G00259568

Magic Quadrant for Application Security Testing

Published: 1 July 2014

Analyst(s): Joseph Feiman, Neil MacDonald

Global-scale scandals around critical applications' breaches have highlighted the need for effective detection of exploitable application security vulnerabilities. Application security testing is the solution for Web, cloud and mobile applications.

Strategic Planning Assumption

Through 2015, more than 75% of mobile applications will fail basic security tests.

Market Definition/Description

Application security testing (AST) products and services are designed to analyze and test applications for security vulnerabilities using static AST (SAST), dynamic AST (DAST) and interactive AST (IAST) technologies.

SAST technology analyzes application source, byte or binary code for security vulnerabilities at the programming and/or testing software life cycle (SLC) phases (see "Hype Cycle for Application Security, 2013").

DAST technology analyzes applications in their running state (in real or "almost" real life) during operation or testing phases. It simulates attacks against a Web application, analyzes application reactions and, thus, determines whether it is vulnerable.

IAST technology combines the strengths of SAST and DAST. It is typically implemented as an agent within the test runtime environment (for example, Java Virtual Machine [JVM] or .NET CLR) that observes possible attacks and is capable of demonstrating a sequence of instructions that leads to an exploit (see "Evolution of Application Security Testing: From Silos to Correlation and Interaction").

AST technology can be delivered as a tool or a cloud service.

AST has been introduced for analysis of Web applications and some legacy applications. AST has also evolved to analyze mobile applications.

For this Magic Quadrant, Gartner has focused on vendors' maturity in offering SAST and DAST features as tools or security as a service for Web applications, and has highly valued vendors' innovation in AST for mobile applications and in IAST.

Magic Quadrant

Figure 1. Magic Quadrant for Application Security Testing

Source: Gartner (July 2014)

Vendor Strengths and Cautions

Acunetix

Acunetix is a Malta-based, privately owned AST vendor focused on DAST. It offers innovative capabilities, such as some IAST functionality aimed at higher accuracy of vulnerability detection; however, it lacks some enterprise-class features, such as integration with some popular integrated development environments (IDEs) and other SLC tools.

Acunetix should be considered by information security specialists and penetration testing professionals that are seeking a reasonably priced DAST offered as a tool or cloud service.

Strengths

- Acunetix offers its DAST technology as a tool (Acunetix Web Vulnerability Scanner) and a cloud service (Acunetix Online Vulnerability Scanner).
- Acunetix offers its AcuSensor IAST technology for PHP and .NET applications. AcuSensor is integrated with its DAST product and focused on higher-accuracy detection and improved reporting of vulnerabilities.
- It offers AcuMonitor cloud service, which interacts with running Acunetix Web Vulnerability Scanners to improve detection of such vulnerabilities as blind cross-site scripting (XSS), email header injection, XML external entity (XXE) and server-side request forgery (SSRF).
- It offers HTML5 and JavaScript testing, as well as testing of applications developed with GWT Web Toolkit.

Cautions

- Acunetix does not offer SAST.
- Its DAST does not support Adobe Flash and Apache Flex testing.
- It does not offer mobile app security testing.
- Acunetix lacks native integration with Microsoft Visual Studio, Eclipse IDE, and Jira and Bugzilla bug tracking systems, although this can be achieved via Acunetix's partnership with Denim Group's ThreadFix product.
- Its DAST is integrated with Imperva's Web application firewall (WAF) only. Otherwise, integration with several other WAFs can be achieved via Acunetix's partnership with Denim Group's ThreadFix product.

Appthority

Appthority is a U.S.-based startup that was founded to provide mobile AST, risk analysis and policy management. It offers a stand-alone portal to upload private or public (third party) apps for analysis,

or to query its database of more than 2.5 million analyzed public mobile apps. This process is fully automated and uses Amazon Web Services (AWS) to achieve the high scalability of its services. Appthority came to the market in early 2012 and has rapidly gained attention. To increase its market presence, Appthority provides technical support in several popular languages; in addition, it has a reseller and technical support network in several countries in Europe and Asia/Pacific.

Appthority's technology is for organizations of any size that are concerned about the security of their own apps or purchased mobile apps, as well as those that are seeking a comprehensive application security analysis, a reputation risk/security rating of mobile apps, and app policy enforcement on mobile devices.

Strengths

- Appthority provides SAST of the disassembled binary code of mobile apps on iOS, Android and BlackBerry devices. Appthority tests native and HTML5 apps.
- It provides behavioral analysis of mobile apps by executing tested apps in the mobile device emulator, and by detecting malicious/risky behavior exhibited in the background, even if that application exhibits manifested benign behavior in the foreground.
- It integrates with mobile device management (MDM) technologies (from AirWatch and MobileIron), enabling protection for mobile devices based on detected application vulnerability analysis.
- It analyzes commercial apps from app stores, provides its proprietary Appthority Trust Score, and allows corporations to build a customized mobile policy by whitelisting or blacklisting application behaviors and taking automated remediation actions.

Cautions

- Appthority does not offer security testing of nonmobile (for example, Web or legacy) applications, and does not test back-end interfaces of mobile apps.
- It does not offer a mobile AST tool, but only a cloud-based testing service or an on-site virtual appliance (in which case a to-be-tested app does not leave an organization's premises).
- Appthority does not offer out-of-the-box integration with application development environments (IDEs) and bug-tracking systems, although it does provide APIs for such integration.
- It does not support Windows Mobile or Windows Phone platforms.

Checkmarx

Checkmarx is an AST vendor based in Israel. Launched as a SAST startup, Checkmarx has significantly improved its marketing and sales force over the past few years (selling its technology in North America, Europe and Asia/Pacific), and earned a strong reputation for the quality of its SAST tools and services.

Checkmarx appeals to application development and security organizations that are seeking a comprehensive SAST tool for a variety of programming languages and frameworks. The SAST tool can test composite applications and provide scalability and quick turnaround times via incremental and parallel tests.

Strengths

- Checkmarx offers one of the strongest SAST technologies, which tests a broad variety of programming languages and is well-integrated into the SLC.
- Checkmarx offers a universal application model that can be queried to discover vulnerabilities, and to check for code adherence to secure programming best practices. The model also enables incremental scans and analysis across components of composite applications that are written in different programming languages and with the use of different frameworks.
- Checkmarx offers SAST as a tool and a cloud service. The vendor is a SAST testing provider that is capable of testing Apex, and is also a major provider of SAST for salesforce.com, its partners and users. In addition, Checkmarx offers support for many cloud platforms and frameworks, such as CloudSpokes, MediaMind and topcoder.
- Checkmarx offers SAST for native Android and iOS mobile apps, and also tests mobile apps with a mobile browser that uses HTML5.

Cautions

- Checkmarx does not offer its own DAST for Web applications, but rather partners for DAST with Cenzic (acquired by Trustwave) and NT OBJECTives.
- It does not offer IAST and runtime application self-protection (RASP), although RASP is currently under development.
- Its SAST integration with Imperva and ModSecurity WAFs is planned for YE14.
- For mobile testing, it provides only SAST; however, it lacks behavioral analysis, testing of communication between mobile side and Web services, and some other features necessary for comprehensive coverage (for example, proactive app testing and risk/security reputation ratings of commercial apps).

Contrast Security

Contrast Security, based in the U.S., is a spinoff of Aspect Security, which moved its technology business to Contrast Security, but kept its application security consulting business. Contrast Security focuses on IAST technology. It aims to bring AST closer to developers and testers and make AST transparent to them, with no need to buy, install and learn security testing tools. This approach aims to reach high scalability by introducing application self-testing. In this case, IAST is instrumented at each test application server. A usual quality assurance (QA) test becomes an inducer for IAST. Recording of possible attack scenarios might serve as an additional inducer. As a

result, each application executed on a test machine automatically undergoes a security test — that is, the security test executes when the application executes.

IAST technology is at the emerging phase of the "Hype Cycle for Application Security, 2013"; therefore, it can be recommended first of all to Type A organizations (early adopters of innovative technologies), and later, when it matures, to Type B organizations (mainstream adopters) and Type C organizations (conservative adopters).

Strengths

- Contrast Security offers a self-testing model, where security testing is driven by a QA test that is executed automatically or manually. This process is transparent to the interested parties (that is, developers and security specialists).
- Use of its technology does not require training. Compared with AST cloud services, Contrast Security does not require submittals of test requests, or waiting for results from AST service providers.
- Its self-testing model is highly scalable.
- It enables nondisruptive analytics of production applications at runtime (if the production server is instrumented).

Cautions

- It is currently limited to test applications written in Java, .NET and ColdFusion.
- It cannot observe and analyze logic executed in the browser only (for example, JavaScript or Java applets). As a result, it will miss attacks such as Document Object Model (DOM) XSS.
- Its tests are driven by QA scenarios, which aim to analyze the usability and quality of an application. However, there is a scope of attacks that QA scenarios would not typically test, such as dedicated attack scenarios developed by hackers. Thus, Contrast Security does not analyze them.
- Contrast Security does not offer integration with WAFs, nor does it partner with WAF vendors.

HP

HP, which is headquartered in the U.S., has a broad portfolio of well-established AST products and cloud services, including DAST and SAST products and cloud services. It also offers a broader set of security technologies that integrates with its AST offerings, including its security information and event management (SIEM) technology, ArcSight and TippingPoint Intrusion Prevention System (IPS).

HP should be considered by organizations seeking AST solutions that are designed to address the needs of larger enterprises — that is, solutions such as SAST and DAST, as well as IAST and RASP products and services within a single enterprise-class console and reporting framework.

Strengths

- HP offers comprehensive SAST capabilities under the Fortify brand name, with one of the broadest lists of tested programming languages. HP's SAST is the most broadly adopted SAST tool in the market.
- HP has evolved its AST to address iOS and Android mobile apps.
- The company has an innovative IAST capability with the Fortify Runtime agent, which integrates with its WebInspect DAST and is bundled with its premium SKU offering. As a result, DAST users can get access to IAST.
- HP is an early innovator with its RASP technology.

Cautions

- HP's mobile AST does not cover all spectrums of features when it comes to behavioral analysis, proactive testing, MDM integration and commercial app reputation ratings.
- While HP integrates with the WAFs from F5 and Imperva (and with TippingPoint's WAF-like IPS capabilities), integration with other WAF tools is not supported.
- The cost of equipping every developer with Fortify's SAST capabilities can be high, if an organization chooses to equip individual developers.

IBM

IBM, a global vendor based in the U.S., has demonstrated its dedication to application security through a number of acquisitions, including DAST and SAST vendor acquisitions. IBM has a large portfolio of security technologies, which, besides application security, include SIEM, identity and access management, data masking, database activity monitoring, endpoint protection, MDM, and Web fraud prevention.

IBM's AST capabilities will appeal to enterprises seeking a variety of enterprise-class technologies in AST, as well as in adjacent security areas.

Strengths

- IBM offers SAST, DAST and IAST technologies. Its IAST for Java and .NET applications is integrated with its DAST offering, thus making IAST available to DAST users.
- IBM offers a choice of DAST as a tool and a cloud service, thus satisfying users' requirements for either or both.
- It offers DAST integration with WAFs for enterprises seeking application security detection as well as protection technologies.
- IBM provides SAST analysis of JavaScript within the context of a DAST scan for testing Web applications that use JavaScript. It also offers innovative taint analysis.

Cautions

- IBM does not offer SAST as a service.
- IBM's IAST works for Java and .NET only.
- IBM's DAST does not support testing of JavaScript Object Notation (JSON) and RESTful applications.
- Its DAST is integrated only with F5 and Imperva WAFs.
- Mobile AST does not include behavioral analysis, commercial application ratings and proactive testing. However, integration with IBM MDM Fiberlink is planned.

N-Stalker

N-Stalker is a privately owned vendor, based in Brazil, with clients worldwide. It has a strong focus on Web AST and appeals to clients that require DAST technology. Its pricing is affordable, and it offers a free, restricted-capability version of its technology. N-Stalker also provides network vulnerability scanning for broader vulnerability management.

N-Stalker should be considered by dedicated security specialists that focus on testing Web applications with DAST technology, and that are seeking competitive pricing. It should also be considered by those seeking regional offerings in Latin America.

Strengths

- N-Stalker offers a user interface (UI), based on HTML5, with native language support for Spanish and Portuguese, which addresses the needs of users who speak those languages.
- N-Stalker offers some enterprise-class console capabilities, including role-based access control (RBAC) and application risk trending. It has out-of-the box integration with WAF vendors/ technologies, such as F5, Imperva and open-source software ModSecurity.
- N-Stalker has expanded into SAST capabilities with PHP, C++ and Java EE; as such, it can help organizations meet the PCI's DAST and SAST requirements.
- N-Stalker is one of the few smaller vendors that offers a DAST-as-a-service option.

Cautions

- N-Stalker offers mobile application testing capabilities that are limited to HTML5 applications or Android applications (with plans to add iOS and Windows 8 by YE14).
- It does not offer behavioral analysis of mobile applications, commercial app ratings, proactive testing and integration with protection technologies (such as MDM).
- N-Stalker does not offer IAST or RASP.
- N-Stalker lacks the name recognition of AST market Leaders and Challengers.

NT OBJECTives

NT OBJECTives (NTO), which is headquartered in the U.S., focuses on DAST solutions offered as products and on testing as a service. It offers several DAST products, including an enterprise-class version with an enterprise-class dashboard, as well as out-of-the-box integration with bug-tracking systems.

NTO should be considered by enterprises seeking an easy-to-use, full-featured DAST that is competitively priced as an alternative to the larger players' AST technologies.

Strengths

- NTO offers enterprise-class DAST, which includes broad, out-of-the-box bug-tracking system integration, and a solid enterprise console with active reporting capabilities (including a user-adjustable vulnerability risk rating).
- For testing of Web services and the back end of mobile-enabled applications, its "universal translator" technology enables the testing of various types of exposed back-end interfaces, such as JSON, REST, SOAP, XML-RPC, GWT-RPC and Action Message Format (AMF).
- NTO's vulnerability reports are "live" so that recipients can reproduce vulnerabilities directly from the reports (a small attack applet re-creates the vulnerability in real time), thereby providing direct feedback to developers and reducing the number of full NTO licenses required for users.
- The company offers extensive WAF integration via its NTODefend offering.
- NTO's DAST as a service includes human augmentation for vulnerability validation as a standard feature.

Cautions

- NTO offers a Win32 stand-alone and a Web-based enterprise testing interface, although the Web interface does not yet offer as granular control of the settings and options for testing as the full Win32 interface does. On 26 May 2014, NTO announced a new release of NTOEnterprise with full support of these features by its Web interface. We recommend that our clients evaluate it.
- NTO offers no SAST or IAST capabilities.
- Its planned partnership with SAST vendor Checkmarx did not materialize. NTO has an evolving partnership with Coverity (a code analysis vendor). This partnership provides correlation of results from NTO's and Coverity's tools, and is planned to provide a line-of-code level of vulnerability details.
- It does not offer out-of-the-box integration with IDEs.

PortSwigger

U.K.-based PortSwigger is a privately owned vendor of Burp Suite DAST tools. PortSwigger offers free editions of Burp Suite and Burp Suite Professional edition; the latter targets advanced testers and is aggressively priced at approximately $300 per user per year. Burp Suite Professional offers advanced testing capabilities for the security professional, but lacks the enterprise features of larger providers (for example, SLC integration or RBAC console access and reporting). The community of Burp users has developed a number of useful extensions/additions to Burp (such as SAML Editor, WSDL Wizard and Payload Parser) that are available to Burp users.

Burp Suite Professional should be considered by organizations seeking a powerful DAST tool at an extremely competitive price.

Strengths

- PortSwigger's Burp Suite is one of the most widely adopted DAST tools in the DAST market. It offers a proxy for the real-time capture of Web interactions, including back-end interfaces for dynamic testing. This technology is highly popular, and other vendors — even some of PortSwigger's competitors — support the use of Burp Suite's proxy recorders.
- PortSwigger's products are highly customizable and extensible and can be API-driven, which increases the use cases for Burp Suite's implementation.
- Burp Suite supports HTML5 testing.
- Burp Suite enables the parallel testing of components of complex and large Web applications.

Cautions

- PortSwigger does not offer SAST and IAST technologies, nor does it offer correlation between its DAST and other vendors' SAST tools.
- PortSwigger does not offer mobile applications code analysis, behavioral analysis, integration with MDM and commercial apps reputation ratings, although some organizations and vendors use its DAST tool's proxy to analyze traffic between Web services and mobile apps.
- PortSwigger does not offer its DAST as a cloud service.
- PortSwigger does not offer integration with WAFs, IDEs, QA and bug-tracking systems.

Pradeo

Pradeo is a privately held company based in France. It is a startup founded for the purpose of developing and providing mobile AST services. Its technology is delivered as three components: (1) AuditMyApps, a platform for app security testing; (2) CheckMyApps, a platform for mobile applications' security policy management; and (3) CheckMyApps API, a set of APIs.

Pradeo's technology is for organizations looking to conduct comprehensive code and behavioral analysis of their mobile applications; however, the vendor's small size and insufficient marketing efforts make its technology poorly visible to interested prospects, especially those outside France.

Strengths

- Pradeo offers AST as a service for iOS, Android and Windows 8 platforms (with Windows Phone in beta testing).
- It offers its technology as a cloud service or as an on-premises virtual appliance.
- It offers static code analysis (reverse-engineered byte/binary code analysis) and behavioral analysis of mobile applications.
- Pradeo offers its own MDM agent, which can act on results from AST.

Cautions

- Pradeo does not offer AST for Web and legacy applications.
- Pradeo technology is available only as a service.
- It does not offer integration with MDM vendors' technologies.
- Pradeo's low visibility inhibits its appearance on customers' shortlists outside France; however, it is working on plans to expand its market presence.

Qualys

Qualys, which is based in the U.S., provides a number of cloud-based security services, including DAST as a service (introduced in 2011). In 2014, it has begun expanding into WAF as a service, using its cloud-based security service platform architecture. Qualys targets the lower-end, price-sensitive sector of the market with fully automated DAST service. It uses integrated Selenium support for the automation of authentication and navigation.

Qualys should be considered by organizations seeking fully automated, low-cost DAST-as-a-service capabilities provided by an easy-to-use management console and interface. Qualys' DAST offering is often combined with other types of managed security services (such as vulnerability scanning).

Strengths

- Qualys is one of the most broadly adopted DAST services in the DAST market.
- Its straightforward console — combined with granular RBAC and a flexible, logical tagging architecture — permits users to customize reports to their organizations' needs.
- Qualys offers aggressive list pricing at $495 per application per year, and customers report high levels of discounting.
- Qualys has demonstrated consistent, solid, double-digit year-over-year growth in its DAST-as-a-service offering for the past three years.
- An integrated, "continuous" malware detection service and Web application discovery capabilities are included as a standard part of its DAST service.

Cautions

- Qualys' offering is provided as a service only; there is no product option (although its offering uses an on-premises footprint for network connectivity and for reducing bandwidth requirements).
- Although Qualys offers WAF integration with F5, Citrix and Imperva, its own WAF offering is not yet integrated into its Web application testing results for automated correlation.
- It has no mobile AST capabilities.
- It has no SAST or IAST. It does not have integration with IDEs or bug-tracking systems. Its JSON and REST support is planned for YE14.
- A fully automated test has limits on the vulnerabilities it can find, but this can be mitigated by human augmentation. Qualys offers no human augmentation of its testing results or business logic testing. In 2013, Qualys partnered with iViZ Security to fulfill this customer need.

Quotium

Headquartered in France, Quotium is a point solution vendor of an IAST product called Seeker. Quotium is still relatively unknown in the U.S., but it is gaining traction because of the effectiveness of its IAST technology.

Quotium should be considered by security and application development professionals who are seeking a way to embed AST into the SLC with a tool that provides efficient and effective vulnerability detection, and that is reasonably easy to adopt.

Strengths

- Quotium pioneered IAST with many innovative capabilities, including security analysis of stored procedures and database transactions; analysis of code and data at runtime (to better understand vulnerability context and actual risk); and JavaScript analysis. Seeker is one of the most broadly adopted IAST technologies in the IAST market.
- The high-accuracy results and straightforward UI of Seeker make it reasonably easy to embed in the development process, primarily in the testing phase (because it requires a running application for its instrumentation). Seeker's Selenium support, quick and accurate results, and out-of-the-box integration with build servers and bug-tracking solutions fit well into agile and DevOps approaches.
- Quotium offers broad IAST support: IAST for Java, .NET and PHP application server platforms, as well as support for PL/SQL and T-SQL.
- IAST agents can be installed on multiple servers that execute a distributed application, enabling the detection of vulnerabilities that are spread across multiple application components. Seeker also enables the analysis of applications that do not have UIs.

Cautions

- Quotium lacks the brand-name recognition of the AST market Leaders, and its market presence is stronger in EMEA than in North America.
- Quotium focuses exclusively on IAST as a product, and does not offer IAST as a service.
- Seeker is not designed for use in a production environment, and it requires instrumentation of the test runtime environment (such as JVM or .NET CLR).
- Quotium does not offer mobile application testing. However, Quotium's Seeker can observe and learn how the mobile application interacts with the back-end servers (for servers that Seeker supports), and it can test these back-end servers.

Trend Micro

In 2012, Trend Micro acquired the technology assets and engineering staff of Indusface, an India-based DAST-as-a-service provider (its DAST testing service is called IndusGuard, and Indusface continues its operations as a licensed reseller of the Trend Micro DAST service). Trend Micro's DAST service has been moved under its Deep Security brand and is called Trend Micro Deep Security for Web Apps.

Enterprises should consider the Trend Micro solution as a cost-competitive alternative to other human-augmented DAST-as-a-service solutions, especially if those enterprises are existing Trend Micro customers.

Strengths

- Trend Micro offers a worldwide sales force and data center presence, as well as tight integration with its Deep Security platform for OS, application and platform vulnerability protection.
- The DAST service offering includes application and platform vulnerability scanning with an integrated console, as well as integration with the following WAFs: Citrix, Imperva, Alert Logic and ModSecurity.
- The Trend Micro offering includes a human-augmented review of the results for improved accuracy.
- Trend Micro offers low-cost Secure Sockets Layer (SSL) certificates (from its acquisition of AffirmTrust) as a bundled part of its DAST offering, thus adding to its ROI. Some customers report that the savings in SSL certificates alone pays for the DAST service.

Cautions

- Trend Micro is not known for application security, and before the technology acquisition, Indusface had a limited market presence outside India, Asia/Pacific and the Middle East.
- The Trend Micro offering has no SAST or IAST capabilities.

- It has no mobile AST capabilities, although it offers a mobile application reputation service as part of the enterprise package of Deep Security for Web Apps.
- The Trend Micro offering is cloud-only. No on-premises tool is offered.
- The basic console interface supports RBAC, but does not provide a separate view that is applicable to developers. For example, there is no specific developer interface, advanced remediation advice or integration with bug-tracking systems.

Trustwave

Based in the U.S., Trustwave provides a broad range of information security technologies, many of which were gained through acquisitions — for example, secure Web and email gateways, data loss prevention (DLP), database audit and protection, encryption, and, most recently, DAST (through Trustwave's 2014 acquisition of Cenzic). Trustwave focuses on a range of DAST products and services — for example, from AST for small or midsize businesses (SMBs) to AST for large enterprises; and from third-party automated application testing platforms to pen testing use cases.

Trustwave should be considered by organizations seeking enterprise-class DAST capabilities as well as good customer service and support — and especially by those looking to meet PCI requirements, because Trustwave has a full set of products and services (including DAST) for achieving PCI compliance.

Strengths

- Trustwave offers DAST as well as pen testing services from its SpiderLabs.
- Trustwave (Cenzic) offers a broad array of DAST products and services with a competitive pricing model for large enterprises, as well as specific offerings targeting SMBs.
- Trustwave has enterprise capabilities, including a console with granular RBAC, the ability to consolidate results across multiple testers, and its own Hailstorm Application Risk Metric (HARM) system for the measurement and baselining of application risk (built on a common platform for Trustwave's products and testing services).
- Trustwave provides integration with WAFs — for example, Trustwave Web Application Firewall, as well as with Barracuda, Citrix, F5, Imperva and ModSecurity. It is one of the few vendors that offers bidirectional WAF integration with DAST.

Cautions

- Trustwave does not have its own SAST. It is currently provided through the partnership with Checkmarx.
- Trustwave does not offer IAST or RASP.
- Trustwave does not have a mobile AST product; rather, it has only a cloud-managed service for testing mobile applications. It also does not provide commercial mobile apps risk/reputation ratings and proactive testing.

- Trustwave's acquisition of Cenzic was announced at the end of 1Q14, and it will take time to evaluate how successful this integration of two vendors will be.

Veracode

Veracode is a well-established provider of AST cloud services, and is one of the pioneers of testing as a service. It has also pioneered the testing of native binary application code, as well as the testing of the software supply chain with its Vendor Application Security Testing (VAST) program.

Veracode technology will meet the requirements of organizations that want to delegate their AST to a third-party expert with a strong reputation for the quality of its services in the Web and mobile AST spaces.

Strengths

- Veracode offers SAST and DAST. Results of both types of testing can be integrated into a single dashboard to simplify vulnerability management and remediation.
- Veracode offers scalable AST as a service and tests tens of thousands of applications per year. Its DynamicMP service — a high-volume, fully automated service — is capable of testing thousands of production websites in a matter of days (although it is not as deep as another Veracode service, DynamicDS, which is intended for testing during the development phase of the SLC).
- Veracode offers comprehensive mobile AST as a cloud service, which includes static byte and binary code analysis as well as behavioral analysis in the mobile device emulator, or in a physical device. It also offers a Mobile Application Reputation Service (MARS) for commercial application risk/security ratings for the most frequently downloaded apps from app stores. Veracode mobile testing supports iOS, Android, BlackBerry and Windows Mobile platforms.
- Veracode is pioneering work on integrating WAF detection results into DAST to increase the accuracy of DAST.
- Veracode offers APIs for integrating its cloud-based services with multiple IDEs, code management and bug-tracking tools, and build servers, thus making AST more seamless, expedient, and better integrated with agile SLC processes.

Cautions

- Veracode does not offer AST tools, but only AST as a service.
- Veracode does not offer IAST for Web application testing. It also does not offer RASP.
- Veracode's DAST technology has not yet earned a reputation that is comparable with its SAST reputation.
- Veracode does not offer mobile testing as a tool or virtual appliance, but only as a cloud service.

- Veracode's WAF integration is limited only to Imperva and ModSecurity.

Virtual Forge

Based in Germany, Virtual Forge is the vendor of a SAST tool, CodeProfiler, which is focused exclusively on the static testing of SAP's Advanced Business Application Programming (ABAP) applications. Virtual Forge was the first vendor to support ABAP testing with specific, deep expertise, and CodeProfiler is one of the few SAST tools available that does it. Virtual Forge should be considered by organizations that have custom ABAP applications and extensions that they wish to test for security vulnerabilities, even if they use other vendors' AST solutions to test other platforms and languages.

Strengths

- With speed and scale, Virtual Forge scans ABAP code for security and quality issues, as well as back-door issues. It can also scan the SAP platform for known, but unpatched, vulnerabilities.
- Virtual Forge offers an automated code correction feature for detected vulnerabilities. Also, its CodeProfiler for Eclipse checks ABAP code in real time, raises warnings and offers fixes interactively, while the programmer writes the code.
- Virtual Forge partners with IBM, which resells Virtual Forge (IBM's own SAST capabilities don't cover ABAP). This is an acknowledgment of Virtual Forge's value in SAP testing.
- Virtual Forge provides innovative, patent-pending, static DLP capabilities in which the customers identify the critical SAP tables and Virtual Forge identifies which programs access this data.

Cautions

- Virtual Forge conducts SAST for SAP systems only and does not support Java testing, even though Java is used within many SAP architectures. Java support can be gained through Virtual Forge's partnership with IBM, or through the use of independent AST vendors that support Java SAST.
- Virtual Forge's UI is complex, although tightly integrated with the SAP graphical user interface within the SAP development workbench. Virtual Forge's UI will be familiar to experienced SAP developers and administrators, but harder for non-SAP users.
- Virtual Forge offers its technology as a product and a service, although the service offering has a much lower adoption than the tool offering.
- It does not have DAST, IAST or mobile AST capabilities; however, DAST functionality is in development.

WhiteHat Security

WhiteHat Security, which is headquartered in the U.S., is a pioneer in AST-as-a-service business model. It has been an established security-as-a-service provider of DAST that, in 2012, also

expanded into SAST. It offers multiple levels of DAST and SAST services with integrated management and reporting.

WhiteHat Security should be considered by organizations looking to delegate their DAST and (to a lesser degree) SAST to an expert third-party testing service provider. Those organizations may also benefit from WhiteHat Security's offering, from which all DAST and SAST services include a human-augmented review of the results to improve the accuracy of the tests.

Strengths

- WhiteHat Security offers SAST and DAST technologies.
- It offers SAST and DAST as a service — as a cloud service or an on-premises appliance.
- It offers correlation between SAST and DAST: SAST discoveries can be submitted for DAST execution to confirm or disprove suspected vulnerabilities.
- WhiteHat Security offers integration between its DAST and the following WAFs: F5, Imperva, Riverbed and Akamai.
- For mobile, it offers testing of communications between app and Web services (often done with PortSwigger's Burp), and it can do source code analysis for Objective-C and Android Java.

Cautions

- WhiteHat Security provides SAST for a limited number of programming languages: Java, C# and PHP. Its SAST has the lowest adoption among SAST vendors.
- For mobile testing, WhiteHat Security does not offer automated behavioral testing (although it can do this manually via third-party consultants). WhiteHat Security also does not offer reputation service, proactive testing and integration with MDM.
- WhiteHat Security does not offer IAST and RASP.
- WhiteHat Security does not sell DAST and SAST tools, but rather testing services only.

Vendors Added and 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's appearance 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. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

- Appthority was added for its offering of AST for mobile applications.

- Contrast Security, a spinoff of last year's Magic Quadrant player Aspect Security, was added for its offering of IAST.
- Pradeo was added for its offering of AST for mobile applications.
- Trustwave was added because it has acquired Cenzic, a player from last year's "Magic Quadrant for Application Security Testing."

Dropped

- Armorize Technologies was dropped because it has been acquired by Proofpoint, a vendor that focuses not on AST, but rather on Armorize's other technologies.
- Aspect Security was dropped because it has spun off Contrast Security as an IAST technology vendor.
- Cenzic was dropped because it has been acquired by Trustwave, which intends to strengthen its AST line of business.

Inclusion and Exclusion Criteria

We included the following in this Magic Quadrant:

- Vendors that provide dedicated SAST, DAST or IAST technology — that is, a tool, subscription service or both.
- Vendors whose technologies (tools or services) are their own.
- Vendors whose products and/or services were generally available (not in beta) before 31 December 2013.
- Vendors that have at least $5 million in specific revenue from AST products and/or services.
- Vendors that have deployments in at least 20 customer production environments, with at least seven contactable references that could be surveyed.
- Vendors that are focused on application security, address it along various SLC phases, and address the needs of security specialists, as well as application development and testing specialists.
- Vendors that Gartner determines to be significant players in the market, because of their market presence or technology innovation:
    - These technology-innovating vendors should have at least $1 million in specific revenue from AST products and/or services, or have at least 20 customers with at least seven contactable references that could be surveyed.

We did not include the following in this Magic Quadrant:

- Vendors that provide services, but not on a repeatable, predefined subscription basis — for example, providers of custom consulting application testing services, contract pen testing, professional services and other nonsubscription services.
- Vendors that provide network vulnerability scanning, but do not offer a separately purchasable AST capability, or vendors that offer only some Web-application-layer dynamic scanning.
- Vendors that offer only penetration testing products and services.
- Vendors that offer network protocol testing and fuzzing solutions.
- Consultancies that offer AST services.
- Vendors that are focused on application code quality and integrity testing solutions, which have some limited AST capabilities.
- Vendors with narrow, specific expertise and/or regional reach.
- Open-source offerings, because they do not offer enterprise-class capabilities and security-as-a-service delivery.

Evaluation Criteria

Ability to Execute

Product or Service: This criterion evaluates the vendor's core AST products and services. It includes current product/service capabilities, quality and feature sets. We give higher ratings for proven performance in competitive assessments. We also give higher ratings to vendors that appeal to a breadth of users (such as information security specialists as well as development and QA/testing specialists), and that appeal with AST products and AST testing services.

Overall Viability (Business Unit, Financial, Strategy and Organization): This is an assessment of the organization or business unit's overall financial health, the vendor's focus on AST, and the likelihood that the company will decide to continue investing in the AST market. We also evaluate a vendor's estimated AST market share, AST revenue amount, the number of AST customers, the number of installed AST tools, AST expertise and overall mind share, including the number of times the vendor appears on Gartner clients' shortlists.

Sales Execution/Pricing: We account for the 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 those activities. This includes customer feedback on deal management, pricing and negotiation, and presales support, as well as the overall effectiveness of and customer receptiveness toward the sales and partner channels worldwide.

Market Responsiveness/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 broader application security capabilities with enterprises' functional requirements, and the vendor's track record in delivering innovative features when the market demands them. We also account for vendors' appeal with security technologies other than AST.

Customer Experience: This is an evaluation of the solution'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 or Service	High
Overall Viability	High
Sales Execution/Pricing	Medium
Market Responsiveness/Record	High
Marketing Execution	Not Rated
Customer Experience	Medium
Operations	Not Rated

Source: Gartner (July 2014)

Completeness of Vision

Market Understanding: We evaluate the vendor's ability to understand buyers' needs and translate them into products and services. AST vendors demonstrating the highest degree of market understanding have responded to emerging customer requirements in areas such as providing comprehensive DAST, SAST and IAST capabilities. Higher ratings are given to techniques and approaches that are proven to improve accuracy. The ability to test highly complex JavaScript applications, HTML5 applications, and mobile and cloud applications is highly rated. We evaluate the ease of an AST solution's native integration with multiple popular IDEs, source code management systems, and bug-tracking and QA systems. The enterprise console is an important element in providing enterprisewide consolidation, analysis, reporting and rule management across a number of installed scanners; user-friendliness; and the ease of identifying and enabling customers to focus on the most severe and high-confidence vulnerabilities. We give higher ratings

to the vendor's ability to provide AST product options and testing as a service with unified visibility and reporting across both.

Sales Strategy: Here, we assess the vendor's worldwide sales presence, channels and partners to target a worldwide installed base, including local sales offices to support regional sales efforts. We also include marketing and market awareness strategies as part of this category.

Offering (Product) Strategy: We assess the vendor's approach to product development and delivery. This addresses the vendor's focus on AST for Web and mobile platforms with tools and services.

We consider the optimal balance to satisfy the needs of Type A (leading-edge), Type B (mainstream) and Type C (risk-averse) enterprises, and the needs of typical enterprises and specialized clients. We give higher scores to the vendors that offer a variety of solutions to meet different customer requirements and testing program maturity levels.

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 that are evolving toward the vision of enterprise security intelligence with DAST/SAST interaction, integration and correlation (including offering IAST), 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 to make security testing more accurate (for example, decreasing false-positive and false-negative rates). In addition, we give higher ratings to vendors' ability to innovate in mobile AST; to provide static, dynamic and behavioral testing; and to provide security/risk reputation scoring of commercial mobile applications, and integration with protection (for example, MDM) technologies. Other areas of innovation include application protection features (for example, RASP); out-of-the-box integration with application protection mechanisms, such as WAFs and IPSs; integration with governance, risk and compliance (GRC) and SIEM technologies; offering software composition analysis; innovative ways of delivery (for example, security testing as a service); support for DAST testing of SOAP and RESTful HTTP applications and cloud services; testing of and integration with cloud applications and platforms (such as salesforce.com, Rackspace and Amazon); and AST for modern rich Internet applications (RIAs).

AST solutions should provide a variety of options for testing — for example, stand-alone engines for security professionals, integration into development tools for developers, and integration into QA for QA testers. The AST solution should provide the options to submit jobs to on-premises testing engines and to a testing service provider, while also providing a unified view and reporting across all these testing options.

Geographic Strategy: Here, we evaluate the worldwide availability of and support for the offering, including local language support for tools, consoles and customer service. Ideally, the vendor would provide worldwide availability, with local language and local service and support options (see Table 2).

Table 2. Completeness of Vision Evaluation Criteria

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

Source: Gartner (July 2014)

Quadrant Descriptions

Leaders

Leaders in the AST market demonstrate breadth and depth of AST products and services. Leaders should provide mature, reputable SAST, DAST and, desirably, IAST techniques in their solutions. Leaders also should provide organizations with AST-as-a-service delivery models for testing, or with a choice of a tool and AST as a service, using a single management console and an enterprise-class reporting framework supporting multiple users, groups and roles. In addition, Leaders should provide capabilities for testing mobile applications.

Challengers

Challengers in this Magic Quadrant are vendors that have executed consistently, typically by focusing on a single technology (for example, SAST or DAST). In addition, they have demonstrated substantial competitive capabilities against the Leaders in this particular focus area, and also have demonstrated momentum in their customer base in terms of overall size and growth.

Visionaries

Visionaries in this Magic Quadrant are vendors that are advancing the emerging areas of IAST and mobile AST. The goal of IAST is fast and accurate security testing that is suitable for use in development, where minimal security expertise is present and accurate results are needed quickly (for example, to support agile development and DevOps development models). Mobile testing is a set of existing and new technologies and methods for ensuring the security of mobile applications.

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, on specific vendor expertise, or when they have an established relationship with the vendor. Niche Players typically focus on a specific type of AST technology or delivery model, or on a specific geographic region.

Context

Cyberattacks have changed from noisy, mass attacks aimed at "freezing" large numbers of computers to targeted and financially motivated attacks. These have included SQL injection, cross-site request forgery (XSRF) and XSS, which are focused on manipulating applications and stealing or tampering with sensitive data. Hackers easily gain access to open-source technologies that enable remote application inspection and probing. New application delivery models and platforms (such as cloud and mobile) and technologies (such as RIAs) pose new security risks, because application security technologies and processes have not been developed or matured for them.

Enterprises are increasingly understanding the necessity to implement application security disciplines. Today's application security markets offer a variety of reasonably mature technologies, and demonstrate innovations that are capable of deterring new threats brought to life by new social and business phenomena, such as cloud and mobile.

Market Overview

DAST and then SAST technologies emerged in early 2000 as two isolated silos. They gained initial adoption in the 2004 to 2006 time frame. At that time, SAST vendors and DAST vendors were adamant in their rejection of the value of the other technology, insisting that DAST (or SAST) alone was sufficient to ensure accurate and comprehensive security testing. In Gartner's 2006 research, "Key Technology Trends in Application Security Testing Markets" and "MarketScope for Web Application Security Vulnerability Scanners, 2006" (Note: These documents have been archived; some of their content may not reflect current conditions), we stated that the future of AST was in using SAST *and* DAST. Since that time, leading AST vendors have adopted Gartner's vision, and have evolved isolated technology silos that featured combined, then correlated, and now interactive solutions.

Vendors have been evolving these technologies, addressing such client needs as user-friendly interfaces, integration with nonsecurity systems (such as application development and testing), integration between security technologies (for example, SAST and DAST), analytics and reporting, and compliance and governance. They have also been building integration capabilities with protection technologies, specifically with WAFs or MDM (for mobile platforms).

To make adoption even easier and broader, many vendors now offer cloud-based security as a service. As a result, these technologies have reached the point where cost and risk of adoption are well-balanced.

Market innovation continues, and we have witnessed the emergence of such technologies as IAST (which promises a significant increase in the accuracy and breadth of vulnerability detection) and RASP (which is capable of detecting and preventing real-time attacks). We have witnessed startups and established vendors innovating in the mobile applications security space. Today's market is filled with numerous vendors, ranging from innovative startups to established large companies, that offer a variety of technologies.

AST Technologies

At a high level, AST capabilities fall into three broad categories — SAST, DAST and IAST:

- SAST technology analyzes applications for security vulnerabilities at programming and/or testing SLC phases. SAST technology's advantages include the following: (1) Vulnerability analysis starts early in the SLC, thus making remediation inexpensive; and (2) SAST determines the exact address of the detected (or, rather, a suspected) vulnerability because it analyzes applications' source code, or byte or binary code. However, at the same time, SAST technology has a serious weakness/limitation: It does not analyze a real application, but rather the code, which can lead to high false-positive rates. A detected vulnerability may never be executed (to say nothing of being exploited) in the application's "real" life, during the operation phase of the SLC.
- DAST technology analyzes applications in real or "almost" real life — that is, during operation or testing phases, which is an important advantage. DAST can often accurately identify the exploitability of the potential vulnerabilities it finds, because it analyzes application responses to the dynamic tests. However, even when a vulnerability is detected, DAST technology cannot point to the line of code where it originates, because DAST is a "black box" technology that does not have access to source code.
- IAST conducts behavioral analysis of applications, and observes applications' input and output, application logic execution, execution of libraries, and data flow. An inducer feature executes test/attack scenarios as inputs for vulnerability testing. An agent residing inside an application server conducts runtime analysis of the application code, memory and data flow. As a result, with increased accuracy, IAST determines whether a vulnerability is exploitable and where it is located in the code (see "Evolution of Application Security Testing: From Silos to Correlation and Interaction").

AST Delivery Models

AST technologies can be delivered as tools or security as a service (a delivery model in which application security is delegated to third-party professional security providers that conduct their services remotely, typically via the Internet). Most application security vendors have begun to deliver their capabilities as a service, and offer these alongside their application security products. Some vendors have exclusively focused on security as a service and do not offer products at all.

Many organizations will use a combination of on-premises tools and application security as a service. In many cases, security as a service's benefits outweigh the challenges it is facing, and it will mature during the next five years. Maturity of the service differs for different technologies. For example, DAST services are more mature, while SAST services are less mature, because they often require uploading of the application's code into the service provider's site — a requirement that complicates clients' willingness to adopt SAST services. We have also witnessed IAST delivered via security-as-a-service model.

AST and WAF Integration

Application security detection and protection technologies have inherent limitations that impact their accuracy and risk assurance capabilities. These limitations could be substantially mitigated if detection and protection interacted and/or shared knowledge.

The accuracy of a WAF increases when DAST (or, in some cases, IAST or SAST) passes detected security vulnerabilities and attack patterns to it, so that the WAF can terminate sessions that match malicious patterns. Even if the WAF, in its log or alert mode, has identified a suspicious traffic pattern, the correlation with DAST analysis results provides greater confidence that the pattern can be safely used in WAF protection mode. Detected mismatches between discoveries made by a WAF and DAST should be forwarded to DAST for further analysis (see "Application Security Detection and Protection Must Interact and Share Knowledge").

The other way around — when a WAF provides input for DAST — is also beneficial. Here, a WAF becomes an integral part of the AST conducted by DAST. There are challenging test cases, which DAST has difficulty overcoming due to its conceptual constraints. These cases are pervasive, and inaccuracies in their analyses carry high-risk consequences. A WAF can help by sharing the results of its analyses with DAST. A WAF has a great deal of information about the size, boundaries and content of the Web application it is monitoring. For example, a WAF can provide lists of reachable URLs and "real" parameters from its logs. DAST could use this for its crawler, or to infer proper page flow and fuzzing parameters. This information should be passed from the WAF to DAST, and then be compared with DAST analyses. If the analyses do not match, then DAST test scenarios should be expanded based on the information received from the WAF. Using a WAF as part of the DAST process also enables better prioritization of DAST scans. A WAF can provide such information as the frequency of which content is requested, as well as which parts of the application/website are the most popular — and, therefore, might be more important to test than others (see "Application Security Detection and Protection Must Interact and Share Knowledge").

AST and RASP

Recently, some vendors have been working on a new technology — RASP — to offer an enhanced way to protect applications (see "Runtime Application Self-Protection: A Must-Have, Emerging Security Technology"). RASP is an emerging technology that "instruments" the application runtime environment. In other words, it extends the functionality by additional functionality — namely, security detection and protection. Thus, becoming an integral part of an application runtime environment (for example, JVM), RASP monitors the execution of an application by the application runtime environment, gets controls when specified security conditions are met, and takes the

necessary protection measures. Those conditions could be an execution of instructions that access a database (which might cause an SQL injection exploit). Actions taken could include the following, for example: user session termination, application termination (without bringing down other applications on the server), an alert sent to security personnel or a warning sent to the user.

AST for Mobile Platforms

Mobile AST aims to analyze applications for coding, design, packaging and deployment conditions that are indicative of security vulnerabilities. Testing can also point to application functions that conflict with an enterprise's security policies (for example, testing can raise warnings that an application accesses the corporate calendar or contact list, or transmits corporate information to external locations). The following actions should be performed:

- Tests should include: (1) code; (2) UI; and (3) behavioral analyses.
- Two layers of the mobile application should be tested: (1) the mobile client side; and (2) the server side.
- Enterprises can choose from two testing delivery models, or combine them. They can: (1) Acquire testing tools to conduct their own tests; and/or (2) procure testing as a cloud service from specialized vendors.
- When an enterprise plans to use third-party applications that it cannot test on its own, it should consider the security/risk reputation score of the tests conducted by independent, reputable security testing vendors.
- Technology must automatically ensure that all applications on the mobile device have been detected and submitted for tests.
- Mobile AST should enable integration of its results with mobile protection technologies — for example, with MDM (see "Technology Overview: Mobile Application Security Testing for BYOD Strategies").

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Magic Quadrant for Application Security Testing"

"Hype Cycle for Application Security, 2013"

"Technology Overview: Mobile Application Security Testing for BYOD Strategies"

"Evolution of Application Security Testing: From Silos to Correlation and Interaction"

"Application Security Detection and Protection Must Interact and Share Knowledge"

"Application Security Testing of Cloud Services Providers Is a Must"

"Cost-Saving Tips for Acquisition and Implementation of Application Security Technologies"

"How Gartner Evaluates Vendors and Markets in Magic Quadrants and MarketScopes"

Evidence

Gartner used the following input in developing this Magic Quadrant:

- Analysis of approximately 300 inquiries that we received during the past year
- Vendors' responses to our detailed Magic Quadrant survey
- Survey of approximately 100 enterprises that used AST technologies and services

Evaluation Criteria Definitions

Ability to Execute

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

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways

customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp