Magic Quadrant for Application Security Testing

Published 29 April 2020 - ID G00394281 - 61 min read

By Analysts Mark Horvath, Dionisio Zumerle, Dale Gardner

Modern application design and the continued adoption of DevSecOps are expanding the scope of the AST market. Security and risk management leaders will need to meet tighter deadlines and test more complex applications by seamlessly integrating and automating AST in the software delivery life cycle.

Strategic Planning Assumptions

By 2025, 70% of attacks against containers will be from known vulnerabilities and misconfigurations that could have been remediated.

By 2025, organizations will speed up their remediation of coding vulnerabilities identified by SAST by 30% with code suggestions applied from automated solutions, up from less than 1% today, reducing time spent fixing bugs by 50%.

By 2024, the provision of a detailed, regularly updated software bill of materials by software vendors will be a non-negotiable requirement for at least half of enterprise software buyers, up from less than 5% in 2019.

Market Definition/Description

Gartner's view of the market is focused on transformational technologies or approaches delivering on the future needs of end users.

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.

We identify four main AST technologies:

- **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. It simulates attacks against an application (typically web-enabled applications and services and APIs), analyzes the application's reactions and, thus, determines whether it is vulnerable.

- **Interactive AST (IAST)** technology combines elements of DAST simultaneously with instrumentation of the application under test. 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 used to identify open-source and third-party components in use in an application, their known security vulnerabilities, and typically adversarial license restrictions.

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

The 2020 Magic Quadrant will focus on a vendor's SAST, DAST, SCA and IAST offerings, maturity and features as tools or as a service. AST vendors innovating or partnering for these were also included.

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 in 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. In addition, Gartner recognizes the growing relevance of containers as an attractive technology for application development, especially for cloud-native applications. We have added support for containers as a factor in the 2020 Magic Quadrant.

Gartner has observed that enterprises today increasingly employ AST for mobile apps. The toolsets for AST, as well as techniques for behavioral analysis, are often employed to analyze source, byte or binary code, and observe the behavior of mobile apps to identify coding, design, packaging, deployment and runtime conditions that introduce security vulnerabilities. While these capabilities are valued, they do not drive the current or evolving needs of customers in the AST space, and thus are similarly not a primary focus of this Magic Quadrant.

Magic Quadrant

Figure 1. Magic Quadrant for Application Security Testing

Source: Gartner (April 2020)

Vendor Strengths and Cautions

CAST

Based in the U.S. and France, CAST is a software intelligence vendor whose product is used to analyze software composition, architecture, flaws, quality grades and cloud readiness. In addition to its code quality testing offering, CAST provides enterprise SAST with the CAST Application Intelligence Platform (AIP). The vendor also offers CAST Highlight, which provides SAST pattern analysis and SCA. The CAST Security Dashboard enables application security professionals to prioritize and resolve application security vulnerabilities. The vendor also provides a desktop version called CAST Lite.

During the past 12 months, CAST continued to expand its language and framework coverage; improved its SCA offering (including the addition of transitive dependencies and visual representation of dependencies); and optimized its scanning for complex projects. CAST also worked on false positive reduction, including the introduction of its autoblackboxing capability. This allows users to fine-tune and customize their analysis (for example, including external code

or recognizing and suppressing specific false positives). CAST also introduced AIP Console, which allows for automated application discovery, configuration and set up.

CAST will appeal to large enterprises requiring a solution that combines security testing with code quality testing, and to existing CAST AIP clients that already use the platform for quality testing.

Strengths

- CAST offers a single solution that can be used for quality analysis as well as security analysis, which can be appealing to organizations with DevSecOps use cases.
- Client feedback highly rated the ability to get a single view into issues across security, quality and architecture. CAST's analysis engine provides an architectural blueprint of the software that helps test composite applications in multiple languages, visualize the architecture to improve code security by detecting insider threats via rogue data access and reduce false positives.
- The vendor provides a scoring mechanism that can be calibrated to organization-specific criteria to track whether an application's health is increasing or deteriorating from security, reliability and multiple other standpoints.
- CAST provides the ability to set up a plan of action based on a particular objective, such as reducing technical debt or improving the security score.
- Client feedback favorably rated the scalability and performance of the SAST engine in analyzing larger applications.

Cautions

- Clients perceive CAST as an application quality testing solution provider, rather than an established application security vendor.
- The vendor does not provide SCA as part of its main SAST offering, AIP, but only with CAST Highlight.
- CAST's SAST solution is missing key software development life cycle (SDLC) integration features, such as a spellchecker, incremental scanning and, most importantly, an integrated development environment (IDE) plug-in.
- CAST clients often cite setup, implementation and customization as areas for improvement. Also, the vendor does not provide 24/7 support.
- CAST does not provide DAST or IAST, and has no partnerships to deliver either.

Checkmarx

Known originally for its SAST offering, Checkmarx has expanded the scope of its portfolio to include SCA, IAST and — via a partnership — managed DAST. An on-demand interactive

educational offering, CxCodebashing, provides developers with just-in-time training about vulnerabilities within code. The vendor's SCA product is essentially new this year, with an internally developed version replacing a previous OEM offering retaining the same name, CxOSA. The SCA offering also supports new container scanning capabilities to aid in identifying problematic open source in images. Another change is the addition of a Docker and Linux-based SAST scanning engine. This addresses past complaints around a requirement for Windows to support local scanning engines, and also enables a new "elastic" scanning facility allowing customers to add (or remove) scanning engines to reflect changing workloads. Another update offers expanded prioritization of results based on a confidence rating (derived from a machine learning [ML] algorithm) and other variables, such as user-defined policies, severity ratings, age and several others.

Checkmarx offers a mix of deployment options for most of its products, with identical capabilities available in on-premises, cloud and managed service forms. Based in Tel Aviv, the vendor offers a global presence in North and South America, Europe, and the Asia/Pacific region, including Japan. Principal support centers are located in Texas, Israel and India. Checkmarx was acquired on 16 March 2020 by private equity firm Hellman & Friedman from Insight Ventures, which retains a minority interest. As this acquisition occurred following the deadline for this Magic Quadrant, any impact on the vendor's position was not addressed.

Strengths

- The vendor's portfolio competes well for various use cases, including DevSecOps, cloud-native development and more traditional development approaches where SAST is a central requirement. SAST capabilities support a broad variety of programming languages and frameworks, and include support for incremental and parallel tests.
- CxIAST employs a passive scanning model and results are correlated with SAST findings, as are issues discovered within open-source packages. This helps with validation of results, and can aid in confirming that a vulnerability is within executable code.
- Tool integration within IDEs and the build environment is frequently cited as a strength by customers.
- Remediation guidance, augmented by the optional CxCodebashing education component, helps developers understand vulnerabilities and how they can be resolved. A graph-based display of code execution paths and vulnerabilities highlights a proposed "best fix" location. Also, chat-based guidance provides fix advice from Checkmarx support staff.
- The product suite offers guidance on the prioritization of vulnerabilities, with reports factoring in data such as the severity of the vulnerability, impact, source and sink information, and confidence level. Confidence levels are derived from a mix of technologies, including an ML algorithm to validate results and correlation between SAST findings and those discovered by IAST or SCA tests.

- Through its various components, the Checkmarx portfolio offers basic support for both API security testing and container scanning. The vendor indicates that it plans to continue investment in these areas.

Cautions

- Reflecting its history, the bulk of the vendor's customers are for its CxSAST product, although Checkmarx continues to invest in expanding its portfolio and capabilities, and other products show growth.
- CxDAST is based on a third-party technology relationship and is only available as part of a managed service offering. For use cases where DAST is a primary — or the only — element of an AST effort, the offering may be less attractive.
- CxOSA, despite retaining the existing name and feature set, is essentially a new product and is available only as an add-on to the CxSAST product.
- Licensing continues to be raised as a source of dissatisfaction by some customers, which may be a consequence of the mix of pricing models offered. Especially for SAST, these are generally based on the number of users or projects/applications — an approach that is emerging as an industry standard. When combined with multiple license models (perpetual, term and subscription), prospective customers gain flexibility, along with complexity. Rankings for negotiation flexibility, pricing and value are on par with competitive vendors, and are generally positive.

Contrast Security

Based in the U.S., Contrast Security is an AST vendor that also sells in the U.K., EU and the Asia/Pacific region. The Contrast platform consists of three primary products: IAST (Contrast Assess), SCA (Contrast OSS) and RASP (Contrast Protect). Contrast Assess incorporates Contrast OSS, which automatically performs SCA through both static scans and runtime analysis, and as a part of the Contrast platform. Contrast Protect) can be licensed independently or jointly with Contrast Assess. The vendor also offers a central management console, the Contrast TeamServer, which can be delivered as a service or on-premises. The testing approach, known as self-testing or passive IAST, does not require an external scanning component to generate attack patterns to identify vulnerabilities; rather, it is driven by application test activity, such as quality assurance (QA), executed automatically or manually.

Contrast is a good fit for organizations pursuing a DevOps methodology and looking for approaches to insert automated, continuous security testing that is developer-centric. Organizations that have developers with previous security experience favor Contrast for its lower operational complexity and a quick start into DevSecOps. Some are skipping the traditional SAST/DAST starting point and going straight to IAST. Contrast offers service integrations with the Eclipse, Rational Application Developer for WebSphere Software, IntelliJ IDEA, Visual Studio (VS) Code and VS IDEs through plug-ins that users can install from the vendor's public IDE

marketplace. Contrast provides a comprehensive REST API, as well as out-of-the-box integrations with common DevOps tools such as Chef, Puppet, Jenkins, Azure Pipelines, Maven and Gradle.

Strengths

- Contrast Assess, combined with the vendor's SCA product (Contrast OSS), is a good choice for organizations leveraging a DevOps or agile approach, offering a quick starting point and rapid integration across the entire SDLC. Gartner client feedback indicates that this also helps in embedding AST among development teams without security testing expertise, because the agent can identify vulnerabilities through normal application testing. Contrast Assess is one of the most broadly adopted IAST solutions and continues to compete on nearly every IAST shortlist.
- Contrast's reporting tool, TeamServer, provides a comprehensive view of code, dependencies, vulnerabilities and project security status in an easy-to-use, intuitive platform. Status is reported as a grade (A through F), making it simple to consume status quickly across complex DevSecOps projects. It also includes a tool for representing dependencies and services in the form of a map, which makes it easier to visualize the attack surface.
- Contrast has put significant effort into scanning COTS software, making it a good choice for enterprises with large implementations of third-party code that might be concerned with COTS application security and dependencies on third-party application libraries.
- Clients highly rate the ease of use of the tool and the vendor's support. Contrast introduced a Community Edition for Assess and Protect to allow users to utilize the fully functional platform for a limited number of applications.
- Contrast's platform support provides AST, SCA and RASP for Java, .NET Framework, .NET Core, Node.js, Ruby, and Python.

Cautions

- Contrast Security offers a full IAST and SCA solution, and does not provide stand-alone SAST or DAST tools or services, although its IAST tools can do similar testing in some cases.
- Client feedback suggests that, due to the passive testing model, effective test coverage requires clients to have mature test automation capabilities or to run Contrast Assess in conjunction with DAST or "DAST-lite" tools. To address this, Contrast introduced a "route coverage" feature to give clients visibility into their test coverage by highlighting which parts of the application were exercised or still need to be covered.
- Contrast can test mobile application back ends, but not the client-side code of the mobile app, and does not conduct behavioral analysis or check front-end code vulnerabilities, such as DOM-based XSS.
- Contrast does not feature some of the nice-to-have ongoing support mechanisms that organizations with no AST experience often look for (for example, IDE gamification, human-

checked results), although it does support chat with staff for specific questions.

GitLab

GitLab is a global company with headquarters in the U.S. GitLab provides a continuous integration/continuous delivery (CI/CD)-enabling platform and offers AST as part of its Ultimate/Gold tier. The vendor combines proprietary and open-source scanner results within its own workflows, and provides SAST and DAST. GitLab also provides SCA functionality with Dependency Scanning. It also provides open-source scanning capabilities with Container Scanning and License Compliance. A new entrant in the Magic Quadrant, in the past 12 months GitLab introduced support for Java, remediation recommendations and a security dashboard. It also integrated the SCA technology, stemming from the acquisition of Gemnasium, into its SCA offering. GitLab also added, among other features, Secret Detection to its SAST. This functionality serves to scan the content of the repository and identify credentials and other sensitive information that should not be left unprotected in the code.

GitLab will prove a good fit for organizations that use its platform as a development environment, and for organizations looking for a broader development CI/CD-enabling solution that comes with a developer-friendly and affordable security scanning option.

Strengths

- GitLab has a single platform for development and security for the entire SDLC, which allows for easier integration of security, as well as easier acceptance and adoption for developers. Security professionals have visibility into the vulnerabilities at the time the code is committed, and when modifications, approvals and exceptions are made, and can also enforce security policies in the merge request flow.
- The vendor's SAST, Secret Detection; DAST, Dependency Scanning; and Container Scanning and License Compliance offerings are included in the Ultimate/Gold tier. Its pricing is publicly available, and provides a relatively affordable option.
- GitLab provides DAST on a developer's individual code changes within the code repository. It does so by recreating a review application based on the code that is already committed in the repository.
- Users can configure requirements for pipelines, and ensure that some, or all, of the security scans are a part of that.
- GitLab provides container scanning for vulnerabilities, and for code deployments in Docker containers and those using Kubernetes.

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. Although GitLab can test

developer code before merging it, it does not have an IDE plug-in and does not provide real-time spell checking.

- GitLab is new to the AST space and Gartner clients haven't traditionally considered it a security vendor. Its security offering is relatively new, and doesn't have extensive end-user feedback.
- GitLab's AST comes as part of the broader development platform. Organizations that do not use GitLab for development will find stand-alone security scanning from the vendor impractical.
- The vendor does not provide specific mobile AST support and its DAST offering is essentially Open Web Application Security Project's (OWASP's) open-source ZAP tool.

HCL Software

HCL Software is, at least in name, a newcomer to this Magic Quadrant, having acquired IBM's AppScan products and technologies after the company exited the application security business. The acquisition was preceded by a two-year span in which HCL was responsible for development and maintenance of the product line, while IBM continued the sales and marketing functions. HCL AppScan is suitable for a variety of use cases, making it attractive to larger organizations with a mix of requirements. HCL Software is based in India. Regional sales and support offices are located in North and Central America, Europe, and several countries in the Asia/Pacific region.

The overall structure of the product portfolio remains largely unchanged, albeit somewhat complex. On-premises products include AppScan Source for SAST, and AppScan Standard and AppScan Enterprise for desktop and on-premises DAST, respectively. AppScan Enterprise Server is an on-premises server platform for sharing policies, results and DAST scanning manually and via automation. Service-based offerings are all grouped under the AppScan on Cloud brand and include both SAST and DAST support. HCL's IAST offering, called Glass Box, is largely an extension of — and tightly integrated with — its DAST products (both on-premises and cloud-based versions). Software composition analysis is provided by the AppScan on Cloud service, and is based on an HCL static analysis engine coupled with an OEM database provided by WhiteSource. Mobile testing is available via AppScan Source for static analysis, and AppScan on Cloud for DAST, IAST and behavioral monitoring. API-specific tests are delivered through a combination of SAST and DAST. In general, products can be deployed on-premises, in the cloud or in a hybrid arrangement.

During the past 12 months, significant effort has been expended on reworking the product line to offer more standard functionality across platforms. For example, its Bring Your Own Language capability enables more consistent language coverage across platforms. Support for Apex, Ruby and Golang, available in the cloud version of AppScan, was added to the on-premises version of the product. Customers and partners can also use the capability, enabling further customization.

Strengths

- 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 single-page applications where not all activity is captured in standard GET/POST operations.

- AppScan, while still owned by IBM, was one of the first products to heavily leverage ML techniques for application security tasks, including the provision of Intelligent Finding Analytics (IFA), which helps improve accuracy and identify a “best fix” location for vulnerabilities. Under HCL, progress has continued with an effort to apply ML-based analytics to DAST findings generated by the vendor’s cloud customers to significantly improve speed and accuracy.
- HCL offers good support for mobile application testing, leveraging its SAST, DAST, SCA and IAST components, as well as behavioral analysis.
- Support for DevOps environments is competitive with other vendors and includes integrations into common IDEs and CI/CD toolchain components. Developers can perform scans in a private sandbox, reviewing results before committing code. The tools provide standard explanatory and supportive information, supplemented by optimal fix information and vulnerability grouping provided by IFA. No formal computer-based training or “just in time” training is provided, although such support — increasingly a staple of AST tools — is reportedly on the roadmap.

Cautions

- Any change in ownership is potentially disruptive, although the two-year transfer period from IBM to HCL appears to have eased the transition. However, HCL is at a disadvantage in acquiring new customers, given its current lack of brand awareness in the market. Thus, while the vendor offers a similar product vision as other portfolio vendors, it is ranked lower for its ability to execute.
- The AppScan portfolio is robust, but complex, with inconsistent features across platforms. For example, Open Source Analysis is only available in the cloud, and mobile testing can span environments. HCL is taking steps — such as with the Bring Your Own Language facility — to rationalize features across the full range of the portfolio, although the result is not yet complete.
- AppScan’s IAST capability is tightly integrated with the DAST offering and cannot be purchased independently. A passive IAST approach, increasingly in favor among DevOps teams, was released on 25 March 2020, after the deadline for this evaluation, and therefore is not considered.
- The overall pricing model for HCL’s portfolio is complex. First, cloud offerings are based on a subscription model, but on-premises products are only available with traditional perpetual licenses (including a term-based variation). That disparity complicates purchasing for organizations wishing to pursue a hybrid deployment model. Other pricing metrics vary and are

based on the number of applications, users (with varied types of user licenses on offer) and per-scan pricing. Buyers must evaluate multiple options to obtain optimal pricing terms.

Micro Focus

Based in the U.K., Micro Focus is a global provider of AST products and services under the well-known Fortify brand. Micro Focus sales has a broad global reach, with a strong presence in North America, EMEA and Central American markets. Fortify offers Static Code Analyzer (SAST), WebInspect (DAST and IAST), Software Security Center (its console), Application Defender (monitoring and RASP) and Fortify Audit Workbench (AWB). Fortify provides its AST as a product, as well as in the cloud, with Fortify on Demand (FoD). The hybrid model allows the FoD tools to scan code and integrate results with the Fortify reporting tool and the developer environment.

During the past year, Fortify has expanded language support (26 app stacks for SAST) and integration with common CI/CD tools like Jenkins/Jira. Micro Focus has also expanded its partnership with Sonatype to a full OEM agreement and integrated its Static Code Analyzer tool directly into FoD, although it still supports Black Duck and WhiteSource. Fortify's AST offerings should be considered by enterprises looking for a comprehensive set of AST capabilities — either as a product or service, or combined — with enterprise-class reporting and integration capabilities.

Micro Focus has put investment into a more DevSecOps developer-centric model. This includes moving DAST more fully into the hands of development by providing coordination between FoD scans and code in the IDE. It is focusing on eliminating impediments to fully automated workflows with features like macro autogeneration and API scanning improvements. Fortify supports cloud-friendly deployment models and simplified orchestration, and is adding support for containerization. To facilitate a faster, cleaner DevSecOps model, Fortify has added RESTful APIs and a command line interface for both static and dynamic testing.

Strengths

Fortify is an excellent fit for large enterprises with multiple, complex projects and a variety of coding styles and experience levels. It has shown flexibility and strength in dealing with issues such as legacy code replacement and modern development styles like microservices, and has experience in M&A activity.

Swagger-supported RESTful APIs and the integrated Fortify Ecosystem were built to support modern DevSecOps organizations, a marked improvement over older versions of the product suite. Open-source integrations, both in FoD and with SSC, Jira and Octane automation, are also important steps in this direction.

Fortify offers mobile testing with FoD directly, as well as the tools with SCA and WebInspect in support of mobile application scanning.

While no one has completely solved the issue of false positives, Micro Focus has made significant improvements in simplifying and reducing FPs. 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.

Cautions

- While Fortify has begun to show the results of Micro Focus' investment, overall market awareness has not yet caught up. Gartner client inquiry calls do not yet reflect the new functionality and are still dominated by discussions about the older versions of the product suite.
- Fortify is known for its depth and accuracy of results, which meets the needs of enterprise customers that then leverage contextual-based analysis. Less mature organizations looking for incremental improvements over time may experience challenges with the complexity and volume of unfiltered results.
- While Fortify offers highly flexible license and pricing models, during inquiries clients report that the pricing remains complicated and the on-premises operational complexity is high.
- Automated scans are faster than they were in older versions of the product, and a good fit for DevSecOps, but optional human-audited scan results in FoD are out of band and can take significantly longer. ·Fortify balances this challenge to human auditing by providing customers with the option to enable in-band, AI-driven audits without human intervention, both on-premises and with FoD.

Onapsis

Founded in 2009 in Buenos Aires, Argentina, Onapsis is a U.S.-based company with centers in the U.S., Germany and Argentina. In June 2019, it acquired Virtual Forge, a prominent player in the SAP code security space. Onapsis has established or strengthened relationships with leading strategic system integrators, managed security service providers (MSSPs), technology alliance partners and value-added resellers (VARs), such as Accenture, Deloitte, Optiv, deepwatch and others, to offer services to protect organizations using SAP and Oracle.

The business-critical application space has traditionally used code reviews by developers and security personnel, and has relied on existing defense in-depth measures to protect these applications. Onapsis offers standard AST tools (SAST/DAST) and makes it easy for ERP developers to integrate them into their existing processes. Onapsis is strictly a business-application-based tool supporting the common languages used in development (e.g., ABAP, ABAP Objects, Business Server Pages [BSP], Business Warehouse Objects, SAPUI5, XSJS and SQLScript) The vendor is a good fit for companies developing tools (in-house or as a third party) that want to adopt more of a repeatable DevSecOps, process.

Strengths

- Onapsis supports the DevSecOps cycle with plug-ins and services that fit into existing business-critical developer workflows.

- The vendor has good support for SAP and Oracle applications as they move to the cloud, such as S/4HANA, C/4HANA, Workday, Salesforce, SuccessFactors, Ariba and others..
- 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 supports a number of complex programming languages and offers a good web-based interface for scanning and managing results across multiple projects that fits well with other ERP development tools.
- The vendor also supports SAP HANA Studio, Eclipse, SAP Web IDE and SAP ABAP development workbench, with similar workflows and processes across the different development IDEs.

Cautions

- Although Onapsis enjoys extensive cooperation with SAP and Oracle, there is some risk as 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, overall programming language support is limited compared to other tools in the AST space, but is focused on common business-critical application developers.
- Onapsis has an IDE plug-in for its toolsets, but the experience varies significantly between them. Results of the scans are available through PDF reports with the developer environment, or via a web interface. Onapsis also offers full integration with SAP's cloud-based Web IDE, which does provide a fully integrated developer experience. For ABAP, there is also a fully integrated experience.
- DAST support is limited to workflow and call graph analysis.

Rapid7

Traditionally known for its DAST solutions, including InsightAppSec, Rapid7 has begun to position other products in its portfolio as application security solutions. This includes the vulnerability assessment solution InsightVM, which provides some software composition analysis as part of its container assessment capabilities. The vendor's tCell product — a RASP offering acquired in late 2018 — provides insights into code execution and vulnerabilities, generally postdeployment. As a RASP offering, tCell relies on the same basic technology as many IAST testing tools, but is designed as an application protection solution, not a testing tool.

Rapid7 retains its reputation for having a strong DAST offering, and is especially suited for use cases where the combination of DAST and vulnerability assessment is valued — such as testing the security of web-based applications, especially where organizations face strong compliance

requirements. The addition of tCell provides organizations with an opportunity to work with RASP-based app protection and the insights it can provide. Improvements over the past year include enhancements to authentication support, with the addition of multiple authentication techniques enabling improved application scanning. The vendor has also added support for multiple application frameworks (such as Angular, React and others), improving its ability to test single-page applications, which are increasingly common. Integration is provided with Jira and a variety of CI/CD tools (with additional support available via API), but most in-depth analysis of results takes place in the product's dashboard. (A Chrome browser extension enables developers and others to interact regarding results without directly accessing the dashboard.)

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. InsightAppSec is offered as a cloud-based service, with options for on-premises deployments and as a managed service.

Strengths

- Rapid7 continues to enjoy a strong reputation for its DAST tool, especially in support of in-depth custom manual assessments. Tests can be performed interactively, allowing for the manipulation of parameters, and aiding troubleshooting and the validation of fixes.
- Rapid7's Universal Translator technology analyzes requests to identify various formats, parses them and normalizes the data to a standard form to create similar attacks across tested formats. For formats that cannot be crawled, such as JSON and REST web services, this is accomplished via user-recorded traffic.
- Expanded support for application frameworks makes Rapid7 an attractive choice for testing modern, single-page applications.
- Rapid7 continues to enjoy good marks from most users for the product's ease of use, dashboard and reporting. 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 inclusion of vulnerability assessment and RASP in its application security portfolio expands the scope of its offering beyond DAST, but the additional tools don't offer feature parity with competitive solutions. For example, while InsightVM and tCell help identify vulnerabilities in built applications and containers, it does not warn of restrictive open-source licenses — a standard capability for SCA tools. (Rapid7 announced a partnership with SCA specialist Snyk as this Magic Quadrant was being finalized. Any resulting improvements in SCA capabilities will be reflected in future evaluations, as those changes materialize.)
- While test results are highly detailed, the tools lack direct integration with IDEs, prompting developers to switch to the InsightAppSec dashboard (or browser extension) to review data

and supporting information. It is possible to incorporate vulnerability data into a Jira ticket, which would assist in providing information to a developer more directly.

- While individual Rapid7 products are built on a common platform, they lack the correlation of results across tools that other vendors provide, such as between IAST and SCA. However, correlation is provided between DAST and a selection of other vendors' SAST tools. (Rapid7 lacks a SAST offering of its own.)
- Rapid7 does not support distributed scanning.

Synopsys

Based in the U.S., Synopsys is a global company with offerings in the software and semiconductor areas. While Synopsys has been executing a strategy to expand its AST portfolio during the past five years, 2019 was primarily spent on integrating the products together technologically and consolidating their offerings. This has been successful, and the market now sees these products as a well-integrated whole with significant movement from single point solutions to multiproduct purchases.

The Polaris Software Integrity Platform has become the central management tool for all Synopsys AST products (except its DAST managed service, which is still stand-alone). Code Sight, the vendor's IDE plug-in management tool, has been integrated into the product suite as well, with the goal of providing a complete in-editor experience for developer-based security testing. While primarily aimed at DevSecOps organizations, this developer-centric model is recommended by Gartner as a best practice, and all developers, regardless of methodology, benefit from that approach. Synopsys should be considered by organizations looking for a complete AST offering that want variety in AST technologies, assessment depth, deployment options and licensing.

In January 2020, Synopsys bought DAST and API security provider Tinfoil Security and is adding it to its suite of products; however, this acquisition occurred after the cut-off date for this Magic Quadrant and our analysis does not take it into account.

Strengths

- The Synopsys suite is a relatively easy entry point for organizations that may be just starting to take a developer-centric approach to security, as well as more advanced organizations that find integrating and managing a set of point solutions to be too time-consuming.
- The Code Sight plug-in is a good fit for DevOps shops. It has strong integration with IDEs to provide feedback early in the development phase. The Code Sight plug-in leverages the IDE to act as an interface to all tools on Polaris, with an emphasis on remediation. This fits well with most development teams, regardless of maturity.
- Support for CI/CD tools (for example, Jenkins and Jira reporting) has increased significantly in 2019, with support in Coverity, Seeker and Black Duck being used as part of the overall build/test/deploy cycle.

- Seeker continues to be one of the most broadly adopted IAST solutions, with good SDLC integration. Synopsys has an agent-only IAST for Seeker that does not require an inducer. This supports the passive testing model offered by some IAST competitors.
- Seeker compliance reports now offer GDPR and Common Attack Pattern Enumeration and Classification vulnerability tracking, in addition to its PCI DSS, OWASP and CWE tracking.

Cautions

- Gartner client feedback indicates that the vulnerability clarification and fix recommendation is limited, compared with some of the competitors.
- Gartner clients from small and midsize businesses have expressed that, despite interest in the vendor's solutions, the price is often outside their budgets, especially for nascent programs, leading them to seek less costly alternatives. Synopsys' sales process is also complicated, and clients have reported trouble navigating it.
- Synopsys offers DAST only as a managed service. Synopsys AST managed services are orchestrated through a cloud-based portal that is separate from Polaris; however, managed service testing results can be viewed through the Polaris reporting tool. Emphasis for dynamic testing is concentrated on the Seeker IAST product line.
- While Seeker has reports for various regulatory compliance regimes, compliance is often much more complicated than a set of scans. Users should be aware that they are responsible for the full scope of audit and regulatory compliance measures.

Veracode

Headquartered in the U.S., Veracode is an AST provider with a strong presence in the North American market, as well as in the European market. The Veracode offering includes a family of SAST, DAST, IAST and SCA services surrounded by a policy management and analytics hub, as well as e-learning modules. Greenlight is a SAST plug-in for the Eclipse, IntelliJ and Visual Studio IDEs. Veracode also provides mobile AST and an application attestation program called Veracode Verified, which enables companies to provide a third-party attestation of their products' security level to a prospective buyer.

During the past 12 months, Veracode introduced support for modern application deployments in the cloud and containers. Also, it merged its original SCA offering and the recently acquired SourceClear SCA product into a new SCA offering that can scan both locally and in the cloud. Veracode also further extended its language coverage and introduced continuous alerting on new vulnerabilities. On 1 October 2019, Veracode released its IAST, which can run in the build phase and the QA test environment.

Veracode will meet the requirements of organizations looking for a comprehensive portfolio of AST services along with tailored AST advice, broad language coverage, and ease of implementation and use.

Strengths

- Gartner clients rate highly the quick setup, ease of use and scalability of the solution, as well as the vendor's willingness to work with customer requirements.
- Veracode's services include tailored vulnerability and remediation advice, and reviews of the mitigations where needed, which can be useful to reduce remediation time and in organizations where developers are not application security experts. Veracode results come with "fix first" recommendations that consider how easy an issue is to fix and how much impact it has, and then recommend the best location to fix the issue.
- Veracode feeds the intelligence collected from its cloud-based scans back to its engine and database. This is used to improve accuracy through SaaS learning, faster SCA updates, as well as advice for rapid response to known vulnerabilities.
- Veracode's SCA offering allows both agent-based local and cloud-based scanning, and provides a unique database with 50% more vulnerabilities than the National Vulnerability Database. Veracode can also scan test third-party applications or SaaS cloud with their consent, as well as COTS applications such as the ones provided by independent software vendors. To help with the focus on exposed applications, Veracode's SCA offering can deprioritize vulnerabilities by checking if they are in the execution path of the application.

Cautions

- Veracode does not offer AST tools that can be installed on-premises, only AST as a service. It provides Internal Scanning Management that can be located on the client's network to support the testing of internal applications, with scanning configured and controlled via the cloud service.
- Veracode does not offer dynamic scanning of APIs, a capability increasingly available from competitors, relying instead on static and interactive AST. Veracode also does not allow discovery of APIs.
- Some Gartner clients have cited first line of support from the vendor as an item to be improved. Additionally, even though Veracode has a worldwide presence, it only provides support in English.

WhiteHat Security

WhiteHat Security's Sentinel platform continues to stand out in use cases where DAST is a requirement, including web-based applications and APIs, both in production and preproduction. In addition, partly by virtue of a partnership with NowSecure, it ranks well for mobile AST, where it combines behavioral testing with SAST and DAST scans of popular mobile languages such as Java, Objective-C and Swift. Software composition analysis is also provided and is now available as a stand-alone product offering. Customers continue to give the vendor compliments for human and ML-based augmentations to testing, including validation of results and optional penetration

testing and business logic assessments. WhiteHat continues to be unique with its Directed Remediation capabilities, where fixes developed by the WhiteHat Threat Research Center are automatically suggested to developers for selected findings. It was the first to offer chat-based assistance to developers for help in understanding specific vulnerabilities, although other vendors have also begun to provide this service. 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 was acquired by NTT Security in July 2019 and operates as an independent subsidiary. Sales and support capabilities have traditionally focused heavily on North America. The vendor has also maintained a limited presence in Europe and the Asia/Pacific region. The NTT acquisition opens the possibility of broader sales and support channels.

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 continues to execute toward its strategy of addressing the requirements of DevOps organizations with differentiated SAST, SCA and DAST products for the development, build and deployment phases of the life cycle. Generally, options earlier in the process — such as SAST and SCA for developers — are optimized for fast return of results by limiting the scope of testing. Later phases provide more in-depth checks and add options for human verification and testing. The vendor continues to expand ML-based automated verification to help speed the process, and to better align to the needs of rapidly iterating development teams.
- WhiteHat's customers continue to value the vendor's strong support services. As noted, these include vulnerability verification, manual business logic assessments/penetration testing and the ability to leverage its Threat Research Center engineers to discuss findings.
- WhiteHat SAST remediation capabilities extend beyond identifying the optimal point of remediation to automatically provide custom code patches that can be copied and pasted into the code to fix identified vulnerabilities for a portion of findings for Java and C#.
- WhiteHat Sentinel Dynamic provides continuous, production-safe DAST of production websites with automatic detection and assessment, and alerts for newly discovered vulnerabilities.
- DAST results can be fed to a variety of web application firewall solutions, enabling the creation of rules to mitigate vulnerabilities until they can be remediated in code.

Cautions

- WhiteHat does not offer an IAST solution. It does use SAST findings to inform DAST scans for improved accuracy.
- Customer feedback indicates some dissatisfaction with the products' user interfaces. IDE plug-ins, for example, are functional, but supplementary and explanatory information is often poorly

formatted. Findings can be fed to defect tracking systems, such as Jira.

- WhiteHat's SAST offering has limited language support, compared with competitive offerings.
- WhiteHat does not offer AST as a tool, only as a cloud service. However, it can provide an on-premises virtual appliance that performs scans at a customer's site, feeding results to the cloud for verification, correlation and inclusion in dashboards for reporting and analysis.

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

Onapsis, HCL Software and GitLab were added to this Magic Quadrant.

Dropped

Acunetix, IBM and Qualys were dropped from this Magic Quadrant based on our inclusion and exclusion criteria.

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 1 November 2019:

- 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.
- Market traction:
  - During the past four quarters (4Q18 and the first three quarters of 2019):
    - Must have generated at least $22 million of AST revenue, including $17 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 top 10 vulnerabilities
    - An offering with the ability to integrate via plug-in, API or command line integration into CI/CD tools (such as Jenkins) and bug-tracking tools (such as Jira)
  - For SAST products and/or services:
    - Support for Java, C#, PHP and JavaScript at a minimum
    - Provide a direct plug-in for Eclipse 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 malware
    - 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)
- 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).

We will not include vendors in this research that:

- Focus only on mobile platforms or a single platform/language
- Provide services, but not on a repeatable, predefined subscription basis — for example, providers of custom consulting application testing services, contract pen testing or professional services
- Provide network vulnerability scanning but do not offer a stand-alone AST capability, or offer only limited web application layer dynamic scanning
- Offer only protocol testing and fuzzing solutions, debuggers, memory analyzers, and/or attack generators
- Primarily focus on runtime protection
- Focus 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-focused solutions
- Container security solutions

Evaluation Criteria

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, etc. These 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, service-level agreements, etc.

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	Not Rated

Source: Gartner (April 2020)

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 (SAST, DAST, IAST and SCA) 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 meeting 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, serverless and microservices architecture. We also evaluate developing methods to make security testing more accurate. We value innovations in IAST, 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 ↓

Evaluation Criteria ↓	Weighting ↓
Market Understanding	High
Marketing Strategy	High
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Not Rated
Vertical/Industry Strategy	Not Rated
Innovation	High
Geographic Strategy	High

Source: Gartner (April 2020)

Quadrant Descriptions

Leaders

Leaders in the AST market demonstrate breadth and depth of AST products and services. Leaders typically provide mature, reputable SAST and DAST, and demonstrate vison through development of other emerging AST techniques, such as container support, in their solutions. Leaders also should provide organizations with AST-as-a-service delivery models for testing, or with a choice of a tool and AST as a service, as well as an enterprise-class reporting framework supporting 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 vendors that are in AST with a strong vision that addresses the evolving needs of the market. It includes vendors that provide innovative capabilities to accommodate DevOps, integrate in the SDLC or identify vulnerabilities. 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 for 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 pick Niche Players when the focus is on a few important functions, or on specific vendor expertise or when they have an established relationship with the vendor. Niche Players typically focus on a specific type of AST technology or delivery model, or a specific geographic region.

Context

The need for application security is ubiquitous across small, midsize and large organizations. With new data privacy requirements, the consequences of a security breach are no longer limited to reputational damage, but also can involve substantial fines and penalties. Vendors have been offering core AST technologies and additional support offerings for well over a decade, and they have matured in speed and efficacy, but common code problems still remain. Most solutions in the market provide some form of code scanning capability, security training services, program development services and remediation support in a growing variety of ways to support developers and security professionals. DevSecOps, agile, and a general demand for greater automation and speed have led to the maturing of the market and the evolution of both full platform solutions offering a wide variety of commonly used testing tools and specialty solutions that offer a deeper dive into a particular technology or combine security testing with other features like code quality.

In general, better accuracy, faster results, easier integrations and enhanced remediation guidance are top of mind for vendors in this market. It has become simpler for end users to find vulnerabilities using AST tools integrated into their workflow or development environment. Solutions that make it easy for developers to be successful at security mesh well with the DevSecOps philosophy (see “Integrating Security Into the DevSecOps Toolchain”) while freeing up some security resources otherwise dedicated to running code scans. In general, anything the developers have to remember to do will be forgotten, but when integrated into their existing workflow, they come naturally. However, Gartner client inquiry feedback still indicates a need to improve remediation guidance, increase testing speed and accuracy, and simplify the operation of AST solutions to support clients adopting, integrating and scaling AST programs.

These challenges are not solved solely by the right technology; they often require changes in organizational culture, better collaboration and sound practices. Still, incompatible security technologies can impede progress, in which case development and security teams risk being driven further apart rather than becoming better collaborators. To cope with these challenges, organizations should:

- Require solutions that expose and integrate automated functionality through plug-ins (including IDE, build, repository, QA and preproduction) into the SDLC. This will enable developers to fix issues earlier in the process, and it will improve coordination between development and security.

- Favor vendors that specialize in comprehensive testing of APIs, applications deployed in containers and other aspects of modern development (e.g., single-page applications, microservices, serverless, edge computing, etc.) to support those use cases. Clients increasingly are seeking out point solutions with a specific focus on these technologies, particularly with respect to testing their APIs.

- Require solutions that provide SCA, which is a critical or mandatory feature of an overall approach to security testing of applications, because open-source and third-party components are proliferating in applications that enterprises build. Vendors in the industry are introducing their own SCA solutions, as well as partnering with specialized SCA vendors. Gartner clients should pay special attention to those SCA solutions that offer OSS governance capabilities to enable the organization to proactively enforce its policy with respect to OSS when components are being onboarded or pulled in from external repositories and package managers. This should be further augmented with production time SCA, such as that available from container security products to alert to new vulnerabilities as they become known.

- Favor a risk-based approach to vulnerability management rather than a “fix all the bugs” mentality. Too often, the perfect becomes the enemy of the good, wasting time and resources and demotivating developers and teams. There is often a trade-off to be made between speed and depth, so buyers should ensure that any resulting diminishment in the accuracy of results that often accompanies lower turnaround times remains acceptable.

- Press vendors for specifics on their roadmap with respect to false positive reduction and how they will be employed to enhance their solutions. Buyers should look past ML hype and marketing to better understand specifics on how the proposed ML implementations will meaningfully improve areas such as enhancing accuracy, automating remediation efforts or achieving better testing coverage. Gartner clients should weigh vendor plans with respect to ML-based improvements, particularly when considering longer-term engagements, and consider the applicability of the proposed approaches. Artificial intelligence (AI) and ML are overused marketing terms, making it difficult to distinguish between hyperbole and genuine value, and should be evaluated closely.

Market Overview

Current Gartner forecasts place the size of the AST market (sales of SAST, DAST and IAST tools) at $1.33 billion by the end of 2020. Through 2022, the AST market is projected to have a 10% compound annual growth rate (CAGR), indicating that the market is growing slightly faster than the overall security market, which is projected to grow at a CAGR of 9% over the same period. Initial examination of updated vendor results suggests the market is growing at a faster pace than originally projected. This is believed to be a function of both increasing buyer demand for core

AST tools, and the growing importance of associated solutions not currently included in the base forecast (such as SCA and mobile AST). Analysis of data continues, and any revisions to the forecast will be published in Gartner's quarterly Information Security Market Forecast.

2019 continued to be a busy year of buyouts and mergers in the AST market. In June 2019, HCL Technologies completed its acquisition of IBM's AppScan product suite as part of its $1.8 billion deal for a variety of IBM products. Also, in July 2019, NTT Security closed its buyout of WhiteHat Security. NTT is keeping the WhiteHat brand distinct from NTT Security, but this does significantly expand WhiteHat's global coverage and partner network. Rapid7 made two purchases, acquiring tCell (runtime application self-protection) in late 2018, and NetFort (network monitoring) in mid-2019. In June, Onapsis completed its acquisition of Virtual Forge and has begun integrating its CodeProfiler suite into the Onapsis product line. Late in 2018, Checkmarx purchased Custodela, an Ontario-based provider of software security program development and consulting services focused on DevSecOps. Finally, in January 2020, Synopsys acquired Tinfoil Security and intends to merge its DAST and API testing product suit with its existing enterprise AST platform (all acquisitions after the Magic Quadrant cut-off date are noted in this research, but their capabilities are not included in the vendors' evaluations).

In addition to this activity, we've seen some interesting moves by infrastructure players like Microsoft and VMware to make inroads into secure development. In 2018, Microsoft bought GitHub, arguably the world's leading development repository. In 2019, GitHub acquired Semmle, a code analytics platform, and became a CVE Numbering Authority. The CVE system provides references for publicly disclosed information about security vulnerabilities and exposures, putting GitHub in a unique position for finding and disclosing code vulnerabilities. Also, on 30 December 2019, VMware announced that it was acquiring Pivotal Software for $2.7 billion (both Pivotal and VMware are part of Dell). This puts VMware in a strong position to manage, among other things, the container and software defined network security spaces. While it's still early, Gartner has seen a market increase in inquiries about container security, so both of these moves are interesting.

The market continues to exhibit signs of increasing consolidation and commoditization, at least with respect to SAST, DAST and SCA for traditional web applications. However, as we can see from the placements in the 2020 AST Magic Quadrant, there continues to be a strong demand for specialty solutions that offer in-depth coverage of specific areas or combine traditional AST with other testing (e.g., code quality, enterprise applications, etc.).

In 2019, the number of Gartner end-user client conversations on DevSecOps and AST increased by 50% over 2018. While most clients do not have a full or even majority DevOps team, many techniques out of the DevOps method are easily adapted to existing coding disciplines. This includes a focus on making security an integral part of the developer work cycle and eliminating "security gates" late in the process. Other trends in 2019 included a rise in interest in container security. While containers continue to be a minor part of the market compared to more traditional applications, inquiry was up 65% over 2018. Similarly, inquiry regarding scanning for known vulnerabilities in open-source code (SCA) rose 20% in 2019.

In general, we have seen the following DevSecOps trends emerging in our client inquiries:

- Integration of security and compliance testing seamlessly into DevSecOps, so developers never have to leave their CI or CD toolchain environments
- Teams embracing a “developers own their code” philosophy, which extends into security (as well as performance, reliability and code quality)
- Scanning for known vulnerabilities and misconfigurations in all open-source and third-party components
- An emphasis on removing vulnerabilities with the highest severity and risk, rather than trying to remove all known vulnerabilities in custom code
- Giving developers more autonomy to use new types of tools and approaches to minimize friction (such as interactive AST) to replace traditional static and dynamic testing
- Scaling their information security teams into DevOps by using a security champion/coach model rather than putting them directly on the teams (which has scalability and cultural issues)
- Treating all automation scripts, templates, images and blueprints with the same level of assurance they would apply to any source code
- Increased interest in containerization

And we see those trends beginning to be reflected in the toolsets, including:

- There is increased availability of SCA tools as part of product offerings across the Magic Quadrant participants.
- IDE security plug-ins have not only become the normal expectation for buyers, but increasingly they are expecting the IDE to be the main conduit for reporting, fix suggestions, lessons, gamification and other developer-centric security activity. Anything that requires developers to go “out of band” is generally disfavored.
- Fix suggestions are becoming more context-aware, not only with specific instructions, but also with options for involving human review and guidance from tool providers. Tool vendors are providing more options for including some human review of results in addition to ML for the elimination of false positives.
- Vendors are starting to deliver options for covering some of the container and microservice attack surfaces, although full container scanning is still a bit off.

See “12 Things to Get Right for Successful DevSecOps” for more on best practices for developers.

This year’s Magic Quadrant shows two distinct trends: One broadening, and one deepening. The first trend is a movement toward all-inclusive platforms that do SAST/DAST/IAST/SCA as well as integrated reporting, CI/CD pipeline integration and a robust developer experience in the IDE.

While each vendor will have specific strengths and weaknesses in individual tools, the common theme is that they are full, broad-spectrum platforms. The second trend is movement by some vendors to concentrate on doing a few things very well, often combining aspects of deep security testing with other functions such as code quality analysis, business-critical apps or specific types of testing not covered well by the broad-spectrum players. Both trends result in more choices for security leads and heads of development, both of which can be purchase decision makers.

We have four notable market observations:

- Clients with experienced security staff are looking more seriously at using IAST solutions. Gartner saw a 40% increase in inquiry volume around IAST in 2019. For organizations with staff that have previously used SAST/DAST, IAST becomes a viable quick-start alternative, especially if they are making their first AST purchase and the staff are experienced in DevSecOps from previous work. It fits well into the DevSecOps workflow and give developers the opportunity to mix and correlate aspects of both dynamic testing and static analysis. While this is still a small percentage of the volume of DevSecOps calls, its growth represents an interesting, if minor, trend.

- Container/microservice security is beginning to appear as an important trend in AST. In 2019, Gartner saw a 60% increase in the number of clients asking about container security. While this still represents a small portion of our call volume on AST, we feel it's significant. Vendors are beginning to address container security concerns by repurposing some of their existing product suites (e.g., SCA for scanning OS components, SAST for payload scanning, etc.). These solutions do not yet cover the full, complex attack surface that containers represent.

- Human-assisted DevSecOps is being offered by more vendors to reduce false positives and to assist developers in their IDE and developer environments. While ML continues to do the heavy lifting for false positive reduction, AST vendors are increasingly offering the option to have results reviewed by humans who can help remove false positives. While fast DevOps organizations continue to prefer automated, rapid turnaround times, other organization with less rigid deadlines and less security experience are taking advantage of FP reduction via human review. Similarly, while many organizations are adopting a "developer security coach" model for assisting coders grappling with security tasks, some are opting to use coaches from vendors provided through chat or other dedicated channels. This supports the goal of making security easy for developers to consume and provides rapid response to common questions.

- Many clients are still seeking "one-stop shop" vendors that offer multiple technologies as part of a unified platform, a trend we noted in 2019. To support this effort, buyers are prioritizing vendors that provide multiple technologies and deployment options. Feedback from clients suggests that efforts to "glue together" various specialty tools suffer from complexity and reporting problems (i.e., the results of one tool not being consumable by others, resulting in a loss of context). Efforts to correlate these in-house do not yield the same level of rich data and project tracking and reporting as integrated, enterprisewide platform providers. Application vulnerability correlation helps with this.

Evidence

"NTT Security Corporation Acquires WhiteHat Security" WhiteHat Security blog.

"Synopsys Acquires Tinfoil Security, DAST and API Testing Solutions Provider," Synopsys blog.

"HCL Technologies to Acquire Select IBM Software Products for $1.8B," IBM.

"Onapsis Completes Acquisition of Virtual Forge," Onapsis.

"GitHub to Integrate Semmle Code Analysis for Continuous Vulnerability Detection," InfoQ.

"VMware Completes $2.7 Billion Pivotal Acquisition," TechCrunch.

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.

or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."