Magic Quadrant for Application Security Testing

2 July 2013 ID:G00246914

Analyst(s): Neil MacDonald, Joseph Feiman

VIEW SUMMARY

The market for application security testing is changing rapidly. Technology trends, such as mobile applications, advanced Web applications and dynamic languages, are forcing the need to combine dynamic and static testing capabilities, which is reshaping the overall market.

Market Definition/Description

Application security testing (AST) products and services are designed to analyze and test applications for security vulnerabilities using static, dynamic and interactive testing techniques. Historically, the market evolved separately to address each of these techniques. Most initial solutions focused on testing applications in a running state, using dynamic application security testing (DAST) techniques to look for application behavior indicative of a security vulnerability. DAST is well-suited for use by security professionals outside of development who lack access to source code. Other solutions focused on static application security testing (SAST) techniques by analyzing an application's source code, bytecode or binaries for coding, and data flow conditions indicative of security vulnerabilities. SAST solutions were typically applied during the development process, and are less widely adopted than DAST. However, testing next-generation modern Web and mobile applications requires a combination of SAST and DAST techniques, and new interactive application security testing (IAST) approaches have emerged that combine static and dynamic techniques to improve testing. Options for delivery of testing as a service have become a necessary requirement for most organizations. Further, integration with adjacent market segments, such as Web application firewalls (WAFs), development environments, and security information and event management (SIEM) systems, has become a critical capability. As a result, the market has evolved, consolidated and converged. While smaller point solutions continue to be offered that focus on a single approach, larger providers offer multiple testing techniques and delivery models (products and testing as a service) so that an enterprise can pick and choose the approaches that make sense for its application and technology portfolio (see Figure 1).

Return to Top

Magic Quadrant

Figure 1. Magic Quadrant for Application Security Testing

EVIDENCE

[1] HTML5 is often referred to as if it is a single standard. In reality, there are many different emerging standards for building modern Web applications that are evolving at different rates and are at different maturity levels that are lumped together under the term "HTML5" (see www.w3.org/html/wg/drafts/html/master). Vendors that use embedded attack engines based on an open standard rendering engine are best positioned to keep pace with this rapidly evolving standard (see "HTML5 to Take on New Role in Mobile App Development").

[2] See http://phonegap.com.

[3] The REST architectural style describes six constraints. These constraints, applied to the architecture, were originally communicated by Roy Thomas Fielding in his doctoral dissertation, and define the basis of RESTful style.

[4] For more on Web application firewalls and DAST integration, see http://blog.spiderlabs.com/2012/06/dynamic-dastwaf-integration-realtime-virtual-patching.html.

NOTE 1
ALTERNATIVE SOLUTIONS

Alternative solutions not included in this Magic Quadrant:

Dognaedis is a smaller SAST testing product and services provider based in Portugal with a presence in EMEA. Dognaedis focuses on PHP and Java, with tight integration into Eclipse. It has a straightforward three-tier RBAC console and an aggressive pricing model.
iViZ Security is a lesser-known DAST-as-a-service provider with offices in India and the U.S. All of its services offer human-based review of the results to reduce false positives The company offers a competitively priced alternative to other DAST-as-a-service providers. A recent partnership with Qualys should increase the exposure of iViZ.
Mavituna Security is a DAST point solution vendor based in the U.K. whose offering, Netsparker, is designed for use by an individual professional security tester.

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, 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 (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

Source: Gartner (July 2013)

Return to Top

Vendor Strengths and Cautions

Acunetix

Acunetix is a privately held company based in Malta with a strong focus on DAST tools. It offers a point solution — Acunetix Web Vulnerability Scanner — and associated tools specifically designed for Web application testing. Acunetix should be considered by information security specialists and penetration testing professionals looking for a reasonably priced, commercially supported Web application security testing tool with supporting tools and compliance reporting capabilities.

Strengths

To complement its core DAST capabilities, Acunetix offers a variation of IAST technology that takes a leading-edge approach.

Its technology is well-suited for penetration testing specialists.

The company offers reasonable pricing and a straightforward pricing model.

Customers surveyed rated Acunetix highly for its accuracy and pricing model.

Cautions

Acunetix does not provide DAST testing as a service, nor does it offer SAST capabilities.

Its IAST works with PHP and .NET, but not with Java applications.

Acunetix offers explicit integration with only Imperva's SecureSphere Web Application Firewall.

The company provides limited HTML5[1] support, and does not offer a solution for testing mobile applications.

Return to Top

Armorize Technologies

Armorize Technologies, based in Santa Clara, California, provides a dedicated point solution, CodeSecure, which is a static application security testing approach focused on testing PHP, ASP, ASP.NET, VB.NET, C# and Java-based Web applications. Armorize is widely known in the Asia/Pacific region, but has much less name recognition in North America, Europe and other regions. CodeSecure will appeal to application developers looking for a reasonably priced testing solution that supports continuous development and security testing of Web applications written in a few, yet popular, programming languages.

Strengths

Armorize provides an innovative variation of IAST technology designed to be used in development, which builds a complete model of the application using static analysis, scans it for vulnerabilities, and, after detecting a potential code vulnerability, executes a dynamic verification of the suspected Web application vulnerability.

Armorize offers a WAF technology and a malware monitoring and alerting service. Its SAST can bidirectionally exchange information with its own WAF in order to increase WAF accuracy of protection.

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, SLAs 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 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.

Armorize can perform its security analysis even if the code is in a state that won't compile, and thus can be used earlier in development.

The company offers its console to be hosted as a service, but does not provide testing as a service.

Cautions

Armorize does not offer its SAST capabilities as a testing service.

Its testing architecture requires access to source code; it cannot work with Java bytecode or .NET Common Language Runtime (CLR) bytecode.

Armorize's offering is designed for testing Web-enabled applications only.

Armorize does not provide mobile application security testing capabilities.

There is no WAF integration for the more widely deployed WAFs, such as F5 or Imperva.

Return to Top

Aspect Security

Aspect Security, headquartered in Columbia, Maryland, is best known as an application security testing consultancy, but it has developed an IAST solution called Contrast that it offers both via testing as a service and as an on-premises solution. Contrast works by automatically instrumenting Java applications as they are loaded into the organization's Java Virtual Machine (JVM), and are monitored for security vulnerabilities as they are executed. Aspect's Contrast is one of two IAST-only solutions in this Magic Quadrant. Aspect's Contrast should be considered by organizations looking for an innovative approach to application security testing using a pure IAST-based approach that is suitable for supporting agile development and DevOps-type development scenarios without requiring a separate testing scan.

Strengths

Without requiring a separate DAST tool or security testing expertise, Contrast can automatically instrument and test Java-based applications as they are loaded into the JVM (typically for quality assurance [QA] testing), without requiring a separate security testing scan.

Innovative security architecture intelligence is provided as a result of the Contrast analysis — for example, identifying which SQL databases are accessed, which libraries are used, and which vulnerable components are useful from a security vulnerability and threat-modeling perspective.

Because IAST combines SAST and DAST techniques, the results are highly actionable, can be linked to the specific line of code and can be recorded for replay later for developers.

Contrast provides a WAF, bug-tracking system and developer environment integration out of the box.

Cautions

Because it's designed to be used in testing by developers and application testers (and not dedicated security testers), Contrast's application testing coverage depends on the thoroughness of the QA or development testing performed.

There is no mobile application security testing or JavaScript testing support.

There is no .NET application platform support, although this is planned for late 2013.

With Contrast's IAST-as-a-service solution, the customer must load the Contrast technology onto its testing or development platforms and enable network connectivity to Aspect Security.

Return to Top

Cenzic

Cenzic, based in Campbell, California, is an established, dedicated solution provider with a strong focus on DAST products (Hailstorm), DAST testing as a service (ClickToSecure Managed) and DAST cloud-based testing (ClickToSecure Cloud). Cenzic should be considered by information security specialists, penetration testing professionals and application development managers looking for enterprise-class DAST testing capabilities of Web application and Web services provided via tools and as cloud services, and with the ability to be integrated with WAFs, bug-tracking systems and SIEM systems.

Strengths

Cenzic offers a broad array of DAST products and services with a competitive pricing model for large enterprises, as well as specific offerings targeted at small to midsize businesses.

Cenzic has an enterprise console with role-based access control, the ability to consolidate results across multiple testers, and its own Harm (Hailstorm Application Risk Metric) measurement and baselining of application risk across both its products and subscription testing services built on a common architecture and vulnerability database.

The company provides extensive out-of-the-box WAF support, tight F5 integration and an API for WAFs it does not explicitly support.

Cenzic receives high marks from customers for service and support, accuracy, and overall satisfaction.

Cautions

Cenzic does not yet have its own SAST capabilities. They will be provided through a recently announced partnership with Checkmarx.

Cenzic does not offer IAST.

Cenzic does not have a mobile application security testing product — it only offers a cloud-

managed service for testing mobile applications. Its mobile application security testing service does not perform SAST, but does perform DAST analysis of the application, including behavioral analysis and back-end Web services communications.

Return to Top

Checkmarx

Checkmarx is a point solution startup based in Tel Aviv, Israel, that focuses on SAST testing. It earned Gartner's Cool Vendor designation in 2010 for its technological and business vision. Checkmarx's CxSuite technology performs parallel analysis of fragmented, distributed composite applications, and is available as a product as well as through a testing-as-a-service offering introduced at the end of 2012. Addressing security of cloud platforms is a growing area of concern and interest to cloud platform providers and their users. Here, Checkmarx appeals to the users and partners of the salesforce.com cloud platform that need to test code based on the Apex programming framework. Checkmarx will also appeal to information security testing professionals looking for a SAST point solution for composite applications written in various programming languages.

Strengths

Checkmarx's universal application model can be queried to discover vulnerabilities and to check for code quality and adherence to standards. The model also enables incremental scans and analysis across components of composite applications written in a large number programming languages and frameworks.

Checkmarx enables testing throughout the development life cycle, with an integrated developer environment (IDE) and other software development life cycle (SDLC) integration to support this vision.

Checkmarx is the only SAST testing provider capable of testing Apex, and is a major provider of SAST for salesforce.com, its partners and users, as well as offering support for many cloud platforms and frameworks, such as CloudSpokes, MediaMind and TopCoder.

Checkmarx offers SAST for native mobile applications written for Java on Android and Objective-C on iOS.

Cautions

Checkmarx does not offer its own DAST. For DAST capabilities, it has partnered with DAST vendors Cenzic and NT OBJECTives.

Checkmarx does not offer IAST.

Checkmarx offers no out-of-the-box WAF integration, although it provides an XML export of vulnerabilities discovered that can be used by the customer to do this.

Checkmarx's SAST as a service was "soft launched" at the end of 2012; its success is yet to be proven.

Return to Top

HP

HP, based in Palo Alto, California, has a broad portfolio of application security testing products and services. HP's acquisitions of SPI Dynamics and Fortify provide its customers with DAST and SAST capabilities available as on-premises installed products or as a service — all under a single management console and reporting framework. HP also offers a broader set of information security capabilities, including its ArcSight SIEM and TippingPoint Intrusion Prevention System (IPS). HP should be considered by organizations looking for application security testing solutions designed to address the needs of larger enterprises — SAST/DAST/IAST, and products and services with a single enterprise console and reporting framework.

Strengths

HP offers comprehensive SAST capabilities with Fortify's strong brand name and breadth of languages tested.

The company has innovative IAST capability with Fortify SecurityScope, which integrates with its WebInspect DAST.

There is strong integration within HP's security portfolio, such as integration of AST knowledge into ArcSight and DAST knowledge into TippingPoint's IPS for WAF-like protection.

HP uniquely offers runtime application self-protection (RASP) technology (see "Runtime Application Self-Protection: A Must-Have, Emerging Security Technology").

Cautions

HP's pace of innovation with its DAST capabilities, and its market growth, have not kept up with the overall market.

While HP integrates with F5 and Imperva's WAF and TippingPoint's IPS, other third-party WAF providers are not yet supported.

Mobile application security testing is available as a premium cloud-based service, but its current on-premises mobile security testing capabilities within Fortify Static Code Analyzer and WebInspect are not offered as an integrated solution.

Among customers surveyed, HP scored near the bottom in satisfaction with the service/support and accuracy of its SAST and DAST products. Customers also voiced concern over the high pricing of HP's SAST offerings.

Return to Top

IBM

IBM, based in Armonk, New York, has demonstrated its dedication to application security through its acquisition of leading DAST (Watchfire) and SAST (Ounce Labs) startup vendors, and by developing its own IAST technology. Supplementing its AST offerings are data masking, database audit and protection, SIEM, and network security technologies that it has combined into a separate security division. IBM's AST capabilities will appeal to enterprises that want a variety of enterprise-class technologies in application security testing, as well as in adjacent areas such as data security and SIEM. IBM's AST offerings will also appeal to those already using the Rational application development suite of tools.

Strengths

- IBM offers a broad portfolio of application security solutions: SAST, DAST and IAST, including DAST testing as a service, as well as application, data, network and SIEM security technologies.
- IBM has historical strength in DAST and innovative IAST capabilities for Java applications using its Glass Box technology within the context of a DAST scan.
- IBM provides SAST analysis of JavaScript within the context of a DAST scan for testing Web applications using JavaScript, and also offers SAST for mobile applications written in iOS Objective-C or Java on Android.
- The company has the vision and technological capabilities to provide a risk-based view of application intelligence.

Cautions

- IBM is not as well known for SAST as it is for DAST, and it does not provide SAST testing-as-a-service capabilities.
- Although IBM offers DAST testing-as-a-service capabilities, it describes its service as a high-touch, "white glove" service, and it is priced accordingly.
- IBM provides only static but not dynamic/behavioral testing of mobile applications.
- Among customers surveyed, IBM scored near the bottom in overall satisfaction and pricing of its SAST product. Its DAST offering was cited most often as having been replaced within the past year.

Return to Top

Indusface

Indusface is an India-based DAST-as-a-service provider (its service is called IndusGuard), with clients primarily in India, Asia/Pacific and the Middle East. In late 2012, the technology assets for the IndusGuard scanning platform and most of the engineering staff were acquired by Trend Micro. Indusface continues to sell the IndusGuard service and will become a licensed reseller of the Trend Micro Web Application Scanning Platform. The launch of the Trend Micro-branded solution is scheduled for mid-2013; organizations should consider the solution as a cost-competitive alternative to other human-augmented DAST-as-a-service solutions.

Strengths

- All IndusGuard offerings include human-augmented review of the results for improved accuracy (as WhiteHat Security and iViZ Security do).
- IndusGuard includes integrated malware scanning as well as OS and Web platform vulnerability scanning.
- Indusface provides mobile application security testing with both SAST and DAST techniques. However, this will not be available in the first release of the Trend Micro offering.
- The acquisition by Trend Micro will provide a worldwide sales force and data center presence, as well as tight integration with Trend Micro's Deep Security platform for OS and platform vulnerability protection when it is released.

Cautions

- Indusface has limited market presence outside of India, Asia/Pacific and the Middle East.
- Its offering is cloud-only; no on-premises tool is offered.
- Indusface has no SAST or IAST capabilities.
- The basic console interface supports role-based access control (RBAC), but does not provide a separate view applicable to developers. For example, there is no specific developer interface, advanced remediation advice or integration into bug-tracking systems.
- There is WAF integration with only ModSecurity, although Trend Micro will expand this list at launch.

Return to Top

N-Stalker

N-Stalker is a privately owned vendor located in Brazil with clients worldwide. It has a strong focus on Web application security analysis, and appeals to the clients that require DAST technology and testing-as-a-service capabilities. N-Stalker's DAST scanner is based on a database of vulnerability patterns and attack scenarios. Its pricing is affordable, and it also offers a free, restricted capability version of its technology. N-Stalker provides network vulnerability scanning for a broader view of vulnerability management, and several enterprise-class capabilities such as RBAC and reporting. N-Stalker should be considered by dedicated security specialists that focus on testing Web application with DAST technology looking for enterprise capabilities with competitive pricing.

Strengths

- N-Stalker supplements its DAST by offering proxy capture and testing tools for analyzing HTTP traffic between the browser and server, testing password strength, providing discovery of Web servers, and testing servers' workload capabilities.

N-Stalker offers some enterprise-class console capabilities, including RBAC and application risk trending.

It has out-of-the box integration with several WAF vendors/technologies (Trustwave, Imperva and open-source software [OSS] ModSecurity).

N-Stalker is one of the few smaller vendors that offer DAST-as-a-service options.

Cautions

Some SAST capabilities were introduced at YE12, but have not yet been integrated into the offering and its capabilities are unproven.

N-Stalker offers no native mobile application testing. Mobile application security testing capabilities are limited to HTML5 applications. The company does not offer SAST or behavioral analysis of mobile applications.

N-Stalker does not offer IAST.

Return to Top

NT OBJECTives

NT OBJECTives (NTO), headquartered in Irvine, California, focuses on DAST solutions for enterprise customers. NTO offers DAST products and testing-as-a-service capabilities. It offers several DAST products, including an enterprise version that includes out-of-the-box integration with bug-tracking systems, along with an enterprise-class console. NTO should be considered by enterprises looking for a "point and shoot" DAST solution combining full-featured enterprise DAST capabilities as a competitively priced alternative to the larger players in the market.

Strengths

The company offers extensive WAF integration via its NTODefend offering.

Its "universal translator" technology enables testing of all types of exposed application back-end interfaces, such as JSON, REST, SOAP, XML-RPC, GWT-RPC and AMF, which are critical for DAST testing of mobile applications.

NTO offers a solid enterprise console with active reporting capabilities.

NTO's DAST as a service includes human augmentation for vulnerability validation as standard.

NTO receives high marks from customers for its service and support, as well as overall satisfaction.

Cautions

The company offers no SAST or IAST capabilities, although it is working on partnerships with Coverity and Checkmarx, which should also address SAST for mobile applications.

There is no IDE integration; developers either get sent a report or use the NTO console.

NTO provides no HTML5 or specific mobile application security testing capabilities, although users can record the application traffic with a proxy for testing its exposed interfaces.

Return to Top

PortSwigger

London-based PortSwigger focuses on DAST testing tools and is best known for its free Burp Suite DAST tool. It also offers Burp Suite Professional, which is targeted at the advanced tester but 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 such as SDLC integration and RBAC console access and reporting. Burp Suite Professional should be considered by organizations looking for a powerful DAST tool at an extremely competitive price.

Strengths

The Burp Suite proxy is a useful tool for the real-time capture of Web interactions, including back-end interfaces for dynamic testing. Many competitors in this space also support the use of the Burp Suite proxy recorder.

Almost all of the Burp Suite Professional tool functionality can be driven via API, and the user interface can be customized by the user directly (such as adding tabs or menu options for the automation of advanced testing scenarios specific to the tester or the organization).

Burp Suite Professional supports live scanning in which the application can be tested in real time as the application is being navigated by the tester, which is extremely useful for applications with complex navigation and state scenarios.

Cautions

Burp Suite Professional provides no WAF, IDE or bug-tracking system integration.

Burp Suite Professional has no SAST or DAST-as-a-service capabilities.

Mobile application testing capabilities are limited to DAST of back-end services recorded by its proxy.

Return to Top

Qualys

Qualys, based in Redwood City, California, is best known for its cloud-based vulnerability-scanning-as-a-service capabilities, but expanded into DAST as a service in 2011 (and has begun expanding into WAF as a service in 2013), leveraging these capabilities from its cloud-based security services platform architecture. Qualys targets the lower-end, price-sensitive portion of the market with fully automated DAST scanning, and uses integrated Selenium support for the automation of

authentication and navigation. Qualys should be considered by organizations looking for basic, low-cost DAST-as-a-service capabilities served from a straightforward management console and interface, often combined with other types of managed security services such as vulnerability scanning.

Strengths

- Qualys has experienced solid growth in its DAST-as-a-service offering since redesigning and relaunching it in 2011.
- Flexible, logical tagging architecture permits the user to customize the Qualys console and reports to his or her organization and structure.
- Qualys features aggressive pricing at $495 per application per year, with high levels of discounting reported by customers.
- Integrated malware detection service is included as a standard part of its DAST services.
- Customers surveyed gave Qualys high marks for its pricing model.

Cautions

- Qualys' offering is provided as a service only; there is no product option.
- A fully automated scan has limits on the vulnerabilities it can find. Qualys offers no human augmentation of its scanning results or business logic testing. In March 2013, Qualys partnered with iViZ Security to fulfill this customer need.
- Qualys has no SAST or IAST capabilities, and no IDE or bug-tracking system integration.
- The company has no mobile application security testing capabilities.

Return to Top

Quotium Technologies

Quotium Technologies, based in France, is a point solution provider of an IAST-only solution, Seeker. For its innovation in IAST, Quotium was named a Cool Vendor by Gartner in 2011 (see "Cool Vendors in Infrastructure Protection, 2011"). Quotium experiences a lack of name recognition due to the newness of IAST and its small size. Quotium should be considered by application development professionals looking for a way to adopt application security testing into the SDLC with a tool that provides effective vulnerability detection and is relatively easy to adopt.

Strengths

- Quotium pioneered IAST and continues its innovation — for example, adding security analysis of stored procedures and database transactions, correlation of end-to-end flow of data with runtime code execution, and JavaScript analysis.
- The company offers 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 detection of vulnerabilities spread across multiple tiered components, including the analysis of applications that do not have user interfaces.

Cautions

- Quotium is not well-known for security testing, has a small installed base of customers and has yet to prove that it can scale its business.
- Quotium focuses exclusively on an IAST product only (no services), and does not offer stand-alone SAST or DAST capabilities.
- Its IAST is not designed for use in a production environment and requires instrumentation of the test runtime environment (such as JVM or .NET CLR), although it delivers higher accuracy vulnerability detection.
- Quotium does not offer client-side mobile application testing. However, it can learn how the application interacts with the back-end servers that Quotium supports and test this. However, Quotium's Seeker can observe and learn how the application interacts with the back-end servers (for servers that Seeker supports), and test these interfaces.

Return to Top

Veracode

Veracode, with headquarters in Burlington, Massachusetts, is an established AST-as-a-service provider with an historical strength in SAST, which now offers DAST as a service as well from a single integrated console. It is a pioneer of the testing-as-a-service business model, as well as a pioneer in the testing of native binary application code. It has also been successful in targeting supply chain ecosystem partners to test with its Vendor Application Security Testing (VAST) program. Veracode should be considered by organizations looking for a mature static-testing-as-a-service provider that also offers dynamic testing and discovery capabilities. In addition, Veracode's binary testing capabilities will be of specific interest to organizations looking for approaches to statically test third-party binaries and libraries.

Strengths

- Veracode offers a well-designed single user interface for consuming its SAST and DAST services complete with RBAC, risk ratings and embedded analytics.
- Veracode is one of only two vendors (the other is GrammaTech) that offer native binary code testing capabilities.
- Veracode receives high marks from customers for its service and support, as well as its customer success program.
- Veracode gained innovative mobile application security testing vision and technology with its October 2012 acquisition of Marvin Mobile Security.

Cautions

Veracode does not offer a stand-alone product (except for a handful of specific defense-related customers), and is only available as a service. Further, even when used as a service, Veracode does not offer an on-premises appliance option to keep binaries and scanning local (although one is planned before YE13).

There is no WAF integration, although ModSecurity and Imperva integration capabilities are currently in beta testing.

To get the most detail from a binary scan — such as the line number of a vulnerability — C, C++ and Objective-C applications need to be compiled with debugging information turned on.

Veracode has no IAST capabilities.

Veracode is not well-known for its DAST capabilities, and the transition of its installed base from NT OBJECTives to its own DAST solution has taken several years.

Return to Top

Virtual Forge

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

Strengths

The company has a partnership with IBM, which resells Virtual Forge (IBM's own SAST capabilities don't cover ABAP).

Virtual Forge scans for security and quality issues with ABAP code, and also scans the SAP platform for known, but unpatched types of vulnerabilities.

Virtual Forge provides innovative, patent-pending static data loss prevention capabilities where the customers identify the critical SAP tables and Virtual Forge identifies which programs access this data.

Cautions

Even though Java is used within many SAP architectures, Virtual Forge only scans ABAP.

Virtual Forge's UI is complex, but tightly integrated with the SAP graphical user interface, and will be familiar to experienced SAP users and administrators.

Virtual Forge has no SAST as a service, DAST, IAST or mobile application security testing capabilities.

Return to Top

WhiteHat Security

WhiteHat Security, headquartered in Santa Clara, California, is an established dynamic application security testing as a service provider that expanded into SAST in 2012 after its 2011 acquisition of Infrared Security. WhiteHat Security has been a pioneer in the pure testing-as-a-service business model, and offers multiple levels of DAST and SAST services with integrated management and reporting under a single integrated console. WhiteHat Security should be considered by organizations looking for a DAST as a service provider that also offers SAST, IAST and mobile application security testing capabilities.

Strengths

All of its DAST and SAST service offerings include human-augmented review of the results to improve accuracy.

For its SAST offering, WhiteHat Security uses an on-site virtual appliance so that a complete copy of the customer's source code never leaves its site, and it offers a 24-hour turnaround SLA.

WhiteHat Security offers out-of-the-box integration with multiple WAFs; five governance, risk and compliance (GRC) products; and bidirectional integration with Jira.

The company offers basic IAST capabilities through which a vulnerability discovered by static analysis is correlated with DAST results, and also uses IAST within its mobile testing capabilities.

Its mobile application security testing as a service combines SAST and DAST techniques to fully test the application for a single fee, but reporting is not yet integrated into its Sentinel console.

Cautions

WhiteHat Security provides only cloud-based testing as a service; no product option is available.

WhiteHat Security is not known for SAST, and its initial SAST offering only supports Java, with .NET support scheduled by YE13 and support for other languages to come later.

WhiteHat Security does not offer a low-cost, fully automated (non-human-augmented) DAST service, and will be challenged at the low end of the market by vendors such as Qualys.

WhiteHat Security offers no IDE integration.

Among customers surveyed, WhiteHat Security was rated near the bottom in service and support.

Return to Top

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.

Return to Top

Added

This is a new Magic Quadrant that replaces the "Magic Quadrant for Dynamic Application Security Testing" and the "Magic Quadrant for Static Application Security Testing." As a result, all vendors in this Magic Quadrant are considered new.

Return to Top

Dropped

As a new Magic Quadrant, no vendors have been dropped.

Return to Top

Inclusion and Exclusion Criteria

Vendors of AST products and subscription services were considered for this Magic Quadrant if their offerings:

- Provided a dedicated static or dynamic application security testing capability — a tool, subscription service or both
- Had at least $2 million in specific revenue from AST-related products or services
- Were generally available (not beta) before 1 January 2013

Vendors must also be determined by Gartner to be significant players in the market, because of market presence or technology innovation.

Vendors were not included in this Magic Quadrant if their offerings did not meet the requirements of inclusion listed above, or they provided services that were 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. Several categories of solutions that may provide application security testing products and services were not included in our analysis: These map into several broad categories:

1. **Network vulnerability scanners that may also provide some basic Web-application-layer dynamic scanning:** This category includes vendors such as nCircle, eEye Digital Security (acquired by BeyondTrust), Rapid7 and Tenable Network Security. These solutions provide only a subset of the capabilities needed for an enterprise application security testing solution. Occasionally, they are used by network security specialists to provide a simple, defense-in-depth application-layer scan in addition to a dedicated AST solution.
2. **Penetration testing products and services:** For example, products such as Core Security's Impact have no application security testing capabilities on their own, but provide an overall framework for the automation of penetration testing.
3. **Application security testing consultancies:** There are a large number of application security consulting specialists such as Cigital, Denim Group and Security Innovation (see "Navigating the Security Consulting Landscape"). These vendors provide specific application security consulting services in areas such as developer training, SDLC process changes, penetration testing and code remediation services. They may offer application security testing, but not as a repeatable, subscription-based service.
4. **Open-source offerings:** These may be mentioned in the research as alternatives, but commercial support of this kind of offering must be available for it to be reviewed. Open-source tools do not have the capabilities of commercial alternatives, and are typically used in conjunction with commercial offerings for basic testing earlier or to provide specific capabilities for penetration testers. The availability of several quality commercially supported solutions in the sub-$1,000 price range has diminished the appeal of open-source software for application security testing.
5. **Network protocol testing and fuzzing solutions:** These are designed to stress-test networked devices and applications, such as switches, IP-PBXs, firewalls and intrusion prevention systems, and include offerings from Codenomicon, Spirent Communications (which acquired Mu Dynamics), Ixia BreakingPoint and others. While these solutions may have some application quality and security testing capabilities, such as testing application-level denial of service or application protocol malformation, they are not a substitute for dedicated application security testing solutions.
6. **Application code quality and integrity testing solutions:** These solutions are designed to perform application testing with a focus on code quality, reliability and architecture, typically via static analysis during application development. While they may provide some application security testing capabilities, they tend to lack the market name recognition and mind share of information security professionals, and the breadth and depth of security capabilities of solutions that focus on security testing. Example vendors include Cast Software, Coverity, GrammaTech, Klocwork and Parasoft.
7. **Vendors and solutions that did not meet the inclusion criteria:** There are several market players with specific expertise and regional support that may be suitable (see Note 1).

Return to Top

Evaluation Criteria

Ability to Execute

Product/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, appeal to a breadth of users (and thus buyers — such as QA/testing specialists, as well as information security specialists), appeal with security technologies other than AST (regardless of whether they are application-security-related), and offering product and AST testing services.

Overall Viability (Business Unit, Financial, Strategy and 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 the applications security testing market and in the broader information security space, AST revenue amount, AST expertise, the number of AST customers, and the likelihood that the vendor will be successful in its acquisition and/or partnership deals.

Sales Execution/Pricing: We account for AST growth rate, 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 them. This includes customer feedback on deal management, pricing and negotiation, presales support, and the overall effectiveness and customer receptiveness of the sales and partner channels worldwide. We also evaluate a vendor's estimated AST market share and overall mind share, including the number of times the vendor appears on Gartner client shortlists.

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 broader application security capabilities with enterprises' functional requirements, and the vendor's track record in delivering new, innovative features when the market demands them.

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

Table 1. Ability to Execute Evaluation Criteria

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

Source: Gartner (July 2013)

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. The single most important criterion for customers evaluating AST solutions is accuracy, so higher ratings are given to techniques and approaches proven to improve accuracy. The ability to test modern RIAs, HTML5 applications, and mobile and cloud applications are critical, including the ability to automatically schedule and coordinate cloud testing of enterprise applications with infrastructure as a service (IaaS) providers. The ease of an AST solution's native integration with multiple, popular SDLC platforms — most notably, source code management systems, bug-tracking systems, and in QA for DAST, and into IDEs for SAST. The enterprise console is a critical element 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. Finally, we look at the ability of the vendor 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 a 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 application security analysis, the optimal balance between satisfying the needs of leading-edge (that is, Type A) enterprises and Type B (mainstream) and Type C (risk-averse) enterprises, and the optimal balance between satisfying the needs of typical enterprises and specialized clients (for example, large organizations with thousands of applications in their portfolio). Vendors should 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 evolving toward the vision of enterprise security intelligence (see "Prepare for the Emergence of Enterprise Security Intelligence") with DAST/SAST interaction, integration and correlation, thus enabling higher accuracy and breadth of security coverage, as well as advanced analytics, contextual assessments, and support for optimal security and risk management decisions across the enterprise. We also give a higher rating to vendors that develop methods that make security testing more accurate (for example, decreasing false-positive and false-negative rates). AST solutions should provide a variety of options for testing — 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 option to submit jobs to server-based scanning engines, and the option to submit jobs to a testing provider (their service or potentially a cloud-based virtual machine) while providing a unified view and reporting across all of these scanning options. Other areas of innovation include application protection features (for example, WAF-like features); out-of-the-box integration with application protection mechanisms, such as WAFs and IPSs; integration with GRC and SIEM technologies; innovative ways of delivery (such as security testing as a service and DAST engine availability as a cloud-based delivery option); 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 mobile and modern RIA Web applications.

Geographic Strategy: Here, we evaluate worldwide availability and support of the offering, including local language support for tools and consoles as well as local language support for customer service. Several providers are well-known regionally, but have little or no presence outside of their region. 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	No Rating
Sales Strategy	Standard
Offering (Product) Strategy	High
Business Model	No Rating
Vertical/Industry Strategy	No Rating
Innovation	High
Geographic Strategy	Standard

Source: Gartner (July 2013)

Quadrant Descriptions

Leaders

Leaders in the AST market provide breadth and depth of application security testing products and services. The more important is the depth and accuracy of testing techniques: Leaders provide static, dynamic and, in most cases, interactive application security testing techniques in their solutions. Leaders should also provide organizations with a choice of delivery models — either as a product, as testing as a service, or both, using a single management console and enterprise-class reporting framework supporting multiple users, groups and roles. Leaders should provide capabilities for testing the next generation of Web and mobile applications.

Return to Top

Challengers

Challengers in this Magic Quadrant are vendors that have executed consistently, typically by focusing on a single type or delivery model of application security testing, and have demonstrated momentum in their customer base in terms of overall size and growth.

Return to Top

Visionaries

Visionaries in the Magic Quadrant are those that are advancing the emerging approach of IAST for fast and accurate security testing, 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). Delivering IAST alone isn't enough to be a Visionary, but we weigh it heavily along with other factors.

Return to Top

Niche Players

Niche Players focus on a specific type or delivery model of application security testing, or a specific geographic region, targeting well-defined AST use cases such as more-thorough testing, combined quality testing, focusing on a single language (such as ABAP) or on penetration testers.

Return to Top

Context

As a direct result of dealing with the threat of advanced target attacks, application security testing has received renewed focus in 2013. There has been a shift to application-level attacks as a way to gain access to the sensitive and valuable information they handle. In addition, most enterprises are expanding their application security testing programs in depth — scanning more of their application portfolio — and breadth — moving back further into development and using both static and dynamic analysis techniques. As a result of these trends, application security has become a top investment area for information security organizations, whether it means improving the security of applications developed in-house, procured from third parties or consumed as a service from cloud providers.

Overall, AST market consolidation continues, and the market now offers a variety of AST technologies from large application development platform vendors offering both DAST and SAST capabilities, as well as dedicated DAST or SAST point solutions from small, innovative startups. Multiple providers offer DAST and SAST testing as a service options, some exclusively.

AST solutions are designed to help organizations identify application-level vulnerabilities in all applications — regardless of whether they are developed in-house, outsourced or acquired. Their use should be considered mandatory by all organizations and service providers.

Return to Top

Market Overview

At a high level, application security testing capabilities fall into three broad categories: DAST, SAST and IAST:

DAST — Originally designed for the detailed analysis of security vulnerabilities in running Web-based server applications, DAST solutions test applications in a running state from the "outside in" by testing their exposed interfaces. For this reason, they are often referred to as "black box" testing tools. The running application is treated as a black box and is tested through its exposed interfaces — largely independent of the language or platform that the application was developed on. Of the multiple AST submarkets, DAST is the most mature and widely adopted.

SAST — In contrast, SAST tests applications from the "inside out" by analyzing an application's source code, bytecode, or, in some cases, native binary code. SAST tools function much like a compiler, and are used on nonrunning applications. Because of this, solutions are highly dependent on the language and platform being used, and are better suited for use in the software development process, typically to gain functions such as QA when security testing is performed.

IAST — A third and emerging capability is interactive application security testing, which delivers the interaction of both static (inside-out) and dynamic (outside-in) testing capabilities with the goal of providing greater testing accuracy (see "Evolution of Application Security Testing: From Silos to Correlation and Interaction").

There has been a convergence of capabilities. This Magic Quadrant reflects this convergence and evaluates static, dynamic and interactive testing solutions, as well as vendors that offer combinations of these. There have been several drivers for this convergence:

Customer requirements: Potential customers know their applications are vulnerable and are looking for solutions to identify these vulnerabilities. SAST and DAST technologies do not completely overlap in the vulnerabilities they find, and are also deployed in different SDLC phases, so both methods are often desired. Ultimately, the customer's priority is to become more secure while doing so in the most efficient manner. How this is accomplished (that is, via SAST, DAST or IAST) is of secondary concern.

Complex Web applications: Web applications are evolving to include greater use of client-side logic in the form of complex JavaScript or RIA technologies such as Adobe Flash. To better test these applications, a combination of DAST with SAST of the client-side code is optimal. In addition, DAST scanning tools should be able to emulate multiple browsers to ensure complete application security testing coverage.

Mobile applications: Mobile applications such as iOS and Android applications require both SAST and DAST techniques to be used for comprehensive security testing. SAST is needed for the mobile application code, and DAST is needed to test the services on the back end that the mobile application "talks to." In addition, DAST scanning tools should be able to emulate multiple mobile browsers to ensure complete application security testing coverage.

All applications — whether internally developed, procured, outsourced or cloud-based — should be tested. As discussed in "Hype Cycle for Application Security, 2012," the adoption of DAST solutions, primarily in the form of Web application testing tools, has been rapid, and are more mature than SAST offerings, but this does not eliminate the need for SAST testing. The market for AST solutions continues to evolve, and new approaches are technologies are required to test next-generation mobile, RIA, cloud and embedded applications (see "Key Trends in Application Security Testing"). The major trends shaping the market are summarized below.

Expansion of Application Testing as a Service

Many of the vendors in this Magic Quadrant offer AST as a service, and most customers consider this a critical capability. Several of the vendors (Qualys, Veracode, WhiteHat and Indusface) focus only on providing testing-as-a-service capabilities, and do not offer their tools for sale independently. Increasingly, organizations tell us they prefer to implement AST using an on-site product combined with a service from the AST vendor — for example, testing their more sensitive applications on-premises using an AST tool and testing their less sensitive applications via AST as a service, or testing deployed applications as a service, with testing of applications in the QA phase of the development process using on-premises AST products. While testing as a service may save on upfront costs, organizations are placing knowledge of their vulnerabilities (and, in some cases,

source code) in the hands of outside third parties.

The Importance of Testing Client-Side Code and HTML5

Increasingly, Web-enabled applications involve rich client-side interfaces for end users. A hallmark of modern Web applications is the use of client-side code, mostly in the form of JavaScript (the "j" in Ajax) and related frameworks. In addition, many applications include client-side logic in the form of Adobe Flash and Flex. In all cases, the use of client-side RIA logic complicates how traditional DAST testing is performed, since JavaScript and other types of code are rendered at the client — not at the server — and can be vulnerable. Leading AST providers will perform SAST of JavaScript in combination with DAST. More recently, interest has shifted to the use of HTML5 for rich user interactions. As a result, testing modern Web and HTML5-enabled applications will become a strategic differentiator for DAST solutions.

The Importance of Explicit Framework Support

Many application developers use frameworks to speed their development. To provide the greatest accuracy, all SAST solutions — whether testing source code, bytecode or binaries — must have an explicit understanding of the framework being used, induding doud-platform-as-a service provider frameworks such as those from CloudSpokes, Force.com and Appirio. This is also true on mobile devices, such as Java on Android, where the specific frameworks being used must be explicitly supported. The same goes for JavaScript frameworks (such as jQuery and jQuery Mobile) and hybrid frameworks (such as the popular OSS framework PhoneGap[2]) that combine native and Web-based code in the mobile application, which complicates testing. Vendors with broader explicit support of frameworks are preferred.

The Importance of Testing Mobile Applications

An emerging requirement for AST solutions is the ability to test mobile applications. Ideally, mobile applications would be tested with a combination of SAST and DAST techniques. However, pure SAST or pure DAST testing can add value. Aside from the use of RIAs and HTML5 we discussed earlier, most Android and iOS applications (even when written as native applications) are Web-like in nature and communicate over Web or RESTful HTTP-based protocols. For the dynamic testing of the back end for mobile applications, there is also a requirement for AST solutions to emulate various mobile browsers in order to test any application functionality specific to a given platform. This is increasingly important for Web applications with various interfaces for different mobile clients to ensure the entire surface area of the application is tested for vulnerabilities. There is also a necessity to apply SAST to the source code or binaries of native mobile applications to understand potential vulnerabilities within the source code. Code written in mobile-specific programming languages should be inspected for security vulnerabilities; new programming frameworks, specific to a particular device/vendor (iPhone or Google Android), should be analyzed.

The Importance of Testing Back-End Interfaces

Like mobile applications, many applications make calls to back-end services that need to be tested. These interfaces should be identified and tested with SAST and then also tested with DAST techniques. Most modern applications (mobile and nonmobile) are shifting to RESTful HTTP[3] interfaces for communication to back-end systems, and these must be tested. In addition, advanced DAST solutions should also be able to explore and test Web-services-based interfaces to applications — specifically, the ability to discover Web services access by understanding Universal Description, Discovery and Integration (UDDI) and WSDL, and then specifically testing the SOAP-based interfaces the crawler has discovered. Advanced DAST solutions also understand, support and can test WS-* protocol implementations, such as WS-Security, and the use of security tokens such as SAML. In addition to REST, some newer applications use other types of XML-based interfaces as well as JSON, all of which should also be able to be analyzed and tested.

SDLC Integration

The proper place for application security testing is during the application development process, where application development professionals should be performing security vulnerability detection and remediation with the help of AST tools as early in the development phase as possible. As responsibility for AST testing expands from information security into the development organization, the importance of gaining role-based views into testing results or, ideally, providing native integration into the development environment becomes increasingly important. Leading AST solutions offer interfaces customized for each, or offer native integration into application development environments — for example, into defect tracking systems, source code management systems, developer IDEs and QA testing tools. The need for this integration complicates delivery of AST as a service. For complex navigation, many QA organizations already use tools such as Selenium to record and replay interactions. AST solutions need a similar capability, and ideally would consume the navigation scripts generated by the same record/replay tools used by the QA organization.

The Importance of Comprehensive Application Discovery

It is important that all AST solutions also offer the ability to inventory and discover applications that the information security organization may not be aware of, including those inside the perimeter firewall. This is much easier for tracking Web-enabled applications than non-Web applications, but, ideally, both would be discovered. Leading AST solutions offer this capability, including the ability to profile and prioritize Web applications based on whether or not they accept input via forms, perform authentication or use Secure Sockets Layer certificates. Likewise, the AST solution must be able to crawl and test complex Web applications, which is increasingly challenging because more and more Web navigation is driven by JavaScript or other RIA constructs.

Delivering Against the Vision of Security Intelligence

There is an emerging understanding among visionary application security testing vendors that the application security market space should evolve into being a security intelligence (SI) enabler (see "Prepare for the Emergence of Enterprise Security Intelligence" and "Application Security

Technologies Enable Enterprise Security Intelligence"). The goal of delivering SI becomes an important strategic criteria to evaluate AST solutions in several important ways:

IAST: Specifically, a software agent is deployed to the application server platform to instrument the application being placed under dynamic testing. The information gathered by this instrumentation agent gives the hybrid solution an inside-out view that complements the outside-in view of a purely DAST solution (see "Evolution of Application Security Testing: From Silos to Correlation and Interaction").

Web application firewall integration: It is also valuable to have some level of interaction and integration of AST solutions and WAFs,[4] as well as intrusion detection and prevention systems. This type of interaction is designed to help assist organizations shield applications that are known to be vulnerable (with the vulnerabilities having been discovered by AST solutions, typically DAST) by using runtime protection capabilities provided by the WAF. For the vulnerability shielding to be effective, explicit (not just a generic XML export of a vulnerability description) integration with the WAF solution must be enabled by the AST provider and the WAF provider (see "Application Security Detection and Protection Must Interact and Share Knowledge").

Runtime application self-protection (RASP): This is an emerging security technology that is built or linked into an application or application runtime environment, and is capable of controlling application execution and detecting and preventing real-time attacks (see "Runtime Application Self-Protection: A Must-Have, Emerging Security Technology").

Queryable repository for understanding application risk: Another foundational element of SI is the integration and correlation of security information and contextual information into a queryable persistent repository. Security analysis results collected by AST technologies and application inventory information, along with contextual information defining the business/compliance/intellectual property aspects of tested applications, should be stored in persistent repositories, thereby enabling querying for the purposes of contextual risk assessments and optimal risk management, as well as business decision making based on those assessments.

Return to Top