Magic Quadrant for Application Security Testing

Published 18 April 2022 – ID G00753626 – 51 min read

By Dale Gardner, Mark Horvath, **and 1 more**

Modern application design 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 seamlessly integrating and automating AST in the software delivery life cycle.

Market Definition/Description

This document was revised on 25 April 2022. The document you are viewing is the corrected version. For more information, see the Corrections page.

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, and 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 on-premises software or, more often, as software as a service (SaaS)-based subscription offerings. 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).

- **Dynamic AST (DAST)** analyzes applications in their running (i.e., dynamic) state during testing or 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, thus, determines whether it is vulnerable.
- **Interactive AST (IAST)** instruments a running application (e.g., via the Java Virtual Machine [JVM] or the .NET Common Language Runtime [CLR]), and examines its operation to identify vulnerabilities. Most implementations are considered passive, in that they rely on other application testing to create activity. IAST tools then evaluate.
- **SCA** is used to identify open-source and, 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 essential 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. 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, are typical functions.
- **Application security orchestration and correlation (ASOC):** ASOC tools ease software vulnerability testing and remediation by automating workflows and processing findings. They automate security testing within and across development life cycles and projects, while ingesting data from multiple sources. ASOC tools correlate and analyze findings to centralize efforts for easier interpretation, triage, and remediation. They act as a management and orchestration layer between application development and security testing.
- **Business-critical AST:** In the context of large-scale business applications (e.g., SAP, Oracle, Salesforce), identifying vulnerabilities within application code (such as ABAP or other vendor-specific customization languages), as well as misconfigurations, known vulnerabilities and errors resulting in security exposures.
- **Container security:** Container security scanning examines container images, or a fully instantiated container before 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 — in stand-alone form or integrated into the development environment.
- **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 leaving the program in an indeterminate state. Fuzzing, sometimes called nondeterministic testing, can be used with most types of programs, although it is particularly useful with 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.
- **Mobile AST (MAST):** This addresses the specialized requirements associated with testing mobile applications, such as those that run on devices using iOS, Android, or other OSs. These tools generally use traditional testing approaches (e.g., SAST and DAST) that have been optimized to support languages and frameworks commonly used to develop mobile and/or Internet of things (IoT) applications. They also test for vulnerabilities and security issues unique to those environments.

Gartner continues to observe that the major driver in the evolution of the AST market is the need to support enterprise DevSecOps and cloud-native application initiatives. Customers require offerings that provide high-assurance, high-value findings, while not unnecessarily slowing down development efforts. Clients expect offerings to fit earlier into the development process, with testing often driven by developers, rather than security specialists. As a result, this market evaluation focuses heavily on the buyer's needs involving support of rapid and accurate testing for various application types, capable of integration in an increasingly automated fashion throughout software delivery workflows.

Magic Quadrant

Figure 1: Magic Quadrant for Application Security Testing
Source: Gartner (April 2022)

A visual representation of 14 application security testing (AST) vendors' positions across the four quadrants (Le

Vendor Strengths and Cautions

Checkmarx

Checkmarx is a Leader in this Magic Quadrant. Its focus remains on providing rich, developer-centric tools, with added functional improvements to its KICS IaC product, increased focus on supply chain security and a tool for correlating test results from various parts of the SDLC. Checkmarx has also added a degree of security

testing for low-code applications and a freemium model, expanding its audience to nontraditional clients.

Checkmarx SCA's supply chain security (via its Dustico acquisition) performs behavioral analyses and adds operational risk metrics for a given open-source package. Checkmarx can generate a software bill of materials (SBOM) with a single click and can also notify when a package's manifest fails to meet SBOM standards.

Checkmarx is a good fit for clients with a strong focus on developer education that are planning for, or currently have, a complex set of development technologies, including cloud native.

Strengths

- Checkmarx has recently revamped its pricing model, which is now more consistent, clearer, and easier to predict when setting up annual AST budgets. This has received positive feedback from Gartner clients.
- Checkmarx's platform correlation engine combines results from its API, IaC and SAST scans, providing developers with a better view of emergent issues that might not be seen as important for a single tool. The design supports the addition of future tool results, reflecting a trend emerging across the market as a whole.
- Checkmarx now supports consuming all its tools (except DAST which is delivered as a managed service, through a partnership) in a SaaS model, meeting a popular demand from development teams.

Cautions

- Checkmarx relies on partnerships for DAST (Invicti). Although this is a good tool, Netsparker doesn't integrate as cleanly into the Checkmarx toolset as its own applications, and, due to the nature of partnerships, its availability is subject to unexpected changes.
- Customers have cited high costs — an increasingly common concern across many vendors. Checkmarx has worked to simplify licensing, with most products tied to the number of contributing developers. CxIAST, as well as the DAST-managed service, are based on applications/projects. Although the pricing model is simpler, cost is still the most-cited issue on Gartner Peer Insights.
- Legacy products have not been smoothly integrated with the portfolio, making automation difficult for users that are not using the most modern iteration of the platform.

Contrast Security

Contrast Security is a Visionary in this Magic Quadrant. It is best known for passive IAST, where, instead of depending on active scanning to generate attacks and identify vulnerabilities, it relies on already-planned non security testing, such as quality assurance (QA).

Contrast Security is based in the U.S., but also sells in the Europe, Middle East and Africa (EMEA) and the Asia/Pacific (APAC) regions. Recently, Contrast added SAST functionality, added AST support for cloud-native applications, such as serverless functions on Amazon Web Services (AWS) Lambda, and improved its SCA by adding SBOM support.

Contrast is a good fit for organizations looking for automated, continuous security testing with low overhead on the development life cycle.

Strengths

- Contrast Assess is one of the most broadly adopted IAST solutions and continues to compete on nearly every IAST shortlist that Gartner reviews. Contrast provides one of the broadest IAST language coverages, including Java, .NET Framework, .NET Core, Node.js, Ruby, Python and Golang.
- Contrast Security enables organizations to introduce AST with low overhead or expertise for developers, by using passive IAST during functional testing, and provides the option to also "shift-right" with Contrast Protect.
- Contrast Security correlates context from within serverless cloud function code, such as AWS Lambda, with the configuration of the services that are used by the function to determine whether service configurations are more permissive than least privilege.

Cautions

- Contrast Security does not provide DAST for traditional web applications, and its Contrast Scan SAST has limited language coverage.
- Contrast Security does not identify IaC or container-level vulnerabilities that other AST vendors increasingly provide.
- Contrast Scan does not offer the stand-alone "spellchecking" of SAST-lite capabilities that some AST vendors provide.
- Contrast Assess instruments and tests only application back ends; hence, it does not test the client-side code of an application, and does not identify front-end code vulnerabilities, such as document object model (DOM)-based cross-site scripting (XSS).

Data Theorem

Data Theorem is a Visionary in this Magic Quadrant. Its products focus on web, mobile, API and cloud AST. Based in the U.S., most of its sales are in North America. It relies primarily on direct sales, although it maintains a small, indirect channel. Technical support is geographically distributed.

Data Theorem products emphasize analysis of executable code, using an engine combining various approaches to testing applications. These include traditional techniques, such as SAST and DAST, along with alternatives (e.g., automated penetration testing). Application discovery is also supported. The late-2021 introduction of an Active Protection capability provides runtime protection and observability for applications, including serverless code and public cloud services.

Strengths

- With the release of the Active Protection capability, the company joins a small group of vendors delivering both AST and protection capabilities. The capability is expected to be of most relevance to more mature DevSecOps teams, in which application security responsibilities encompass both

coding and operations/runtime.

- A software supply chain offering, also introduced in 2021, provides the capability to deliver insights into potential security issues with business partners. An SCA component leverages multiple scanning engines to identify open source, then delivers traditional insights into vulnerabilities and potential licensing issues with code, along with some indicators of operational risk.
- Developer enablement features, including the ability for users to "chat" with Data Theorem application security engineers and the provision of more-routine guidance on findings, have improved. Feedback is delivered through multiple channels, including ticketing systems and integrated development environments (IDE) plug-ins.

Cautions

- Language support for static analysis is limited, especially compared with more-traditional SAST vendors. Support is provided for more-popular languages, although requirements for less common or legacy languages will need to be addressed by alternative tools.
- Data Theorem's client roster includes a variety of well-known organizations, although it is one of the smaller companies examined in this Magic Quadrant and does not commonly appear on client shortlists. Nevertheless, the overall approach taken and the combination of testing and protection may be popular with more-advanced development and security teams.
- Data Theorem does not have an out-of-the-box, on-premises option; however, it does provide container-based offerings in which customers can run elements of Data Theorem within their private/on-premises data centers. This may not be a good fit for organizations in the early phase of their security programs or that don't have a private cloud.

GitHub

GitHub is in the Niche quadrant in this Magic Quadrant. GitHub's AST products cover SAST, secrets scanning and SCA as part of an Advanced Security offering for GitHub Enterprise. As with some other vendors, other capabilities are delivered through a series of partnerships and via open-source tools. GitHub is more generally recognized as a Value Stream Delivery Platform, with AST functions being only a part of that value stream. The partner ecosystem offers users a wide array of choices; however, the large number of partner products can make it difficult to create a seamless, coordinated experience.

GitHub is often the source code repository of choice for many organizations, and the company successfully leverages integration of their security offering into the developer workflow. The company makes some security functionality available at no cost, as part of a free service tier.

Strengths

- GitHub's approach allows multiple users to work simultaneously on the same project and even the same code without confusion. Customers on Gartner Peer Insights have cited this collaborative ability as a huge benefit for security reviews and coaching.

- GitHub's SCA offering is good, centered around its well-regarded Dependabot tool. Dependabot can proactively identify direct and transitive dependencies with known security vulnerabilities and automatically update them.
- Customer's familiarity with GitHub, and its familiar workflows and seamless integration with their established toolchain, appeals to developers who wish to get started with a secure SDLC, and value preintegrated security capabilities.

Cautions

- The company relies on partner integrations and open source for functions that are integral to a secure SDLC beyond SAST and SCA. Although this can allow wider choice than is usually available in more-integrated platforms, it increases total cost of ownership (TCO) for the customer and operational complexity, because they need to procure, maintain and update additional tools from partner providers.
- Support for MAST is comparatively weak, compared with other vendors. Its CodeQL engine does most of the SAST heavy lifting, and lacks support for testing user authentication and for testing against actual devices or simulations.
- If you are not a GitHub user, this toolset will not work for your organization.

GitLab

GitLab is a Challenger in this Magic Quadrant. It provides AST as part of its broader value stream delivery platform with its Ultimate tier. It combines proprietary and open-source scanning tools and functionality in its own workflows to provide SAST and DAST.

During the past year, GitLab introduced IaC scanning, and strengthened its open-source container security, adding Trivy. In addition, Gitlab introduced Compliance Pipelines, which allows it to define immutable pipeline configurations aligned with specific compliance frameworks, such as Payment Card Industry (PCI). In 2021 Gitlab filed for IPO and entered the Nasdaq stock exchange.

GitLab is a good fit for organizations that use its platform for continuous application delivery and need a secure application development workflow.

Strengths

- The vendor's AST offering — including SAST, Secrets Detection and Dependency Scanning — is included in its Ultimate tier, which is predictably and transparently priced. Also, SAST and secret detection come as part of GitLab's free edition.
- Because it provides the development environment in which its AST operates, Gitlab provides numerous options to impose security and compliance controls throughout the development pipeline. For example, any alerts for vulnerabilities are displayed in the developer's merge request, and a pipeline can be configured to scan the main/default branch on a regular cadence and identify any components that are now known to be vulnerable.

- GitLab provides container scanning, including automated remediation for SCA vulnerabilities. Its fuzzing capabilities are granular and easy-to-use, with a low level of expertise required, thanks to the automation provided.

Cautions

- GitLab lacks some features that are available in more-mature AST offerings. Language coverage is limited, and the dashboard lacks the granularity and customizability of more-established AST tools. Its SAST offering lacks features, such as quick-fix recommendations and real-time spell checking.
- GitLab does not provide IAST options in its offering.
- GitLab uses different tools for different languages and frameworks, many of which are open source, although it actively contributes to their development and maintenance. For example, the vendor's DAST offering currently is the Open Web Application Security Project's (OWASP's) open-source ZAP tool, its mobile offering consists of MobSF and its container scanning offering consists of Trivy.

HCL Software

HCL Software is a Leader in this Magic Quadrant. Its products offer a mix of AST capabilities via a variety of delivery channels. Products are available globally, with strong penetration in North America and the APAC region, with sales and support delivered via a mix of direct and indirect channels.

Following a period of rationalization of product features across products, HCL Software is focusing on additional enhancements to the product portfolio to address customer requests and better align with the overall direction of the AST market. Changes include a plan to combine the company's "best fix location" analysis (a longstanding first in the market, which optimizes remediation efforts) with a new auto-remediation feature.

Strengths

- The IDE-based CodeSweep tool enables near-real-time static analysis of code, using the same engine as AppScan. Free for individual developers, as are similar tools from other vendors, CodeSweep enables collaboration when used with a licensed AppScan instance. Automated remediation guidance has been introduced into CodeSweep, and the company claims more than 50% of findings have auto-remediation available.
- The company's DAST offering makes effective use of statistical analysis and machine learning (ML) to optimize scan times and results. ML-based crawling of apps helps suggest optimal targets for tests, while statistical analysis of programs enables users to balance testing speed against requirements for completeness and accuracy.
- HCL Software is one of multiple vendors delivering correlation and consolidation of findings across testing methods. In this case, IAST results are automatically correlated with SAST and DAST findings, simplifying the workload associated with prioritization and triage efforts.

Cautions

- Products are licensed through a variety of delivery methods and pricing options. Although this provides customers with flexibility, it comes at the cost of complexity in pricing and difficulty in comparing prices across vendors.
- Customers tend to score the quality of technical support somewhat lower than other Magic Quadrant participants. User interfaces (UIs), which tend to vary from one product to another, are another area noted by clients as needing improvement.
- The company's SCA product is based in part on technology sourced via an original equipment manufacturer (OEM) relationship with WhiteSource Software, although the company is implementing a completely proprietary solution. Customers should know the status and roadmap for this transition to avoid potential disruptions in capabilities and support.

Invicti

Invicti is a Challenger in this Magic Quadrant. Its Invicti products (formerly Acunetix and Netsparker) are focused on IAST and DAST, the latter being Invicti's core competency. Netsparker is one of the oldest brands in the space, and they enjoy a good reputation with developers and security researchers.

Invicti does not have a SAST offering, so any SAST tool would need to be procured through another vendor. It offers DAST tools to Checkmarx clients through a partnership. Partnerships can offer broader access to other tools. The experience doesn't have the smooth integration that characterizes larger platform players, and partnerships are subject to change.

Invicti operates principal offices in the U.S., Malta and Turkey. Sales and distribution are supported directly and through a reseller channel. The company shows a strong presence in multiple geographies.

Strengths

- Invicti offers one of the few active IAST products on the market, making good use of its DAST technology to invoke attacks against the application, which can then be observed through instrumentation. This results in a low false-positive rate; however, as with all IAST products, the trade-off is adding instrumentation to the code.
- Invicti's DAST technology is the cornerstone of its offering, getting good reviews from both clients and the security community more broadly.
- Invicti offers its own SCA product, which is combined with its IAST and DAST tools to create SBOM for all applications in the enterprise. This has been a frequent question from Gartner clients for the past year, and Invicti is one of only a handful of AST vendors offering this functionality.

Cautions

- The Invicti products focus on traditional web applications, where their DAST expertise can be more heavily leveraged. There is no support for SAST, container scanning, IaC scanning, or mobile or business-critical application assessment capabilities, nor can any partners fill this gap. This makes it

a less-than-ideal fit for cloud-native development.
- Integration into the SDLC is broad, although developer enablement is only mixed. Support is provided for a broad range of issue tracking, project management, continuous integration (CI) servers, productivity and communication tools, and privileged access management (PAM) solutions (for authentication purposes). However, there is no integration with an IDE, although developers can access information about findings via trouble ticket integrations, or via CI tools.
- Although its Enterprise IAST product covers the most common modern languages (Java, .NET, Node.js), overall language support is quite limited. More languages (Python, Ruby, Go etc.) are expected to be added in 2022.

Micro Focus

Micro Focus is a Leader in this Magic Quadrant. Its Fortify product line provides comprehensive AST, with broad language coverage. Micro Focus is based in the U.K. and is a global provider of IT products and services.

In 2021, Micro Focus improved its DAST to support applications that require two-factor authentication (2FA), to correlate with SAST findings, to scale and support analysis of client-side JavaScript by using distributed processing, and to detect client-side XSS. Micro Focus expanded its capabilities for AST for cloud-native applications, improved its SDLC integrations and improved its JavaScript SAST. The company announced plans to acquire debricked, a vendor of SCA tools based in Sweden, during the preparation of this analysis.

Fortify is a good fit for enterprises with complex application projects and AST users with experience and advanced requirements.

Strengths

- Fortify Security Assistant is a real-time security checker that operates in the IDE. It is not a replacement for a comprehensive SAST scan; however, it can provide a lightweight automatic check for developer security errors as the developer codes.
- Micro Focus has extended its Fortify Audit Assistant feature to provide teams the flexibility to manually review artificial intelligence (AI) predictions on issues, or to opt in to "automatic predictions," which support completely in-band automated triaging of findings. This contributes to reducing false positives.
- Micro Focus provides DAST that can address many of the challenges with modern applications, such as scanning client-side vulnerabilities or support for 2FA among other things

Cautions

- Organizations without extensive AST knowledge looking to start their application security program are often overwhelmed with the comprehensiveness, granularity and cost of Fortify's product line.
- Fortify does not provide an option for stand-alone passive IAST, nor stand-alone fuzzing. It only offers active IAST, delivered and induced by its DAST. Its SCA is offered through a partnership with Sonatype.

- Fortify's on-premises UI is complex and the user experience (UX) feels dated, compared with its competitors in this space.

NTT Application Security

NTT Application Security (formerly WhiteHat Security) is a niche vendor in this Magic Quadrant. Its products, which are in significant transition, emphasize static and dynamic AST, as well as SCA and IaC scanning. Despite gaining access to the global NTT sales channel, most sales remain in North America. Primary support is provided from the U.S. and Ireland, with supplemental support offered by NTT in 57 countries.

In December 2021, NTT announced the new Vantage Platform. It includes Vantage Inspect (an OEM version of the ShiftLeft product, providing SAST, SCA and IaC); Prevent (on-premises DAST); and Detect (SaaS-based DAST). Sentinel products remain available, but will be focused on managed service offerings.

Strengths

- Traditional strengths, particularly DAST, remain above average, and the Vantage Prevent "directed DAST" offering is in keeping with industry trends to tie dynamic and interactive AST to functional testing. Generally, this supports DAST testing earlier in the development process.
- The company continues to offer its popular and unique Directed Remediation patches — fixes to security flaws detected in testing. It was also among the first to offer direct access to support, connecting clients to security engineers from within the Sentinel testing platform to assist with questions.
- The company will provide support for clients performing their own testing activities with the Vantage platform, and will generally use the existing Sentinel products for managed testing offerings.

Cautions

- The company has grown more slowly during the past year than the overall AST market. Appearance on customer shortlists has declined, and it's mentioned less frequently during inquiry than in the past. This may result partly from the branding change from WhiteHat Security to NTT Application Security. Such changes frequently create confusion among potential customers.
- The introduction of the Vantage line introduces execution and roadmap risks. The company indicates it plans to maintain both products for the foreseeable future and will work to harmonize underlying product technology. This could result in a reduction in new product development in favor of capability and technology alignment and integration. Overall product focus may change over time. Current and prospective clients must monitor roadmaps to ensure that products remain appropriate choices for their requirements.
- As is the case with some other vendors, NTT Application Security relies on OEM technology relationships to provide elements of its offering. The company has a longstanding relationship with Now Secure for mobile AST. The new Vantage Inspect offering relies totally on ShiftLeft's scanning engine for SAST, SCA and IaC testing. In both cases, this reliance could lead to operational disruptions in customer environments, should such an OEM relationship falter at some point.

Onapsis

Onapsis is a Niche Player in this Magic Quadrant. Onapsis has a strong focus on business-critical applications and an excellent reputation with clients in that space.

Business-critical applications are those organizations depend on to manage their daily and ongoing processes, such as customer relationship management (CRM) and human capital management (HCM). Onapsis continues to stand out for its deep understanding of these environments, the needs of developers and the often-specialized security risks business-critical applications face. They are the only participant in this Magic Quadrant that has a team dedicated to business-critical vulnerability research.

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

Strengths

- Onapsis offers integration for an increasing array of business-critical languages and frameworks, such as SAP, Oracle and Salesforce (Apex).
- Beyond vulnerability severity, Onapsis frames its findings in terms of risk to the business, including an approachable explanation of the business risk, examples and, where possible, automated quick fixes.
- Onapsis has added SAP-Certified Add-ons to its portfolio. This allows them to discover SAP systems and extract technical information for further analysis. Add-ons run as a component on top of SAP systems and do not interact with any functional (business-related) modules.
- Plug-ins available for IDE environments include Eclipse, SAP Web IDE, SAP HANA Studio, Visual Studio Code and SAP Business Application Studio for real-time feedback. Also additional CI/continuous deployment (CD) integrations scan ABAP, SQLScript/AMDP, CDS ABAP, CDS HANA Views(XSA) in a GIT Repository, SAP TMS-UI5, SAP TMS-HANA, Jenkins, and from a local file repository.

Cautions

- Other AST platform vendors now support languages, such as ABAP and Apex. However, these new entrants don't have the expertise in working in specific frameworks, or the deep knowledge of the business-critical application vulnerability landscape, gained from Onapsis Research Labs, although that is likely to change. Although Onapsis enjoys extensive cooperation with SAP and Oracle, both are still competitors in this space with their own products (e.g., SAP's Code Vulnerability Analyzer). To date, these native products do not have the sophistication seen in the Onapsis suite.
- With a focus on applications supported by SAP and Oracle, testing is largely focused on those frameworks, forgoing support for broader, less-specific kinds of coding and typical language support, making integration into a larger or more-traditional AST environment somewhat challenging.

- Partnerships with traditional AST vendors (and cross-vendor correlations of results and suggestions) are not present.

Rapid7

Rapid7 is a Visionary in this Magic Quadrant. Its core competencies have been in the DAST and the vulnerability management spaces. Other core functions are addressed with partnerships for SAST (Checkmarx and Snyk) and SCA (Snyk). Rapid7 has combined its Alcide and DivvyCloud acquisitions into a single unified solution — InsightCloudSec.This adds new capabilities around Kubernetes and Cloud Security Posture Management and, combined with its tCell assets, puts it in a strong position for companies seeking IaC, API and other cloud-native application security tools.

Strategic acquisitions and investments in existing products have put Rapid7 in a strong position for companies moving production into the cloud, checking the boxes on many commonly requested tools for cloud-native development and for transitioning applications to the cloud.

Strengths

- Rapid7's modern developer workflows reflect a sense of cohesion across many aspects of the DevSecOps life cycle, including features for discovery, APIs, policy management and continuous monitoring.
- The Insight platform does a good job of providing visibility across a wide array of tools and security problems to give a 360-degree view of the applications and their environment and security context.
- Rapid7 continues to receive positive feedback from Gartner clients for DAST, improving on traditional tools with its Universal Translator (available through the InsightAppSec offering), which normalizes formats, data and protocols for more-effective testing.

Cautions

- Although many organizations want to move to the cloud, tooling alone isn't sufficient. Rapid7's complexity can be a drawback for organizations that lack experience in the cloud and can be a steep learning curve for early and intermediate stage organizations.
- Pricing is still one of the most-cited issues from customer feedback, in both ticket price and complexity.
- Rapid7 lacks a native static analysis solution. The company leverages partnerships with Snyk and Checkmarx to service customers requiring the capability. Again, prospective buyers should ensure that they understand the roadmap and prospects for any partnerships or integration.

Snyk

Snyk is a Challenger in this Magic Quadrant. Snyk is a well-known SCA vendor that has expanded into AST, and has a global presence. Its AST offering includes SCA with Snyk Open Source and Snyk Container, as well as SAST with Snyk Code and Snyk Infrastructure as Code.

During the past year, Snyk acquired FossID to provide SCA for C/C++. It also introduced Snyk Learn, its developer security training offering, and SAST support for API vulnerability testing. Via its acquisition of CloudSkiff, Snyk introduced configuration drift checks for IaC. In February 2022, Snyk also acquired Fugue, a cloud security posture management company, expanding its cloud security capabilities.

Snyk is a good fit for DevSecOps pipelines and organizations that need a developer-centric SCA and SAST solution with good SDLC integration, and that can identify vulnerabilities in the application code and the underlying containers and IaC.

Strengths

- In its offering, Snyk continues to reflect the main traits of cloud-native application development, namely that AST is mainly used by developers and that application and infrastructure layers increasingly blur together. Snyk platform provides a developer-friendly AST tool focused on IaC security, container security and application security, in third-party and homegrown code.
- Snyk provides detailed information about identified vulnerabilities, as well as automated remediation advice for IaC and containers. Snyk also checks whether the vulnerability can be reached inside the code to prioritize fixes.
- The vendor's AST product packaging and pricing is clear, and prices are publicly available for as many as 150 developers. Snyk also offers a free edition of all of its products, including unlimited use for open-source projects.

Cautions

- Snyk's AST offering lacks in-built AST functionality, which can be found in other offerings, including IAST (partners with Hdiv to provide it), DAST (partners with Rapid7 to provide it) and fuzzing. Clients should ensure they understand and monitor the status of OEM and other relationships to avoid potential disruptions.
- Enterprises that primarily buy AST to be used by security professionals, rather than developers, may find that Snyk does not provide the setup and functionality that they require.
- Organizations with traditional applications that run on-premises, and those developing with established, but legacy language and frameworks, will not be able to leverage Snyk's IaC and container-scanning capabilities, and will encounter limited language support for their legacy applications.

Synopsys

Synopsys is a Leader in this Magic Quadrant. Its AST portfolio is one of the broadest in the industry, including core testing capabilities, as well as more-specialized tools. Its operations are geographically diversified, concentrating on the North American market, the APAC region and the European market.

The company is embracing an open-platform model, where results from disparate testing tools are integrated in a single location for analysis, triage and prioritization. This has been supported by the ongoing development of an Intelligent Orchestration capability, along with the acquisition of the Code Dx ASOC platform.

Strengths

- A broad product portfolio — spanning SAST, DAST, IAST, SCA, IaC scanning, container checks, fuzzing, API testing and more — along with support for orchestration and integration. This makes Synopsys a good fit for organizations with complex, multiteam development, using a mix of development styles and programming technologies.
- Synopsys has experienced strong growth, resulting in part from a large sales team and a significantly increased focus by the company on indirect sales and support via value-added resellers (VARs), system integrators (SIs) and managed services partners (MSPs). The company has also invested in customer support, offering an expanded global multilingual support team.
- Concerns over software supply chain risks have led to improved SBOM creation, and other SCA enhancements. The Black Duck SCA component is now able to produce SBOMs in the standard Software Package Data Exchange format, and the company reports it plans to expand this support to other formats (e.g., Cyclone DX).

Cautions

- A history of growth through the acquisition of disparate products has led to an environment with a wide variety of UIs and UXs. Although good integration with developer tools helps mask this complexity from developers, application security teams must navigate different tools to articulate scans to be performed and relevant policies. This has resulted in mixed views on integration and configuration, with most customers citing configuration as a shortcoming.
- User-based pricing has emerged as an industry standard, and Synopsys continues to migrate toward such a model across its portfolio. Given the breadth of the product line, and the availability of add on services and capabilities, pricing can become complex. However, clients generally report satisfaction with pricing and contract flexibility that is on par with peer vendors.
- Reporting is cited as a weak point by customers. This is likely to be another consequence of the dissimilar interfaces offered by individual product components. Aggregation and correlation of results from across tools in Code Dx, available at extra cost, may help users realize a more consistent experience.

Veracode

Veracode is a Leader in this Magic Quadrant. Veracode is a well-known AST provider with a comprehensive SaaS AST offering that includes SAST, DAST, SCA and IAST.

During the past year, Veracode introduced a data-resident European Union (EU) instance of its SaaS product, flexible policy capabilities supporting open-source license risk management use cases in SCA, an API scanning offering and limited secrets management in dynamic analysis.

Veracode is a good fit for organizations looking for multiple AST capabilities, especially those that need AST expert support to grow their internal AST knowledge.

Strengths

- The company's DAST offering is complemented by a stand-alone Veracode Discovery service, which scans a client's perimeter for previously unknown web applications.
- In addition to the usual sources of open-source vulnerability data, Veracode's SCA product is supported through a natural language processing (NLP)-based ML engine that proactively identifies vulnerabilities and sources of operational risk in open-source libraries. This scanning effort extends from analysis of code commits to review of logs, bug reports and other sources.
- Veracode provides extensive support for organizations that need to grow their AST knowledge, through the Veracode Security Consulting team that provides detailed remediation guidance, the Veracode Customer Success Manager and the broader Veracode Customer Community.
- Veracode has made well-thought-out changes to its longstanding AST offering to adapt to DevOps scenarios. Examples are its on-demand IDE scans, the addition of IAST in the IDE and experiential security training for developers.

Cautions

- Unlike many other AST vendors, Veracode does not provide IaC scanning, has limited support for container security scanning, and does not provide fuzzing. Veracode has been slower than some of its competitors to add functionality to support newer application security needs, such as container scanning and API security scanning.
- Although Veracode positions itself as a global vendor, most of the company's revenue comes from North America.
- Veracode also only offers its product as SaaS, which limits its entry possibilities in emerging markets that are not yet comfortable with exposing their code to the cloud.

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 22 November 2021.

Market Participation:

- Provide a dedicated AST solution that supports at least two of the following four AST capabilities as described in the Market Definition/Description section and the Technical Capabilities Relevant to Gartner Clients:
  - Static application security testing
  - Dynamic application security testing
  - Interactive application security testing
  - Software composition analysis
- And, provide at least one of these additional capabilities:
  - API testing
  - Container security scanning
  - Fuzzing
  - Infrastructure as code testing
  - Mobile application security testing
- In addition:
  - Vendors must conform to a repeatable, consistent engagement model using mainly their own testing tools to enable testing capabilities.
  - Tools must be delivered as on-premises software or appliance, a cloud-based appliance or container, SaaS, or some combination of the three form factors.

Market Traction:

During the past four quarters (4Q20 and the first three quarters of 2021):

- Must have generated at least $25 million of AST revenue, including $20 million in North America and/or EMEA (excluding professional services revenue).

Technical Capabilities Relevant to Gartner Clients:

Specifically, technical capabilities must include:

- An offering primarily focused on security tests to identify software security vulnerabilities, with templates to report against OWASP Top Ten and other common vulnerability definitions and standards.
- An offering with the ability to integrate via plug-in, API or command line into developer environments (IDE plug-in/security linter), CI/CD tools (such as Jenkins) and bug-tracking tools (such as Jira).
- Developer support or guidance for remediation of vulnerabilities.
- For SAST products and/or services:
  - Support for common development languages (e.g., Python, Java, C#, PHP, JavaScript)
  - Provide a direct plug-in for Eclipse, IntelliJ IDEA or Visual Studio IDE, at a minimum
- For DAST products and/or services:
  - Provide a stand-alone AST solution with dedicated web-application-layer dynamic scanning capabilities

    - Support for web scripting and automation tools, such as Selenium
- For IAST products and/or services:
    - Support for Java and .NET applications
- For SCA products and/or services:
    - Ability to scan for commonly known vulnerabilities
    - Ability to scan for out-of-date vulnerable libraries
- For container security scanning products and/or services:
    - Ability to integrate with application registries and container registries
    - Ability to scan open-source OS components for known vulnerabilities and to map to common vulnerabilities and exposures (CVEs)
- For IaC support:
    - Ability to do static code tests prior to deployment
    - Evaluate IaC artifacts for security issues, such as misconfigurations, embedded secrets, unneeded services or other potential risks
- For fuzz testing
    - Ability to run automated, continuous fuzz tests
    - Support for common programming languages.
- For API testing
    - Ability to provide tests identifying vulnerabilities associated with APIs, such as those articulated in the OWASP API Top Ten and similar guides.
    - Ideally, the ability to support common and emerging API types and protocols (e.g., REST, GraphQL)
- For mobile AST
    - Ability to test languages and frameworks commonly used for mobile and/or IoT applications (e.g., Swift, Java and Kotlin)
    - Ability to provide tests identifying vulnerabilities associated with mobile applications, such as those articulated in the OWASP Mobile Top Ten and similar guides.
- Business capabilities relevant to Gartner clients: Have phone, email and/or web customer support. They must offer contract, console/portal, technical documentation, and customer support in English (either as the product's/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 weights 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 and detailed in the subcriteria. This criterion specifically evaluates current core AST product/service capabilities, quality and accuracy, and feature sets. Also, the efficacy and quality of ancillary capabilities and integration into the SDLC are valued.

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 are looking at capabilities such as how the vendor supports proofs of concept or pricing options for both simple and complex use cases. The evaluation also includes feedback received from clients on experiences with vendor sales support, pricing and negotiations.

Market Responsiveness/Record: This criterion assesses the ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. It also considers the vendor's history of responsiveness to changing market demands. We evaluate how the vendor's broader application security capabilities match with enterprises' functional requirements, and the vendor's track record in delivering innovative features when the market demands them. We also account for vendors' appeal with security technologies complementary to AST.

Marketing Execution: This criterion assesses the clarity, quality, creativity and efficacy of programs designed to deliver the organization's message 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 or account support. This may also include ancillary tools, customer support programs, availability of user groups and service-level agreements (SLAs).

Operations: This criterion assesses the ability of the organization 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

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 2022	

Source: Gartner (April 2022)

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 customer demands, and they can shape or enhance market changes with their added vision. It includes the vendor's ability to understand buyers' needs and translate them into effective and usable AST products and services.

In addition to examining a vendor's key competencies in this market, we assess its awareness of the importance of:

- Integration with the SDLC (including emerging and more-flexible approaches)
- Assessment of third-party and open-source components
- The tool's ease of use and integration with the enterprise infrastructure and processes
- How this awareness translates into its AST products and services

Marketing Strategy: We look for clear, differentiated messaging 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 are looking at the product and service AST offering, and how its extent and modularity can meet different customer requirements and testing program maturity levels. We evaluate the vendor's development and delivery of 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 are innovating to address evolving client requirements to support testing for DevOps initiatives, as well as API security testing, and serverless and microservices architecture. We also evaluate developing methods to make security testing more accurate. We value innovations 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 specific needs of geographies outside the "home" or native geography, directly or through partners, channels and subsidiaries, as appropriate for that geography and market. We evaluate the worldwide availability and support for the offering, including local language support for tools, consoles and customer service.

Table 2: Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	High

Evaluation Criteria	Weighting
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 2022	

Source: Gartner (April 2022)

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 supporting 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 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 a particular technology (for example, SAST, DAST or IAST) or by focusing on a single delivery model (e.g., on AST as a service only). In addition, they have demonstrated substantial competitive capabilities against the Leaders in their particular focus area, and have demonstrated momentum in their customer base in terms of overall size and growth.

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 support 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. 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 critical 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

Welcome to the 2022 Magic Quadrant for Application Security Testing. Many of the trends we identified in last year's Magic Quadrant — security maturity, tool use and organizations increasingly moving to the cloud — continued to evolve and are even more important issues today. In 2021, we talked about team maturity in terms of Early, Intermediate and Advanced phases, briefly summarized below.

Phase	Description
Early	Teams in this phase are making the transition from having penetration testing as their primary secure development control, to using tools from the standard AST toolset, often SAST and SCA.
Intermediate	Teams have established a basic process and are moving from a "criticality-based" set of metrics to "risk-based" metrics. Teams in this phase generally have all or most of the basic tools and are looking to make incremental improvements in the overall process and security posture. Beyond SAST/DAST/SCA, we typically see more use of IAST (and sometimes RASP), API testing, fuzzing and early work on IaC and container security tools.

Advanced	Advanced teams are characterized by all or mostly container-based and cloud-native development. Typically, cloud native or containerized applications have graduated from the proof of concept (POC) stage into the full production environment. In addition to tools from the earlier stages, we see a focus on security posture management (CSPM) Cloud workload protection platform (CWPP)/CSPM tools and CNAPP.

This continues to hold in 2022, although there are some changes. The Early phase group is still the largest; however, it's smaller relative to last year, representing about half the inquiry volume (down from roughly two-thirds), with the other two splitting the remainder. This is reflected in some of the topics we see from clients.

Moving Into the Cloud: We see more organizations finally making the transition from on-premises to the cloud in production. Although this has long been the purview of pilots and POCs, applications are increasingly moving from their existing environment and defense in depth into the cloud. Gartner is increasingly seeing that the cloud attack surface and defense options are not well understood by developers and security teams. The security context for the application has changed, but the degree of change, and the defense-in-depth options offered by cloud providers are not always understood. In part, this is related to another problem: Security teams may not be up to speed on containerized development and their security options. Given that both developers and security teams are moving at a fast pace, neither has a lot of spare time to understand the details and consequences of the other team's technology. This can lead to awkward, costly delays and exposure.

AST vendors are increasingly adding cloud native security utilities to their portfolios, and we have been evolving the Magic Quadrant criteria to match. Many of those vendors are working with security teams to bring them up to speed on options. However, the industry isn't where it needs to be yet. We see security coaches (see DevOps Security Coaches Help Organizations Gain Leverage Without Training Everyone) playing an important role here, acting as a bridge between both teams, but it's often a heavy lift for developers who are part-time coaches.

Risk-Based Metrics: An important trend we saw in 2021, and an indicator of the increasing maturity of the DevSecOps market is the growing emphasis on risk-based metrics. Many early phase teams use vulnerability criticality as a metric, and this is a good start. It is a handy approximation for risk, e.g., the OWASP Top 10 are often the riskiest vulnerabilities, if they are reachable. However, risk and criticality soon diverge and, of the two, risk survives context changes better, and is more broadly understood by senior management.

Unfortunately, real security risk calculations that are fungible with other measures, such as business risk, are unique to each organization, because they depend on implementation details such as defense-in-depth measure and incident response measures. Across the vendor landscape, we see growing recognition that risk is playing an increasingly important role in security decision making, and we expect this trend to continue in 2022 .

Market Overview

The application security testing market continues to rapidly grow and evolve, largely along the lines outlined in last year's Magic Quadrant. At a high level, three trends are observed:

- Continuing rapid growth and increased competitive complexity
- Expansion in the scope of testing required
- An emphasis on the shift of many application security functions directly into the hands of development and operations teams

Growth and Complexity: An analysis of end-user spending within the market shows end-user spending reaching $2.6 billion in 2021, a 20% year-over-year increase. That growth rate exceeded expectations, and reflects strong underlying demand. Geographically, the North American market grew in size, although its overall share of the market declined — from 73% to 68% — as market share growth in Europe and the United Kingdom (17%) and the APAC region (12%) increased.

Market drivers, centered on increasing regulatory and compliance mandates and a growing recognition of the risks associated with software, remain. A variety of high-profile software supply chain attacks underscored those risks, and — at least in the U.S. — prompted regulatory actions that will continue to drive overall application security demands. Based on these drivers, we expect worldwide AST end-user spending to exceed $3.1 billion in 2022.

The AST market continues to see increased competition, among traditional participants and new sources, such as development infrastructure vendors. These include GitHub, GitLab, Jfrog and Sonatype. Cloud security vendors continue to show some overlap, and competition, particularly in areas such as container security and IaC scanning. Increased competition has led some vendors to simplify and reduce pricing, as well as to expand the scope of their offerings to offer a better fit to customer requirements. This includes both organic growth, as well as the addition of functionality via acquisitions. Examples include Checkmarx's purchase of Dustico; Rapid7's buy of Alcide; Snyk's picks of FossID, CloudSkiff and Fugue; Sonatype's purchase of MuseDev; and Synopsys's acquisition of Code Dx.

Expanded Scope: Changing application architectures and new technologies, both of which bring increased complexity and diversity to organizations' software portfolios, require new approaches to, and types of, AST. Testing approaches that were considered niche or infrequently applied, such as IaC scanning, have become increasingly mainstream. Vendors continue to innovate around more-traditional approaches to testing.

An increase in white space to the right of the Magic Quadrant reflects the need for vendors to continue to innovate, even within well-established market segments. Static analysis, for example, shows high penetration rates, but vendors have introduced new approaches in efforts to boost speed and accuracy. Dynamic testing, long a standard for web application testing, is seeing new life and growth as a means of testing APIs. And SCA has begun to incorporate features designed to warn of operational risks associated with supply chain attacks and other threats.

Developer-Centric Application Security: Although organizations remain at various stages in their journeys toward a "shift left" focus in AST, the underlying developer enablement and automation/integration features required to achieve that vision have become essential, generally ubiquitous requirements for buyers. Although the quality of execution can vary considerably, all vendors in the Magic Quadrant have delivered these capabilities to market, and espouse a developer-centric approach to application security.

Differentiation here — beyond the typical requirements to improve flexibility, ease of use and speed — is emerging in areas such as application security orchestration and correlation capabilities, and the addition of more cloud-native application security and protection features. These help manage the increased complexity of testing, simplify the inclusion of third-party and open-source testing tools in an application security program, and aid in prioritization and triage of findings.

Hands-on responsibility for application security design and testing tasks is shifting to development and engineering teams. Gartner research reveals that more than half of software engineering leaders are directly responsible for application security, and another third share responsibility. Despite the overall shift, traditional application security groups remain highly relevant. We see the role of these groups moving toward a focus on policy setting and enforcement (e.g., with respect to acceptable levels of risk), and supervising and reporting on an organization's overall application security program. This shift will drive its own innovations, focused on simplifying the ability of organizations to manage their application security programs from a risk-based posture.

Evaluation Criteria Definitions

Ability to Execute

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.
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.

Revision #1
Created 2023-01-21 16:10:04 KST
Updated 2025-04-19 01:39:15 KST