Critical Capabilities for Application Security Testing

Published 27 April 2020 - ID G00394439 - 29 min read

Application security testing is common, but technology changes such as containers, APIs and open source challenge existing toolsets. Security and risk management leaders must evaluate current capabilities and product roadmaps to ensure tools will contribute value in an evolving business environment.

Overview

Key Findings

- AST offerings are evolving, both in function and in packaging, to address emerging use cases while still supporting traditional tasks.
- Buyers — usually led by the application security team, but by developers in a small but growing number of cases — continue to favor platform offerings combining multiple tools. However, special testing requirements and the emergence of nontraditional AST vendors further complicate the evaluation and selection process.
- Organizations struggle to engage with developers who lack appropriate security training and focus, and inadequate security staff to properly support expansive development teams.
- Just as application security teams have begun to successfully adapt to agile and DevOps development processes, they're now forced to adapt to growing reliance on APIs, containers and cloud-native applications that stress existing tools and processes.

Recommendations

Security and risk management leaders responsible for the security of applications and data should:

- Favor solutions that provide developer support via rapid feedback of test findings, along with educational materials and remediation guidance, within the IDE. These capabilities ease friction between development and security teams, and help yield superior outcomes.
- Engage with development and application architecture teams to better understand their technology roadmap, and plan testing tool acquisitions accordingly. This will ensure application security remains an enabler of the secure deployment of software-based initiatives.

- In the bulk of cases, view — and evaluate — platform-based testing suites as a baseline method for satisfying core requirements for SAST, DAST, SCA and IAST testing tools. Supplement platforms, in whole or part, with specialized solutions where development use cases or application technologies cause platforms to fall short or offer a poor match to requirements.

What You Need to Know

This Critical Capabilities guide provides application security testing (AST) tool buyers with vendor rankings for five common use cases, based on relevant evaluation criteria. Buyers can view vendor rankings for each use case to help formulate lists of vendors that, based on Gartner assessments, are well-suited based on product capabilities to address a given use case. Using the online interactive tool, buyers can also formulate custom use cases, and corresponding vendor rankings, where predefined use cases do not offer an appropriate match to an organization's specific requirements. Using scoring for specific capabilities, buyers can also identify vendors with a product offering that is well-suited for a specific function, such as analysis of mobile applications or APIs.

Each vendor's product or service is evaluated in terms of how well it delivers each capability, on a five-point scale. Ratings and summary scores range from 1.0 to 5.0:

- 1 = Poor or Absent: Most or all defined requirements for a capability are not achieved
- 2 = Fair: Some requirements are not achieved.
- 3 = Good: Meets requirements.
- 4 = Excellent: Meets or exceeds some requirements.
- 5 = Outstanding: Significantly exceeds requirements.

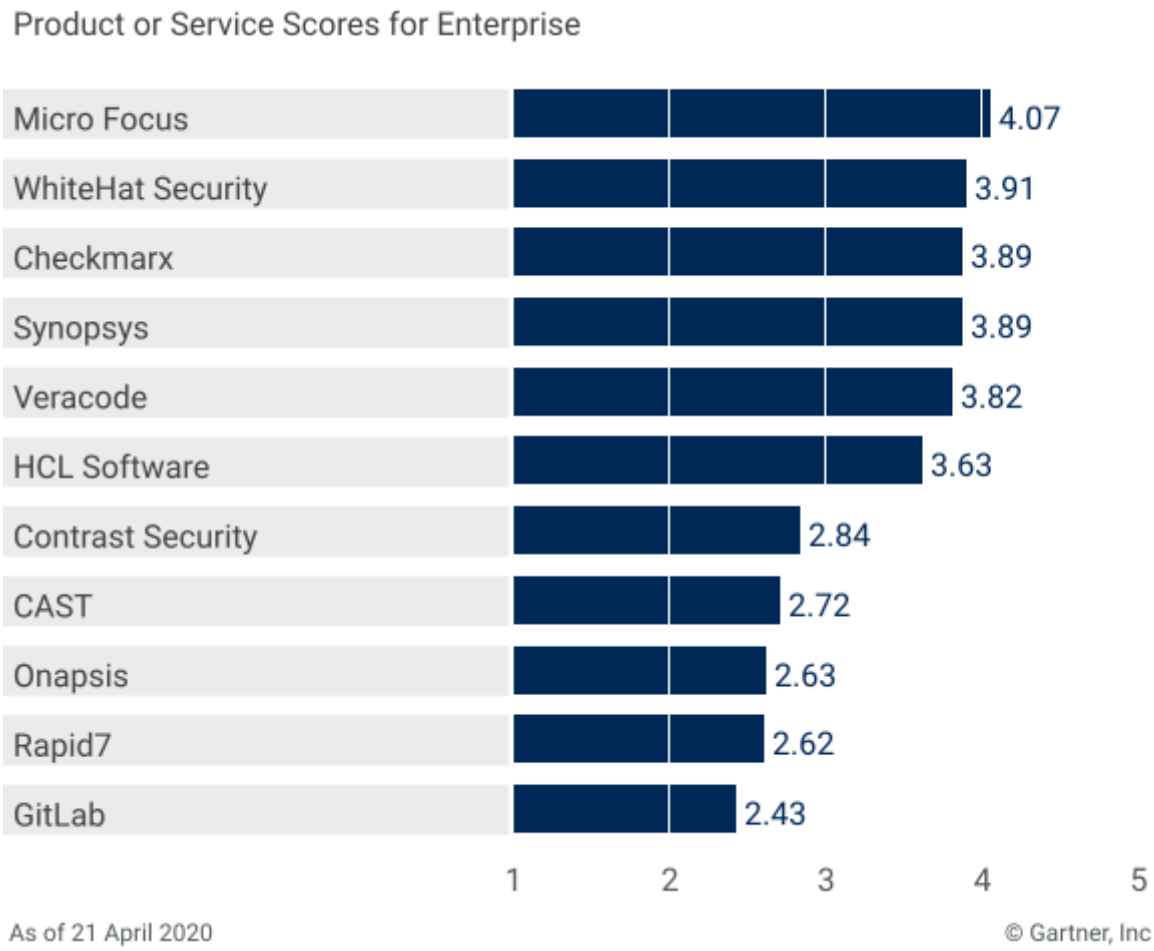
To determine an overall score for each product in the use cases, capability ratings are multiplied by weightings reflecting the relative importance of the capability to supporting a use case.

This analysis complements "Magic Quadrant for Application Security Testing." That defines the market and highlights a broad set of factors, including corporate viability, vision, marketing and geographic focus, and specific strengths and cautions associated with the vendors offering these tools. We strongly recommend organizations use this research in conjunction with the Magic Quadrant, inquiries with Gartner analysts and other Gartner research to define their requirements and select the solutions that match their needs.

Analysis

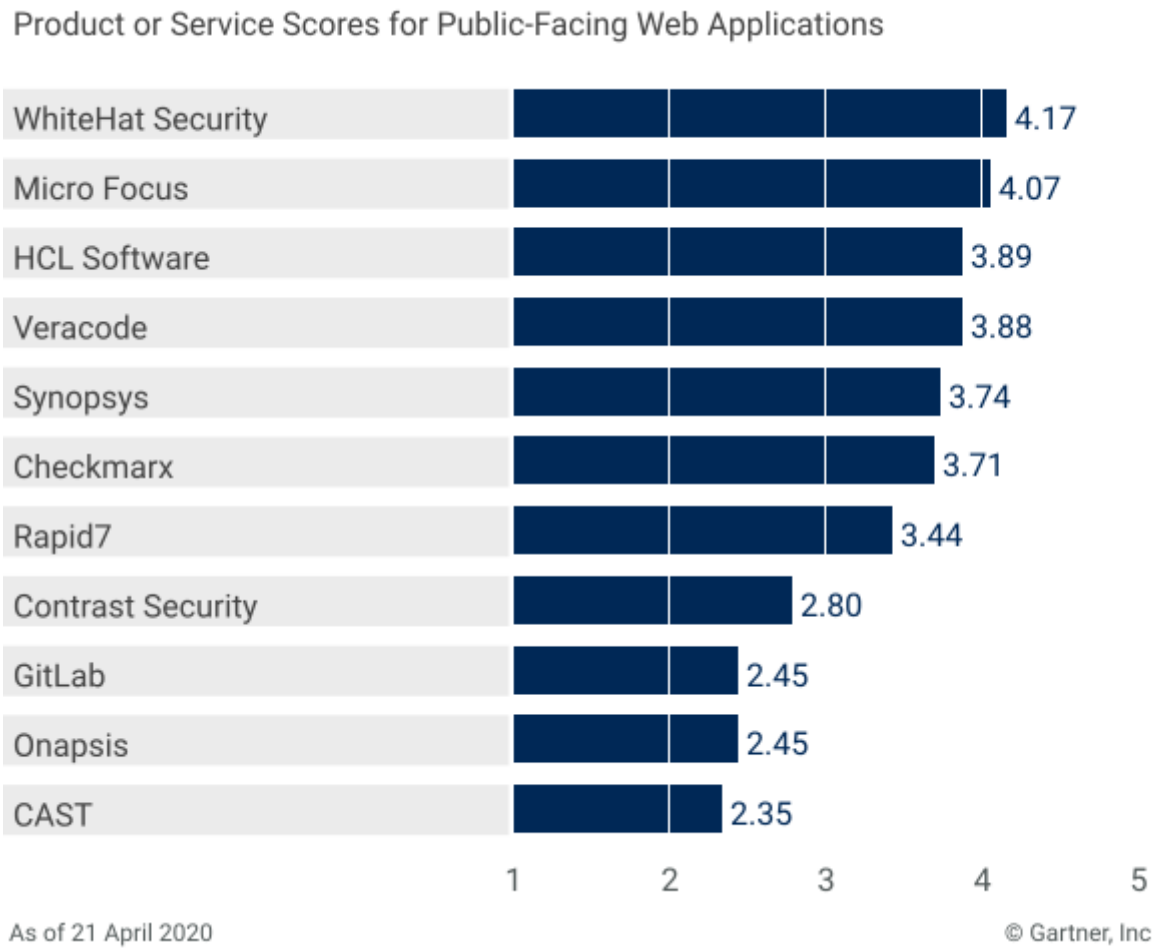
Critical Capabilities Use-Case Graphics

Figure 1. Vendors' Product Scores for Enterprise Use Case



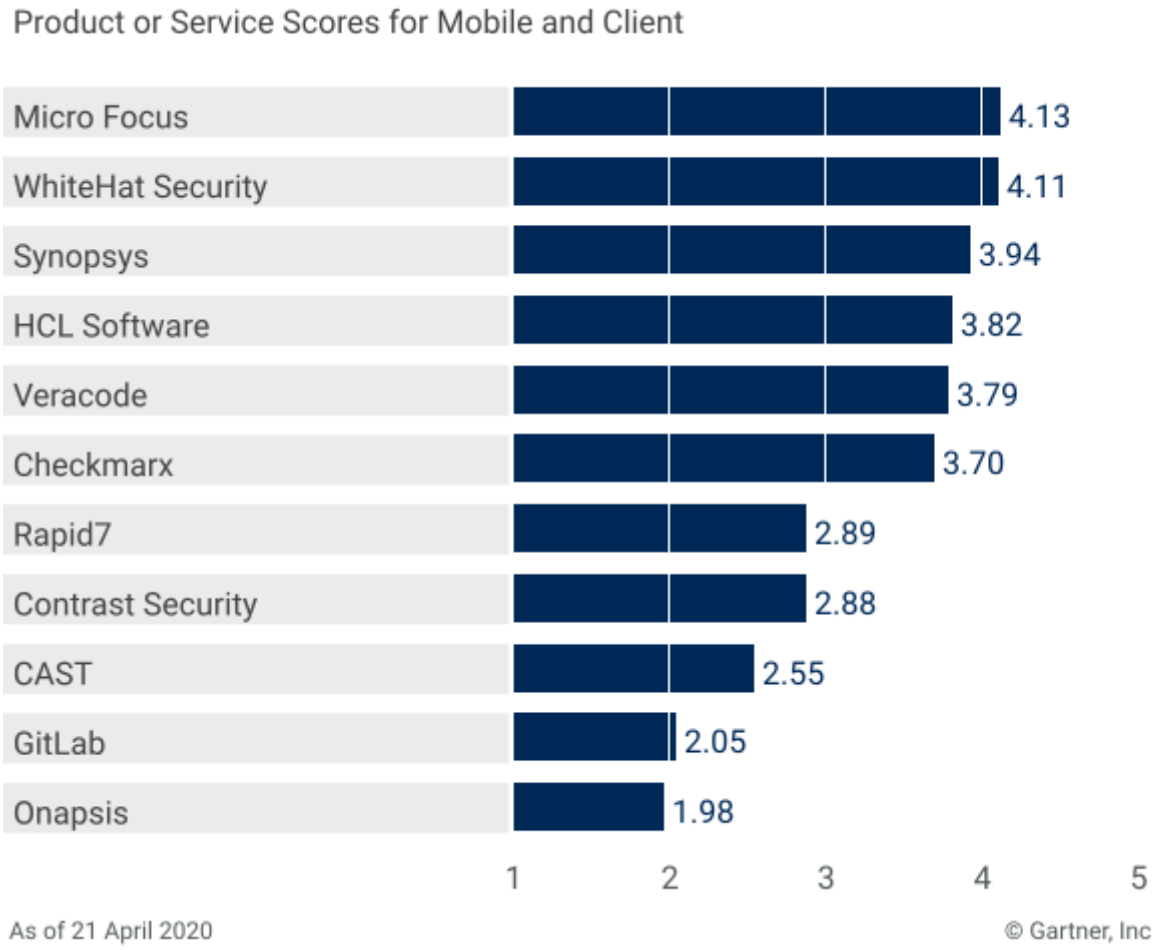
Source: Gartner (April 2020)

Figure 2. Vendors' Product Scores for Public-Facing Web Applications Use Case



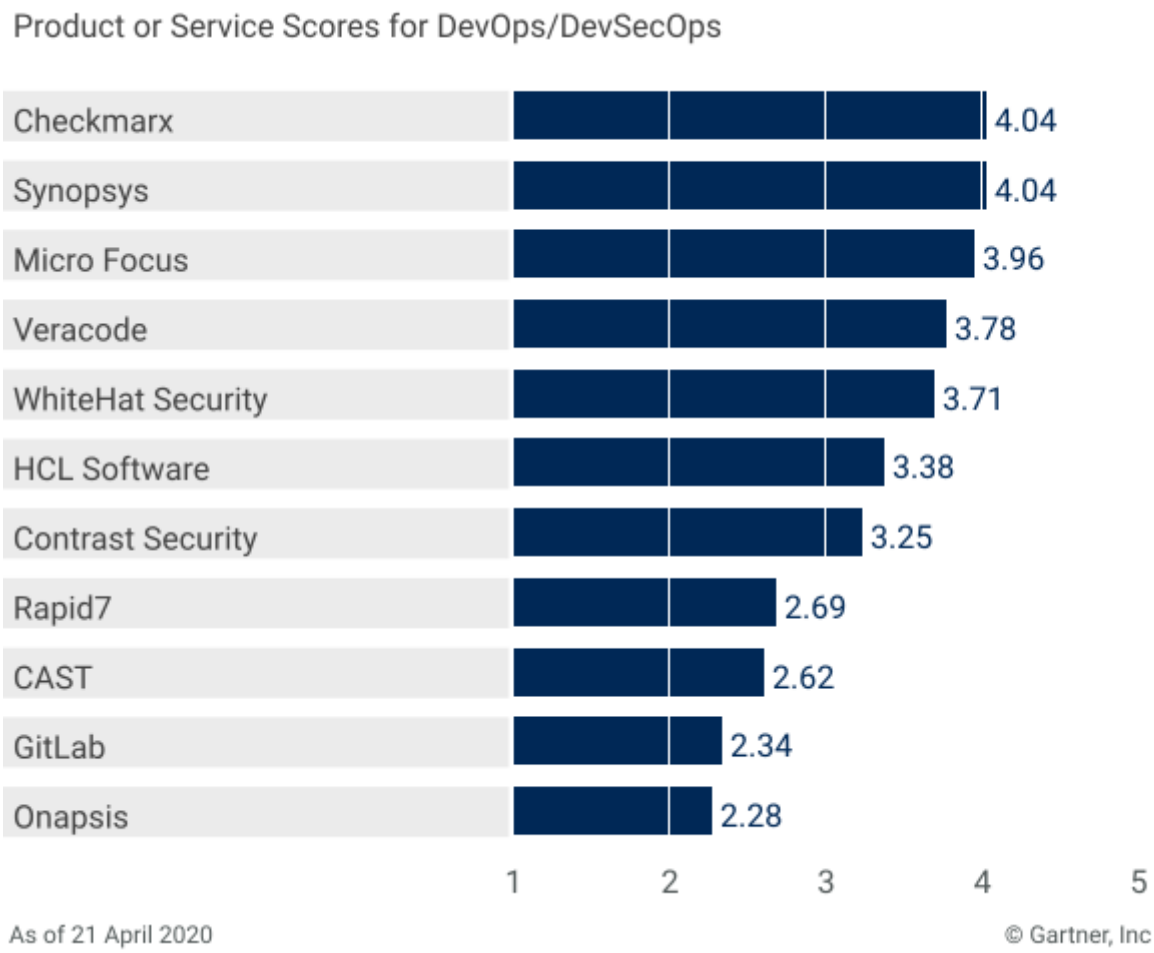
Source: Gartner (April 2020)

Figure 3. Vendors' Product Scores for Mobile and Client Use Case



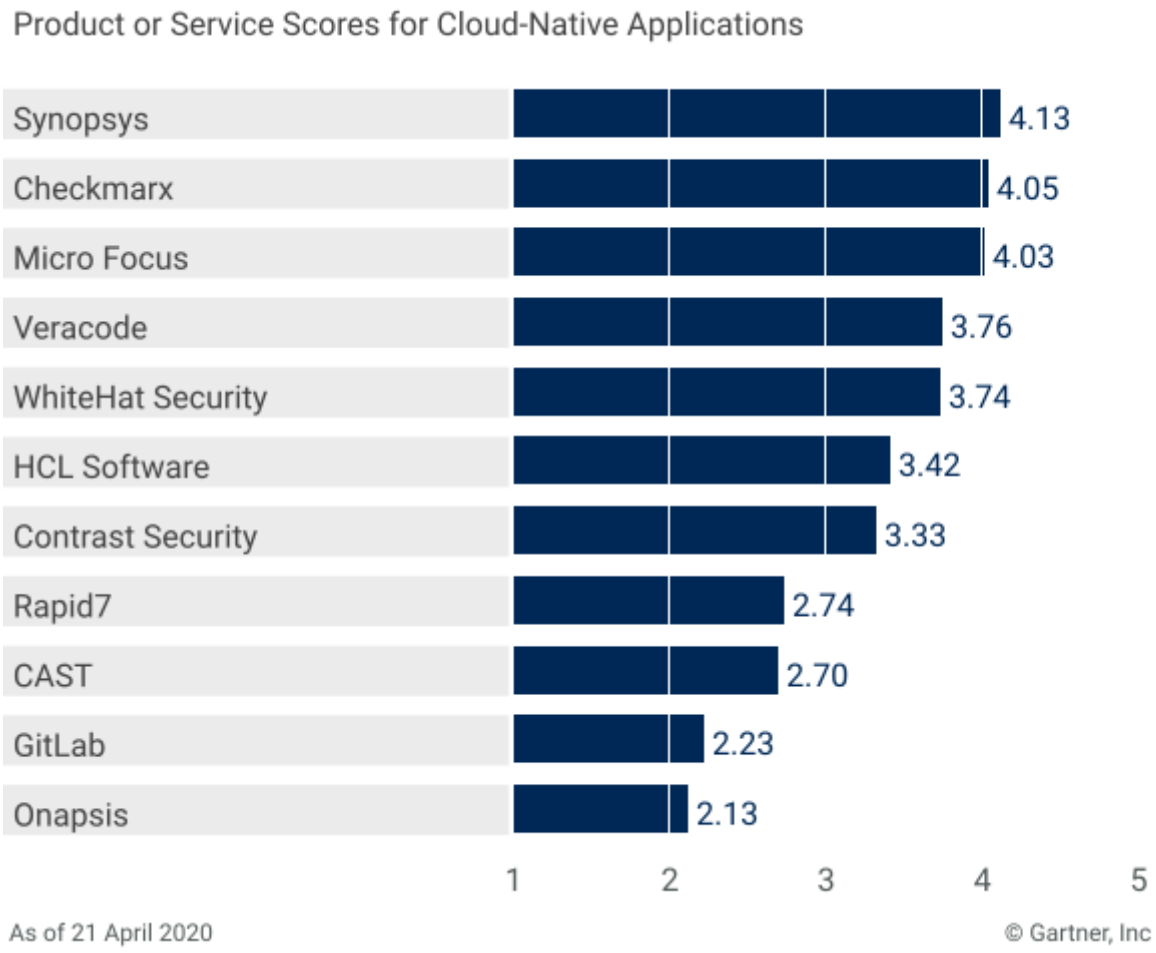
Source: Gartner (April 2020)

Figure 4. Vendors' Product Scores for DevOps/DevSecOps Use Case



Source: Gartner (April 2020)

Figure 5. Vendors' Product Scores for Cloud-Native Applications Use Case



Source: Gartner (April 2020)

Vendors

CAST

CAST is a software intelligence vendor used to analyze software composition, architecture, flaws, quality grades and cloud readiness. CAST combines its code quality testing offering enterprise static AST (SAST) with the CAST Application Intelligence Platform (AIP), and SAST pattern analysis and software composition analysis (SCA) with CAST Highlight. CAST also provides a desktop SAST called CAST Lite. CAST has introduced AIP Console, which allows for automated application discovery, configuration and setup. With CAST Imaging CAST provides an architectural blueprint of the software that helps test complex applications, and via Highlight an interactive, visual representation of dependencies. Although it does not provide dynamic AST (DAST), nor an integrated development environment (IDE) SAST plug-in, CAST supports, among other things, business-critical application SAST for languages used by SAP and Oracle PeopleSoft. CAST will appeal to large enterprises that require a solution that combines security testing with code quality testing, and to existing CAST AIP clients that already use the platform for quality testing.

Checkmarx

Offering a broad portfolio of AST products, Checkmarx is suited for a variety of use cases, especially where SAST and strong software development life cycle (SDLC) integration are requirements. An updated approach to prioritization aims to focus attention on more critical results, guiding remediation efforts. Interactive AST (IAST) is supported via a passive approach,

and results are correlated to SAST findings. Tool integration with IDEs (including an optional developer education component offering gamification features) and the build environment is cited as a strength by customers. The company replaced a previous OEM SCA solution with its own technology. While the recast SCA product adds features — including container scanning and correlation with SAST results — it's essentially a new product. DAST continues to be offered via a third-party technology relationship with Netsparker and is available only as part of Checkmarx's managed service offering. As a result, it's less attractive for situations where DAST is a central element of an organization's AST program. Native support for programming languages used for business-critical applications is limited, although a customization facility enables organizations to add support.

Contrast Security

Contrast provides IAST tools (Contrast Assess) for enterprise customers in lieu of the traditional SAST/DAST testing options. While Contrast Assess has SAST/DAST-like functions, its core strength is as a fully integrated IAST tool. This also included SCA and runtime application self-protection (RASP), which can be licensed independently or jointly with Assess. Contrast 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's developer-centric. The vendor also supports out-of-the-box integrations with common DevOps tools such as Chef, Puppet and Jenkins.

GitLab

GitLab provides AST as part of its Ultimate/Gold tier for its continuous integration/continuous delivery (CI/CD)-enabling platform. 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, as well as open-source scanning capabilities with Container Scanning and License Compliance. GitLab integrates security testing in its development environment. Security professionals have visibility into vulnerabilities at the time the code is committed and when modifications, approvals and exceptions are made, and they can also enforce security policies into the merge request flow. GitLab does not provide an IDE plug-in, but it does allow testing of an individual developer's changes, within the code repository. GitLab also provides functionality that is useful when testing modern applications, such as container scanning and secret detection. GitLab will prove a good fit for organizations that use GitLab's 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.

HCL Software

HCL offers a full suite of testing technologies, with on-premises and cloud-based offerings for most products. The company is best-known for its SAST and DAST products (originally acquired from IBM in 2018), which fare well competitively. In the DAST product, 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. IAST is available but only as an add-on to HCL’s DAST product. SCA is provided via HCL’s SAST scanning engine, leveraging an OEM database from specialist WhiteSource. Mobile testing is enabled via a combination of standard SAST, DAST and IAST tools backed up by mobile-specific behavioral monitoring. SDLC integration ranks highly.

HCL offers a new “Bring Your Own Language” support that simplifies language support ports (helping to rationalize product capabilities across environments) and that is also available for customers and partners who wish to add support for nonsupported languages. A broad set of capabilities makes HCL a potentially good choice for organizations needing to support varied use cases.

Micro Focus

Micro Focus is a global provider of AST products and services under the well-known Fortify brand (formerly Hewlett Packard Enterprise). Fortify offers a full-service platform including SAST, DAST, IAST and SCA, as well as RASP and mobile AST (MAST). AST products are available both on-premises and as a service (with the latter referred to as Fortify on Demand [FoD]). Fortify is one of the oldest names in AST and is seeing a refresh of its platform under the new Micro Focus ownership.

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

Onapsis

Onapsis specializes in AST, monitoring and compliance solutions for business-critical applications, such as SAP, Oracle, Salesforce and Workday. The vendor offers standard AST tools (SAST/DAST) and makes it easy for developers to integrate them into their existing development processes. Onapsis is strictly focused on supporting the common languages used in business application development (e.g., ABAP, ABAP Objects, Business Server Pages [BSP], Business Warehouse Objects, SAPUI5 and XSJS). Onapsis 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. The vendor offers comprehensive support for common HR and business-critical application coding languages as they move to the cloud (e.g., S/4HANA, C/4HANA, Workday, Salesforce and SuccessFactors). Onapsis offers data flow and tracking options that are especially useful for monitoring compliance risks in business-critical applications. Onapsis has a good web-based

interface for scanning and managing results across multiple projects that integrates well with other development tools.

Rapid7

Traditionally known in AST circles for its DAST products, Rapid7 has begun to more aggressively position other parts of the product portfolio as AST tools. For example, the InsightVM vulnerability assessment product now also leverages SCA technology in its container assessment functionality (absent the licensing checks typically found in such products) and a container scanning solution. The tCell RASP product, acquired in 2018, is presented as an IAST solution. While the underlying technology for IAST and RASP products is very similar, tCell was designed primarily to support runtime application protection needs. Rapid7 doesn't offer a SAST product, but it partners with other vendors to provide the capability where needed. Rapid7 scores well for API testing, an increasingly important requirement for many organizations.

Improvements over the last year include enhancements to authentication support, with the addition of multiple authentication techniques enabling improved application scanning. The company has also added support for multiple application frameworks (such as Angular and React), improving its ability to test single-page applications. The combination of DAST vulnerability assessment with application monitoring and protection makes Rapid7 a good choice for environments where the combination can be useful in identifying both vulnerability risks and satisfying compliance mandates.

Synopsys

Synopsys has been executing a strategy to expand its AST portfolio during the past five years, and 2019 was primarily spent on integrating the products together technologically and consolidating its offerings. The vendor offers a fully featured SAST/DAST/IAST/SCA platform that offers a comprehensive array of testing options. Code Sight, the vendor's IDE plug-in management tool, has been integrated into the product suite 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 the 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 provider Tinfoil Security. Synopsys is adding Tinfoil's offerings to its suite of products to expand its DAST and API testing capabilities. However, this was after the cutoff for the AST Magic Quadrant, and our analysis does not take this acquisition into account.

Veracode

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. Its services include vulnerability and remediation advice via its own security analysts, and mitigation reviews where needed. Veracode results come with "fix first" recommendations that consider how easy an issue

is to fix and how much impact it has, and recommends the best location to fix the issue. Veracode provides Greenlight as a SAST plug-in for development environments. Its mobile AST performs both static analysis on the mobile app, as well as dynamic analysis toward the back end. On 1 October 2019, Veracode released its IAST, which can run in the QA test environment. Although Veracode provides only AST services, it does accommodate on-premises requirements with Internal Scanning Management to support local testing, as well as an SCA agent. 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.

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. The company's SAST offering is also competitive, although it supports analysis of fewer languages, emphasizing coverage of the most common ones. MAST, buttressed by a partnership with NowSecure, is a strength. For MAST, WhiteHat combines behavioral testing with SAST and DAST scans of popular mobile languages such as Java, Objective-C and Swift. SCA is provided and is now available as a stand-alone product offering. The company does not offer an IAST product.

Customers continue to give WhiteHat compliments for human- and machine-learning-based augmentations to testing, including validation of results and optional penetration testing and business logic assessments. WhiteHat has long been known for its Directed Remediation offering, providing a fix for a portion of vulnerabilities discovered, and enabling developers to chat directly with support teams for help in understanding findings.

Context

Evidence of the relevance of application security as an enabler for an organization's digital initiatives continues to emerge in the form of security incidents related to software vulnerabilities and continued growth of compliance and audit requirements. As more organizations rely on software for an ever-increasing element of product or service delivery, risks of all kinds grow. For many, if not most, organizations, AST is the first element of an overall application security program where attention is focused. This increases the criticality of AST, and the need for individuals to carefully consider the suitability of the tools they select for their specific requirements.

In this analysis, we consider a variety of AST capabilities, including both a significant number of stalwart technologies that have withstood the test of time, along with new and emerging capabilities that are rapidly growing in relevance. The individual use cases identified are those most common among Gartner clients in hundreds of inquiries over the course of the last year. Most organizations will find one use case to be largely representative of their needs. Given the ongoing transition to DevOps (and DevSecOps), some organizations may find a mix of use cases to be most relevant. In such cases, buyers can consider vendors that appear in common across the most relevant use cases or utilize customization facilities in the online version of the analysis to adjust criteria weightings to provide an optimal mix, reflecting their needs.

The analysis is focused largely on the needs of application security teams. However, we observe an increasing number of others — developers and members of DevOps teams — who have begun to assume greater responsibility for the selection of AST tooling. Those individuals will also find the analysis of interest, including sections on automation and turnaround and SDLC integration, as well as various testing technologies.

Product/Service Class Definition

AST suites are groups of varied AST technologies from a single vendor. They blend SAST, DAST, SCA and often IAST or secure coding training into a single offering. These solutions are delivered as a tool and/or a service. Ideally, the individual tools are integrated within a single enterprise console and reporting framework.

Critical Capabilities Definition

Static AST

SAST technologies analyze applications to identify coding and design conditions that indicate security vulnerabilities or weaknesses. These solutions analyze applications as written, rather than during application runtime. SAST solutions can be deployed on-premises or in the cloud.

A SAST solution must be able to analyze the source code, bytecode or binary code of multiple programming languages. The solution should enable enterprises to customize and fine-tune the testing, according to specific coding practices and standard libraries, reducing the occurrence of false positives. A SAST solution can be deployed as a tool and in the cloud. Potential vulnerabilities should be categorized based on their severity and on the level of confidence they are real, providing enterprises a way to focus on the highest-confidence, most-severe vulnerabilities first.

Dynamic AST

DAST technologies are designed to detect conditions that indicate a security vulnerability in an application in its running state. DAST solutions analyze applications during the operation, preproduction or testing phases. DAST solutions can be deployed on-premises or in the cloud.

DAST can identify whether an application contains vulnerabilities that may be detected only when the application operates in a runtime environment. Because DAST dynamically carries out tests against running code, including underlying application frameworks and servers, its findings are typically more likely to be actual vulnerabilities. DAST technology typically cannot point to the line of code where a vulnerability originates, because DAST is a “black box” testing technology that does not have access to the source code.

Most DAST solutions test only the exposed HTTP and HTML interfaces of web-enabled applications. However, some solutions are designed specifically for testing non-web protocol and data malformation. Some DAST solutions can test web services, complex JavaScript applications, HTML5 applications and other types of applications that involve client-side code. DAST solutions should have mechanisms to import test scripts to control scanner behavior, exercise applications, and restrict URL scope and scan policies to reduce scan times. DAST solutions typically have a

crawling component but should be able to use login macros or scripts to navigate complex applications intelligently and obtain authenticated context. DAST solutions also increasingly need to accept API schema definitions as input to guide security testing of APIs, and many include SAST functionality to enhance effectiveness — for example, to evaluate discovered JavaScript dependencies.

Interactive AST

IAST analyzes applications by internally observing behavior, including input and output, as well as logic and data flow. An inducer feature executes test/attack scenarios, although some IAST solutions do not require an inducer and instead work while the application is being regularly tested.

An agent residing inside an application server conducts runtime analysis of the application code, memory and data flow. Depth of instrumentation of the runtime environment is key to providing higher accuracy, as is the solution's breadth of inducers and its language and platform coverage. An IAST inducer can be a vendor's DAST or attack generator. For some IAST solutions, any type of test (such as QA or user acceptance and performance) can serve as an inducer (this is also called passive testing or self-testing).

SAST and DAST correlation (e.g., submitting SAST findings for DAST validation) does not equate to IAST. Nonetheless, this correlation can help confirm, prioritize or disprove suspected vulnerabilities (see the Application Security Orchestration and Correlation section in the "Hype Cycle for Application Security, 2019").

Software Composition Analysis

This capability evaluates whether and how the AST solution provides analysis of external and open-source dependencies to verify that the underlying application frameworks, as well as open-source components, are free from vulnerabilities.

Warnings regarding overly restrictive open-source licenses are also frequently generated, although this data may be beyond the strict scope of AST efforts.

The evaluation also looks at the ability to proactively enforce organizational open-source software security and governance policy at the time of component onboarding. SCA functionality is increasingly being offered by AST vendors as a homegrown feature in their AST offerings; however, some AST solutions still partner with third-party, stand-alone vendors to offer SCA, and these are evaluated in this research. The level of granularity, breadth and integration of the solution (in the case of partnerships with SCA vendors) plays an important role.

Mobile AST

MAST involves vendor products that identify vulnerabilities in mobile applications using SAST, DAST or IAST, and how the solution tests code running on iOS and Android. We also look at how offerings map interaction of the mobile app with the back end, and whether the solution tests it fully.

Business-Critical Applications

Organizations increasingly seek a means of testing the security of third-party commercial off-the-shelf software and custom extensions to other applications. The latter scenario is common with a variety of business application, sales and marketing, HR, and general ledger systems, among others.

This capability assesses the effectiveness of the testing suite in identifying vulnerabilities within application code (such as ABAP or other vendor-specific customization languages), as well as misconfigurations, known vulnerabilities and errors resulting in security exposures. Some solutions may offer additional capabilities, such as monitoring and auditing the application while running. However, these are viewed as primarily an application protection mechanism, rather than a testing feature, and are not factored into the tool rating.

API Testing and Discovery

API security testing assesses capabilities a vendor offers to support testing of APIs. The ability to discover APIs in production environments, test API source code and test APIs in runtime is evaluated, as well as the capability to ingest recorded traffic or API definitions to support API testing.

SAST vendors should be able to test source code for APIs in supported languages. DAST solutions should provide mechanisms to understand the structure of the data for REST API requests and responses to properly exercise and test an API that exchanges data via JSON payloads. DAST tools may ingest API definitions (typically OpenAPI Specification [OAS]/Swagger, RAML, Web Services Description Language [WSDL] in the case of SOAP, WADL or API Blueprint) or import recorded traffic to support testing. IAST solutions should provide agent support of the technology stack delivering the API, which still requires APIs to observe internal application calls to facilitate testing. Where available, other approaches to API testing and discovery are also evaluated.

Automation and Speed

This capability evaluates the vendor's AST solution's level of automation and ability to provide rapid scans with accuracy. A process and usable interface to schedule tests should be available. Manual intervention should be limited to exceptions, or for when the end user wants to customize tests.

This capability focuses on automation and speed, as distinct from the vendor's ability to support integrations with the development environment, which is evaluated elsewhere.

Especially in DevOps and other rapidly moving environments, short turnaround times for tests are crucial, as is the ability to deliver scanning results immediately. The possibility of performing incremental scans, focusing exclusively on the code that has changed, rather than rescanning the entire application, can reduce these times. Machine-learning-based technologies and other techniques can filter findings to reduce false positives.

The nature of certain AST solutions somewhat determines their turnaround times. A DAST solution, for example, is likely to deliver slower results than a passive IAST solution, because the latter one does not require its own dedicated testing but can leverage other testing (such as QA). Conversely, an active IAST relying on DAST to launch tests would have turnaround times similar to the DAST solution.

SDLC Integration

This capability captures a vendor's ability to deeply and seamlessly integrate the AST solution into the SDLC. This is particularly critical in DevOps environments; however, tools are evaluated for their ability to support integration across multiple types of development environments.

The vendor should provide APIs and plug-ins to IDEs, code repositories, and bug-tracking and QA tools for its AST solution.

Further additions (such as near-real-time or real-time security checks integrated within the development environment) in the AST offering can provide real-time feedback early in the development process, as the developer is writing code in an IDE. Other types of IDE plug-ins deliver the results of AST assessments of a developer's project. In both cases, it's desirable to also offer explanations, training and suggested remediation strategies to the developer to simplify efforts to eliminate the vulnerability. The capability also considers the vulnerability-specific data provided to the developer as a criterion.

Use Cases

Enterprise

This use case considers the needs of organizations with a mix of applications and development approaches, requiring a comprehensive approach to application security.

Public-Facing Web Applications

This use case focuses on the needs of organizations particularly concerned with ensuring externally facing applications are secure and satisfy audit and compliance mandates.

Mobile and Client

In this use case, application security teams are focused specifically on testing applications on endpoints, such as mobile devices, within browsers, and the like.

DevOps/DevSecOps

This use case emphasizes the requirements of organizations with significant adoption of DevOps and other fast-moving, iterative development methodologies.

Cloud-Native Applications

This use case emphasizes the ability of tools to address security testing for a variety of more modern application architectural and deployment styles.

Vendors Added and Dropped

Added

GitLab, HCL Software and Onapsis were added.

Dropped

Acunetix, IBM and Qualys were dropped based on our inclusion and exclusion criteria.

Inclusion Criteria

To qualify for inclusion, vendors need to meet the following criteria as of 10 December 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 of the accompanying Magic Quadrant.
- Market traction:
  - During the last 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 the Open Web Application Security Project (OWASP) Top Ten 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 scan application registries and container artifacts
        - Ability to scan open-source OS components
- 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 and Critical Capabilities guides 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 Critical Capabilities 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

Table 1: Weighting for Critical Capabilities in Use Cases

Critical Capabilities	Enterprise	Public-Facing Web Applications	Mobile and Client	DevOps/DevSecOps
Static AST	20%	10%	15%	17%
Dynamic AST	15%	30%	15%	5%
Interactive AST	5%	0%	0%	15%
Software Composition Analysis	15%	10%	10%	17%
Mobile AST	7%	10%	25%	5%
Business-Critical Applications	8%	0%	0%	0%

Critical Capabilities	Enterprise	Public-Facing Web Applications	Mobile and Client	DevOps/DevSecOps
API Testing and Discovery	5%	10%	20%	10%
Automation and Speed	10%	20%	5%	16%
SDLC Integration	15%	10%	10%	15%
Total	**100%**	**100%**	**100%**	**100%**
As of April 2020				

Source: Gartner (April 2020)

This methodology requires analysts to identify the critical capabilities for a class of products/services. Each capability is then weighed in terms of its relative importance for specific product/service use cases.

Critical Capabilities Rating

Each of the products/services has been evaluated on the critical capabilities on a scale of 1 to 5; a score of 1 = Poor (most or all defined requirements are not achieved), while 5 = Outstanding (significantly exceeds requirements).

Table 2: Product/Service Rating on Critical Capabilities

Critical Capabilities	CAST	Checkmarx	Contrast Security	GitLab	HCL Software
Static AST	3.5	4.7	1.0	2.5	4.5
Dynamic AST	1.0	3.0	2.0	2.5	4.7
Interactive AST	1.0	3.6	5.0	1.0	2.4
Software Composition Analysis	3.5	4.0	3.5	3.0	1.7

Critical Capabilities	CAST	Checkmarx	Contrast Security	GitLab	HCL Software
Mobile AST	2.5	3.0	3.0	1.0	4.2
Business-Critical Applications	4.0	2.5	3.5	2.0	2.5
API Testing and Discovery	2.5	3.5	4.0	1.5	3.0
Automation and Speed	3.0	4.0	3.5	3.0	3.5
SDLC Integration	2.5	4.9	3.5	3.0	4.4
As of April 2020					

Source: Gartner (April 2020)

Table 3 shows the product/service scores for each use case. The scores, which are generated by multiplying the use-case weightings by the product/service ratings, summarize how well the critical capabilities are met for each use case

Table 3: Product Score in Use Cases

Use Cases	CAST	Checkmarx	Contrast Security	GitLab	HCL Software
Enterprise	2.72	3.89	2.84	2.43	3
Public-Facing Web Applications	2.35	3.71	2.80	2.45	3
Mobile and Client	2.55	3.70	2.88	2.05	3
DevOps/DevSecOps	2.62	4.04	3.25	2.34	3
Cloud-Native Applications	2.70	4.05	3.33	2.23	3

Use Cases	CAST	Checkmarx	Contrast Security	GitLab	HCL Software
As of April 2020					

Source: Gartner (April 2020)

To determine an overall score for each product/service in the use cases, multiply the ratings in Table 2 by the weightings shown in Table 1.

Critical Capabilities Methodology

This methodology requires analysts to identify the critical capabilities for a class of products or services. Each capability is then weighted in terms of its relative importance for specific product or service use cases. Next, products/services are rated in terms of how well they achieve each of the critical capabilities. A score that summarizes how well they meet the critical capabilities for each use case is then calculated for each product/service.

"Critical capabilities" are attributes that differentiate products/services in a class in terms of their quality and performance. Gartner recommends that users consider the set of critical capabilities as some of the most important criteria for acquisition decisions.

In defining the product/service category for evaluation, the analyst first identifies the leading uses for the products/services in this market. What needs are end-users looking to fulfill, when considering products/services in this market? Use cases should match common client deployment scenarios. These distinct client scenarios define the Use Cases.

The analyst then identifies the critical capabilities. These capabilities are generalized groups of features commonly required by this class of products/services. Each capability is assigned a level of importance in fulfilling that particular need; some sets of features are more important than others, depending on the use case being evaluated.

Each vendor’s product or service is evaluated in terms of how well it delivers each capability, on a five-point scale. These ratings are displayed side-by-side for all vendors, allowing easy comparisons between the different sets of features.

Ratings and summary scores range from 1.0 to 5.0:

1 = Poor or Absent: most or all defined requirements for a capability are not achieved

2 = Fair: some requirements are not achieved

3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

To determine an overall score for each product in the use cases, the product ratings are multiplied by the weightings to come up with the product score in use cases.

The critical capabilities Gartner has selected do not represent all capabilities for any product; therefore, may not represent those most important for a specific use situation or business objective. Clients should use a critical capabilities analysis as one of several sources of input about a product before making a product/service decision.