Magic Quadrant for Application Security Testing

Published 27 May 2021 - ID G00733839 - 52 min read

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

Modern application design and the continued 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.

Strategic Planning Assumption(s)

By 2023, 90% of web-enabled applications will have more surface area for attack in the form of exposed APIs rather than the user interface (UI), up from 50% in 2020.

By 2022, API abuses will move from an infrequent to the most frequent attack vector, resulting in data breaches for enterprise web applications.

Market Definition/Description

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.

Gartner identifies three main styles of AST:

- **Static AST (SAST)** technology analyzes an application's source, bytecode or binary code for security vulnerabilities typically at the programming and/or testing software life cycle (SLC) phases.
- **Dynamic AST (DAST)** technology analyzes applications in their dynamic, running state during testing or operational phases. DAST simulates attacks against an application (typically web-enabled applications and services), analyzes the application's reactions and, thus, determines whether it is vulnerable.
- **Interactive AST (IAST)** technology combines elements of SAST and DAST simultaneously. It is typically implemented as an agent within the test runtime environment (for example, instrumenting the Java Virtual Machine [JVM] or .NET CLR) that observes operation or attacks and identifies vulnerabilities.

Software composition analysis (SCA) technology is used to identify open-source and third-party components in use in an application, and their known security vulnerabilities.

AST can be delivered as a tool or as a subscription service. Many vendors offer both options to reflect enterprise requirements for both a product and service.

Over the last three years, Gartner has seen clients request additional services and tools to round out their AST coverage and include new development methods and artifacts. This year, we've decided to address these trends and expand the scope of AST to include:

- **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 support centers around the application of the process and disciplines traditionally associated with software development to manage IT infrastructure. IaC is also

commonly called programmable infrastructure (PI), although PI can include other aspects of cloud-native automation, including containers and immutable infrastructure.

- **Container security:** Container security is the application of security processes, testing and controls to Linux container-based environments, ideally with support for Kubernetes. Comprehensive container security starts in development with an assessment of the risk/trust of the contents of the container, secrets management and a Kubernetes configuration assessment. It should extend into production with runtime container threat protection and access control.
- **Fuzz testing:** Fuzz testing is the practice of deliberately feeding garbage to your objects to ensure that they degrade gracefully or manage the bad data properly. As an example, for API testing, testers would include text characters as a parameter for a call that is expecting a number. Fuzz testing is also called "nondeterministic testing" and has become a popular way to introduce some of the tools commonly used in penetration tests into AST.
- **API testing:** APIs have become an important part of modern applications (e.g., single-page applications) but do not fit well within the traditional AST toolsets. As APIs become a significant security concern, security support must continue to keep pace.
- **Cloud-native support:** As development moves increasingly toward the cloud, developer security tools need to follow. We view support for cloud-native environments to be, simply, having security tools offered as part of the integrated development experience in a public cloud — for example, Amazon Web Services (AWS), Microsoft Azure or Google Cloud Platform (GCP).

This 2021 Magic Quadrant focuses on vendors' traditional AST offerings, their maturity and features as tools or "as a service," and their ability to secure some portion of the attack surface represented by some of the more modern application development concerns.

Gartner has observed the major driver in the evolution of the AST market is the need to support enterprise DevOps 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 more heavily on the buyer's needs when it comes to supporting rapid and accurate testing capable of being integrated in an increasingly automated fashion throughout the software development life cycle (SDLC).

Magic Quadrant

Figure 1: Magic Quadrant for Application Security Testing

Source: Gartner (May 2021)

Vendor Strengths and Cautions

Checkmarx

Checkmarx is a Leader in this Magic Quadrant. Dynamic analysis continues to be deemphasized in the vendor's portfolio, available only as a managed service. The company is competitive in a variety of use cases, but performs best in DevSecOps and cloud-native environments, or where SAST is a high priority.

Checkmarx conducts business globally, with principal offices in the U.S., Europe, Israel and Singapore.

The most recent addition to the Checkmarx portfolio is an infrastructure-as-code scanning tool, which the company has released as an open-source project. Keeping Infrastructure as Code Secure (KICS) provides support for Terraform, Kubernetes, Docker, AWS CloudFormation and Ansible environments, offering over 1,000 checks that search for vulnerabilities and misconfigurations.

Strengths

- CxSCA is now available as a stand-alone solution, although it continues to benefit from integration with SAST, which enables exploitable path detection. The feature, which has also been added by other vendors, aids in prioritizing open-source package upgrades and fixes.
- CxIAST, a passive IAST tool, helps identify vulnerabilities in code and with discovery of APIs. It offers a graphic representation of flow, highlighting control and data paths across microservice environments. The specific feature, still rare among AST products, helps developers better understand where best to focus remediation efforts.

- Checkmarx has strong developer enablement, providing guidance for vulnerability assessment and remediation across environments, complemented by CxCodebashing, a developer training tool.

Cautions

- While positioning itself as a hybrid solution (on-premises and cloud-based), Checkmarx notes that some customers pass it by in favor of a stronger SaaS offering. The company indicates it plans to expand SaaS support in 2021.
- DAST is only available via managed service, and relies on another vendor's tools. Lack of control over the direction of the tool and the potential for disruptions in the relationship make Checkmarx a less viable option for users if DAST is a primary requirement.
- Customers cite high costs — an increasingly common concern across many vendors. Checkmarx has worked to simplify licensing, with most products tied to the number of users. CxIAST, as well as the DAST managed service, are based on applications/projects.

Contrast Security

Contrast Security is a Challenger in this Magic Quadrant. It is known for passive IAST, where instead of depending on active scanning to generate attacks and identify vulnerabilities, it uses already planned nonsecurity testing such as quality assurance.

Contrast Security is based in the U.S., but also sells in the EMEA and Asia/Pacific regions. Its platform consists of IAST (Contrast Assess), SCA (Contrast OSS) and RASP (Contrast Protect). Contrast Assess includes Contrast OSS, which automatically performs SCA. Recently, Contrast Security acquired CloudEssence to expand its cloud-native testing capabilities, and partnered with NowSecure for mobile AST. It also expanded language coverage, made its TeamServer possible to host in a container, and introduced vulnerability prioritization.

Contrast is a good fit for organizations looking for approaches to insert automated, continuous security testing that is developer-centric.

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.
- Gartner client feedback indicates that Contrast Security helps in embedding AST among development teams without security testing expertise, as the agent identifies vulnerabilities by "piggybacking" on normal application testing. Clients also suggest that the vendor's approach to passive IAST provides a low number of false positives.
- 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 only offers an IAST and SCA solution, and does not currently provide stand-alone SAST or DAST tools or services.
- Even though Contrast Security provides integrated development environment (IDE) integration to discover and fix vulnerabilities while coding, it does not offer the stand-alone "spellchecking" SAST-lite capabilities that some vendors provide.
- Contrast Security only instruments and tests application back ends, hence it does not test the client-side code of the web or mobile apps, and does not identify front-end code vulnerabilities such as DOM-based XSS.

Data Theorem

Data Theorem is a Visionary in this Magic Quadrant. It addresses cloud-native and containerized applications with core competencies around security for cloud-native development, APIs and single-page applications (SPAs). It is therefore a good fit for organizations focusing on these apps.

Data Theorem offers an API, IaC testing and mobile application testing, while providing visibility into data flows. It also offers a high degree of automation and continuous compliance. The vendor provides SAST/DAST and IAST through its Analyzer Engine, which uses results from its Web Secure, Mobile Secure and API Secure products to generate a robust view of the applications, APIs and data flows.

While Data Theorem offers traditional SAST/DAST/SCA, clients who only want those tools might be better served by some of the other vendors evaluated in this research.

Strengths

- Data Theorem's setup includes a novel automated discovery phase. This looks through all your APIs, web calls and other signals to determine the scope of your attack surface in a way similar to that used by professional security researchers and hackers. This is surprisingly easy to use and can help bring a complex set of applications and services into sharp focus for both developers and security professionals.
- Data Theorem watches for and remediates cloud misconfigurations. This allows cloud-native applications to protect against configuration drift and accident by automatically undoing harmful changes.
- Data Theorem has comprehensive support for SPAs with Web Secure, which runs an agentless dynamic runtime analysis and also provides an array of hacker toolkits for use in testing critical applications.

Cautions

- Data Theorem has support for SCA but at a generally lower level than other AST vendors, and has not developed partnerships for supporting this.
- Data Theorem does not have the level of developer education support for core tools like SAST and DAST that many AST Leaders and Challengers have developed. For example, it has no in-editor security lessons, IDE plugin or security linter.
- While currently supporting application development on Amazon and Google, Data Theorem is still in the early stages of supporting Microsoft Azure Marketplace and Alibaba, although it expects to support them more fully later in the year.

GitHub

GitHub is a Niche Player in this Magic Quadrant. The company provides an example of a new approach to AST, where testing tools are a part of the underlying development environment. GitHub's position within the development infrastructure enables tight integration and ease of use for GitHub users.

GitHub's primary focus is on SAST and SCA, although integrations for other types of testing are offered. Availability and cost of specific features varies across service levels, although many security functions are included at no extra cost for public repositories. Code scanning and more complete SCA capabilities are available to commercial GitHub Enterprise users as part of an Advanced Security offering, priced by the user.

Strengths

- Tight integration with GitHub Actions and the GitHub source code repository is a core strength and attraction of the solution. Organizations can enable checks, either at the organizational or project level, and analysis is performed automatically as code is committed or pull requests are generated.
- Developer enablement is good, albeit essentially limited to developers working in the context of GitHub itself. (A plug-in for the Visual Studio IDE is available.) Results are displayed during a pull request and on a security tab within the GitHub interface, and clicking through reveals details about the vulnerability. For example, its cause, code paths, consequences,

related common vulnerabilities and exposures (CVEs), suggested fixes for problems in code, or issues associated with a particular open-source package, along with an automated pull request to remediate an open-source flaw (where a fix exists).

- Prospective customers' familiarity with GitHub, combined with its tight integration of security capabilities, make it an attractive solution for organizations that rely on the underlying repository.

Cautions

- GitHub has comparatively limited language support. Its primary focus is on code analysis (using a form of semantic/variant analysis) and SCA. Support is provided for more common languages — C variants, Java, JavaScript, TypeScript, Python and Go — but organizations with more diverse portfolios will require alternative or supplementary tools.
- The company relies on partnerships and its marketplace to support several capabilities outlined in this Magic Quadrant. Integration with the platform and presentation appear robust for supported partnerships, although depending on the choice, some tools may entail extra cost. Some functions, however, aren't available — these include dynamic and interactive scanning, as well as mobile application testing.
- Support for IDE integration is currently limited to a Visual Studio Code plug-in. The product's focus is on the native GitHub platform. Although that's a strength for GitHub users, it's a disadvantage for those who don't use the platform, or only use it for part of their overall portfolio.

GitLab

GitLab is a Challenger in this Magic Quadrant. It provides AST as part of its broader DevOps platform. GitLab offers AST as part of its Ultimate/Gold tier. It combines proprietary and open-source scanning tools and functionality within its own workflows to provide SAST and DAST. It also provides SCA with Dependency Scanning. GitLab's security offering includes secrets management, open-source scanning capabilities with Container Scanning, and License Compliance.

In the past year, GitLab has acquired Peach Tech for its instrumentation and Fuzzit for its crash analysis technology. It has added mobile AST, integrating the Mobile Security Framework (MobSF) into the platform, as well as API and coverage-guided fuzzing capabilities. It has also added support for offline environments and vulnerability management. GitLab has partnered with IBM to provide GitLab Ultimate within IBM Cloud Paks.

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

Strengths

- The vendor's AST offering — including SAST, Secrets Detection and Dependency Scanning — is included in its Ultimate/Gold tier, which is predictably and transparently priced. Also, SAST and secret detection come as part of GitLab's free edition.
- GitLab's AST offering includes secrets management functionality, which scans the content of the repository and identifies credentials and other sensitive information that should not be left unprotected in the code.
- GitLab provides container scanning for vulnerabilities, and for code deployments in Docker containers and those using Kubernetes. Its fuzzing capabilities are both granular and easy to use with a low level of expertise, thanks to the automation that is provided.

Cautions

- GitLab's SAST lacks features that are available in more mature offerings. Language coverage is limited and the dashboard lacks the granularity and customizability of more established tools. Its SAST offering lacks features such as quick-fix recommendations and real-time spell checking.
- GitLab does not currently provide IAST options in its offering, even though its recent acquisition of Peach Tech provides it with instrumentation options.

- GitLab uses different tools for different languages and frameworks, many of which are open source, even though it actively contributes to their development and maintenance. As an example, the vendor's DAST offering is essentially the Open Web Application Security Project's (OWASP's) open-source ZAP tool, while its mobile offering consists of MobSF.

HCL Software

HCL Software is a Leader in this Magic Quadrant. It is a good fit for organizations with a wide variety of development styles.

HCL AppScan offers a mix of deployment options, including on-premises, SaaS and hybrid. On-premises products include AppScan Source for SAST, AppScan Standard for DAST and AppScan Enterprise for DAST and IAST. Service-based offerings are all grouped under the AppScan on Cloud brand and include SAST, DAST, IAST and SCA support.

For IaC scanning, HCL AppScan examines YAML configurations for Docker and Kubernetes, as well as command line scripts used to run Docker images. AppScan is offered as part of the vendor's SAST integration, making it easy for developers to use without leaving their workflow. HCL also has extensive API testing and offers CodeSweep, a community edition of AppScan that plugs directly into Visual Studio and performs many of the functions of the full AppScan product.

Strengths

- AppScan's Intelligent Finding Analytics (IFA) helps improve accuracy and identify a "best fix" location for vulnerabilities. This is a popular feature with development teams and was the most common highlight in Gartner's Peer Insights reporting on AST for 2020.
- AppScan enjoys a good reputation for DAST scanning, sharing the same basic technology across the portfolio. The desktop-based AppScan Standard is a customizable offering especially suited for manual assessments. Incremental scanning allows for faster scans, and an "action-based" browser recording technology enables testing of complex workflows and improved insight into SPAs.
- AppScan's IAST capability has been broken out from its DAST functionality since last year. A passive IAST approach, increasingly in favor among DevOps teams, was released in mid-2020, to generally favorable reviews.

Cautions

- Gartner clients mentioned that HCL's technical support team takes a relatively long time to provide guidance on more complex use cases.
- HCL has made improvements to AppScan's user interface in terms of layout and customization, but clients still mention it as an area of relative weakness.
- The overall pricing model for HCL's portfolio remains complex and is frequently mentioned by customers as a weakness. (Price complexity is common, but not a universal complaint across vendors).

Invicti

Invicti is a Niche Player in this Magic Quadrant. The company sells products under two well-known brands, Acunetix and Netsparker. Invicti will be of interest to organizations with a principal requirement for DAST scanning.

Functionality is similar across product sets, with the exceptions of interactive analysis and fuzzing. As of the time of this report, these features are available only in the Acunetix Premium offering.

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

Strengths

- Both Netsparker and Acunetix are well-regarded by users, and compare favorably with competitors in overall customer experience. The Acunetix product modestly outperforms Netsparker based on Gartner Peer Insights data.

- Multiple approaches are provided to allow testers to minimize wasted time from scans of code that hasn't changed. Incremental scans can be enabled for URLs where a hash change indicates a code change. Alternatively, the tool supports a Retest option that looks specifically at issues discovered in a previous scan, testing only those flaws to confirm a fix.
- Netsparker provides an ongoing scan of a specified range of IP addresses, discovering errant and forgotten websites. While not unique, the feature is helpful for security teams trying to keep pace with developer and business unit activity.

Cautions

- The Invicti products are best suited to organizations with a heavy emphasis on DAST. There is no native support for SAST, container scanning, IaC scanning, mobile or business-critical application assessment capabilities. The Acunetix IAST solution, providing support for PHP, .NET and Java, largely informs the DAST scanner of code locations for discovered vulnerabilities.
- 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 solutions (for authentication purposes). But there is no integration with an IDE, although developers can access information about findings via trouble ticket integrations, or via CI tools.
- Trouble tickets, such as Jira, provide basic information, but more detailed data requires the developer to click back to the Netsparker console. Similarly, within the development toolchain, an executive-level report — similar to PDF and HTML reports generated by the console — is presented, but securing additional detail requires a visit to the console.

Micro Focus

Micro Focus is a Leader in this Magic Quadrant. Its Fortify products provide comprehensive AST, with broad language coverage and a range of customization and integration options.

Micro Focus is based in the U.K. and is a global provider of IT products and services. It has a global sales reach, with a strong presence in North America, EMEA and Central America markets. Fortify offers Static Code Analyzer (SAST), WebInspect (DAST and IAST), Software Security Center (its console) and Fortify Audit Workbench (AWB). Through its integration with Sonatype, Fortify provides SCA. Fortify provides its AST as a product, as well as in the cloud, with Fortify on Demand.

In 2020, Fortify introduced ScanCentral, an evolution of its CloudScan framework, to run scans on-premises in a centralized fashion. Fortify also partnered with Secure Code Warrior to offer secure development training to developers.

Fortify is a good fit for a broad number of use cases, and especially for large enterprises with multiple, complex projects and a variety of coding styles and experience levels.

Strengths

- Micro Focus has one of the most complete AST offerings, with excellent capabilities for all main AST technologies, as well as good capabilities for the additional newer areas of AST.
- Fortify Security Assistant is a real-time security checker that operates within the IDE. It is not a replacement for a comprehensive SAST scan, but it can provide a lightweight automatic check for developer security mistakes as the developer codes.
- Micro Focus has extended its Fortify Audit Assistant feature to allow teams the flexibility to either manually review artificial intelligence (AI) predictions on issues, or to opt in to "automatic predictions," which allow for a completely in-band automated triaging of findings. This contributes to reducing false positives.

Cautions

- Fortify is known for its depth and accuracy of results, which meets the needs of enterprise customers that then leverage contextual-based analysis. However, less mature organizations looking for incremental improvements often express

experience challenges with the complexity and volume of unfiltered results.

- Fortify does not provide an option for stand-alone IAST, nor stand-alone fuzzing. It only offers active IAST, meaning in conjunction with DAST.
- Gartner clients report that the pricing remains complicated and expensive, notwithstanding Fortify's efforts to offer flexible license and pricing models.

Onapsis

Onapsis is a Niche Player in this Magic Quadrant. It is a U.S.-based company with centers in the U.S., Germany and Argentina. Onapsis has a strong focus on business-critical applications, and has developed a good reputation with global companies and clients focusing on that market.

Onapsis continues to stand out for its deep understanding of the specialized development framework, needs of developers and the environment in which these applications are developed and executed, such as SAP Business Application Studio in Cloud Foundry.

The Onapsis portfolio also includes technology integrated from its 2019 acquisition of Virtual Forge, a prominent player in the SAP code security space that enjoys strong developer support.

Onapsis is a good fit for business-critical modernization projects, such as S/4HANA transformation and cloud migrations. New features include support for integration with CI/CD tools (e.g., SAP ChaRM), automated code correction of vulnerabilities and improved data and control flow logic.

Strengths

- Onapsis offers integration with container environments (i.e., SAP Business Application Studio) in the Cloud Foundry environment.
- Its data flow and tracking options are especially useful for monitoring compliance risks in applications in financial services, human capital management (HCM), supply chain management (SCM) and other applications.
- Onapsis has increased its developer support options and offers an auto remediation function that allows developers to confirm security fixes.

Cautions

- Other, large vendors are entering the AST space with support for languages like ABAP and Apex. However, these new entrants don't have the expertise in working within specific environments like SAP, although that will likely change over time.
- 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).
- With a focus on applications supported by SAP and Oracle, testing is largely focused on those frameworks, making integration into a larger or more traditional AST environment somewhat challenging. Onapsis plans to expand its support for additional business-critical applications throughout 2021.

Rapid7

Rapid7 is a Visionary in this Magic Quadrant. While the company is known for dynamic scanning and vulnerability management, it is aggressively expanding its portfolio and making changes in direction.

SCA is supported via a new partnership with Snyk. In late April 2020, the company announced the acquisition of DivvyCloud, a cloud security posture management vendor, enabling support for capabilities such as IaC scanning.

Rapid7 is based in the U.S., with sales and support offices primarily located in North America and EMEA, and with some presence in the Asia/Pacific region. All products are available as SaaS offerings, with most also available as on-premises solutions. (Notable exceptions are InsightVM and tCell.)

Strengths

- Rapid7 continues to enjoy a strong reputation for DAST, especially in support of in-depth custom manual assessments. Tests can be performed interactively, allowing for the manipulation of parameters, aiding troubleshooting and the validation of fixes.
- Acquisitions such as DivvyCloud and Alcide help move the company toward more modern application security requirements, and are expected to provide support for application portfolios more aligned with cloud-native applications.
- Rapid7 continues to enjoy good marks from users for the product's ease of use, reporting and support. For example, developers are provided information such as recommendations, description and error information, and attack replay functionality, which enables them to understand, patch and retest vulnerabilities.

Cautions

- Rapid7's aggressive expansion of its portfolio means that, in the short to midterm, it faces the complex undertaking of managing multiple relationships and integrating various technologies. Gartner does note some user complaints around complexity. Buyers seeking to leverage the company's expanded capabilities should ensure they carefully examine and understand the roadmap and timetable for planned integrations.
- Rapid7 lacks a native static analysis solution. At present, the company leverages a partnership with Checkmarx to service customers requiring the capability. Again, prospective buyers should ensure they understand the roadmap and prospects for any partnerships or integration.
- While test results are highly detailed, Rapid7's tools continue to lack direct integration with IDEs, prompting developers to switch to the InsightAppSec dashboard (or browser extension) to review data and supporting information.

Snyk

Snyk enters this Magic Quadrant as a Visionary. Snyk is a well-known SCA vendor that has expanded into AST, with extensive knowledge of developer environments and a developer-friendly approach.

Headquartered in the U.S., Snyk has main offices in North America, Europe and Israel, as well as a small virtual workforce. Its AST offering includes SCA with Snyk Open Source and Snyk Container, as well as SAST with Snyk Code and Snyk Infrastructure as Code.

In the past year, Snyk has acquired SAST provider Deepcode.ai, which provides an ML-based scanning of interpreted code. The vendor has also refined its support for fix recommendations for unsecure Kubernetes and Terraform configurations, and added real-time feedback in the IDE.

Snyk is a good fit for organizations that need a developer-centric SCA and SAST solution, and that can scan both application code and IaC.

Strengths

- Snyk envisages that application and infrastructure layers increasingly blur together, as do development and runtime phases. This vision and its offering align with what Gartner finds enterprises experience as they undergo digital transformation.
- Snyk's cloud-native AST capabilities are mature and granular. The vendor provides detailed information about identified vulnerabilities, as well as automated remediation advice. Snyk also checks if the vulnerability is actually reachable inside the code or not, in order to prioritize fixes.

- The vendor's AST offering is predictable and prices are publicly available for up to 150 developers. Snyk also offers a free edition of all of its products, including unlimited use for open-source projects.

Cautions

- Snyk has a relatively new AST offering and, while it is a well-known vendor in the SCA space, there is not much awareness among Gartner clients of Snyk as an AST option. Gartner sees Snyk mainly competing with SCA and cloud workload protection platform (CWPP) players.
- Snyk's offering is not as complete as that of many other traditional AST vendors. For example, it doesn't provide SAST for iOS applications. It also lacks IAST, fuzzing and its own DAST capabilities, as it partners with Rapid7 to offer them. Also, Snyk doesn't support business-critical applications such as SAP, Salesforce and other CRM and ERP applications.
- Enterprises with traditional development approaches such as waterfall, and those that primarily buy the product for it to be used by security professionals, rather than developers, may find that Snyk doesn't provide the setup and functionality that they require.

Synopsys

Synopsys is a Leader in this Magic Quadrant. Based in the U.S., Synopsys has continued to make a series of strategic acquisitions to define and expand a suite of secure SDLC tools. The most recent example is Tinfoil Security, acquired in January 2020, which adds significant API testing capabilities to the Synopsys suite, a theme we are seeing in other Magic Quadrant players.

Synopsys has added a microservices analysis to Seeker, its IAST tool, giving users a visual interface into the data flow between components. This can help identify potentially unsafe data flow issues. The vendor's new Intelligent Orchestration solution integrates into CI/CD pipelines and uses policy as code to automatically coordinate security testing activities across its portfolio of tools, as well as third-party tools, based on the significance of code changes and the risk profile of the application. While this is a recommended practice in the industry, the addition of data from third-party tools is a significant step forward.

Synopsys is a good fit for large organizations with complex, multiteam development using a variety of development methods (e.g., Agile, DevOps).

Strengths

- Synopsys has containerized its offering as a series of orchestrated microservices (Intelligent Orchestration), which allows for scans to be triggered by events in the DevSecOps process (e.g., code pull requests, build events). This allows a very high degree of flexibility and forward compatibility as developers mature their process.
- The Synopsys Code Sight plug-in is a good fit for DevOps shops, with the ability to both suggest and autofix and do fix verification. This fits well with most development teams, regardless of experience.
- Synopsys introduced a new microservices analysis feature to its Seeker IAST product, which provides a graphical view and insights into the data flow of microservices-based applications for both developers and security.

Cautions

- Gartner client feedback indicates that initial integration with existing software development practices, and ongoing maintenance, can be complicated depending on tools and existing workflows.
- Feedback from small and midsize businesses indicates that, despite interest in the vendor's solutions, the price is often outside their budgets. Synopsys' sales process is also complicated, and clients have reported trouble navigating it.
- Intelligent Orchestration is a good idea, but is currently still in its early phases, resulting in a mixture of reporting from both it and Synopsys Polaris.

Veracode

Veracode is a Leader in this Magic Quadrant. The company's products perform well in several use cases, including both traditional development methodologies and DevOps. They lag in cloud-native use cases due to shortcomings in areas like IaC and container scanning.

Veracode has increased its investment in DevSecOps. Its platform now supports a pipeline approach to optimize scan times across the development life cycle. Veracode has also expanded integrations into developer ecosystems, including AWS CodeStar. Support for GitHub Actions was added, as well as feedback to the GitHub Security Console and GitLab issues and pipelines.

Veracode offers a global presence, with several regional offices supported by an expanding reseller channel.

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-based machine learning engine that proactively identifies vulnerabilities in open-source libraries. This scanning effort extends from analysis of code commits to review of logs, bug reports and other sources.
- Veracode performs well in the area of developer enablement. IDE-based on-demand scans return results rapidly, directly to the IDE. An assortment of remediation guidance is readily available. Uniquely, Veracode flags security best practices in code, providing positive reinforcement. Users can request one-on-one consultations with Veracode AppSec consultants to get assistance in understanding results. The company also introduced Veracode Security Labs early in 2020, a "hands on" lab-based offering that delivers interactive training to developers.

Cautions

- Although Veracode has made significant strides in support of DevOps environments, some areas require additional attention. The company doesn't yet support IaC scanning. Container scans are limited to Docker, and are delivered via the SCA product, limiting their scope to open-source vulnerabilities. Veracode has no stand-alone API testing product, although it does support testing via DAST.
- During client inquiries, Veracode customers noted high pricing, especially at renewals.
- While Veracode positions itself as a global vendor, it has a small number of regional offices that are supported by an expanding reseller channel. Most of the company's business remains largely focused on North America.

WhiteHat Security

WhiteHat Security is a Challenger in this Magic Quadrant. It is a reliable player in the market, able to accommodate a wide array of development styles and applications. WhiteHat offers a complete set of AST tools — including SAST, DAST, SCA and Mobile ASTs — API discovery and testing, as well as IAC testing and fuzz testing of web applications. WhiteHat has a consistent level of quality and ease of use across its toolset, and its human-augmented false positive reduction is very popular with clients. The Sentinel platform focuses on DAST (i.e., on vulnerability discovery and testing at the application runtime phase). WhiteHat now offers its SCA separate from its SAST product offering.

The vendor continues to refine its patented Directed Remediation capabilities, where fixes are automatically suggested to developers for selected findings. WhiteHat's offerings are service-based, although the vendor offers a virtual appliance for local scanning, with results sent to the cloud for verification, correlation and inclusion in dashboards and reporting.

WhiteHat is a good fit for most teams starting or maturing their secure SDLC.

Strengths

- WhiteHat has a strong reputation among Gartner clients as a DAST-as-a-service provider and should be considered by buyers seeking an AST SaaS platform. WhiteHat has continued down the DAST path with its Intelligence-Directed (ID) DAST offering, which is built for integration into DevSecOps, native API testing and cloud-native environments.
- In a market known for high price and complexity, WhiteHat offers relatively straightforward and clear pricing, making it a comparatively simple exercise to project costs for budgeting.
- WhiteHat Sentinel Dynamic provides continuous, production-safe DAST of production websites with automatic detection and assessment, and alerts for newly discovered vulnerabilities, thus serving as production applications' protection and early warning layer.

Cautions

- WhiteHat does not offer an IAST solution. While not a traditional IAST tool, ID DAST serves a similar function.
- WhiteHat's strategic focus centers on using runtime security technologies (such as DAST) as the central tool for the secure SDLC. However, the market seems to be moving very quickly toward newer technologies that support containers and "modern" development styles.
- Customers report that scanning isn't as fast as they had expected, and that the WhiteHat UI and reporting tools could use some refinement. WhiteHat is currently addressing this in ongoing development.

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

- Data Theorem
- GitHub
- Invicti
- Snyk

Dropped

- CAST

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 that analysts believe are necessary for inclusion in this research.

To qualify for inclusion, vendors needed to meet the following criteria as of 21 December 2020:

- **Market participation**:
  - Provide a dedicated AST solution (product, service or both) that covers at least two of the following four AST capabilities: SCA, SAST, DAST or IAST, as described in the Market Definition/Description section; *and*

- Provide at least one of these additional capabilities: IaC testing, container testing, fuzzing, API testing, or availability in a cloud-native environment such as AWS, Azure or GCS

- **Market traction:**
  - During the past four quarters (4Q19 and the first three quarters of 2020):
    - Must have generated at least $25 million of AST revenue, including $20 million in North America and/or Europe, the Middle East and Africa (excluding professional services revenue)

- **Technical capabilities relevant to Gartner clients:**
  - Provide a repeatable, consistent subscription-based engagement model (if the vendor provides AST as a service) using mainly its own testing tools to enable its testing capabilities. Specifically, technical capabilities must include:
    - An offering primarily focused on security tests to identify software security vulnerabilities, with templates to report against OWASP and other common vulnerability definitions
    - An offering with the ability to integrate via plug-in, API or command line integration 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 developer 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 containers:
    - 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
    - Ability to monitor live environments for security violations

- For container support:
    - Ability to scan containers for open source vulnerabilities
    - Ability to identify common security vulnerabilities in code payload

- For fuzz testing
    - Ability to run automated, continuous fuzz tests
    - Support for C,C#,Java and Golang

- For API testing
    - Ability to test against API brute forcing and access
    - Ability to test for API abuse and credential stuffing

- For cloud-native support:
    - Support for major public cloud providers (e.g., Azure, AWS, GCP)

- **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).

Exclusion Criteria

We excluded vendors from this research if they:

- Focused only on mobile platforms or a single platform/language
- Provided services, but not on a repeatable, predefined subscription basis — for example, providers of custom consulting application testing services, contract pen testing or professional services
- Provided network vulnerability scanning but did not offer a stand-alone AST capability, or offered only limited web application layer dynamic scanning
- Offered only protocol testing and fuzzing solutions, debuggers, memory analyzers and/or attack generators
- Primarily focused on runtime protection
- Focused on application code quality and integrity testing solutions or basic security testing solutions, which have limited AST capabilities

Open-Source Software Considerations

Magic Quadrants are used to evaluate the commercial offerings, sales execution, vision, marketing and support of products in the market. This excludes the evaluation of open-source software (OSS) or vendor products that rely heavily on or bundle open-source tools.

Other Players

Several vendors that are not evaluated in this Magic Quadrant are present in the AST space or in markets that overlap with AST. These vendors do not currently meet our inclusion criteria; however, they either provide AST features or address specific AST requirements and use cases.

These providers range from consultancies and professional services to related solution categories, including:

- Business-critical application security
- Application security orchestration and correlation (ASOC)
- Application security requirements and threat management (ASRTM)
- Crowdsourced security testing platforms (CSSTPs)
- API-security-only solutions
- Container-only security solutions

Evaluation Criteria

This is how your organization and product(s) will be evaluated. The evaluation criteria and weight tell you the specific characteristics and their relative importance that support the Gartner view of the market and that will be 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 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 or account support. This may also include ancillary tools, customer support programs, availability of user groups and service-level agreements.

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	Medium
Market Responsiveness/Record	High
Marketing Execution	High
Customer Experience	High
Operations	NotRated
As of April 2021	

Gartner (May 2021)

Completeness of Vision

Market Understanding: This refers to the ability to understand customer needs and translate them into products and services. Vendors that show a clear vision of their market listen to and understand customer demands and 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 (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' existing 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 the "home" or native geography, either 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
Marketing Strategy	High
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	NotRated

Evaluation Criteria ↓	*Weighting* ↓
Vertical/Industry Strategy	NotRated
Innovation	High
Geographic Strategy	High
As of April 2021	

Gartner (May 2021)

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. While 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 (for example, 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 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. 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

Welcome to the 2021 Magic Quadrant for Application Security Testing. One of the most notable changes this year is the expansion of the vendor inclusion criteria from a focus on firms offering just traditional AST tools (e.g., SAST/DAST/IAST/SCA)

to a broader view incorporating API testing, mobile, container, IaC, and other tools addressing cloud and modern applications. This reflects the use of new tools by security and development teams, which itself is a reaction to the increased diversity of development styles that Gartner clients are using, and the adoption of DevOps. The COVID-19 pandemic has accelerated trends we have been following for the past three to four years, as more development teams work remotely and as product teams need to react quickly to an unpredictable market. Gartner saw a significant rise in inquiry for the security of containers and cloud-native applications during 2020 — up over 50% from 2019 — while overall application security inquiries were up only 20%.

Another popular area of inquiry surrounds the issue of pricing. Complaints and concerns over high pricing continue to be both more common and vociferous. Given market trends toward increased competition, such complaints have merit and will prompt vendors to revisit pricing to remain competitive. In the interim, buyers should be prepared to negotiate aggressively and be alert for unfavorable terms and conditions. For most, simple user-based pricing models will offer the best balance of value and cost, and will avoid the need for complex, difficult-to-manage pricing schemes.

Development style and evolution is a good way to set the context for the 2021 AST Magic Quadrant. Looking at the market and our clients, we generally see three categories of teams using AST:

- **Early phase secure development:** This is by far the largest group of consumers of AST products, roughly twice the size of the two other categories combined. 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. They are looking for repeatable, risk-reducing secure development that they can use iteratively to establish, then improve, their process. The majority of these teams are in small and midsize businesses, usually with gross revenue under $200 million per year.
- **Intermediate phase secure development:** The next largest group has already established a basic process and is 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. They are looking to add tools like fuzzing, threat modelling, code signing, application security orchestration and correlation (ASOC), and API testing. Generally, intermediate teams are exploring some degree of cloud-native and microservices development (often in the form of Kubernetes or Docker), as well as SPAs, but this is not yet their primary deliverable. In 2020, this group accelerated its adoption of these technologies.
- **Advanced secure development:** Advanced teams are characterized by all or mostly container-based and cloud-native development. They are concerned with IaC, SPAs (and API management), CWPPs and similar tools for securing their applications. Within this group, there are generally two subgroups. The smaller of these two comprises teams that have moved up from the intermediate phase. They are characterized by a well-practiced secure development rhythm and are confident users of security tools. The other, larger group comprises development teams who were "born in the cloud," have a fast-paced, flexible development style but are not used to secure development. These teams are moving from DevOps to DevSecOps. In addition to the tools mentioned above, this second subgroup often needs training, coaching or other ways of bringing security knowledge into the team (see Integrating Security Into the DevSecOps Toolchain).

The 2021 AST Magic Quadrant has been expanded to include some tools for each of these styles, encompassing a truly holistic view of secure development.

Market Overview

Market Evolution

Since our last Magic Quadrant, the application security testing (AST) market has continued to see significant, fundamental changes that have substantially increased the size and scope of the market. In addition, existing vendors face new competitive pressures as firms not traditionally associated with AST move into the market. Other structural changes include the continued adoption of new application form factors (for example, containerization, greater reliance on APIs, mobile and cloud native), which demand new testing and security capabilities. We have also observed continued shifts in buying centers — and budgets — as developers and engineering teams take on greater day-to-day responsibility for the security of the code they develop,

especially among more mature organizations. These changes are reflected in the vendors selected for inclusion in this Magic Quadrant, and the functionality they offer.

Gartner had originally forecast a modest, temporary weakening in AST spending during 2020, as a consequence of the COVID-19 pandemic. Based on a review of company results and other data, that slowdown did not occur. Indeed, an increased focus on digitalization — often supported by software — appears to have spurred interest, and spending, in application security tools. A variety of vendors in the space reported substantial revenue gains, on the order of 20% to 30% year over year.

The nature of the market has changed. We have traditionally viewed the market through the lenses of static, dynamic and interactive AST tools. While such tools remain backbones of an AppSec program, they've been joined by a host of other tools — including software composition analysis (SCA), mobile testing, business-critical (e.g., SAP, Salesforce) application testing, API testing, container scanning, and infrastructure as code (IaC) scanning. The lines between application and cloud security blur.

Market Sizing

Taking all these factors into consideration, Gartner estimates end-user spending in this expanded AST market reached $2.2 billion worldwide in 2020. We have also increased our growth rate projections, to 18% for 2021, resulting in a forecast spend of $2.6 billion for 2021. Geographically, the market remains highly North-American-centric, with that region accounting for almost three-quarters of spending. Over time, we predict spending in other regions — notably Europe and Australia and other Southeast Asian countries — will account for almost half of spending on AST. These updates will be reflected in Gartner's Forecast Analysis: Information Security and Risk Management, Worldwide, to be published in 2Q21.

In several cases, vendors are attempting to leverage stronger demand by increasing prices. While they'll enjoy some success, at least in the short term, over the next three years we expect to see significant market forces that will drive pricing down. As already observed, traditional vendors face new competitive pressure both from larger cloud and network security firms and lower cost options such as open-source tools. While pricing will decline, we anticipate increased demand and broader market penetration will support the aggressive growth targets outlined.

Mergers and Acquisitions

M&A activity within the market reinforced the acceleration of a trend noted last year, which sees nontraditional competitors digging deeper into the AST market. This first began with application development vendor GitLab acquiring tools to expand its AST capabilities. During 2020, GitLab built on previous acquisitions with the purchase of both Peach Tech and Fuzzit, announced in June, expanding dynamic and fuzz testing capabilities. Meanwhile, GitHub incorporated its 2019 acquisitions, Semmle (static code scanning) and Dependabot (software composition analysis).

Network and cloud security vendors also made acquisitions that extend their reach further into the development element of DevOps. Most recently, in February of 2021, Palo Alto Networks continued its string of acquisitions with the announcement of its intent to acquire Bridgecrew for $156 million. Bridgecrew focuses on IaC security tools, and created the open source Checkov IaC scanner. The acquisition builds on previous purchases by Palo Alto Networks, notably container security vendor Twistlock (for $410 million in July 2019) and serverless application security company PureSec (June 2019, terms undisclosed). Cisco also moved into the market, announcing the acquisition in October 2020 of Portshift, a Kubernetes security specialist. We expect continued movement by vendors such as these, which, in combination with the increasing prevalence of containerized and cloud-native applications, will significantly increase competitive pressures on more traditional AST platform vendors.

Existing market participants were also active:

- In January of 2021, Rapid7 acquired Alcide, a Kubernetes security specialist. Rapid7 had earlier, in May of 2020, acquired DivvyCloud. DivvyCloud offers a broad mix of security and compliance capabilities for cloud-native applications including expanding into IaC scanning.
- IAST and runtime application self-protection (RASP) specialist Contrast Security expanded the scope of its offering to add cloud-native application security support with the December 2020 acquisition of startup CloudEssence.

- Snyk acquired DeepCode, an AI-based (semantic analysis) code review tool in September 2020. The product was relaunched as Snyk Code in October.
- SonarSource, whose SonarQube code quality analysis tool is sometimes used for security testing, in May acquired dedicated security specialist RIPS Technologies in May 2020. RIPS Technologies focuses on PHP, Java and Node.JS security testing.
- Industry veteran Checkmarx was acquired at a valuation of $1.15 billion in April from Insight Partners by Hellman & Friedman, another private equity firm.

Conclusion

The AST market is far from settled and offers a larger, more diverse opportunity than previously. Participants must account for a broader range of maturities and functional needs, while preparing for competition from new quarters. Buyers should expand the scope of vendors considered when evaluating options for tooling, while understanding the likely impact of increased competition and demand on pricing to avoid lock-in at current pricing levels.

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.