proactive analysis of software from external sources (open source or commercial) to identify components that may pose an unacceptable risk (e.g., poorly maintained projects, inadequate security controls, presence of malware or malicious code, etc.).
  - Creation and management of artifacts to enable software users to evaluate the security of software produced by an organization (such as software bills of materials [SBOM] or application security attestations).
  - Ensuring the integrity of source code and other development or deployment artifacts, and the underlying systems used to produce them, to prevent direct attacks on the development process.

Gartner observes that the evolution of the AST market is largely driven by the need to support enterprise DevSecOps and cloud-native application initiatives. Customers require offerings that provide high-assurance, high-value findings, while not slowing down development efforts unnecessarily. Clients expect offerings to fit into the development process at an earlier stage, with testing often driven by developers, rather than security specialists. As a result, this market evaluation focuses heavily on

the buyer's needs, including support for rapid and accurate testing of various application types and the ability to integrate into software delivery workflows with an increasing level of automation.

Magic Quadrant

Figure 1: Magic Quadrant for Application Security Testing

Vendor Strengths and Cautions

Checkmarx

Checkmarx is a Leader in this Magic Quadrant. Checkmarx provides a full suite of capabilities, including SAST, DAST, SCA, container checks, API testing, IaC security and other functions, both on a stand-alone basis and via its Checkmarx One platform. Most are available either as SaaS or as managed services. Checkmarx IAST is a separate product and IaC is also available as an open source tool (KICS by Checkmarx). Checkmarx is headquartered in the U.S., but operates globally.

Its focus is largely on enhancing the developer experience and providing customers with prioritized and risk-based findings. Apart from the core AST capabilities, Checkmarx also provides developer training and security research, which adds autoremediation capabilities to its portfolio. Checkmarx enjoys a good reputation among developers, and is a good fit for organizations starting to work with DevSecOps.

Strengths

- Repository integration: Checkmarx Fusion, its correlation and prioritization engine, can now correlate all of its findings at repository level and integrate them into the console, giving developers insights into their applications.
- Developer integration: Checkmarx is focused on developer integration throughout the life cycle. Its recent launch of DevHub addresses developers' needs by providing them with complete information about open-source vulnerabilities, along with suggestions for remediation.
- DAST tooling: Checkmarx has introduced a new DAST capability. This was previously a significant gap in its product, although it still provides DAST through Invicti as an OEM.

Cautions

- Complex pricing: Customers have cited Checkmarx's pricing as a challenge, which is a common concern across many AST vendors. However, Checkmarx has worked toward providing lower-cost products, such as the recently introduced "Developer Edition" of its platform, which is intended to meet both developers' needs and application security requirements.
- Set-up and configuration: Customers have cited that, despite Checkmarx's flexibility, its implementation can be complicated due to its high level of configurability.
- Weekend customer support: Customers have remarked on a lack of availability of customer support at weekends as a relatively common issue. However, weekend support is available in Premium support package.

Contrast Security

Contrast Security is a Visionary in this Magic Quadrant. Its IAST product, Contrast Assess, can either leverage active scanning from another tool (e.g., Burp Suite from Portswigger for DAST) to generate attacks and identify vulnerabilities, or rely on existing testing, such as quality assurance (QA).

In 2021, Contrast added SAST functionality (Contrast Scan) and AST support for cloud-native applications (such as serverless functions on Amazon Web Services [AWS] Lambda). It also improved its SCA, Contrast Scan, by adding SBOM support.

Contrast Security is based in the U.S., but also sells in the EMEA and Asia/Pacific regions. It is a good fit for organizations looking for automated, continuous security testing with a low overhead on the development life cycle.

Strengths

- Runtime application self-protection: Gartner is increasingly seeing renewed interest in RASP (see the Context section of this research) as development organizations are becoming increasingly cloud-focused. Contrast's experience in the IAST/RASP space puts it in a good position to take advantage of this trend.
- Interactive application security testing: Contrast Assess is one of the most broadly adopted IAST solutions, and continues to compete on nearly every IAST shortlist reviewed by Gartner. As IAST solutions gain popularity with cloud-native clients, Contrast's developer experience stands out and gets good reviews for ease of use and accuracy.
- Developer support: Contrast offers a free version of CodeSec (developer enablement), along with GitHub Actions for Scan and SCA to streamline developer adoption.

Cautions

- Partners for some functions: Contrast Security does not provide DAST, ASOC or mobile testing. While it does have partner agreements to offer these capabilities, it should be noted that partner agreements can change unexpectedly, and the burden of adding these tools is firmly on the client.
- SAST language support: Contrast Security's SAST supports relatively few languages compared with competitors. However, it has begun to partner with other companies (e.g., Kiuwan) to leverage its partners' extensive language support library, which should significantly expand its coverage. This doesn't apply to IAST language support, which is fairly broad.
- 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 Japan, and supports the English, German, French and Japanese languages.

GitHub

GitHub is a Challenger in this Magic Quadrant. GitHub offers AST capabilities via the GitHub Advanced Security (GHAS) add-on SKU for GitHub Enterprise. This includes proprietary capabilities for SAST, SCA, secrets scanning and software supply chain security, in addition to open-source, commercial and third-party integrations for DAST, API security, MAST, IaC scanning and container security.

During the past year, GitHub has added a capability to proactively prevent secrets from being pushed to source code repositories, a feature it calls “push protection.”

GitHub is a good fit for organizations with GitHub Enterprise looking to either rationalize their application security investments or better integrate security practices into their development workflows.

Strengths

- Developer enablement: GitHub’s ownership of source code management and CI/CD tools positions it well to tightly integrate security into development workflows (e.g., dependency review), which can improve the developer experience and shift left application security practices.
- Open-source community: GitHub’s popularity as the largest open-source code repository helps open-source developers to access GHAS capabilities and provide feedback. The feedback loop from the community helps GitHub to continually improve its AST capabilities.
- npm package scanning: GitHub owns the public npm registry, which is the largest collection of open-source JavaScript packages. It has dedicated teams for threat hunting and malware detection to continuously scan npm packages. GitHub Advisory Database includes over 10,000 GitHub-reviewed CVEs and security advisories, over 2,800 of which are specific to npm. This intelligence feeds into Dependabot alerts, dependency reviews and a dependency graph.

Cautions

- Mobile support: GitHub does not offer proprietary MAST capabilities, and relies on partner integrations with NowSecure and open-source tool/framework Mobile Security Framework (MobSF). At the time of writing, CodeQL’s support for Swift (iOS) is in private beta, while its support for Kotlin (Android) is in public beta on GHEC.
- Outer development loop: GitHub’s product innovation lags behind other leading providers in securing the outer development loop, where it relies on third-party integrations. Examples of affected areas include DAST, IAST, fuzz testing, IaC scanning, API security and container security.
- Release cadence mismatch between SaaS and on-premises: GitHub customers may see feature disparity between GitHub Enterprise Cloud and GitHub Enterprise Server. Being on GHEC enables customers to receive fixes and features sooner.

GitLab

GitLab is a Challenger in this Magic Quadrant. GitLab provides AST capabilities as part of its broader DevSecOps platform. Parts of the functionality, such as SAST, IaC scanning, container scanning and secret detection, are available across all tiers, whereas DAST, dependency scanning, fuzz testing and ASOC are limited to the Ultimate tier of the platform.

During the past year, GitLab transitioned away from many of its language-specific SAST analyzers to a common Semgrep-based analyzer, which brings consistency across more programming languages and frameworks.

GitLab is a good fit for organizations that want to advance their DevSecOps maturity by adopting a platform with built-in capabilities that integrate security into application development workflows.

Strengths

- Single DevSecOps platform across the SDLC: GitLab takes a single application approach to integrate security into multiple phases of the DevOps life cycle. This enables shared visibility and reduces the cognitive load, making it easier for teams to adopt AST practices.
- Software supply chain security: GitLab has full visibility and traceability into the software delivery pipeline, from code commit to applications running in production. Recognizing the advantage this provides in securing the software supply chain, GitLab has introduced support for SBOM generation (CycloneDX), build artifact attestation and verified code commits with SSH keys to better align with the SLSA framework.
- Integrated DAST and fuzzing: GitLab's browser-based DAST is a fundamental shift from the previous OWASP ZAP-based DAST capabilities. The technique uses a browser, rather than a proxy, to scan web applications for vulnerabilities, which is more reliable for modern web applications. GitLab is the only DevOps platform with a natively inbuilt fuzz testing capability.

Cautions

- IDE integrations: GitLab's SAST and SCA capabilities currently lack IDE integrations to help surface vulnerabilities or provide developers with exact code suggestions in first- and third-party code within the IDE outside the CI pipeline.
- Advanced SCA use cases: GitLab does not currently support binary scanning of dependencies, dependency visualization or verification of the provenance of upstream dependencies.
- AST capabilities split across platform editions: Although GitLab's Free, Premium and Ultimate editions share aspects of security capabilities, most enterprises will need to invest in the Ultimate edition to meet their security and compliance requirements. For example, some aspects of container scanning are available across all tiers, while scanning containers deployed in clusters is limited to Ultimate. Likewise, SAST analyzers are included in the GitLab Free edition, but you would need the Ultimate edition to customize the SAST rulesets.

HCLSoftware

HCLSoftware is a Challenger in this Magic Quadrant. The HCL AppScan portfolio offers a mix of AST capabilities available through a variety of distribution channels. Products are available globally, with strong penetration in North America,

Asia/Pacific, the U.K. and the EU, and sales and support are delivered via a mix of direct and indirect channels.

During the past 12 months, HCLSoftware has launched a proprietary SCA solution, which includes both project scanning and container scanning. HCLSofware has also added a hybrid analysis technique for SAST, which sits between traditional SAST and CodeSweep. This allows for contextual data flow and horizontal scaling for speed, and bridges the gaps between security analysts and developers. AppScan Standard has delivered a newly designed UI which better meets users' needs.

Strengths

- Unified user experience: HCL AppScan provides comprehensive coverage of various application security testing techniques in one consolidated platform, with unified user experiences (UX) and visibility of multiple stages of the SDLC.
- Machine learning: HCL AppScan uses mature machine learning (ML) and natural language processing techniques to enhance accuracy and reduce false positives in its findings. The Intelligent Findings Analytics (IFA) and Intelligent Code Analytics (ICA) features improve the security analysis process by grouping findings and investigating new and unknown APIs.
- Role-based views: HCL AppScan provides tailored views and experiences to different roles. Scan profiling is flexible to implement, and enables the user to apply different AST technologies at different points along the software development pipeline. Workflows can be customized to match an organization's specific security policies and priorities.

Cautions

- On-premises tooling: All products are available as on-premises, SaaS, IaaS and managed services, except for SCA, which is only available as SaaS and managed services. The on-premises SAST does not have the same breadth of out-of-the-box plug-ins and integrations.
- Longer scan times: Some customers have encountered long scanning times, especially for large web applications. While AppScan has an impressive variety of controls that allow the user to tune the speed of execution, which seems to be somewhat confusing and will take time for users to understand the options and trade-offs. This can lead to the perception of longer scan times.
- Pricing and support: The pricing of HCLSoftware's AST platform is cited by some customers as a concern, especially for organizations with limited budgets or smaller development teams. Customer support services in some regions may not be as comprehensive as expected.

Mend.io

Mend.io is a Visionary in this Magic Quadrant. Its products focus on SCA and supply chain security, along with static analysis, container scanning and IaC testing. Although smaller in size, Mend.io competes with Leaders for global sales and

support capabilities. Its customers represent software, services, finance, telecommunications and other industries, and include small and very large organizations.

Mend.io was previously limited to SCA and container security. Recently, it has invested in supply chain security, including capabilities for the detection of malicious code in open-source projects, along with automated remediation for both open-source and first-party code.

Strengths

- SCA and supply chain security: The company's SCA product is a comprehensive solution for the assessment of both open-source and container images and works with package managers to block and detect malicious code. Mend.io Supply Chain Defender works with package managers to detect malicious code. Mend.io SCA both imports and exports SBOMs in either CycloneDX or SPDX formats. Imported SBOMs can be analyzed for security issues or violations of organizational policies.
- Automated remediation: Mend.io offers a variety of approaches to assist with automated remediation. Renovate, available as an open-source project, automatically generates pull requests with upgrade information when a new version of a dependency becomes available. Tools support a Merge Confidence feature for open-source upgrades, providing guidance on the probability that the upgrade will introduce a breaking change. Mend.io SAST automatically generates a proposed fix for Java programs that developers can apply as a pull request.
- Risk-based reporting: The product enables users to incorporate business impacts and risk indicators to be used as factors in the prioritization and triage of vulnerabilities. Examples include the nature of the application's attack surface, the presence of sensitive data, etc. For open-source issues, the tool reports data including (but not limited to) vulnerability severity, reachability and the presence of known exploits.

Cautions

- Product scope: Mend.io does not offer either a DAST or IAST capability. This will limit the product's appeal among organizations using a significant number of applications that benefit from such tests. Mend.io also offers no dedicated API security or mobile application testing capability, although the SAST engine can analyze common mobile programming languages, such as Swift and Kotlin.
- Maturity: Mend.io has broadened its application security product portfolio and only recently introduced its SAST solution in 2022.
- Limited IaC functionality: Scanning for misconfigurations that may adversely impact security is supported for multiple IaC formats. However, the tool lacks support for secrets detection and is unable to detect configuration drift in production environments.

Onapsis

Onapsis is a Niche Player in this Magic Quadrant. Onapsis has a strong focus on business-critical applications, especially those built on SAP, Oracle and Salesforce Apex. The Onapsis Platform offers SAST/DAST/IAST/SCA, as well as mobile and software supply chain. Onapsis' execution of IAST differs from other vendors, as its IAST tool is custom built to suit its clients' preferred environments.

Onapsis Research Labs is the industry's only threat intelligence team that is wholly dedicated to protecting business-critical applications. This focus enables Onapsis to develop intelligence about new code vulnerabilities, threat actor exploits and zero-day solutions or workarounds for its clients. In 2022, Onapsis surpassed a milestone by discovering and mitigating its 1,000th vulnerability.

Onapsis is a good fit for organizations that have made large investments in line-of-business (LOB) and business-critical applications.

Strengths

- Support for business-critical frameworks: Onapsis is one of very few vendors that supports the full range of languages used in SAP systems, including Git-style repositories, ABAP/HANA repositories and SAP BTP Neo/CloudFoundry environments.
- Risk analytics: Going beyond the severity of a vulnerability, Onapsis frames its findings in terms of risk to the business, providing an approachable explanation of the business risk, examples and, where possible, automated quick fixes.
- Microsoft Azure support: Enterprises that leverage Azure Pipelines to streamline the deployment process for SAP Ecosystem can now add Onapsis Control scans to their existing development process, adding security to the DevOps life cycle.

Cautions

- 18/5 support: Onapsis does not offer 24/7 worldwide support. However, it does offer 18/5 support (2 a.m. to 8 p.m. U.S. Eastern, Mondays through Fridays). Onapsis claims a 90 min response time for critical S1 issues, but this could be a concern for larger multinational organizations operating across multiple time zones.
- Nontraditional IAST: Compared to other vendors, Onapsis' IAST offering looks different, but its conceptually similar offering is designed for and operates within the context of the specific frameworks it supports. Its tests are built into the runtime, and checks are executed during code execution using a specialized JavaScript runtime.
- Few AST partnerships: Onapsis does not have many partnerships with traditional AST vendors (or cross-vendor correlations of results and suggestions). However, in clouds like Azure, these services can be available from other vendors on an ad hoc basis.

OpenText

OpenText is a Leader in this Magic Quadrant. Its Fortify products span the range of capabilities evaluated in this Magic Quadrant, and the company is well known for static and dynamic analysis tools. It delivers SCA and developer enablement features in part via its partnerships with OEMs.

Headquartered in Canada, OpenText is a global corporation, with dedicated sales and support for Fortify throughout the world. Large banking and financial services, IT service providers and governments figure prominently among its clients.

OpenText acquired Micro Focus in January 2023. Over the past 12 months, the company has made significant improvements across its entire portfolio. Most notably, OpenText has invested in SCA, supply chain security and the use of ML.

Strengths

- SCA and SSCS investments: Fortify has made significant strides in the SCA and supply chain security segments via its acquisition of Debricked and the expansion and extension of a long-standing OEM relationship with Sonatype. A notable example is the introduction of Open Source Select, which provides easily digestible guidance on the risks associated with open-source software prior to its selection and use.
- Machine learning: OpenText has employed ML technologies to offer new capabilities and improve existing ones. The Open Source Select offering is powered in part by ML. Fortify has also leveraged OpenText's analytics capabilities to significantly improve false positive detection among test findings, addressing a long-standing complaint about the product.
- Flexible deployment: The scope of the company's product portfolio ranks among the broadest in the industry, and is supported by multiple deployment options. These include traditional on-premises packages, SaaS offerings and options for private cloud and managed services installations.

Cautions

- Acquisition: OpenText's acquisition of Micro Focus introduces a number of routine concerns regarding the stability of product roadmaps, support and other operations. Clients are encouraged to take precautions to minimize the impact of any disruptions.
- User experience: Fortify's product portfolio has expanded significantly over several years. While beneficial, additions have not always followed a consistent UX theme. Product managers have expanded integrations to help provide developers with an interface consistent with their existing tools. The company is in the process of launching an updated Audit Assistant, and expanded reporting, promising an improved experience for security- and management-focused users.
- Pricing: Its longevity in the market, combined with a broad array of deployment options, have led to OpenText having one of the more complex pricing models in the market. While this does offer increased flexibility, it can

complicate negotiations as buyers seek the optimal licensing approach for their specific needs.

Snyk

Snyk is a Leader in this Magic Quadrant. Snyk is a relative newcomer to this body of research, but is an established and popular AST vendor. Headquartered in the U.S., Snyk has a global presence, with strong penetration in North America. Its AST offering includes Snyk Code (a cloud-based SAST platform), Snyk Open Source (an SCA solution), Snyk Container, Snyk Infrastructure as Code and Snyk Cloud (CSPM).

During the past year, Snyk has launched a new UI by integrating its TopCoat acquisition and offering new built-in reports. Snyk has also extended its app-centric focus to IaC and Cloud (via the acquisition of Fugue), enabled security standards to be consistently enforced from IDE to cloud, and provided line-in-code context for fixes to DevOps and cloud teams.

Strengths

- Cloud-native support: Snyk has strong cloud-native application security capabilities, including the ability to provide a comprehensive application context, scan cloud infrastructure and container images across different cloud environments and guide developers to fix issues.
- Developer support: Snyk's products are designed to integrate with development workflows, enabling developers to easily adopt the platform and design in better security practices. The platform orchestrates the execution of multiple products on automated schedules and push-based events.
- SCA vulnerability database: Snyk has a comprehensive database of vulnerabilities, which is regularly updated to provide the most accurate and up-to-date information on security threats. It also offers automated scanning and remediation of security vulnerabilities for applications, IaC and containers.

Cautions

- Go-to-market partnerships: Snyk's AST offering does not include inbuilt DAST (which Snyk provides in partnership with Rapid7 and StackHawk), IAST or fuzzing. It is important for clients to be aware of Snyk's partnership status to avoid any potential disruptions in service.
- 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.
- Alert frequency: Clients have reported that Snyk's platform may generate a large number of alerts, which can be overwhelming for some users, particularly in large or complex environments. This would require users to spend additional time and resources reviewing and addressing the alerts.

Sonatype

Sonatype is a Niche Player in this Magic Quadrant. It has built up a strong reputation in the SCA and open-source management spaces over the past 10 years, and recently added Lift, a SAST tool, to its offering. Sonatype is a U.S.-based company with clients based primarily in the U.S., U.K. and EU.

Sonatype has long been best known for its Nexus IQ server (now Sonatype IQ), a policy engine for managing open-source components. Sonatype has cultivated a good reputation in the open-source software (OSS) community for its in-depth security research and contributions back to the community.

Lift, a SAST scanner that compliments Sonatype's existing toolset, is a new product built through the vendor's acquisition of MuseDev in late 2021. Lift, along with Sonatype's SCA capabilities, forms the core of its software supply chain offering.

Sonatype is a good fit for clients wishing to focus on OSS and software supply chain issues, where they can leverage Sonatype's experience.

Strengths

- Strong SCA history: Sonatype has a long history of working with OSS security and SCA. It has an experienced team of researchers that has identified and remanded vulnerable OSS code for more than a decade.
- Default blocking: Sonatype Firewall Release Integrity uses ML systems to identify suspicious and malicious components and block them by default. This can be a handy feature, especially for organizations new to (or just developing) a secure SDLC.
- Legal aid: Sonatype's Advanced Legal Pack is designed to reduce complications between development and legal departments. It can automatically comply with open-source licensing obligations (e.g., attributions, attestations), provides extensive legal data to legal reviewers, and its workflows create a bridge between legal and development.

Cautions

- New product: Sonatype is new to the SAST space and, while its offering seems competitive, Lift has not had the level of real-world exposure to customers typical of vendors in this Magic Quadrant.
- Limited tools: Sonatype does not support DAST or IAST, nor does it have partnerships or joint go-to-market agreements with other vendors to provide these functionalities.
- Price: In a market already saturated with SAST and SCA tools, it may be difficult for a new company to be competitive among established platform players.

Synopsys

Văn phòng Hà Nội
Tầng 7, Tòa nhà San Nam, 78 Duy Tân
Phường Dịch Vọng Hậu, Quận Cầu Giấy, Hà Nội, Việt Nam
Tel: (84-24) 3938 0390 Fax: (84-24) 3775 9550

Văn phòng Hồ Chí Minh
Lầu 5&6, Toà nhà Nam Việt, 307D Nguyễn Văn Trỗi
Phường 1, Quận Tân Bình, Tp.HCM, Việt Nam
Tel: (84-28) 3845 1542 Fax: (84-28) 3844 6448

Synopsys is a Leader in this Magic Quadrant. It offers a broad range of AST capabilities, including products like Coverity (SAST), WhiteHat Dynamic (DAST), Black Duck (SCA), Seeker (IAST), Polaris (Cloud-based AST) and Code Sight (IDE plug-in). Synopsys is headquartered in the U.S., but its offerings are geographically diverse, with a presence in North America, Asia/Pacific and Europe.

In June 2022, Synopsys completed the acquisition of WhiteHat Security from NTT Security. This adds a new and improved DAST capability to Synopsys' product suite. It also launched the new version of Polaris (fAST Static and fAST SCA), which is now available as a SaaS solution.

Synopsys has indicated that it plans to incorporate elements of WhiteHat recently launched Vantage platform, and previous acquisitions, including Tinfoil Security, into forthcoming Polaris fAST offerings. The company has also expanded its Rapid Scan Static offering, adding new checks and integrating the tool into other portfolio components.

Strengths

- Polaris upgrade: Synopsys has introduced a new version of Polaris, which can now provide SAST and SCA capabilities as an integrated SaaS solution, complementing their on-premises product and IDE plug-in to cover broad deployment needs.
- Partner integration: In order to tighten its integration into DevOps toolchains, Synopsys has expanded its support for developer tools like GitHub, GitLab and Artifactory. Security scans can now be triggered by pull requests or GitHub Action workflows, with results published back to the developer directly in GitHub.
- ASOC: Synopsys' 2021 purchase of CodeDx, an ASOC tool, has been integrated into the product suite. CodeDx handles much of the data analysis and orchestration between the tools in the platform.

Cautions

- Pricing: Synopsys' pricing is considered extremely complicated by customers, especially small and midsize companies, and has come up as an issue in pricing reviews.
- Complex UI: The UI is still cited as a weak point in Gartner Peer Insights. The most common feedback is that it is complex to use, and sometimes confusing for some kinds of scanning. However, some organizations have been using it more effectively in "headless" mode.
- SaaS delivery: SaaS and hybrid delivery (a mix of SaaS and on-premises) are still lacking for Coverity, SBOM generation and ASPM. All other tools are available as SaaS and/or managed services.

Veracode

Veracode is a leader in this Magic Quadrant. It offers comprehensive AST capabilities, including SAST, DAST, IAST, SCA, container scanning and IaC scanning, manual penetration testing, application security and remediation consulting as well as experiential and course-based security training for developers.

During the past year, Veracode has acquired Crashtest Security, improving its DAST and penetration testing capabilities for web applications and APIs. It has also acquired Jaroona (a Gartner Cool Vendor in 2021) to detect and remediate software vulnerabilities through ML.

Veracode is a good fit for organizations looking to improve the maturity of their application security initiatives using a combination of SaaS-based security tools, developer training, support for program management and expert consultation.

Strengths

- EU/U.K. support: Veracode now offers dedicated support for the European region, which currently provides static analysis and SCA capabilities. This could be of use to European organizations concerned about data residing in locations outside European jurisdictions.
- Peer benchmarking: Building on an anonymized dataset that also feeds its annual State of Security report, Veracode added new capabilities in 2022 that help organizations benchmark the progress and maturity of their application security programs against their peers in the same industry. This enables security leaders to make a strong business case for their application security investments.
- FedRAMP compliance: In 2022, Veracode achieved the U.S. Federal Risk and Authorization Management Program (FedRAMP) moderate authorization, which certifies that it meets specific security requirements, including controls specified by the Federal Information Security Management Act (FISMA) and the NIST 800-53 publications.

Cautions

- SaaS-only offering: Veracode offers a SaaS-only product, which limits its entry possibilities in select markets that are not yet comfortable exposing their code to the cloud. The UI can appear sluggish when packaging and uploading large files for scanning.
- Limited support for IaC security: Although Veracode made significant progress on adding container security and IaC scanning capabilities in 2022, it does not currently support infrastructure configuration drift detection or enable organizations to define their own custom IaC policies.
- Lack of SBOM ingestion: Veracode currently lacks the ability to ingest and attest SBOMs as part of automated policy decisions in CI/CD pipelines.

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

- Mend.io
- Sonatype

Dropped

The following vendors appeared in the previous iteration of the AST Magic Quadrant, but have been dropped due to the new inclusion criteria.

- Invicti
- Rapid7
- Data Theorem

NTT Security has been dropped due to its acquisition by Synopsys.

Inclusion and Exclusion Criteria

For Gartner clients, Magic Quadrant and Critical Capabilities research identifies and then analyzes the most relevant providers and their products in a market. Gartner uses, by default, an upper limit of 20 vendors to support the identification of the most relevant providers in a market. On some specific occasions, the upper limit may be extended where the intended research value to our clients might otherwise be diminished. The inclusion criteria represent the specific attributes analysts believe are necessary for inclusion in this research.

To qualify for inclusion, vendors needed to meet the following criteria as of 1 November 2022.

Market Participation:

Vendors must:

- Provide a dedicated AST solution that is planned to be generally available (GA) as of 31 December 2022 that supports, at a minimum, both of the following AST capabilities as described in the Market Definition/Description section and the Technical Capabilities Relevant to Gartner Clients:
  - Static application security testing

- Software composition analysis
- Conform to a repeatable, consistent engagement model using mainly their own testing tools to enable testing capabilities.
- Deliver tools as on-premises software or appliance, a cloud-based appliance or container, SaaS, or some combination of those three form factors.

“General availability” means the product or service is available on a price sheet/card for purchase by clients.

Market Traction:

Vendors must also satisfy one of the following standards for business traction:

During the past four quarters (4Q21 and the first three quarters of 2022), the vendor must:

- Have generated at least $100 million in annual (GAAP) revenue for AST products.

Or

- Have generated at least $35 million of AST revenue with at least 20% coming from more than one geographic region.

And

- Rank among the top 20 organizations in the Market Momentum index defined by Gartner for this Magic Quadrant. Data inputs used to calculate AST MQ market momentum include a balanced set of measurements:
  - Gartner customer search, inquiry volume or pricing requests.
  - Frequency of mentions as a competitor to other AST MQ vendors in reviews on Gartner’s Peer Insights forum as of 1 November 2022.
  - Scores and frequency of mentions as measured in Gartner Peer Insights.
  - Significant innovations in the market as noted by major publications, product enhancements or introductions, or industry awards.
  - Other significant developments in corporate posture, e.g., M&A activity.

Or

- Have generated at least $20 million in AST revenue and rank in the top 10 vendors in the Market Momentum index as defined above.

Technical Capabilities Relevant to Gartner Clients:

Specifically, vendors must offer the following technical capabilities:

- An offering primarily focused on security testing to identify software security vulnerabilities, with templates to report against OWASP Top Ten and other common vulnerability definitions and standards.
- Developer support or guidance in the remediation of vulnerabilities.
- For SAST products and/or services:
  - Support for common development languages (e.g., Python, Java, C#, PHP, JavaScript)
- For SCA products and/or services:
  - Ability to scan for commonly known vulnerabilities
  - Ability to scan for out-of-date vulnerable libraries
  - Ability to scan for undesirable or inappropriate licenses

Business Capabilities Relevant to Gartner Clients

Vendors must:

- Offer phone, email and/or web customer support.
- Offer contract, console/portal, technical documentation and customer support in English (either as the product or service's default language, or as an optional localization).

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

Văn phòng Hà Nội
Tầng 7, Tòa nhà San Nam, 78 Duy Tân
Phường Dịch Vọng Hậu, Quận Cầu Giấy, Hà Nội, Việt Nam
Tel: (84-24) 3938 0390 Fax: (84-24) 3775 9550

Văn phòng Hồ Chí Minh
Lầu 5&6, Toà nhà Nam Việt, 307D Nguyễn Văn Trỗi
Phường 1, Quận Tân Bình, Tp.HCM, Việt Nam
Tel: (84-28) 3845 1542 Fax: (84-28) 3844 6448

can be offered natively or through OEM agreements/partnerships, as defined in the Market Definition/Description section and detailed in the subcriteria. 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: This criterion assesses the organization's ability to meet goals and commitments. Factors include quality of the organizational structure, skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently.

Table 1: Ability to Execute Evaluation Criteria

Enlarge Table

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

Operations	NotRated

As of April 2023

Source: Gartner (May 2023)

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: This criterion assesses the design, logic and execution of the organization's business proposition to achieve continued success.

Vertical/Industry Strategy: We assess the strategy to direct resources (e.g., sales, product, development), skills and products to meet the specific needs of individual market segments, including verticals.

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.

Table 2: Completeness of Vision Evaluation Criteria

Enlarge Table

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
As of April 2023	

Source: Gartner (May 2023)

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/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 and 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 a specific geographic region.

Context

Since 2021, Gartner has talked about the maturity level of organizations in terms of early, intermediate and advanced (see the 2022 iteration of Magic Quadrant for Application Security Testing). While this categorization is still largely valid, in 2022 we saw the market express a more complicated mix of technologies, trends and maturity than we have before. Some highlights:

“Shift Left” Has Already Been Achieved

While security teams have played, and will always play, an important role in the secure SDLC, Gartner now receives more inquiries about it from development teams than from security leads. Legacy organizations certainly exist, often very large, multinational organizations that have a variety of development styles, and small-to-midsize businesses for which existing patterns of security and development work well. Development leads are increasingly looking to merge what have historically been considered security tasks into the earlier phases of the SDLC. These tasks include vulnerability detection, code remediation and security testing. A 2021 Gartner survey of software engineering leaders found that over half of respondents had primary responsibility for the security of the applications they build. While this may seem to slow the pace of production ("velocity"), especially at first, fixing vulnerabilities as early as possible saves money, time and energy in the long term.

More importantly, security and development team leaders are framing these security tasks as development issues and mapping them directly into the existing developer workflow. They are also mapping successful security outcomes to metrics and KPIs that are more meaningful to developers. For example, security issues are often indicators of other code quality issues; that is, security issues that can be addressed by developers often arise where there are poor code quality metrics. By reframing the discussion around developer-centric issues, security team leaders are finding developers to be a more cooperative audience. Most vendors in Gartner's Magic Quadrant for Application Security Testing now rank developer experience as an important metric to track alongside the usual tool metrics like accuracy, speed and reproducibility. The AST industry has long sought to "shift left" to make it easier and faster to remediate vulnerabilities, and at this point in 2023, that seems to be the default, accepted position.

Increasing Experimentation With AI and Chatbots

Developers and security professionals rate just-in-time remediation advice to be about as important as formal classroom training. While classroom work is important, especially for teams that are just starting to include security in their development cycle, this kind of formal training tends to fade over time. While security coaches are a good resource to help improve security outcomes, they often do not scale to the required degree. Advances such as chatbots are starting to be included with many SAST and SCA tools. They can answer simple questions with preprogrammed responses, and connect the user to a human support agent to resolve more complex issues. This has proven to be a popular feature of many tools. While the use of fully featured AI code assistants (e.g., GitHub Copilot, ChatGPT) is still at an early stage, Gartner has begun to receive inquiries on how they may be used to address security issues, and specifically code remediation. It remains to be seen how effective this will be, as security remediation often involves specific knowledge outside the actual code, such as defense-in-depth issues or exploitability.

Software Supply Chain Risks/SBOMs

Since May 2021, U.S. software vendors have been required to provide buyers with SBOMs for each product purchased, either directly or by publishing it on a public website.[1] This requirement has pushed some of the biggest issues in software security into the public eye, especially in relation to commercial off-the-shelf software. Tools for performing software assessments and composition analysis have existed for many years, especially focusing on the use of open-source code. However, the introduction of this requirement moved the issue forward in significant ways, enabling a lot of software to come into scope and giving customers a chance to understand the security posture of many of the applications they purchase.

In this year's iteration of the Magic Quadrant and Critical Capabilities report for AST, we note that most AST companies have staked out a position on SBOMs and have at least some capacity to address them. However, it should be noted that, at this early stage, although a lot of SBOMs are being produced, far fewer are being consumed and operationalized. Furthermore, vendors are inconsistent in terms of which standard formats they support, although there are signs that they are starting to coalesce.

Market Overview

Over the past year, the AST market has undergone explosive growth and expansion. Worldwide end-user spending on application security tools reached approximately $3.4 billion in 2022, a dramatic jump of 27% compared to 2021's total of $2.6 billion. Geographic spending trends remain largely unchanged year over year. North America remains the largest overall market, representing approximately 68% of total spending. The EU and U.K. ranked second, at 17%, with the Asia/Pacific region totaling 12% of spending. The Middle East and Africa, at 2%, and South America, at 1%, remain nascent but growing markets.

This increase in customer demand is driven by a combination of factors, which appear to be largely resilient to adverse global macroeconomic trends. First, we note greater urgency around application security, driven by various regulatory and industrial mandates, along with multiple high-profile security incidents traced back to unsecure code and development practices. Additionally, we observe signs of a retooling initiative, as organizations reassess the ability of their existing tools to properly address changing application architectures and continually evolving development approaches. The emergence of new concerns — specifically, software supply chain security, along with an increased focus on cloud-native applications — is creating opportunities for both new features and vendors in the market.

The increased focus on application security, and the subsequent increase in demand for tooling, creates both benefits and disadvantages for buyers. On the positive side, buyers enjoy a greater choice, as new vendors enter the market to address emerging requirements, such as software supply chain security and application security posture management. Existing vendors have also acted aggressively to meet these needs. However, despite this increased competition, extremely strong

demand has enabled vendors to maintain higher pricing than might normally be expected. Well-prepared buyers can expect to obtain discounts, especially if economic conditions eventually lead to the deceleration of market growth, although aggressive negotiation may be required.

The AST vendor landscape remains dynamic. Mend.io (formerly WhiteSource) acquired Xanitizer and DefenseCode in February 2022 to support its entry into the static analysis segment of the market. This follows the vendor's 2021 acquisition of Diffend, which supports software supply chain security. Software supply chain concerns also prompted Micro Focus to acquire Debricked in March 2022. Micro Focus itself was subsequently acquired in whole by OpenText, in a $6 billion transaction that closed in January 2023. Snyk acquired Fugue, a cloud security posture management vendor, in February 2022, aiding the vendor's expansion into the cloud-native application security market. Snyk also acquired TopCoat, a data analytics firm, in March as an avenue to enhance data reporting and visualizations within its broader portfolio. Synopsys acquired WhiteHat Security from NTT in June 2022, enhancing its dynamic scanning capabilities. WhiteHat was previously acquired by NTT Security Corporation in March 2019, but failed to achieve the initially expected growth. In April 2022, Veracode acquired Jaroona for its ML-powered autoremediation technology, which has since been integrated into the Veracode portfolio. Jaroona was a 2021 Gartner Cool Vendor for DevSecOps.

Evidence

The 2021 Gartner Enabling Cloud Native DevSecOps Survey was conducted online from 12 through 21 May 2021 to identify the emerging governing structures, security owners, technologies used and the current challenges in the DevSecOps pipeline to secure cloud-native applications. In total, 85 IT and business leaders with involvement in DevSecOps initiatives participated in the survey. Eighty-two were from Gartner's IT and Business Leaders Research Circle — a Gartner-managed panel — and three were from an external sample. Participants from North America (37), EMEA (29), Asia/Pacific (7) and Latin America (11) responded to the survey.The survey was developed collaboratively by a team of Gartner analysts and Gartner's Research Data, Analytics and Tools team.

Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[1] Executive Order on Improving the Nation's Cybersecurity, The White House.

Evaluation Criteria Definitions

Ability to Execute

Văn phòng Hà Nội
Tầng 7, Tòa nhà San Nam, 78 Duy Tân
Phường Dịch Vọng Hậu, Quận Cầu Giấy, Hà Nội, Việt Nam
Tel: (84-24) 3938 0390 Fax: (84-24) 3775 9550

Văn phòng Hồ Chí Minh
Lầu 5&6, Toà nhà Nam Việt, 307D Nguyễn Văn Trỗi
Phường 1, Quận Tân Bình, Tp.HCM, Việt Nam
Tel: (84-28) 3845 1542 Fax: (84-28) 3844 6448

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor'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.

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

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Văn phòng Hà Nội
Tầng 7, Tòa nhà San Nam, 78 Duy Tân
Phường Dịch Vọng Hậu, Quận Cầu Giấy, Hà Nội, Việt Nam
Tel: (84-24) 3938 0390 Fax: (84-24) 3775 9550

Văn phòng Hồ Chí Minh
Lầu 5&6, Toà nhà Nam Việt, 307D Nguyễn Văn Trỗi
Phường 1, Quận Tân Bình, Tp.HCM, Việt Nam
Tel: (84-28) 3845 1542 Fax: (84-28) 3844 6448

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.