Magic Quadrant for Static Application Security Testing

In this research, we analyze the evolution of the static application security testing market, and evaluate its vendors according to their business and technology vision, as well as their ability to execute against that vision in their products and services.

WHAT YOU NEED TO KNOW

As attacks have become more financially motivated, and as organizations have improved the security of their network, desktop and server infrastructures, there has been a shift to application-level attacks. Static application security testing (SAST) is one of the technology markets aimed at securing applications.

SAST should be considered a mandatory requirement for all IT organizations that develop or procure applications. Even though the market has not reached maturity, enterprises must adopt SAST technologies and processes because the need is strategic.

SAST technology is maturing slowly: The SAST market only recently passed through the Trough of Disillusionment in Gartner's "Hype Cycle for Data and Application Security, 2010." It will take more than five years for the market to fully mature and for the technology to be widely adopted, primarily because application security adoption requires not only technological advancements, but also changes in application development and maintenance processes. Addressing application security cannot be resolved simply with the purchase of a SAST solution or another application security technology. Changes in mind-set and to processes will also be needed, but these are more difficult to implement.

Market consolidation continues, and the market now offers SAST technologies from large application development platform vendors, as well as point solutions from small, innovative startups.

STRATEGIC PLANNING ASSUMPTIONS

By 2012, leading SAST vendors will make the enablement of enterprise security intelligence their strategic objective.

By 2015, more than 60% of enterprises will use SAST solutions in their application development processes.

By 2015, more than 70% of enterprises will require proof of SAST testing from their outsourcing, SaaS, cloud, and commercial software providers.

**Gartner**

MAGIC QUADRANT

Market Overview

During the past 18 months, we have witnessed the emergence of some new key trends, as well as the further evolution of trends we have previously identified.

Early adoption of enterprise security intelligence (ESI): There is an emerging understanding among SAST (and dynamic application security testing [DAST]) vendors that the application security market space should evolve into being an ESI enabler. ESI is a concept that recognizes *security intelligence* as an *explicit deliverable*, and designates this intelligence as a strategic security objective for the enterprise's IT security and risk management programs. ESI aims to provide increased accuracy and breadth of security detection and protection, as well as optimal security and risk management.

ESI enablement is based on two critical elements: (1) the interaction and correlation of technologies, and (2) the integration and correlation of information. The interaction of different security technologies aims at providing *higher accuracy and breadth of security detection and protection*, as well as providing higher accuracy and breadth of security information for integration and correlation with business context data. When combined, these provide *contextual assessments* that enable *optimal security and risk management*. Enterprises should apply the ESI concept as a core architectural principle when developing security systems or solutions, and technology vendors should do the same when developing security tools or platforms (including SAST):

1. SAST and DAST interaction: One of the foundational elements of the ESI concept is the interaction of different technologies. During the past 18 months, we have observed this capability being delivered from leading application security solution providers, which offer SAST and DAST technologies/ services (directly or indirectly through partnerships). The more advanced solutions provide the interaction of SAST and DAST technologies with subsequent analyses of correlated results. The interaction and correlation of these two testing technologies offer significant advantages. By using SAST and

Figure 1. Magic Quadrant for Static Application Security Testing

Source: Gartner (December 2010)
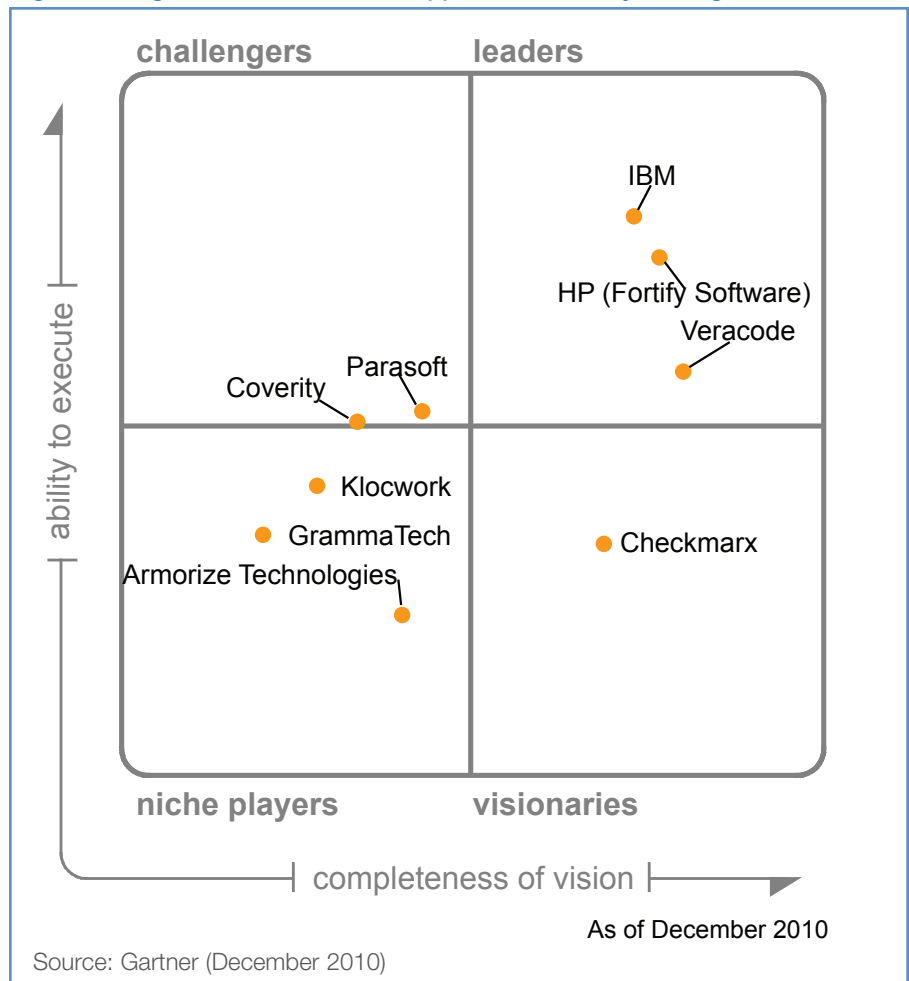
DAST technologies, more phases (e.g., programming, testing and operations) of the software life cycle (SLC) will be analyzed than when using either one in isolation. More importantly, vulnerabilities suspected by one technology may be confirmed or disproved by the other technology, thereby raising the accuracy of detection by reducing false positives and false negatives associated with the technologies used in isolation. Some of the vendors evolving their offerings in this direction are:

• IBM, with its AppScan SAST and DAST technologies

• Fortify Software, with its SAST, partnering with HP and its DAST (Fortify was acquired by HP in 2H10)

- Veracode, with the planned interaction of its SAST and DAST services in 2011

2. Another foundational element of ESI is the integration and correlation of security information and contextual information. Security analysis results collected by SAST (and DAST) technologies, along with contextual information defining the business/compliance/intellectual property/etc. aspects of tested applications, should be stored in persistent repositories, thereby enabling querying for the purposes of contextual risk assessments and optimal risk management, as well as business decision making based on those assessments. For example, vendors such as Checkmarx and Veracode have started offering repositories and querying capabilities.

We expect that, in the future, vendors will enable the addition of security information from other security technologies, such as identity and access management (IAM), network security, and database security. Security information and event management (SIEM) technologies will play a critical role in collecting security information from various security scanners and monitors across various sources (e.g., network, IAM, endpoint protection). The ability of application security technologies to integrate their analyses as well as their application models with SIEM technologies will grow in importance.

Security testing as a service and evolution to cloud delivery: Gartner believes that security testing as a service has many benefits to enterprises – for example, as a way to reduce upfront costs and to augment limited internal resources. Vendors such as Checkmarx and Veracode offer SAST capabilities only as a service (Checkmarx also offers product licensing, but not as its preferred model). Vendors such as HP and IBM have worldwide professional and cloud-based service capabilities, and they offer SAST services in addition to selling technology licenses.

Testing as a service is making an increasingly significant impact on the application security market. More and more, we hear from organizations that prefer to use a product *and* a service from the SAST vendor – for example, testing their more-sensitive applications on-premises using a SAST product, and testing their less-sensitive applications as a SAST service; or testing deployed applications as a service, with testing of applications in the development process using on-premises SAST products.

Cloud and security-as-a-service offerings are appealing to enterprises for multiple reasons – for example, capital savings, because, instead of buying/maintaining their own hardware and software, enterprises will use services from cloud SAST vendors, which own their respective hardware and software. Enterprises also expect to save on hiring, training, and managing their own human resources when respective SAST services are provided by the cloud.

Another cost-saving feature is the "pay per play" principle that is expected from cloud providers, in which enterprise clients pay for only the services they consume. This makes the cloud accessible not only to big enterprises, but also to small ones, which cannot afford to buy their own technology products, but which can afford to pay for respective services.

The cloud lowers the barriers to adoption: Enterprises can now try technology services before committing to a large-scale service. The cloud also bridges dispersed geographical locations.

Quickly working through a large backlog of deployed applications is another reason to use outside service/cloud providers. As part of the service, SAST providers should be expected to reduce the number of false positives associated with the technology by some amount via human filtering of the scan results.

A cloud-based model for application security services, including SAST, will pose a number of problems. Among them is the concern over the service provider's access to source or binary code, as well as the service provider's intimate knowledge of an enterprise's application vulnerabilities. Also, there is a gap between the location of vulnerability detection and the location of vulnerability remediation – for example, while detection will be performed by SAST as a service, remediation – a software fix – will need to be performed by on-site programmers. The gap can also be organizational: While detection will be done by cloud specialists, remediation will be done by enterprise employees. Detecting without remediation makes little sense. Therefore, closing gaps becomes critical.

Enterprise and cloud providers should define and establish control over these processes. Neither an enterprise nor a cloud provider will own the detection-remediation process in its entirety, so defining boundaries and establishing service-level agreements, feedback, and collaboration are essential. Enterprises and cloud providers should decide on process specifics, such as whether the process will be synchronous or asynchronous – for example, whether the cloud provider will run SAST tests synchronously (such as on the last day of every month) or asynchronously (such as running SAST tests once the next version of a newly developing application is ready).

Cloud and on-site processes should be integrated. For example, the results of a cloud-conducted security test should be entered into on-site-located/accessible bug-tracking systems, so that on-site specialists will be informed and able to assume and conduct remediation efforts. Optimally, the integration process will be automated and transparent. For example, the completion of a newly programmed application's module will automatically trigger SAST testing by the cloud SAST provider.

Security and quality technology offerings combined: Some vendors, which historically have specialized in application quality testing, have been adding application security testing to their portfolios of testing tools. Some of these vendors have acquired SAST vendors, and have been working on making a combined quality and security portfolio available to their clients – for example, IBM with its Rational application platform, into which it added AppScan DAST technology in 2007 and Ounce Labs SAST technology in 2009; or HP with its Quality Center platform, which it started marketing along with its Application Security Center (ASC) platform, which offers DAST technologies and will be marketed with the Fortify SAST technology that was acquired in 2010. Also, Parasoft has offered SAST and DAST security testing technologies combined with its own quality testing technologies for years.

Other application quality testing vendors (e.g., Coverity) with some security testing capabilities (in addition to their primary focus on quality testing capabilities) have started partnering with SAST pure-play vendors (such as Armorize Technologies) to offer a combined quality and security portfolio of testing capabilities. The degree of technological integration between quality and security testing features differs. It ranges from mostly marketing efforts, in which two isolated products are simply sold together, to a technological integration of the results of quality and security testing into the same repository, in which the results could be correlated and analyzed (e.g., in the case of Coverity and Armorize's partnership).

SAST integration with SLC platforms: The proper place for application security testing is in the SLC process, where application development professionals should be performing security vulnerability detection and remediation with the help of SAST tools as early as the programming phase, and then continuing the process into the build/test phase, and later into the production/operation phase, where operations professionals may also be involved in the testing. Most organizations will prefer having SAST capabilities tightly integrated with SLC platforms, especially if those capabilities are included with the SLC platform at little cost. Even if SAST is procured via software as a service (SaaS)/cloud, having it tightly integrated with the SLC process/platform for remediation purposes is highly desirable.

Magic Quadrant Overview

- In Gartner's 2009 "Magic Quadrant for Static Application Security Testing," the two market Leaders were Fortify and Ounce Labs: two startup vendors that provided dedicated SAST point solutions. Since then, both have been acquired: Ounce Labs by IBM in 2009, and Fortify by HP in 2010. These acquisitions have combined the worldwide resources of two of the largest IT vendors with the innovation and thought leadership of these point solution vendors.

One of the smaller, innovative point solution vendors, Veracode, has also moved into the Leaders quadrant. Its presence there emphasizes that the SAST market has not yet reached its Plateau of Productivity, and is still evolving and innovating.

All three Leaders have made application security their strategic objective. They are strengthening the ESI capabilities of their application security platforms; specifically, all three offer DAST technologies, and have made progress in SAST and DAST interaction and correlation. They are also working on other ESI capabilities, such as repositories, queries and contextual assessments. Veracode has been an innovation leader with SAST as a service, and has made SaaS/cloud its only delivery model. IBM and HP have historically been product-focused, but have also made SaaS/cloud a priority and are executing along those lines.

Proving its vision and execution capabilities in the application security space, IBM offers a broad portfolio of application security solutions. Before its 2009 acquisition of Ounce Labs for SAST technology, IBM acquired Watchfire in 2007 for its DAST technology. Both have been successfully integrated into IBM's structure, culture, and technology portfolio. In addition, IBM has made acquisitions in adjacent application security areas for database activity monitoring and data masking, which enables it to address its clients' broader application and data security needs.

HP's 2010 acquisition of Fortify offers further evidence of HP's vision in the application security testing market, but HP must deliver strong execution to realize that vision and prove its ability to integrate Fortify into its culture, product and service offerings (HP's integration of a leading DAST vendor, SPI Dynamics, which it acquired in 2007, was not executed to its full potential). HP lacks a clear security strategy that encompasses all of its security offerings, not just application security.

Veracode is the only startup vendor among the Leaders. To compete against two other Leaders – i.e., two of the industry's largest vendors – it should demonstrate continued strong revenue and customer growth. Veracode's innovative security-as-a-service offering gives it some extra time to prove its stability, and offers additional opportunities, such as third-party security testing and certification of various cloud providers' software. An alternative for Veracode is to be acquired by some large security and/or cloud provider (e.g., a general-purpose cloud provider, such as Google or Amazon; or a security provider with evolving SaaS/cloud aspirations, such as Symantec).

- With HP and IBM becoming major players and leaders in the SAST market, the bar for execution and vision capabilities has been raised for the entire market, shifting some of the other vendors lower since Gartner's 2009 "Magic Quadrant for Static Application Security Testing." Klocwork has shifted into the Niche Players quadrant, and Parasoft and Coverity, while remaining Challengers, have shifted closer to the line separating Challengers from Niche Players. The acquisitions made by IBM and HP have made it much more difficult for Klocwork, Coverity and Parasoft to challenge IBM and HP in vision or execution capabilities in this market. Those acquisitions have also pressured Veracode to strengthen its DAST testing capabilities, and to demonstrate continued growth to remain competitive.

The main distinction of Coverity, Klocwork and Parasoft is that they bring a unified view of the quality and security testing of applications, and they have been focusing primarily on quality testing. They focus on selling security testing products to existing customers of their quality/functionality testing products. In the security market, Coverity, Klocwork and Parasoft suffer from lack of appeal to information security specialists, and from lack of clout and brand-name recognition in the security community. To remain competitive, they should focus on expanding their capabilities that address the security needs of mainstream enterprises, in addition to specialized software and hardware vendors; and they should focus on growing their security revenue. Also, they should appeal with strong DAST capabilities and SaaS/cloud offerings, and strengthen the appeal of their offerings outside their installed bases.

- Besides Klocwork, there are two other Niche Players: Armorize and GrammaTech. Both vendors are new to this Magic Quadrant, and both came to the market from different directions.

Armorize is a security-focused vendor that offers SAST and some other security technologies, such as a Web application firewall (WAF) and a Web application anti-hacker alert monitoring capability. Armorize aspires to become a prominent security vendor, but it

currently lacks name recognition and suffers from not having a more complete set of technologies and services (e.g., it does not offer DAST technology and SAST SaaS/cloud services).

GrammaTech is a vendor with a unified quality/security view (with a focus on quality). It specializes in the in-depth analysis of C/C++ source and binary code testing for specialized applications in areas such as defense, avionics and intelligence. It aspires to be the best-of-breed vendor in static analysis for that range of clientele, with a focus more on the depth rather than the breadth of its technology offerings.

- One vendor is in the Visionaries quadrant: Checkmarx, which demonstrates thought leadership in its technology and its business. Technologically, it innovates in ESI, storing normalized models of scanned applications and results of its analyses in a persistent repository, thereby enabling customizable queries and impact analysis. Businesswise, Checkmarx has broadened its efforts to extend to emerging software platform vendors – namely salesforce.com, analyzing the application code that salesforce.com, its partners and its users upload to the platform. Addressing the security of cloud platforms is a growing area of concern and interest to cloud platform providers and their users.

Market Definition/Description

SAST is a set of technologies designed to analyze application source code, bytecode, or binaries for coding and design conditions that are indicative of security vulnerabilities. Much like a compiler, SAST tools analyze an application's code line by line, following information flows and looking for conditions that indicate potential security vulnerabilities. SAST tools are used to analyze applications in a nonruntime state, as opposed to DAST tools, which analyze applications in a runtime state.

Proactively detecting security vulnerabilities early in the application development process is less expensive than fixing the vulnerability later, when the application is in production, and reduces the overall security exposure of the application and its data. Because of the development process changes and cultural changes necessary to incorporate these tools, it will take more than five years before SAST technologies and their adoption reach the Plateau of Productivity.

SAST should be a mandatory requirement for all IT organizations that develop or procure applications. Ideally, application vulnerability detection would be conducted throughout the entire SLC. Enterprises that lack application security skills and resources should consider application security testing as a service. False positives and false negatives are always a concern. Therefore, enterprises should fine-tune the tools so that detection and remediation efforts can be focused first on high-confidence, high-severity vulnerabilities, starting at the unit test, build or quality assurance (QA) phases of the SLC.

For outsourced application development, as part of the contract, organizations should require external service providers to perform SAST and provide evidence that testing has been conducted.

Enterprise cloud-computing adopters and enterprise cloud-computing providers should conduct SAST of the applications being uploaded to the cloud, and SAST of the software that provides cloud services (such as databases or application management services).

Enterprises should start requiring their application security vendors to deliver ESI-enabled solutions, specifically those that offer different security technology and information interaction, integration and correlation. In particular, enterprises should look for solutions with SAST and DAST technology interaction and correlation, because they typically enable higher accuracy and breadth of vulnerability detection. Enterprises should also look for solutions that enable the integration of SAST, DAST and other security information in a persistent repository that can be supplemented with contextual information, such as the business value of the application or the sensitivity of the content that the application handles. Such a repository should enable information querying and analytics – e.g., solutions that might be offered by SIEM vendors in collaboration with SAST and DAST vendors.

In contract negotiations, enterprises should consider the ongoing consolidation of this market, and expect that point solutions will eventually be replaced by platforms and supplemented with an evolving paradigm of cloud computing. Enterprises should also expect that security as a service will become mainstream.

The most critical impact of using SAST is minimizing the risk of possible exploitation of application vulnerabilities. Adopting this technology will enable organizations to detect the vulnerabilities embedded in applications before hackers detect them. As with any security investment, a cost and risk analysis should be performed. Making a definitive return-on-investment calculation will be difficult, because the primary purpose of SAST is risk reduction, not cost savings. Catching vulnerabilities early saves money, but this must be balanced against the cost of the process changes and cultural changes necessary for implementing SAST adoption. In the longer term, another source of cost savings will come from automating security testing and procuring security testing as a service.

Inclusion and Exclusion Criteria

For this Magic Quadrant, we have set up the following inclusion and exclusion criteria:

- Vendors must offer a SAST security testing product or service, or, ideally, both.

- Vendors must have been in the market for 18 or more months.

- The vendor's revenue exceeds $1,000,000, and/or the vendor has at least 20 customers that have deployed its products/services into production.

- Startup vendors have a proven ability to secure funding, and have at least 12 months of operational cash reserves.

- Open-source SAST offerings were not considered for this Magic Quadrant. Currently, they lag far behind in enterprise-class capabilities when compared with commercial offerings.

Added

- Armorize Technologies

- Checkmarx

- GrammaTech

Dropped

- Compuware, due to its decision to withdraw from the SAST market.

- Fortify, due to its acquisition by HP in 2010, during our work on this Magic Quadrant. In this research, we are treating Fortify and HP as one company: HP.

- Microsoft – although it provides very basic SAST capabilities with Visual Studio, it is not competitive with commercial offerings and refers its customers to its third-party ecosystem for those capabilities.

- Ounce Labs, due to its acquisition by IBM in 2009.

Evaluation Criteria

Ability to Execute

Product/Service: This is the vendor's core products and services that compete in the SAST market. It includes current product/service capabilities, quality and feature sets. We give higher ratings for: proven performance in competitive assessments; SAST revenue volume; the number of SAST customers, and the number of installed and used SAST products; appeal outside of the installed base of SLC products; appeal to the breadth of users (e.g., programmers, QA/testing specialists); appeal to information security specialists; appeal with technologies other than SAST (regardless of whether they are application security); and offering product and SaaS/cloud services.

We also evaluate a vendor's product market share and "mind share."

Overall Viability (Business Unit, Financial, Strategy, Organization): This is an assessment of the organization's or business unit's overall financial health; the likelihood of the company's decision to continue investments in its SAST offerings, and in a broader application security space; SAST expertise; and the likelihood that the vendor will be successful in its acquisition and/or partnership deals.

Sales Execution/Pricing: We account for SAST growth rate, company's global reach, pricing model, and product/service/support bundling. We review 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 worldwide.

Market Responsiveness and Track Record: We look at the vendor's ability to respond, change directions, be flexible, and achieve competitive success as opportunities develop, competitors act, customer needs evolve, and market dynamics change. We evaluate market awareness; the vendor's reputation and clout among security specialists; the match of the vendor's SAST (and broader application security) offering to enterprises' functional requirements; and the vendor's track record in delivering new, innovative features when the market demands them.

Customer Experience: This is an evaluation of the product's functioning in production environments. The evaluation includes ease of deployment, operation, administration, stability, scalability and vendor support capabilities. It also includes relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support, as well as the vendor's willingness to work with its clients to customize the product or service, to develop specific features requested by the client, and to offer personalized customer support (see Table 1).

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	High
Overall Viability (Business Unit, Financial, Strategy, Organization)	High
Sales Execution/Pricing	Standard
Market Responsiveness and Track Record	High
Marketing Execution	No Rating
Customer Experience	Standard
Operations	No Rating
Source: Gartner (December 2010)	

Completeness of Vision

Market Understanding: We evaluate the vendor's ability to understand buyers' needs and translate them into products and services. SAST vendors that show the highest degree of market understanding are adapting to customer requirements in areas such as: providing a single tool that combines most of the features that clients need for SAST; comprehensiveness of application security technology coverage that expands beyond SAST; offering DAST in addition to SAST; enterprise-class breadth of programming languages that SAST covers (aka "covered" programming languages); ease of SAST tools' native integration with multiple, popular SLC platforms; enterprisewide consolidation, analysis, reporting, and rule management; user-friendliness, ease of focusing on the most severe and high-confidence vulnerabilities; providing security as a service and cloud delivery; and offering product and service.

Marketing Strategy: A clear, differentiated set of messages that is consistently communicated throughout the organization and is externalized through the website, advertising, customer programs and positioning statements. We give a higher score to vendors that clearly state their dedication to security markets, that clearly define their target audience, and that market appropriate packaging of their products and/or services.

Offering (Product) Strategy: We assess the vendor's approach to product development and delivery. This addresses the vendor's focus on security analysis; the optimal balance between satisfying the needs of leading-edge (that is, Type A) enterprises, and Type B and Type C enterprises; and the optimal balance between satisfying the needs of typical enterprises and specialized clients (for example, hardware vendors and embedded application vendors).

Innovation: Here, 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 give a higher rating to vendors evolving toward ESI-enablement, thus enabling higher accuracy and breadth of security coverage, as well as advanced analytics, contextual assessments, and support for optimal security and risk management decisions across the enterprise. We also give a higher rating to vendors that develop methods that make security code testing more accurate (for example, decreasing false-positive and false-negative rates). We give a higher rating to vendors that offer DAST, in addition to SAST, and interaction and correlation of SAST and DAST; binary code analysis; application protection features (for example, WAF-like features); integration with governance, risk and compliance (GRC) and SIEM technologies; innovative ways of delivery (such as security testing as a service and cloud computing); SAST for cloud platforms; and SAST for mobile platforms (see Table 2).

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Standard
Sales Strategy	No Rating
Offering (Product) Strategy	High
Business Model	No Rating
Vertical/Industry Strategy	No Rating
Innovation	High
Geographic Strategy	No Rating
Source: Gartner (December 2010)	

Leaders

Leaders demonstrate balanced progress in execution and vision. Their actions raise the competitive bar for all vendors and solutions in the market, and they tend to set the pace for the industry. A Leader's strategy is focused on the security of applications; its offering addresses the needs of application security specialists within the SLC; and its brand is broadly recognized in the application security space. Leaders reach beyond SAST capabilities and encompass the broader application security discipline. At the same time, Leaders are able to amass a relatively large clientele and revenue in this evolving market. A leading vendor is not a default choice for every buyer, and clients are warned not to assume that they should only buy from Leaders. Some clients may find that vendors in other quadrants better address their specific needs.

Challengers

Challengers typically have entered the application security space from application quality testing, with a unified view of quality and security. Their primary emphasis is on quality of applications, while security is their secondary priority (but growing in importance). Challengers are able to sell application security to their "application quality" clientele, yet they experience security brand-recognition issues when reaching beyond their installed bases. Challengers have solid products that address the general needs of users. They are good at competing on basic, "good enough" functions, rather than on advanced features and broader ranges of application security products and services. Challengers are efficient and expedient choices to address narrowly defined problems.

Visionaries

Visionaries invest in the leading/"bleeding"-edge features that will be significant in the next generation of products, and they will give buyers early access to greater security assurance. Visionaries can affect the course of technological developments in the market, but they lack the ability to execute against their vision compared with the market Leaders. Enterprises typically choose Visionaries for their best-of-breed evolving features. Other vendors watch Visionaries as indicators of innovation and thought leadership, attempting to copy their technologies or acquire these vendors.

Niche Players

Niche Players offer viable, dependable solutions that meet the needs of specific buyers. Niche Players are less likely to appear on shortlists, but they fare well when considered for business and technical cases that match their focus. Niche Players may address subsets of the overall market, and often can do so more efficiently than the Leaders. Enterprises tend to choose Niche Players when the focus is on a few important functions or on specific vendor expertise, or when they have an established relationship with the vendor.

Vendor Strengths and Cautions

Armorize Technologies

Strengths

- It has a strong focus on security. Specifically, it focuses on static code analysis of Web applications.

- It analyzes Hypertext Preprocessor (PHP), a popular dynamic programming language used in Web application development (the only other vendors that offer this language analysis are market Leaders).

- It has a set of offerings that includes SAST, but goes broader. In addition to a SAST tool, Armorize offers a WAF and a malware alerting and monitoring service.

- Although its original SAST offering was appliance-based, Armorize now offers its SAST solution via on-premises licensed software.

- Armorize entered into a partnership with Coverity to offer a combined quality and security feature set.

- Armorize has a strong presence in the Asia/Pacific region, and has engaged efforts to increase its presence in Europe and the U.S.

- Armorize customers report lower rates of false positives during their SAST technology evaluations.

Cautions

- Armorize is a smaller, venture-capital-backed vendor.

- Armorize does not have a DAST offering, does not partner for a combined SAST/DAST offering, or for SAST/DAST interaction/correlation.

- Armorize does not have SAST SaaS/cloud offerings.

- Armorize lacks market clout, as well as name and brand recognition among enterprises' information security professionals.

- Armorize's partnership with Coverity has yet to demonstrate results.

- Armorize has only a short list of analyzed programming languages: Java, C#, VB.NET and PHP.

Checkmarx

Strengths

- Checkmarx converts analyzed source code into a single common-language model held in persistent storage, which enables repeatable queries and impact analysis. There is no need to run additional application tests if the applications have not changed. Applications can be tested for vulnerabilities to new attacks simply by modifying queries with patterns from new attacks.

- Checkmarx offers a relatively broad range of supported languages. It analyzes code written in Apex (used by salesforce.com), Java, C#, VB.NET, and VB6; in addition, it has a limited availability offering for C and C++ analyses (with general availability planned for year-end 2010).

- Checkmarx primarily offers a security-testing-as-a-service/cloud business model, but it also offers product licenses.

Cautions

- Checkmarx is a smaller, venture-capital-backed vendor.

- Checkmarx lacks market clout, as well as name and brand recognition among enterprises' information security professionals.

- Checkmarx does not have a DAST product or service; it does not partner with DAST vendors for a SAST and DAST combined offering, or for SAST and DAST interaction/correlation.

- Its list of analyzed languages is shorter than the one supported by the market Leaders.

Coverity

Strengths

- Coverity tests applications for quality and security issues.

- Coverity is a proven provider of static code analysis for specialized software and hardware vendors and hardware-embedded applications.

- Coverity offers a dynamic thread analysis tool, which detects race conditions and deadlocks in multithreaded Java applications that might cause application failures at runtime, and also tracks tainted data flows throughout an application.

- Coverity entered into a partnership with Armorize to integrate the quality and security test results of Coverity's tool with Armorize's security test results for reporting and analysis.

- Coverity's sales and marketing extend beyond North America into Europe and Asia/Pacific.

Cautions

- Coverity mainly focuses on application quality, with a lesser focus on security (supplemented by the Armorize partnership).

- Coverity does not have a DAST product or service; it does not partner with DAST vendors for a SAST and DAST combined offering, or for SAST and DAST interaction/correlation.

- Coverity does not have SaaS/cloud offerings.

- Coverity's partnership with Armorize has yet to demonstrate results.

- Coverity has a smaller list of analyzed programming languages: C, C++, Java and C#.

- Coverity has limited market clout and name recognition among enterprises' information security professionals.

GrammaTech

Strengths

- GrammaTech has a unified view of quality and security.

- Its strong reputation for thorough static analysis is targeted at software engineers in the aerospace and defense industries.

- It conducts binary code analysis in addition to source code analysis (Veracode is the only other vendor that offers true binary analysis).

- GrammaTech has direct sales in the U.S. and Canada. It has distributors in Europe and Asia/Pacific.

Cautions

- GrammaTech has a limited security focus. It does not check for the most severe vulnerabilities, such as SQL injection and cross-site scripting.

- It has a limited set of analyzed languages: C and C++ only (although it does conduct source code analysis and binary code analysis).

- It has no support for Java and .NET languages, and no short-term plans to add Java and .NET languages – which are used in most enterprise applications.

- GrammaTech has basic enterprise-class aggregation and reporting features.

- It has no SaaS/cloud offerings.

- It does not have a DAST product or service; it does not partner with DAST vendors for a SAST and DAST combined offering, or for SAST and DAST interaction/correlation.

- GrammaTech lacks market clout, as well as name and brand recognition among enterprises' information security professionals.

HP (Fortify Software)

Strengths

- HP has moved into the Leaders quadrant as a result of its acquisition of Fortify Software – a leading vendor in Gartner's 2009 "Magic Quadrant for Static Application Security Testing." HP's original SAST product, DevInspect, has been phased out. Fortify's suite of application security products has become HP's SAST flagship.

- In addition to SAST, HP Fortify 360 offers a technology for runtime application security protection (Real-Time Analyzer [RTA]), which is a "software firewall" that resides inside an application to protect vulnerable locations within it, and can also monitor and report on application activity.

- HP Fortify 360 also offers a technology that increases the accuracy of vulnerability detection (Program Trace Analyzer [PTA]) – for example, it enables testers to enter malicious input into applications dynamically, to observe malicious data and logic flow, to analyze the application's security controls, and to indicate whether additional/other controls are needed.

- HP Fortify 360 technologies are integrated into a single studio; however, HP's DAST technology is still sold as a separate offering.

- HP Fortify 360 offers the broadest range of supported programming languages: C, C++, Java, C#, VB.NET, COBOL, ColdFusion, Transact-SQL, PL/SQL, VB6, PHP and Python.

- HP Fortify 360 technologies are integrated with the most popular SLC platforms, such as those from HP, IBM and Microsoft.

- HP Fortify 360 is a recognized mind share and market share leader in the SAST market.

- HP Fortify 360 has a large worldwide SAST installed base with customers in the U.S., Europe and Asia/Pacific.

- Since 2009, HP and Fortify have been offering and evolving their SAST/DAST interaction and correlation features. The offer remains available, and we expect that it is continuing to mature and become further enhanced.

- HP Fortify 360 technology is available via the SaaS/cloud delivery model.

Cautions

- HP must resolve any cultural differences with Fortify's team and incorporate Fortify into the HP organization.

- Expect Fortify's partnerships with other DAST providers to be phased out over time and be replaced by HP's DAST technology.

- HP should provide a road map for the integration of HP Quality Center technologies and security testing technologies, including Fortify's offerings.

- HP should provide a product road map for the further evolution of its SAST/DAST technology interaction.

- HP Fortify 360 tends to be the most expensive of all SAST vendors, because the pricing model typically requires seats for any developer who might use the tool.

- While HP has a large installed base in quality testing (where, in the test/QA phase, DAST is likely to be used), it does not have a large presence earlier in the SLC, where SAST testing would likely be used.

- Some customers have expressed dissatisfaction with Fortify's aggressive sales process and licensing practices. It is unclear how this will change under HP.

- In addition to maintenance fees for software updates, Fortify charges separately for ongoing language vulnerability updates. Fortify is the only vendor that charges separately for ongoing language pack updates. It is unclear how this will change under HP.

IBM
Strengths

- IBM offers SAST and DAST technologies.

- IBM Rational provides its AppScan Reporting Console, which correlates results of SAST and DAST scans.

- IBM is well-positioned to leverage its SLC installed base for integrating and selling SAST and DAST tools to Rational and Eclipse platform clients.

- IBM has demonstrated a broader vision of application security by adding (through acquisitions) technologies for data masking and for database activity monitoring. These technologies are not part of SAST or DAST products, but rather are part of a broader application security portfolio.

- IBM is one of the world's largest multinational organizations, with a significant sales force, a global service organization and a worldwide network of partners.

- IBM offers innovative string taint analysis for identifying sources of potentially corrupted input and following their flow throughout the application.

- IBM's pricing is viewed by its customers as being more reasonable than its nearest competitor, HP/Fortify.

- IBM supports a good-size list of analyzed programming languages: Java, C, C++, C#, VB.NET, VB6, PHP, Perl, and ColdFusion.

Cautions

- There is potential overlap and customer confusion with IBM Global Services offering managed services for application security testing/penetration testing.

- While IBM has begun its work on SAST and DAST interaction, it has not yet finished it.

- IBM supports a shorter list of analyzed programming languages than HP.

Klocwork
Strengths

- Klocwork tests applications for quality and security issues.

- Klocwork is a proven provider of static code analysis for hardware vendors and hardware-embedded applications.

- Klocwork is a proven provider for the professional software engineering market in such spaces as mobile devices, consumer electronics, medical, telecommunications, military and aerospace.

Cautions

- Klocwork lacks market clout, as well as name and brand recognition among enterprises' information security professionals.

- Klocwork lags in satisfying the SAST (and broader application security) needs of typical enterprises (as opposed to the needs of software engineering clients).

- Klocwork does not provide DAST technology, nor does it have a partnership for DAST testing and interaction/correlation between SAST and DAST.

- Klocwork does not provide SaaS/cloud services.

- Because of its focus on embedded systems, Klocwork has a shorter list of analyzed programming languages: C, C++, Java, and C#.

Parasoft

Strengths

- Parasoft tests applications for quality and security issues.

- Parasoft provides SAST and DAST solutions, and has a feature for correlating its SAST and DAST analyses.

- Parasoft offers a set of tools for functional testing, load testing, protocol testing and collaborative code reviews.

- Parasoft supports a relatively long list of languages: C, C++, Java, C#, and VB.NET.

- Parasoft has been in the market for more than 20 years, and has proved its reliability as an application testing vendor.

- In 2009, Parasoft released its security testing offering, which was targeted specifically at security testing professionals.

- Parasoft is a self-funded, privately held company, and reports that it is profitable.

- Geographically, Parasoft's sales and marketing reach beyond North America into Europe and Asia/Pacific.

Cautions

- Parasoft lacks market clout, as well as name and brand recognition among enterprises' information security professionals.

- Parasoft mainly focuses on application quality, with a lesser focus on security.

- Parasoft has not shown the rapid growth rate in security that newer vendors, such as Fortify (now HP) and Veracode, achieved in just a few years.

- Although Parasoft provides DAST capabilities, as a DAST provider, it lags well-behind DAST market leaders IBM and HP, which also offer SAST and the interaction of SAST and DAST.

- Parasoft does not provide SAST security testing as a service/cloud.

- Parasoft's list of analyzed languages is shorter than one from market Leaders.

Veracode

Strengths

- Veracode has a strong focus on application security and offers SAST and DAST technologies.

- Veracode has pioneered the security-testing-as-a-service business model, and has also innovated in this area.

- Veracode's SaaS/cloud model will appeal to enterprises that lack the application security skills or resources to conduct their own application security testing, to enterprises that need to rapidly scale to a large number of tested applications, and to enterprises to which application development and testing processes are geographically dispersed.

- Veracode is one of only two vendors in the Magic Quadrant (the other is GrammaTech) that offers a commercial implementation for the SAST of native binary code for C/C++. Some other vendors offer only bytecode analysis for Java and .NET applications.

- SAST technology has always been Veracode's own, while DAST technology has been licensed from NT Objectives. By the beginning of 2011, Veracode expects to replace the licensed DAST technology with its own internally developed DAST technology, which will be natively integrated with Veracode's platform.

- Veracode's specialists review the results of its automated analysis before forwarding them to clients, thereby decreasing the number of false positives.

- Veracode provides a third-party independent software testing service, especially for ISV software (e.g., packages/commercial off-the-shelf) and cloud software testing. Veracode then issues its "VERAFIED" certification to the software that passed the test.

- Veracode offers support for Windows Mobile and BlackBerry mobile platforms.

- Veracode stores the results of its analyses (as well as some application-related business context) in a persistent repository, which enables queries. For queries, there is no need to run additional application tests if the applications have not changed. However, it does not enable customers to query a model of the application tested.

- Veracode has an integration feature with the GRC system Archer from RSA, the Security Division of EMC, which feeds application risk content into the Archer SmartSuite Framework to support the management of GRC processes for customers of Veracode and Archer.

- Veracode can analyze binaries encapsulated within virtual machine containers.

- To assure its clients security and privacy, Veracode does not host its services on its own premises, but rather hosts them in a SAS 70 Type II hosting facility with independent SysTrust Certification conducted annually by Ernst & Young for security and confidentiality.

- Veracode offers APIs and plug-ins that enable customers to integrate Veracode remote testing results with customers' on-premises integrated development environments, build systems and bug-tracking systems.

- Veracode supports analysis of the following programming languages: Java, C, C++, C#, VB.NET, PHP and ColdFusion (compiled as Java).

Cautions

- Veracode is a smaller, venture-capital-backed startup vendor.

- Veracode is a pure-play application security testing service provider. It generally does not sell its technology as a product (although, as an exception, it has implemented an on-premises service for government customers in the intelligence community). Other Leaders sell their technologies as products and services, thus satisfying the needs of the clients that want to have one or the other, or both.

- Clients' byte and/or binary code must be uploaded for testing to Veracode's testing site. Veracode is the sole provider of its services – i.e., as a general offering, there is no "private"

Veracode feature that can be installed at some enterprise's premises and run by the enterprise itself. Some organizations may not want outside entities, like Veracode, to have access to their sensitive software assets and information. Parting with the code (even if it is not a source code) might be a sensitive issue for some of them.

- Veracode's detection capabilities are language-, platform-, chipset- and OS-specific, so that not all binaries on all platforms are supported.

- Veracode's internally developed DAST technology, which replaces NT Objectives', has not been proved yet.

- Veracode SAST and DAST interaction capability has been planned for year-end 2010.

- Veracode tests applications remotely, and, on its cloud platform, provides centralized reporting on detected vulnerabilities, but clients perform the respective vulnerability remediation on their local sites. Therefore, Veracode's clients should enact processes for integrating Veracode reporting into their own application remediation systems.

- Veracode supports a shorter list of analyzed programming languages than the other market Leaders.

Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Evaluation Criteria Definitions

Ability to Execute

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

Overall Viability (Business Unit, Financial, Strategy, Organization): 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 pre-sales activities and the structure that supports them. This includes deal management, pricing and negotiation, pre-sales support and the overall effectiveness of the sales channel.

Market Responsiveness and Track 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.