

# Magic Quadrant for Static Application Security Testing

Gartner RAS Core Research Note G00164100, Joseph Feiman, Neil MacDonald, 6 February 2009, R2997 02102010

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

## WHAT YOU NEED TO KNOW

As attacks become more financially motivated and as organizations get better at securing their network, desktop and server infrastructures, there has been a shift in attacks to the application level. To address those new risks, several technology markets for application security have emerged, including static application security testing (SAST).

SAST for security vulnerabilities should be a mandatory requirement for all IT organizations that develop or procure applications. Although the market is relatively new and consolidating, enterprises must adopt SAST technologies and processes because the need is strategic. Enterprises should use a short-term, tactical approach to vendor selection and contract negotiation due to the relative immaturity of this market.

## STRATEGIC PLANNING ASSUMPTIONS

By 2010, leading DAST and SAST vendors will provide hybrid static-and-dynamic application security testing.

By 2010, leading application security testing vendors will offer security as a service.

By 2013, SAST will effectively disappear as a stand-alone market, as technology and services vendors integrate SAST technologies into their SLC platforms and service offerings.

## MAGIC QUADRANT

### Market Overview

This is the first Magic Quadrant for the SAST market. The SAST market leaders are smaller, innovative, security-focused vendors (Fortify Software and Ounce Labs) that provide static security testing tools as their primary offerings. Both of these vendors offer broad language support and integration into a variety of software life cycle (SLC) platforms.

However, the majority of SLC platform vendors will recognize the need to add security testing capabilities to their platforms and perform this integration over the next several years. Most of the large SLC vendors (for example, HP and IBM) have taken steps in that direction (Microsoft has some basic capabilities). Yet, in all these cases, the offerings fall short of the breadth of coverage options available from dedicated point-solution vendors.

Also challenging the market leaders are SLC vendors that focus on overall application quality testing tools, where security is treated as one aspect of application quality (for example, Coverity, Klocwork, Parasoft and Compuware). These vendors are able to sell security testing capabilities to their installed base, typically to the same development teams that were interested in application quality. The notion of application “resilience” and “robustness” spans quality and security issues. For some customers already using these tools, working with these vendors becomes an easy and pragmatic way to add security testing to their environments.

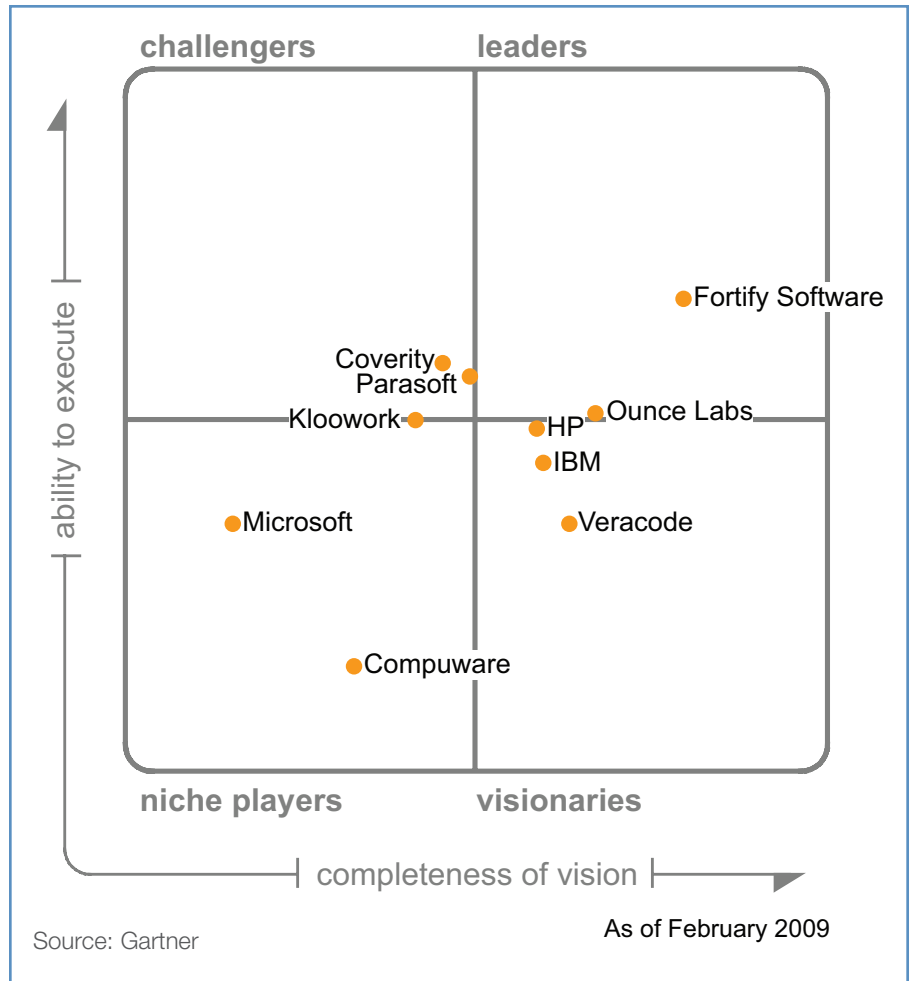
The market for SAST will experience significant changes:

- Commoditization of some capabilities
- Consolidation of features and products
- Delivery of testing as a service
- Integration of SAST at little or no cost into SLC platforms

Enterprises considering SAST should expect ongoing market and product consolidation, as well as downward pricing pressures during the next 24 months. The difficult economic conditions of 2009 (that are likely to extend into 2010) will place tremendous pressure on smaller vendors of SAST point solutions. As with any contract negotiation, organizations are advised to include appropriate protection clauses in their contracts in the event of a vendor merger, acquisition or failure. We recommend contract terms of no longer than 24 months.

Delivering security testing as a service is a growing area of interest for Gartner clients as a way to reduce upfront costs and to augment limited internal resources. Indeed, one of the vendors, Veracode, offers SAST capabilities only as a service. Testing as a service will have a significant impact on the application security market. During the next 18 months, most application security testing vendors will offer their SAST, as well as dynamic application security testing (DAST), solutions optionally or exclusively as a service. Increasingly, we hear from organizations that prefer to use a product and a service from the SAST vendor. For example, they test critical applications but use services to augment the testing for less-critical applications, or they start with services and then make the transition to a product as their staff gains experience.

Figure 1. Magic Quadrant for Static Application Security Testing



Another significant trend is the ability of SAST solutions to scan applications where the source code is unavailable. At a minimum, SAST solutions that scan Java and .NET code should be able to scan the byte code representations of the actual source code. This capability is straightforward and should be required in any vendor’s offering that scans Java and .NET applications. Veracode is the only vendor that has delivered the capability to scan executable code in its binary format. This is an important area, especially in software architectures where calls are made to programs — such as packaged applications, services subscribed to over the Internet and dynamic link libraries — whose source code is unavailable for security testing, but for which binaries are available. With this approach, users must analyze the code in its compiled state so

The Magic Quadrant is copyrighted February 2009 by Gartner, Inc. and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner’s analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the “Leaders” quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

© 2009 Gartner, Inc. and/or its Affiliates. All Rights Reserved. Reproduction and distribution of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner’s research may discuss legal issues related to the information technology business, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The opinions expressed herein are subject to change without notice.

that any externally included library- or platform-specific problems can be identified. Thus, this capability is useful even when source code is available.

The SAST market risks disappearing as a stand-alone market during the next five to seven years as the major SLC platform providers supply SAST technologies or acquire SAST startup vendors. The proper place for application security testing is in the SLC process. Most organizations will consume SAST via security testing capabilities integrated with SLC platforms, especially if SAST capabilities are included with the SLC platform at little or no additional perceived cost.

## Magic Quadrant Overview

Two vendors are in the Leaders quadrant:

- Fortify has a broader vision and greater ability to execute than Ounce Labs. To keep its leadership and remain independent, Fortify should acquire or build in-depth DAST capabilities in addition to its SAST offering, and also become a full-fledged testing-as-a-service provider. An alternative is for the vendor to be acquired by a large SLC platform vendor, preferably a leader in DAST, to combine leadership in SAST and DAST in one vendor offering.
- Ounce Labs could strengthen its position by adding DAST capabilities, partnerships and expanded testing-as-a-service offerings. An alternative is for the vendor to be acquired by a large SLC platform vendor, preferably a leader in DAST, to combine leadership in SAST and DAST in one vendor offering. Considering that it is positioned lower than Fortify in vision and execution, Ounce Labs should act faster and more decisively than it is doing now.

Several vendors are grouped closely around the center of the Magic Quadrant. They have the potential to move into other quadrants and, most importantly, into the Leaders quadrant. To realize that potential:

- HP and IBM should substantially increase SAST capabilities to fulfill their leadership ambitions in the overall application security space. Each vendor's vision and execution in SAST should increase substantially to match its leadership in the DAST market (which was made through acquisitions). Currently, they are lagging behind the SAST market leaders in vision and execution. That gap should be bridged by acquisitions (a fast approach) or internal technology development (a longer approach). Both vendors should develop SAST testing-as-a-service offerings that leverage their worldwide presence — HP with the acquisition of EDS, and IBM with its Global Services organization.
- Veracode should modify/enhance some aspects of its vision to attract more clients — for example, by providing a version of its technology for organizations that want to perform testing themselves. Veracode should invest maximum efforts to improve its execution capabilities and do it rapidly, considering its smaller size and emerging competition from larger vendors.
- Coverity and Klocwork should consider making security analysis (rather than quality analysis) their strategic objective; focus on expanding their capabilities that address the needs of mainstream enterprises, in addition to specialized software and

hardware vendors; and grow their security revenue. Also, each vendor should develop DAST capabilities and strengthen the appeal of its offerings outside its installed base.

- Parasoft should grow awareness and strengthen the application-security reputation among its enterprise prospects, develop broader security testing capabilities with offerings and packaging that appeal to all enterprises, reach beyond its installed base, and expedite the rate of growth to match startup vendors, such as Fortify and Coverity.

Two vendors are in the Niche Players quadrant:

- Microsoft is barely visible in SAST, and even less so in DAST. It is especially noticeable in comparison with Microsoft's SLC platform rivals IBM and HP, which play leadership or visionary roles in those markets. While Microsoft plays a niche role in SAST, other vendors successfully provide application security testing technologies for Microsoft's SLC platform. With substantial resources and a large installed base of Visual Studio developers, Microsoft should improve its security testing capabilities as its closest competitors also evolve them.
- Compuware should send a clear message of intentions regarding the role it wants to play in the SAST and DAST markets. Its early entrance into both markets has not been supported by further vision and execution, which has relegated Compuware to its current niche role.

## Market Definition/Description

SAST is a set of technologies designed to analyze application source code, byte code, or binaries for coding and design conditions that are indicative of security vulnerabilities. Much like a compiler, SAST tools analyze applications 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, in contrast to DAST tools, which analyze applications in a runtime state.

Conceptually, SAST tools test the application from the “inside out,” whereas dynamic testing tools test the application from the “outside in.” These SAST and DAST techniques are complementary. Ideally, an application security testing tool vendor will provide both tools. This is another key trend in application security. We have noted that vendors have higher vision if they offer both types of capabilities and use the correlated results of the tools' analyses to increase the accuracy of vulnerability detection. The ability to provide DAST capabilities is secondary when selecting SAST technology. However, for some enterprises — especially Type B (mainstream IT users) and Type C (technologically conservative users) — it is appealing to get SAST and DAST technologies from a single vendor. For established DAST vendors that also have SAST technologies, selling SAST to their DAST clientele provides a path of least-resistance upsell opportunity and threatens SAST-only offerings.

SAST enables security vulnerability detection early in the application life cycle — at construction (programming) and testing phases when the code is being written, built and tested. Proactively detecting and fixing security vulnerabilities earlier in the application development process reduces an application's overall security

exposure and is less-expensive than fixing the vulnerability when the application is in production.

Enterprises are beginning to understand the importance of application security vulnerability detection, which is creating market demand for security testing tools. Because of the process and cultural changes required to incorporate these tools into the SLC, it will take more than five years before SAST technologies reach the Plateau of Productivity.

## Inclusion and Exclusion Criteria

Through year-end 2007, the SAST market players' total revenue was approximately \$100 million, growing close to 100% each year from 2004 to year-end 2007. This is an evolving market, attracting new players — small startup vendors, as well as large software vendors offering their latest (sometimes recently released) products.

For the SAST Magic Quadrant, we have set up the following inclusion criteria:

- Vendors have been in the market for six or more months (including vendors that offered beta or first production releases of their SAST technologies during the past six months).
- Vendor's revenue exceeds \$500,000, and/or a vendor has at least 10 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.
- Vendors must offer a SAST security testing product or service, or both.

Vendors were excluded from this research for the following reason:

- Open-source SAST offerings lag well behind in capabilities compared with commercial offerings.

### Added

This is the first Magic Quadrant for the SAST market.

### Dropped

Not applicable.

## Evaluation Criteria

### Ability to Execute

**Product/Service:** These are the vendor's core products and services that compete in the SAST market. This 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 information security specialists; and appeal with technologies other than SAST (whether or not they are application security).

**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 application security strategy.

**Sales Execution/Pricing:** We account for SAST growth rate, 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 buyers' functional requirements; and the vendor's track record in delivering new, innovative features when the market demands those features.

**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 that customers receive technical support or account support, as well as the sales process. This also can include ancillary tools, customer support programs and service-level agreements (see Table 1).

**Table 1. Ability to Execute Evaluation Criteria**

Evaluation Criteria	Weighting
Product/Service	high
Overall Viability (Business Unit, Financial, Strategy, Organization)	standard
Sales Execution/Pricing	standard
Market Responsiveness and Track Record	high
Marketing Execution	no rating
Customer Experience	standard
Operations	no rating
Source: Gartner	

## Completeness of Vision

**Market Understanding:** We evaluate the vendor's ability to understand buyers' needs, and translate those needs 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; enterprise-class breadth of programming languages that SAST covers (aka "covered" programming languages); ease of SAST tools' native integration into multiple, popular SLC platforms; and enterprisewide consolidation and reporting. We rate highly the tools that help focus developers' efforts on the most severe and highest confidence vulnerabilities.

**Offering (Product) Strategy:** We assess the vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature set as the vendor's strategy maps to current and future requirements. This addresses the vendor's focus on security analysis; the optimal balance between security and quality analyses; the optimal balance between satisfying the needs of leading-edge (that is, Type A) enterprises, as well as Type B and Type C enterprises; and the optimal balance between satisfying the needs of typical enterprises and specialized clients (for example, hardware vendors, embedded application vendors).

**Vertical/Industry Strategy:** This criterion includes the vendor's ability to direct resources, skills and offerings to meet the specific needs of the market and a commitment to vertical markets (for example, security analysis of hardware-embedded applications, such as mobile handsets). This addresses the vendor's focus on satisfying the needs of a broad spectrum of enterprises (scored higher) or a smaller vertical segment (scored lower).

**Innovation:** Here, we evaluate the vendor's development and delivery of a solution that is differentiated from the competition in a way that uniquely solves critical customer requirements. We give a higher score to vendors that develop methods that make security code testing more accurate (for example, decrease false-positives rates). We give a high rating to vendors that offer DAST, in addition to SAST and hybrid SAST-DAST; binary code analysis; application protection features (for example, Web-application firewall-like features); frameworks that allow for comprehensive quality and security testing; testing of Web services/service-oriented architecture (SOA); and innovative ways of delivery, such as security testing as a service.

**Geographic Strategy:** This includes the vendor's ability and commitment to direct resources to meet the specific needs of geographies outside the "home" or native geography — directly or through partners, channels and subsidiaries, as appropriate for the geography and market (see Table 2).

**Table 2. Completeness of Vision Evaluation Criteria**

Evaluation Criteria	Weighting
Market Understanding	high
Marketing Strategy	no rating
Sales Strategy	no rating
Offering (Product) Strategy	high
Business Model	no rating
Vertical/Industry Strategy	standard
Innovation	high
Geographic Strategy	low
Source: Gartner	

## 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 security of applications; its offering addresses the needs of application security specialists; 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, they are able to amass a relatively large clientele and revenue in this emerging market. A leading vendor is not a default choice for every buyer, and clients are warned not to assume that they should buy only from leaders. Some clients may find that vendors in other quadrants better address their specific needs.

## Challengers

Challengers have typically 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 (although growing in importance). They are able to sell application security to their "application quality" clientele, yet experience security-brand recognition issues when reaching beyond their installed base. Challengers have solid products that address the general needs of the users. They are good at competing on basic, "good enough" functions, rather than on advanced features. Challengers are efficient and expedient choices to address narrowly defined problems, and typically are aggressive on pricing.

## Visionaries

Visionaries invest in the leading/"bleeding"-edge features that will be significant in the next generation of products and 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 that vision compared with the market leaders. Enterprises typically pick visionaries for their best-of-breed evolving features. Other vendors watch them 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 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 pick niche players when the focus is on a few important functions and features, or when they have a relationship and experience with the vendor.

## Vendor Strengths and Cautions

### Compuware

#### Strengths

- Compuware's DevPartner Studio treats application security as part of application quality, and offers testing capabilities for quality and security. This approach is similar to one demonstrated by Coverity, Klocwork and Parasoft, and appeals to organizations already using Compuware's tools for application quality testing.
- Compuware offers SAST and DAST basic testing capabilities within DevPartner Studio.
- Compuware's large installed base of enterprises that uses its testing tools represents a sizable population that would benefit from security-testing technologies.
- Compuware provides tight integration and focus on Visual Studio via its partnership with Microsoft. It also has provided early support within DevPartner Studio for newer Microsoft technology stack elements, such as ASP.NET, Ajax components, Linq, WPF, and the latest versions of the Microsoft .NET framework.
- Compuware DevPartner Studio supports legacy Microsoft languages such as VB6, Visual C++ and the older .NET 1.1 framework.

#### Cautions

- Compuware does not offer SAST software testing as a service.
- During a reorganization in 2007, Compuware retired its stand-alone SecurityChecker product and incorporated only some of its security testing capabilities into DevPartner Studio. Compuware has withdrawn from the dedicated security testing market entirely and does not consider itself a competitor in the security testing tool market.

- Compuware's security testing capabilities focus on Microsoft's .NET environment. There are no security testing capabilities in DevPartner Java edition.
- Compuware has made an explicit business decision not to compete directly in the security testing market. Most users are unaware that Compuware has any security testing capabilities. The security testing capabilities it provides fall short of a dedicated security vendor.
- Without a specific focus on security, Compuware has lost its "promising" position in the DAST market and in the emerging hybrid SAST-DAST technology market.

### Coverity

#### Strengths

- Coverity tests for software quality and security issues:
  - Coverity Prevent conducts security and quality analysis of an application's source code.
  - Coverity Architecture Analyzer provides a visual representation of an application's architecture, including dependencies, the design's excessive complexities, and data and control paths through the application.
  - Coverity Software Readiness Manager collects the analyzed code's metrics, and points to violations of best programming practices. Architecture Analyzer and Readiness Manager indicate potential causes of quality and performance problems, as well as security problems.
- Coverity has expanded its technologies beyond source-code analysis. For example, Coverity Thread Analyzer detects race conditions and deadlocks in multithreaded Java applications that might cause application failures at runtime. This tool also tracks tainted data flows throughout an application. Coverity is building on that capability a tool that detects SQL injection, cross-site scripting, and other attacks based on incorrect input validation. The combined use of Coverity Prevent and Thread Analyzer helps to increase accuracy of analysis.
- Coverity's revenue in 2007 was \$27.2 million, according to Gartner estimates. Coverity has more than 500 customers for its quality/security testing technologies.
- Geographically, Coverity's sales and marketing extends beyond North America. In 2007, approximately 30% of its revenue came from sales in Europe, Japan and Asia/Pacific.
- Coverity has proven itself in providing code analysis for hardware vendors and hardware-embedded applications.

#### Cautions

- Coverity's unified view on quality and security has been focused on quality, and Coverity only recently increased the importance of its security analysis. Coverity's emphasis on quality testing has resulted in less market awareness in the security space among enterprise prospects, and less emphasis on enterprisewide security capabilities.
- Coverity does not offer DAST solutions or partnerships.
- Static code analysis is limited to C, C++, Java and C#.

- Most major Coverity clients have been vendors of hardware-embedded software, but only a limited number of clients were enterprises.
- Coverity's tools have limited enterprise-class capabilities, which typical Type B and Type C enterprises want. For example, Coverity does not have a central dashboard with enterprisewide aggregation and reporting capabilities; and it does not provide remediation advice. Compared with the market leaders, Coverity tools have more limited integration capabilities for popular development and testing platforms — that is, for IBM Eclipse and Microsoft Visual Studio, but not IBM Rational Application Developer and HP Quality Center.
- To conduct analysis of C, C++, Java and C# codes, enterprises must acquire and use three Coverity tools.
- Coverity does not provide SAST as a service.

## Fortify Software

### Strengths

- Fortify is one of the largest SAST vendors, with strong innovation as well as execution capabilities. It has expanded its technologies beyond SAST into a broader spectrum of application security disciplines that supplement its core SAST capabilities:
  - Fortify pioneered a technology for runtime application security protection (Real Time Analyzer), which is a “software firewall” that resides inside an application protecting vulnerable locations within the application.
  - Fortify also pioneered a technology that increases the accuracy of vulnerability detection (Program Trace Analyzer), which enables testers to enter malicious input into tested applications, observe malicious data and logic flow, analyze the application's security controls, and indicate whether new controls are needed.
  - Fortify was one of the first vendors offering hybrid SAST-DAST capabilities via its partnerships with Watchfire and Cenzic. However, the subsequent IBM acquisition of Watchfire has ended the partnership. Fortify can integrate results from the IBM Rational AppScan DAST tool into Fortify SAST reports. This allows for limited correlation of results of static and dynamic testing.
  - All Fortify technologies are integrated into a single Fortify 360 studio, thus simplifying a combined use of its security detection and protection features.
- Fortify offers a broader range of covered programming languages than any of its competitors. Its SAST technology analyzes code written in Java, JSP, ASP.NET, C#, VB.NET, C, C++, COBOL, ColdFusion, Transact-SQL, PL/SQL, JavaScript/Ajax, Classic ASP, VBScript, VB6 and PHP.
- Fortify technologies natively integrate into the most popular SLC platforms, such as those from HP, IBM and Microsoft, thus providing higher user-friendliness and productivity for application developers and security testers.

- Fortify is the market-share leader, with 2007 revenue of \$29.2 million, according to Gartner estimates. It has more than 400 customers, and approximately 20% of its revenue came from sales in Europe, Japan and Asia/Pacific.
- Fortify has several partnerships with large external service providers (such as Wipro and Accenture) that offer security testing services using Fortify SAST tools.

### Cautions

- Fortify does not have DAST technology, although some of its competitors offer SAST and DAST technologies. Furthermore, the DAST partnership with IBM/Watchfire has ended since IBM's acquisition of Watchfire.
- Fortify does not currently offer SAST as a service, although it is building a capability for providing it.
- Fortify tends to be the most expensive of all the SAST vendors, as the pricing model typically requires seats for any developer that might use the tool.
- Some customers have expressed dissatisfaction with Fortify's aggressive sales process and licensing practices.
- Fortify testing tools provide remediation advice, but not actual code replacement suggestions.
- In addition to maintenance fees for software updates, Fortify charges separately for ongoing updates to its language packs that provide additional scans and language vulnerability updates. Fortify is the only vendor that charges separately for ongoing language pack updates.

## HP

### Strengths

- HP's DevInspect is a hybrid tool, providing SAST and DAST testing capabilities. DevInspect conducts static source code analysis and invokes DAST functionality to confirm that detected vulnerabilities are real and exploitable, or to indicate that they are false-positives.
- HP is a leader in the DAST market with its WebInspect tool, and will be able to sell its DevInspect to its WebInspect installed base.
- HP is a global leader in software quality and performance testing (through its acquisition of Mercury Interactive). This is a secondary criterion when selecting SAST technology; however, for some enterprises (especially Type B and Type C enterprises), it is appealing to get a full spectrum of testing technologies from a single vendor.
- HP Assessment Management Platform allows for consolidation, analysis, and reporting of data collected from many DAST and SAST tools, thus enabling enterprisewide application security initiatives and fuller security coverage of the application life cycle.
- HP DevInspect provides “safe” code replacement suggestions for vulnerable code using its SecureObjects library.

## Cautions

- HP's DevInspect tool focuses only on the security testing of Web-facing (HTML/JavaScript) applications written in Java, C# and VB.Net.
- HP's DAST tool WebInspect has always been HP's flagship product and is the focus of its investments. There are indications of growing recognition inside HP that having a leading SAST technology is critical to HP's security strategy, but it remains to be seen whether that vision will be executed through improvements in DevInspect or through a SAST technology acquisition.
- Compared with market leaders' products, DevInspect scans a narrower set of languages: Java, Java ServerPages (JSP), C#, VB.NET, ASP.NET and JavaScript. Notably absent are C, C++ and Visual Basic 6 (VB6), which are not typically used for the development of Web-enabled applications.
- Acquisition and use of two separate HP DevInspect tools are necessary to conduct analysis of Java and .NET languages.
- HP does not provide SAST as a service, although it provides testing as a service for DAST.

## IBM

### Strengths

- IBM offers static (AppScan Developer Edition [AppScan DE]) and dynamic testing capabilities (IBM AppScan) providing hybrid (that is, correlated static and dynamic) analysis. IBM (along with HP) is a leader in the DAST market and can sell its AppScan DE to its installed AppScan DAST base.
- IBM is well-positioned to leverage its SLC installed base for integrating and selling SAST and DAST tools to Rational Application Developer and Eclipse clients.
- IBM has delivered a patented string analysis as an alternative for taint analysis, which is intended to increase accuracy and reduce the need for manual configuration of input sanitizers.
- IBM has demonstrated a broader vision of application security by adding (through acquisition) a technology for data obfuscation at the application testing phase to its application security portfolio. This technology is not part of a SAST or DAST product, but is part of a broader application security offering.
- IBM has demonstrated strength, reputation and breadth of its security strategy and product offerings, such as vulnerability and threat research conducted by IBM/ISS X-Force Labs; and ongoing updates for the SAST and DAST testing tools.
- There are also potential areas of synergy with Internet Security Systems' network vulnerability scanner and intrusion-prevention system product — a potential offer of application security and network security solutions from a single vendor.
- IBM has separate and distinct offerings designed for developers, build teams and quality assurance (QA) groups.
- AppScan Tester Edition (AppScan TE) offers integration into IBM QA tools, as well as the HP Quality Center QA tool.

- IBM is a large, multinational organization with a significant sales force, a global service organization, and a worldwide network of partners. IBM Global Services has a significant worldwide presence to provide application security consulting, integration, and SAST and DAST testing as a service.

### Cautions

- IBM is a new entrant to the SAST market. Relatively few customers are using its AppScan DE SAST tools.
- The scale, performance and accuracy of IBM's SAST analysis on large, production applications are unproven.
- IBM AppScan DE tests Java and JSP source code and bytecode only. PHP and .NET support is planned for 2009. A narrow spectrum of tested languages is a significant limitation of the first release, and is not suitable for organizations that use a variety of languages and development platforms.
- IBM has built and delivered products that are sold separately for security and quality (AppScan DE and IBM Rational Software Analyzer, respectively). These tools provide integrated management and reporting, and target different buying centers. However, vendors such as Coverity, Klocwork and Parasoft each have delivered a single offering that addresses application quality and security, which appeals to enterprises.
- Despite the worldwide presence and scope of IBM Global Services, IBM has not yet delivered a SAST as a service offering.

## Klocwork

### Strengths

- Klocwork has a unified view of software quality and security. As such, the Klocwork Insight tool scans for quality and security issues, so that users do not have to purchase separate products.
- Klocwork provides specific tools for the Symbian mobile operating system (OS) platform, and has plans for similar capabilities for Java analysis specific to Google's Android smart device platform.
- Klocwork's Insight is designed to be used at the developers' desktops with plug-in integrated development environment (IDE) support for Microsoft Visual Studio, IBM Rational Application Developer, Eclipse and IntelliJ.
- Klocwork provides capabilities beyond security. For example, it provides a tool for the graphical architectural analysis of source code, which enables real-time design experimentation.
- Klocwork's 2007 revenue was \$26 million, according to Gartner estimates. It has 330 customers of its quality/security testing technologies. Approximately 25% of its revenue came from sales outside North America.
- Klocwork is a proven provider of static code analysis for hardware vendors and hardware-embedded applications.

## Cautions

- Klocwork has historically focused on application quality testing for the professional software engineering market, while gradually raising the importance of security. This has resulted in less market name and brand awareness among information security and audit professionals, as well as less emphasis on enterprisewide security capabilities.
- Klocwork does not provide DAST technology, nor does it have a partnership for DAST testing.
- Klocwork originally focused on C, C++ testing and later added support for Java. It added support for C# and the Microsoft .NET framework at the end of 2008.
- Klocwork's historical focus on embedded systems (telecommunications and avionics) has resulted in enterprise-class language support that is not as well-established as competitors' support.
- Klocwork lacks a central dashboard with enterprisewide aggregation and reporting capabilities, although it provides metrics that could be used to perform them.
- Klocwork does not provide security testing as a service as a standard offering.

## Microsoft

### Strengths

- Microsoft provides basic security scanning capabilities out of the box at no additional cost with Visual Studio Team System 2005 and higher.
- Microsoft's bundled security scanning tools are variants of the ones it uses internally to detect application software security defects.
- In addition to SAST testing capabilities, Microsoft provides a threat-modeling tool, as well as consulting services for organizations looking to integrate security into their SLC processes.
- Microsoft has a large installed base of Visual Studio developers to whom it targets its security testing capabilities.

### Cautions

- Microsoft's Visual Studio Team System provides only basic SAST security testing capabilities. Although there is no explicit charge for these capabilities, they are only included in the higher-priced Team System version of Visual Studio.
- Microsoft's SAST language support for security scanning is focused primarily on the .NET family of languages. Microsoft currently does not support Java applications. Although Microsoft provides static testing tools for C, C++, these tools do not provide many security-specific rules. The C, C++ tools can find a large number of common C, C++ security coding errors, such as buffer overflows.
- Microsoft does not have a DAST solution or a formal DAST partnership for hybrid SAST-DAST analysis.

- Microsoft provides no integration with quality assurance testing tools (including for Microsoft offerings).
- Microsoft has no formal SAST software testing-as-a-service offerings.

## Ounce Labs

### Strengths

- Ounce Labs offers a broad range of covered programming languages: C, C++, Java, JSP, .NET (including C#, VB.NET, ASP.NET and Managed C++), Classic ASP (JavaScript and VBScript) and VB6.
- Ounce Labs provides bytecode analysis of Java call libraries and .NET assembly bytecode.
- Ounce Labs offers SAST solutions for use throughout the IT organization, not solely for use within development. For example, it offers a stand-alone testing tool for auditors and security professionals outside of development IDEs.
- The output reports produced by Ounce Labs provide users with a two-dimensional matrix that enables customers to quickly and easily focus on the highest severity vulnerabilities, and place a lower priority on "exceptions" (which represent a lower level of confidence and tend to have higher levels of false-positives).
- Ounce Labs' Automation Server automates static application security integration into build environments, and has developed and donated a free-standing command line interface (Apache Maven) plug-in to the open-source community.
- For custom or nonsupported languages and scripts, customers can define rules for scanning using pattern-based semantic analysis.
- Ounce Labs has several partners for SAST software testing as a managed service, and plans to offer its own capabilities by 2Q09.
- Ounce Labs has been aggressive with pricing and offers sitewide and organizationwide unlimited use of licenses on a perpetual or term basis, as opposed to per-seat or concurrent licenses.
- Ounce Labs recently secured another \$7.5 million in venture capital funding.

### Cautions

- Ounce Labs is a smaller independent vendor, with 2007 revenue of \$9.5 million, according to Gartner estimates, and is a likely acquisition target.
- Ounce Labs has a historical weakness in marketing. It is not well-known, even among information security and testing professionals.
- Ounce Labs recently experienced senior management turnover; a new CEO and chief marketing officer joined the company in 2H08. Ounce Labs has also undergone a 15% workforce reduction.

- As a smaller company, Ounce Labs provides no option for 24/7 support.
- Ounce Labs has no formal DAST partnership for hybrid analysis. However, it has demonstrated proof of concept with DAST vendor Cenxic, using its third-party data access application programming interfaces.
- Ounce Labs has not yet offered support for PHP, Perl or ColdFusion. Support for these languages is planned for 1Q09.
- Ounce Labs does not yet provide quality assurance integration for HP's Quality Center. This is targeted for 1Q09; however, Ounce Labs supports integration with IBM Rational ClearQuest.

## Parasoft

### Strengths

- Like Coverity, Klocwork and Compuware, Parasoft provides a unified view of software quality and security.
- Parasoft goes beyond SAST technology:
  - As one of the pioneers in securing Web applications, SOA and Web services, Parasoft provides DAST technology.
  - It also offers a set of tools for functional testing, load testing, protocol testing and collaborative code reviews.
- Parasoft's SAST technology supports a variety of languages: Java, C, C++, C#, VB.NET, Managed C++, .NET, JavaScript and VBScript/ASP.
- Parasoft can sell to its installed base of testing tool users, as well as provide native integration into Eclipse and Visual Studio.
- Parasoft has been on the market for more than 20 years, and has proven its reliability as a vendor.
- Parasoft is privately owned, does not have venture capital support and reports that it is profitable.
- Parasoft's 2007 total revenue was \$36.5 million, according to Gartner estimates. Parasoft estimates that \$18 million of its revenue comes from static code analysis sales.

- Geographically, Parasoft's sales and marketing go beyond North America. In 2007, approximately 45% of its revenue came from sales in Europe and Asia/Pacific.

### Cautions

- Parasoft suffers from lack of brand awareness in the security space.
- Parasoft has not shown the rapid growth rate in security that newer vendors, such as Fortify and Coverity, have achieved in just a few years.
- Parasoft does not provide correlated, hybrid SAST-DAST analysis.
- Although Parasoft provides DAST capabilities, as a DAST provider it lags behind DAST market leaders IBM and HP, which also offer SAST and hybrid SAST-DAST.
- Parasoft offers a narrower set of analyzed languages than the market leaders.
- Parasoft does not provide SAST security testing as a service.

## Veracode

### Strengths

- Veracode is the only vendor on the Magic Quadrant for SAST that offers a commercial implementation for the static analysis of native binary code. Other vendors offer bytecode analysis for Java and .NET applications; however, the ability to scan binary executables natively is unique to Veracode.
- Veracode does not sell its technology as a product, but rather provides software security testing services through an automated security-testing-as-a-service business model. This approach should appeal to enterprises that lack the application security skills or resources to conduct application security testing.
- Veracode provides DAST security as a service (through a partnership with NT Objectives).

- Veracode's pricing model is clear and simple: per megabyte of analyzed code.
- Veracode specialists review results of automated analysis before forwarding the results to clients, thus additionally filtering out some false-positives.
- Veracode's testing services are attractive to independent software vendors as a "seal of approval" for prospective clients without releasing sensitive source code.

### Cautions

- Veracode's appeal is limited to enterprises that want to use a security testing service. It excludes enterprises that prefer to purchase a tool to conduct testing themselves.
  - A critical element of Veracode strategic execution will be earning the trust of clients that will be uploading their code to the Veracode platform for testing. This is a sensitive issue, because Veracode gets access to its clients' intellectual property (albeit in binary format), as well as information on clients' security vulnerabilities.
  - Because Veracode is the only vendor on this Magic Quadrant that analyzes binary code, the accuracy of its analysis (for example, the rate of false-positives) cannot be easily compared with other SAST approaches.
  - Veracode needs to prove that it can scale to host a large number of clients, each of which has many applications.
  - Part of Veracode's value proposition is finding vulnerabilities in applications where the organization doesn't have access to the source code (for example, in packaged applications); however, without source code, an organization's remediation options are limited once Veracode finds the problems.
  - Veracode's detection capabilities are language-, platform-, chipset- and OS-specific, so that not all binaries on all platforms are supported. Furthermore, application-specific libraries, such as Struts, should be explicitly supported.
- Obfuscated or optimized binary code makes analysis difficult (if possible).
  - Although Veracode provides DAST as a service through a partnership with NT Objectives, its SAST and DAST test results are not correlated. NT Objectives, as a DAST provider, lags behind DAST market leaders IBM and HP, which also offer SAST and hybrid SAST-DAST.
  - Veracode tests applications remotely and ships reports on detected vulnerabilities, but clients do the respective vulnerability remediation on their local sites. Veracode should streamline the detection-remediation process by integrating its testing output natively and seamlessly into requirements management, quality control, and software change- and configuration-management tools.

### 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 presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

**Market Responsiveness 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 Web site, 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.