G00225672

Magic Quadrant for Dynamic Application Security Testing

Published: 27 December 2011

Analyst(s): Neil MacDonald, Joseph Feiman

Dynamic application security testing (DAST) solutions should be considered mandatory to test all Web-enabled enterprise applications, as well as packaged and cloud-based application providers. The market is maturing, with a large number of established providers of products and services.

Strategic Planning Assumption(s)

By 2016, 40% of enterprises will make proof of independent security testing a precondition for using any type of cloud service.

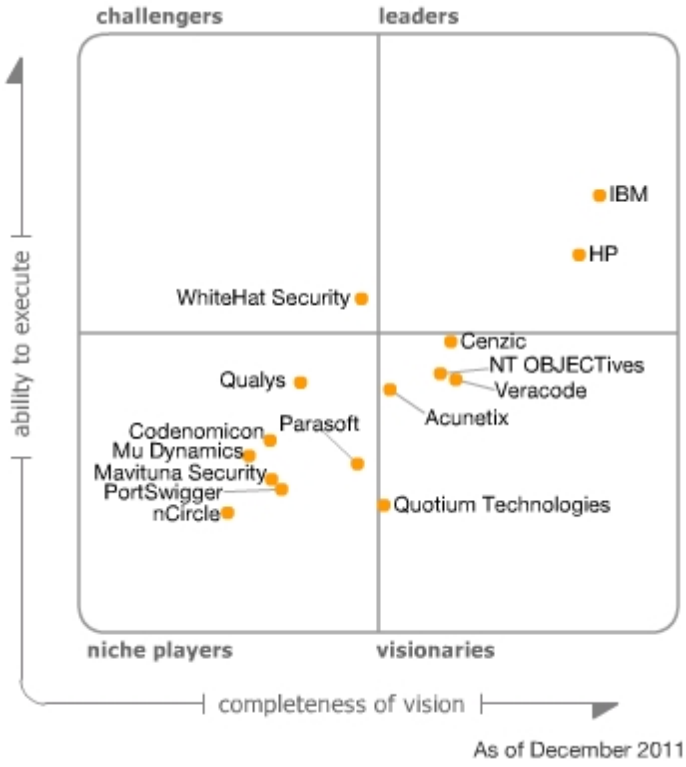
Market Definition/Description

Dynamic application security testing (DAST) technologies are designed to detect conditions indicative of a security vulnerability in an application in its running state. Most DAST solutions test only the exposed HTTP and HTML interfaces of Web-enabled applications, and many also test Web services using protocols and formats, such as Simple Object Access Protocol (SOAP), representational state transfer (REST), Extensible Markup Language (XML) and JavaScript Object Notation (JSON). However, some solutions evaluated in this Magic Quadrant are designed specifically to expand well beyond Web protocols to include non-Web protocols (for example, remote procedure calls, Server Message Block, Session Initiation Protocol [SIP] and so on) as well as data input malformation. This is especially critical for the dynamic security testing of applications used within embedded devices, such as storage appliances, telecommunications and networking equipment, directories, automated teller machines, medical devices and so on.

DAST technology is the focus of this Magic Quadrant. Static application security testing (SAST) solutions are explored in detail in "Magic Quadrant for Static Application Security Testing." DAST technology has matured and has advanced well into the "Slope of Enlightenment," in contrast to SAST, which is still emerging out of the "Trough of Disillusionment" (see Gartner's "Hype Cycle for Application Security, 2011"). We estimate market penetration of DAST solutions at 60% to 70% of enterprises. However, the percentage of applications tested within a given enterprise varies broadly. Enterprises typically apply DAST first to external-facing, Web-enabled applications and then expand its usage over time.

Magic Quadrant

Figure 1. Magic Quadrant for Dynamic Application Security Testing



Source: Gartner (December 2011)

Vendor Strengths and Cautions

Acunetix

Acunetix is an established vendor with a strong focus on application security that has offered its stand-alone DAST Web vulnerability scanner since 2002. Acunetix is a smaller, privately held startup vendor, and its smaller size and lack of enterprise-class features could be an inhibiting factor for some users. Acunetix should be considered by information security specialists and penetration testing professionals looking for a lower and straightforwardly priced, commercially supported Web application security testing tool.

Strengths

- Acunetix provides interactive application security testing (IAST) capabilities with its AcuSensor implementation for applications written in .NET and PHP.
- Acunetix products are among the most inexpensive in the market.

- Acunetix has a straightforward pricing model, an advantage compared to many vendors' convoluted models.
- Customers indicate that the solution is easy to use and that it can be configured for advanced and deep scanning.

Cautions

- Acunetix does not have DAST as a service offering.
- Its IAST offering doesn't support Java-based Web application platforms.
- Acunetix does not offer out-of-the-box capabilities for integration with development/testing platforms typically requested for enterprise-class implementations.
- 24/7 support is not available.
- Testing of rich Internet applications (RIAs) based on Flash/Flex is not supported.
- There is no Web application firewall (WAF) integration.

Cenzic

Cenzic is an established, dedicated DAST solution provider with a strong focus on application security, offering DAST products (Hailstorm), testing as a service (ClickToSecure Managed) and cloud-based testing (ClickToSecure Cloud). Cenzic has demonstrated vision by providing a DAST product, and was an early provider of DAST testing services. Cenzic also offers enterprise-class features, such as software life cycle (SLC) integration and enterprisewide visibility and reporting across multiple DAST scanners. Cenzic should be considered by information security specialists, penetration testing professionals and development managers looking for enterprise-class DAST testing capabilities across multiple users (including pen testers) and those considering expanding DAST testing from information security into development.

Strengths

- Cenzic offers out-of-the-box integration into the SLC, with integration for HP's Quality Center, IBM Rational ClearQuest and Bugzilla. Other integration can be performed via its XML APIs.
- Generic XML-based vulnerability protection information is exposed for Barracuda, Citrix, F5, Imperva and Trustwave WAFs. Specific integration with several providers is planned for 2012.
- The ability to pause a test in process, modify the test and resume it, as well as the ability to step through an assessment and set specific breakpoints (for example, at particular events and URLs) appeals to information security professionals and pen testers.
- An interactive scanning feature provides the ability to have a user navigate an application and have the Cenzic engine simultaneously attack the application in real time for vulnerabilities, such as cross-site scripting, SQL injection and buffer overflows.

- There are a large number of out-of-the-box Smart Attack libraries for testing that are updated weekly and directly modifiable, if needed, by customers.
- Hailstorm provides XML-based protocol fuzzing for generic RESTful API testing, as well as JSON-based application testing.
- Cenzic partners with cloud service providers for testing services. For example, Cenzic has announced relationships with OpSource, Engine Yard and Microsoft's Azure cloud platforms.
- Customers cite high levels of satisfaction with Cenzic's user interface and ease of use.

Cautions

- Cenzic is a lesser known DAST provider that infrequently appears on the shortlists of Gartner clients.
- Cenzic doesn't have the captive development installed base of IBM or HP for which to sell its SLC-integrated capabilities.
- It has no SAST or IAST capabilities that other DAST market leaders and visionaries offer.
- Premium support is required for 24/7 support coverage.

Codenomicon

Codenomicon is a smaller dynamic testing vendor that has focused on comprehensive dynamic fuzz testing of any application and in all ways the application consumes data (network, wireless, file, programming interfaces, interprocess communication and so on), including comprehensive protocol testing. Fuzz testing of applications appeals to operations (to test for performance, health monitoring and bugs) and security professionals (to test for vulnerabilities) as well. Although not designed specifically to test Web-enabled applications, Codenomicon should be considered by information security, operational testing and penetration testing professionals looking for an application fuzz testing solution with broad protocol support and multiple options for deployment, and that complements traditional Web application scanning tools.

Strengths

- Broad protocol test coverage with stated coverage for 190 protocol fuzzing models is available. For protocols not covered by the base test modules, Defensics offers capture-based fuzzing capabilities.
- Licensing is available for internal information security specialists and consultants to use Defensics as an audit/pen-testing tool.
- As a software-based model, it can be deployed on enterprise stand-alone, blade or virtualized servers, as well as stand-alone workstation/laptops support. Physical testing appliances are available if requested by the customer.
- It provides integration with test automation frameworks, such as HP Quality Center, and direct integration to debuggers and analyzers, such as WinDbg, the GNU Project Debugger and

Valgrind, to provide more-detailed information as a part of the bug tracking and remediation process.

- A command-line interface and RESTful HTTP API for integration with third-party test harnesses, test automation and bug-tracking systems are available.
- Testing as a service capabilities are available, with an automated cloud-based fuzzing service planned for 2012.
- Customers cite high levels of satisfaction with Codenomicon's customer service and support.

Cautions

- Although not designed for general-purpose DAST of Web-enabled applications, it has capabilities here — Codenomicon was the first to support testing of XML-based Web services applications, and SQL injection attacks are part of the tests Defensics performs.
- Even without the cost of a hardware appliance, there is potentially higher licensing costs based on the number of fuzz testing modules and the number of concurrent users for organizations with extensive testing requirements.
- Customers indicate that customization beyond out-of-the-box defaults requires significant technical expertise, a desire for increased automation capabilities and simplified integration into the build process.
- For extensive XML SOAP testing, WS-Security and WS-Authentication are not yet supported, but are on the road map.

HP

HP has the potential to become a security powerhouse with a broad portfolio of security offerings — application, network security and security information and event management (SIEM) — that HP is currently integrating both organizationally and technologically. HP moved into the DAST market as a result of its 2007 acquisition of SPI Dynamics — one of the market pioneers and historical leaders at the time, which fit well and provided an upselling capability to HP's installed base of quality testing capabilities from its acquisition of Mercury Interactive. However, execution of the acquisition has been suboptimal, and HP lost some of SPI Dynamic's momentum. After its 2010 acquisition of Fortify for SAST and the 2011 formation of a dedicated security business unit, HP is refocusing on its DAST capabilities as a product, and testing as a service. Information security professionals and application development managers should consider HP for DAST product and security testing capabilities with worldwide support, with an enterprise-class management framework and for tight integration into HP Quality Center and looking for advanced features, such as IAST.

Strengths

- HP is one of the pioneers of IAST with its SecurityScope (formerly Fortify Program Trace Analyzer) tool.

- HP is a recognized mind share and market share leader in the SAST market.
- HP's Fortify Software Security Center offers a technology for runtime application security protection (Real-Time Analyzer), which is a "software firewall" that resides inside an application to protect vulnerable locations within it, and can also monitor and report on application activity.
- HP's Fortify Software Security Center technologies are integrated into a single product offering and enterprise console, and are available as a product and also via a testing-as-a-service model.
- In addition to integration with its own SLC platform, HP Fortify Software Security Center technologies are integrated with IBM and Microsoft's SLC tools.
- HP provides out-of-the-box vulnerability shielding protection via integration with TippingPoint.
- HP Fortify Software Security Center has a large worldwide installed base, with customers in the U.S., Europe and Asia/Pacific.

Cautions

- The reputation of HP's DAST technology (WebInspect) has been damaged, by some degree, as the result of its suboptimal integration of SPI Dynamics into HP's structure and culture after its acquisition. The recovery process is under way, but more work remains.
- HP's application-security-testing-as-a-service offerings are not as well known as those from WhiteHat and Veracode, and may be less suitable for smaller engagements.
- HP must demonstrate its ability to execute against its vision to provide synergy with its entire portfolio of security capabilities: SAST, DAST, IAST, intrusion prevention system (IPS) and SIEM products.
- HP doesn't have the broad application security portfolio of IBM and is missing data and application security offerings, such as database activity monitoring (DAM), static data masking, dynamic data masking and XML gateway services.

IBM

IBM has a broad portfolio of application security technologies spanning DAST and SAST, as well as DAM and data masking. IBM was the first major application development vendor to acquire into DAST with its 2007 acquisition of Watchfire (an established, innovative DAST vendor at the time) and indicates that it now has more than 2,000 customers. IBM offers both DAST product and testing as a service with AppScan, although its testing-as-a-service capabilities are less well-known than its product. IBM's large installed base of developers (Rational and Eclipse) and quality assurance (QA) (Quality Manager and ClearQuest) provides a way for IBM to natively integrate and upsell AppScan's security testing capabilities. IBM's DAST capabilities should be considered by organizations looking for enterprise-class DAST capabilities delivered as a product, service or both, and looking for advanced capabilities, such as IAST and DAST/SAST correlation.

Strengths

- Its DAST and SAST testing results feed into the AppScan enterprise console for correlation of results.
- Even though IBM competes with HP for application and security testing, it provides native integration into HP Quality Center.
- IBM provides IAST capabilities with its "Glass Box" technology, introduced in 2011, which observes the application at runtime under test.
- For client-side JavaScript analysis, IBM uses its JavaScript execution engine (which emulates user interactions) and JavaScript Security Analyzer, which employs static and taint analysis of JavaScript code in conjunction with dynamic analysis.
- For client-side Flash and Flex code, AppScan uses a Flash execution engine that executes SWF files and simulates user interactions, as well as parsing, analysis and testing Adobe's Action Message Format (AMF)-based communications.
- AppScan's Web services testing can leverage IBM's Rational Web services/service-oriented architecture (SOA) testing suite and can observe SOAP flows and automatically generate the test based on this.
- AppScan includes a malware detection engine that scans for malware and malicious links as websites are scanned.
- IBM has a large worldwide installed base and customer support organization.

Cautions

- IBM's Glass Box IAST solution is only available on Java platforms.
- IBM's application-security-testing-as-a-service offerings are not as well known as those from WhiteHat and Veracode, and may be less suitable for smaller engagements.
- AppScan Enterprise contracts can be expensive; however, to compete at the lower end of the DAST market, IBM offers a stand-alone AppScan Standard edition starting at $9,000 per license.
- Although IBM's AppScan Enterprise console can report across DAST and SAST, it cannot be used to orchestrate the SAST tests directly.
- IBM must continue executing against its vision to provide synergy with its entire portfolio of security capabilities: SAST, DAST, IAST, IPS, DAM, data masking, SIEM, and identity and access management products.
- Customers cited a desire for improvements in reporting, as well as improved usability for developers to speed the resolution of identified issues.

Mavituna Security

Mavituna Security is a dedicated DAST product vendor providing a low-cost tool, Netsparker, that augments the security testing work of dedicated information security and pen-testing specialists. However, Netsparker lacks many of the enterprise-class capabilities requested by larger organizations. Netsparker should be considered by technically advanced security and testing professionals looking for ways to automate their testing efforts using a solid DAST technology at an extremely low cost.

Strengths

- Netsparker uses a combination of techniques to detect security vulnerabilities. It uses an embedded browser and JavaScript rendering engines to analyze HTTP responses for issues that are directly HTML related. Other issues are detected using signatures and specific task-related analysis engines.
- JavaScript applications are supported by simulating JavaScript and all related distributed output management (DOM) events in memory and observing outcomes (such as newly created content, executed attacks).
- To reduce false-positives, Netsparker uses a safe exploitation-based vulnerability confirmation engine to confirm most vulnerabilities.
- Customers cite ease of use as a differentiator.

Cautions

- Mavituna is a lesser-known provider and rarely appears on Gartner customer shortlists.
- It doesn't offer DAST testing as a service, SAST or IAST.
- Live support is not available 24/7.
- Mavituna does not offer out-of-the-box capabilities for integration with development/testing platforms typically requested for enterprise-class implementations.
- Netsparker does not support attacks that are specific to JavaScript.
- There is no explicit support for Flash/Flex or Silverlight; however, interaction of rich components with the Web application can be tested via the proxy mode feature.
- There is no Web services or WS-* protocol testing support.
- Generic XML-based remote procedure call (RPC)/API fuzz testing is not available.
- There is no WAF integration.

Mu Dynamics

Mu Dynamics is a smaller dynamic testing vendor that has focused on the dynamic protocol malformation and fuzz testing of embedded devices. Fuzz testing of embedded applications

appeals to operations (to test for performance, health monitoring and bugs) and security professionals (to test for vulnerabilities). Although not designed specifically to test Web-enabled applications, Mu Dynamics should be considered by information security, operational testing and penetration testing professionals looking for a protocol fuzz testing appliances with broad protocol support that complement traditional Web application scanning tools.

Strengths

- Mu Dynamics has stated coverage for 70 out-of-the-box standards-based protocols (such as SMB, SIP and CIFS) and the ability to use application traces (captured using an embedded version of Wireshark) for test scenario input when out-of-the-box support is not provided.
- Mu Dynamics fuzz testing appliance is capable of generating attacks based on known protocol vulnerabilities from the updated Common Vulnerabilities and Exposures database.
- The appliance provides recording, fuzzing and playback capabilities for comprehensive security testing and application-level distributed denial of service testing.
- Its appliance understands generic XML structures and can generate relevant tests for Web services and other types of RESTful XML-based APIs.
- Its integrated fault isolation mechanism helps to isolate and reproduce vulnerabilities.
- Customers cite ease of use and simplicity of its appliance model to achieve the desired testing and results.

Cautions

- Mu Dynamics is a lesser-known, specialized provider and rarely appears on Gartner customer shortlists.
- It provides a hardware appliance-based delivery model only. There are no pure software- or testing-as-a-service options.
- Customers indicate a desire for more scalability and throughput in order to test a large number of devices.

nCircle

nCircle is a privately held provider of a security and compliance auditing suite (Suite360), including a vulnerability management product (IP360), and was one of the first vulnerability management (VM) providers to expand into Web application vulnerability scanning based on customer requests to test Web applications as a part of their normal vulnerability scanning. For IP360 customers, WebApp360 provides a straightforward way to scan Web applications and meet compliance requirements, such as the Payment Card Industry's Data Security Standards (PCI DSS). nCircle's DAST capabilities should be considered by customers of IP360 looking for an inexpensive way to dynamically test applications for many security vulnerabilities and as a straightforward way to demonstrate compliance efforts, or for organizations looking for a combined VM/DAST solution. However,

nCircle's DAST capabilities should not be viewed as a replacement for testing performed by a full-fledged DAST solution from a dedicated DAST provider.

Strengths

- IP360 can identify all Web applications within an enterprise and, combined with WebApp360, can assess the entire stack (OS, Web platform and Web application) for security vulnerabilities.
- Most functionality of WedApp360 can be programmatically controlled through an XML-RPC API.
- Customers report WebApp360 is highly automatable and can scale to handle large jobs.

Cautions

- WebApp360 is not sold separately from IP360, so the offering will appeal only to nCircle's installed base.
- WebApp360 lacks the advanced DAST capabilities of the market leader’s offerings.
- There is no dedicated DAST as a service offering; however, WebApp360 is used as part of the nCircle Certified PCI Scan Service, which is a pure service offering.
- WebApp360 is designed for use postdevelopment, and there is no integration with SLC tools.
- There is no out–of-the-box integration with WAF vendors.
- Customers indicate slow scanning speeds. nCircle claims it is working on a variety of performance improvements.

NT OBJECTives

NT OBJECTives (NTO) is an innovative vendor with a strong focus on application security that offers a lower-cost DAST technology, NTOSpider. NTO has many capabilities typically associated with larger providers, such as available 24/7 support, an enterprise-class management and reporting console, out-of-the-box WAF integration, and the option to purchase DAST as a service. NTO is licensed and white-labeled by eEye as the foundation for its Web application scanning capability, and was licensed by Veracode as the technology behind Veracode's DAST-as-a-service offering. Stronger marketing, proven ability to scale, and long-term partnerships or acquisition by a committed larger vendor would help NTO increase its ability to execute and make its innovations available to a broader audience. Information security specialists and penetration testers looking for a technically advanced DAST solution capable of handling complex websites with extensive JavaScript usage should consider NTO.

Strengths

- Unlike most of the smaller DAST players in this Magic Quadrant, NTO offers DAST-as-a-service NTOSpider On-Demand, which delivered 40% of NTO's revenue in 2011.

- NTO offers centralized reporting and policy management for large enterprise deployments with scheduling, reporting and role-based access control.
- In 2011, NTO introduced NTODefend technology, which generates rules for intrusion prevention/detection systems and WAFs, with-out-of-the-box support for ModSecurity, Sourcefire Snort, Nitro Snort, Imperva and Deny All, and with explicit support for Barracuda, Citrix and F5 planned for January 2012.
- NTOCloud enables NTOEnterprise and NTOSpider On-Demand to create, track and use cloud-based scanning engines as an alternative to on-premises engines.
- NTOSpider provides out of the box for SLC integration with Visual Studio and Eclipse as well as Jira and Remedy for defect tracking.
- Customers report high levels of satisfaction with NTO's technical capabilities — specifically its ability to successfully crawl and test complex JavaScript-based websites and to deliver high accuracy in testing.

Cautions

- Although NTO is known to security specialists, it lacks widespread recognition among Gartner clients and rarely appears on shortlists.
- It has no SAST capabilities or partnerships.
- There are no IAST capabilities, although the company plans to release its IAST capability, NTODev, in March 2012 for .NET and Java.
- Veracode has started phasing out NTO's technology and replacing it with its own DAST technology.
- Advanced SOAP attack capabilities, WS-* support and SAML support are planned for 2012.

Parasoft

Parasoft is a self-funded, privately held company, and reports that it is profitable. Parasoft's policy-based approach is targeted toward automated defect prevention, with a goal of preventing vulnerabilities by identifying and remediating vulnerabilities as early as possible in the SLC. Parasoft has been in the application testing market for more than 20 years, offering a set of integrated tools for automated defect prevention (Static Code Analysis, Automated Unit Testing, Peer Code Review and Coverage Analysis), automated functional testing, integration testing and load testing targeted primarily at application development and QA professionals. As a part of this suite of offerings, Parasoft offers DAST (and SAST) capabilities; however, it doesn't actively target security professionals with these capabilities. Parasoft's DAST solutions should first be considered by its installed base, which may not be aware of Parasoft's security capabilities, and by developers looking for solutions focused on automated defect prevention with a set of integrated tools.

Strengths

- Parasoft has historical strength in the dynamic testing of SOA-enabled applications and Web services with its SOAtest offering, with full support for major WS-* standards.
- Parasoft has added IAST capabilities with its runtime error detection.
- Native integration for Eclipse, Visual Studio, Serena and other SLC platforms is provided.
- Geographically, Parasoft's sales and marketing reach beyond North America into Europe and Asia/Pacific.
- Parasoft's Concerto offering provides visibility, reporting and monitoring across all of Parasoft's testing offerings and provides integration for other tools via open APIs, including an option for correlating its DAST and SAST analyses.

Cautions

- Parasoft lacks market clout, as well as name and brand recognition among enterprise information security professionals, and rarely appears on shortlists of Gartner customers looking for DAST capabilities.
- Parasoft has not shown the rapid growth rate in security that newer vendors, such as Veracode or WhiteHat Security, have achieved in just a few years.
- Parasoft's WebKing DAST offering was functionally merged into its SOAtest offering, a name that doesn't clearly reflect its ability to dynamically test Web applications.
- Parasoft does not provide DAST as a service.
- There is no specific Adobe Flex/Flash or Microsoft Silverlight support.
- The company has no WAF integration or partnerships.

PortSwigger

PortSwigger is small, lesser-known, dedicated DAST provider offering a tool, Burp Suite Professional, targeted at augmenting the security testing work of dedicated information security and pen-testing specialists. However, Burp Suite Professional lacks many of the enterprise-class capabilities requested by larger organizations. PortSwigger should be considered by technically capable security and testing professions looking for ways to automate their testing efforts using a solid DAST technology at an extremely low cost.

Strengths

- PortSwigger offers a very low-cost DAST product ($275/user/year) targeted squarely at advanced security professionals.
- PortSwigger offers a free edition (Burp Suite), which it reports has more than 10,000 downloads per month, which it uses to refine and upsell to its commercially supported version.

Cautions

- PortSwigger indicates that it has only one person dedicated to its DAST offering.
- The purchase of a license for Burp Suite Professional does not entitle the user to product support. Any support is provided at PortSwigger's discretion.
- PortSwigger does not offer DAST as a service.
- PortSwigger does not offer SAST or IAST technologies.
- PortSwigger does not offer such capabilities as integration with development/testing platforms typically requested for enterprise-class implementations.
- PortSwigger does not provide any out-of-the-box WAF or IDS/IPS integration.
- PortSwigger does not target application developers or lower-skill-level security specialists.

Qualys

Qualys is a privately held, established managed security services provider that is best known for its flagship vulnerability management (VM) scanning-as-a-service offering, but it is less well known for its DAST capabilities. Qualys originally introduced its DAST as a service offering, Web Application Scanning (WAS) in 2010; however, the capability was quite limited. Qualys is now on the second generation of WAS, which was released in 2011 and was rewritten for automation and scalability on the Qualys security-as-a-service platform using the same common portal as all Qualys services. DAST services offer Qualys an ability to upsell to its VM installed base as a logical adjacency. The OS and Web application platform can be scanned for vulnerabilities with its VM service, and the Web application scanned with its DAST service, providing a "360 degree view" of Web application security. Qualys needs to prove that its v.2 DAST capabilities are scalable and provide accurate, useful results to regain the confidence of its v.1 adopters, and it needs to show continued momentum in v.2 adoption. Qualys' DAST capabilities should be considered by organizations looking for an inexpensive way to dynamically test applications for many security vulnerabilities and as a straightforward way to demonstrate compliance efforts. However, Qualys DAST services should not be viewed as a complete replacement for human-augmented security testing.

Strengths

- Even though Qualys provides DAST exclusively as a service, it uses an on-premises appliance option to keep scanning traffic local.
- Anti-malware scanning is optional.
- WAS has low, potentially disruptive pricing, with a list price of $499 per application per year for unlimited scans (in quantities this drops down to the $100 range) and includes 24/7 support.
- Qualys has the ability to upsell and bundle application vulnerability scanning to Qualys VM-as-a-service customers.

- Complex interactions and navigation scenarios are supported via Selenium integration.
- WAS results are available in XML via an open, RESTful API.
- Basic SOAP XML fuzzing is provided; however, JSON testing is slated for 2012.
- Customers report that the Qualys console is straightforward and easy to use.

Cautions

- Qualys only provides DAST as a service. There is no DAST product option.
- There are no IAST or SAST capabilities or partnerships.
- There is no option for human validation of the testing results for organizations that want it. The customer is responsible for all scanner configuration and vetting of the results.
- There are no pen-testing or business logic vulnerability testing options (these would require human involvement).
- There is no out-of-the-box SLC integration into bug tracking, development tools, workflows and so on.
- Out–of-the-box WAF integration is limited — Imperva only. F5 support is planned.

Quotium Technologies

Quotium is a small startup vendor based in EMEA offering an IAST-only solution, Seeker, designed to be used by developers in the development process, not by information security professionals. Quotium's Seeker was built from the beginning using a different approach to application security testing (IAST) that performs a runtime analysis of the application code to create and execute test scenarios for vulnerability testing, including memory and data flows of the application. If a vulnerability is found, Seeker provides the details of the verified vulnerability to the developer.

Quotium deserves close attention for its innovation in IAST and was identified by Gartner in 2011 as a Cool Vendor (see "Cool Vendors in Infrastructure Protection, 2011"), but needs to demonstrate rapid progress in executing on its vision, including making the tool more applicable to information security professionals. Quotium should be considered by application development professionals looking for an easier way to integrate DAST into the SLC with a tool that provides effective vulnerability detection and is relatively easy to adopt.

Strengths

- Quotium is the only vendor in this Magic Quadrant that focuses exclusively on IAST technology.
- Seeker offers visualization (a video-like replay) of an exploit, which helps in more-accurate remediation of the detected and confirmed vulnerabilities.
- Seeker's agents can be installed on multiple servers that execute a distributed application, enabling detection of vulnerabilities spread across multiple components, including the analysis

of applications that do not have user interfaces (for example, applications that directly call other applications; however, the first component of a distributed application still has to have a Web or Web services interface).

- Seeker can also analyze stored procedures, and supports the analysis of some vendors' proprietary database languages.
- Seeker includes out-of-the-box SLC integration, such as the ability to open a bug ticket, as well as integration with HP Quality Center, IBM ClearQuest and Microsoft Team System.
- Customers rate Quotium highly on ease of use, low false-positives and usable results that ease adoption in development.

Cautions

- Quotium has a small base of customers and has not proven yet its ability to scale.
- Seeker is not designed for use in production environments.
- Quotium does not offer DAST as a service.
- Quotium's Seeker IAST currently supports .NET and Java platforms, with PHP support planned for 2012, but does not support other Web platforms, such as Ruby and Python.
- Customers report that, when technical issues with the tool are encountered, the complexity of the tool requires vendor support.
- Customers cited vulnerability remediation workflow capabilities as an area for improvement.
- Testing of JavaScript and other RIAs is limited to what Seeker sees through its proxy recorder.

Veracode

Veracode is a smaller, venture-capital-backed startup vendor and is a pure-play application security testing service provider. Veracode has earned a strong reputation providing SAST as a service and is one of the SAST market leaders. However, it is less well known for its DAST capabilities. From 2008 until 2011, Veracode's v.1 DAST technology was licensed from NTO, and is currently being phased out. It is not expected that Veracode will fully replace its licensed technology with its own DAST technology until 2012. Veracode needs to prove that its DAST capabilities are as strong and accurate as its patented binary SAST code testing services. Veracode's DAST capabilities should be considered by information security professionals already using Veracode's static-testing-as-a-service offering or looking for a dedicated DAST-as-a-service offering as an alternative to other DAST solutions.

Strengths

- Veracode's v.2 of its DAST service was introduced in 2011 and is a fully automated service using a minimal amount of human augmentation for quality control with an objective of no more than 15% false-positives.

- Veracode stores the results of its analyses (as well as some application-related business context) in a persistent repository, which enables enterprise security intelligence (ESI)-like queries, providing application intelligence where customers can view trends, report by business units, benchmark against others in the industry, and view unified reports from DAST and SAST scans. In addition, the console has an optional integration with EMC's governance, risk and compliance (GRC) tool, Archer.
- Veracode offers APIs and plug-ins that enable customers to integrate Veracode remote testing results with customers' on-premises integrated development environments, build systems and bug-tracking systems.
- A new parallel scanning offering, DynamicMP, introduced in 2011, is built to leverage cloud-based computing resources (for example Amazon Elastic Compute Cloud) for running its scanning engines and is designed to quickly perform a one-time automated scan of large numbers of applications for a limited set of high-risk, high-confidence vulnerabilities at a price of $150 per website (500-scan minimum). Options are also available for scanning of all vulnerability types (one-time or unlimited).
- For DAST, Veracode has added support for Selenium script for recording and scripting authentication and how a Web application should be exercised. This aids SLC integration in organizations using Selenium in QA.

Cautions

- Validation services are not included with the base level of Veracode's automated DAST service. These are available and negotiated on a custom basis. If validation services are not included, it is expected that customers will need to verify the DAST results for further false-positive reduction.
- It generally does not sell its technology as a product (although, as an exception, it has implemented an on-premises service for government customers in the intelligence community). Many (if not most) other players sell their technologies as products and services, thus satisfying the needs of the clients that want to have one or the other, or both.
- Even though Veracode offers DAST and SAST, there is no integration or correlation between them, other than automatically merging the results together on the console and in reports.
- Customers report a desire for console improvements: more detailed, live-linked reports and the ability to see the progress of a given set of scanning requests in real time.
- Veracode has reference integrations for DAST for Bugzilla and Trac. Veracode has chosen not to have integrations with integrated development environments, such as Eclipse and Visual Studio for DAST (they do exist for SAST). Likewise, there is no native DAST integration into QA. Integration can be accomplished using the Veracode open API; however, customers indicate a desire for an easier, standardized API for DAST automation.
- For integration into the development process, a tighter turnaround target than the stated 24- to 72-hour turnaround goal would be useful.
- There are no automated record/replay vulnerability capabilities.

- The v.2 DAST engine built on Firefox Mozilla supports testing of JavaScript and other RIAs; however, the RIA code itself is not statically tested using Veracode's SAST technologies.
- There is no support for testing Web-service-enabled applications dynamically, although these are supported by SAST. XML fuzz testing and JSON are not supported.
- There is no WAF integration.

WhiteHat Security

WhiteHat Security is an early pioneer in DAST as a service, with a strong reputation and momentum for its testing-as-a-service model. WhiteHat Security offers multiple levels of service offerings at different price points (PreLaunch, Base Edition, Standard Edition and Premium Edition), including enterprise unlimited licensing for larger deals, most of which include some level of human interaction for configuration for in-depth testing. In 2011, a free SecurityCheck 30-day evaluation was introduced and has generated market uptake and upsell opportunities. In 2011, WhiteHat acquired a small SAST vendor, Infrared, to expand into SAST services in 2012. Successful launch of this service, as well as delivery of an IAST capability, will establish WhiteHat's vision in application security testing.

Strengths

- WhiteHat offers an on-premises appliance or virtual appliance option to provide network connectivity to internal Web applications; however, the testing and results are not kept locally.
- WhiteHat has introduced a service specifically targeted at preproduction/staging environments with a 24-hour turnaround goal, unique to the testing-as-a-service providers.
- All vulnerabilities, regardless of service offering, are manually verified and confirmed exploitable by WhiteHat's security engineers.
- All pricing includes an unlimited number of scans per year, per application.
- WhiteHat provides an XML-based RESTful API for SLC integration, and also offers a native connector for Jira bug tracking.
- Generic XML fuzzing and JSON support over HTTP are available.
- WhiteHat provides basic benchmarking and visibility into security, as compared to peers with more detailed comparative information to be exposed in 2012.
- Native WAF integration with F5 and Imperva is offered, as well as Sourcefire's Snort IPS engine; others can be supported via XML API.
- Customers report very few, if any, false-positives.

Cautions

- DAST is offered as a service only, not as a DAST product option.

- There are no current SAST testing capabilities. The 2012 planned offering is unproven, and service levels are unknown. The planned SAST technology is language-specific and will only support Java initially, with .NET C# support planned for 2H12.
- There is no road map for truly integrated DAST/SAST or IAST.
- There is limited out-of-the-box native integration with SLC tools.
- The ability to perform basic testing of RIA (JavaScript, applets and so on) is included in every version of Sentinel; however, advanced testing requires security engineer involvement and, thus, requires WhiteHat's Premium Edition level of scanning service. Attack browser and DOM scanning capabilities are planned for 2012.
- Customers indicate a desire for better integration with development to quickly and effectively communicate vulnerability details to developers.

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.

Added

This is a new Magic Quadrant, so all vendors are new.

Dropped

No vendors have been dropped, because this is a new Magic Quadrant.

Inclusion and Exclusion Criteria

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

- Vendors must provide a DAST capability — tool, subscription-based service or both. Typically, these solutions are designed for the purpose of testing Web-enabled applications, but this is not a requirement.
- Solutions must have been generally available as of July 2011.
- The vendor's revenue must exceed $1 million, or the vendor has at least 10 customers that have deployed its products/services into production.
- Vendors must also be determined by Gartner to be significant players in the market, because of market presence or technology innovation.

- Open-source DAST offerings were not considered for this Magic Quadrant unless a commercially supported version was available

Excluded

Open-source technologies: Several of the vendors reviewed in this Magic Quadrant have low-cost or no-cost offerings that compete with pure open-source offerings. However, there are several pure open-source tools available for DAST that were not included in this evaluation (see Note 1). Larger clients have indicated that these tools provide useful capabilities to their internal pen-testing teams, in addition to more-formalized DAST solutions from commercial solutions discussed in this Magic Quadrant. However, clients have indicated that the lack of enterprise-class scalability, management and reporting inhibits their wider adoption. Also, the lack of service and support from a named vendor is also an issue. These solutions tend to be used by organizations with limited budgets, but with adequate human resources to work within the limitations of the solutions. Organizations that have large, internal pen-testing organizations should consider the use of these tools to help automate their manual testing processes.

Pen-testing solutions: There is a small market for solutions that are designed specifically to augment human-based full stack penetration testing of networks, OSs and applications. For example, Core Security Technologies' Core Impact. These tools were not evaluated as a part of this Magic Quadrant.

Application security testing boutique consultancies: For application testing service providers, this Magic Quadrant has a requirement of providing repeatable, subscription DAST testing services. Vendors offering custom pen testing, professional services, consulting or other nonsubscription DAST solutions were not evaluated. Many offer DAST testing professional services, but do not offer the repeatable subscription DAST testing like the services provided by vendors such as Veracode, WhiteHat and Qualys. There are dozens of these types of service firms. Examples of some of the larger specialized application security testing consultancies include Cigital, Denim Group and Security Innovation.

Network vulnerability scanners: Several of the network vulnerability-scanning tool vendors now offer DAST capabilities. However, testing a network and software stack for missing patches and known vulnerabilities is a different problem than testing application code for unknown and yet-to-be-discovered vulnerabilities. Unless the vendor makes a significant commitment and investment to deliver DAST capabilities, these solutions provide only basic Web application testing using signature-based Web scanning, lack most of the advanced features discussed in this Magic Quadrant, and appeal primarily as an upsell to its vulnerability management installed base. The solutions are most commonly used as a quick way to claim compliance with regulations such as PCI:

- **Tenable and Rapid7 —** These vendors provide only basic dynamic application testing capabilities and do not position themselves as DAST providers.

- **eEye —** In conjunction with its vulnerability scanning offering, it has added Web application scanning technology licensed and white-labeled from NTO. The capabilities of this offering are covered in the section on NTO.

Evaluation Criteria

Ability to Execute

Product/Service: This criterion evaluates the vendor's core DAST 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 (such as QA/testing specialists, as well as information security specialists), appeal with security technologies other than DAST (regardless of whether they are application-security-related), and offering product and DAST 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 dynamic testing market and in a broader application security space; DAST revenue amount; DAST expertise; the number of DAST customers, and the number of installed and used DAST products; and the likelihood that the vendor will be successful in its acquisition and/or partnership deals.

Sales Execution/Pricing: We account for DAST 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 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 DAST 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 DAST (and broader application security) offering to enterprises' functional requirements, and the vendor's track record in delivering new, innovative features when the market demands them.

Customer Experience: This is an evaluation of the 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/Service	High
Overall Viability (Business Unit, Financial, Strategy and Organization)	Standard
Sales Execution/Pricing	Standard
Market Responsiveness and Track Record	High
Marketing Execution	No Rating
Customer Experience	Standard
Operations	No Rating

Source: Gartner (December 2011)

Completeness of Vision

Market Understanding: We evaluate the vendor's ability to understand buyers' needs and translate them into products and services. DAST vendors that show the highest degree of market understanding are adapting to customer requirements in areas such as comprehensiveness of application security technology coverage that expands beyond DAST, offering SAST in addition to DAST, integrated DAST/SAST capabilities that go beyond post factum correlation, the ability to test next-generation RIA applications, and the ability to test mobile and cloud applications and the ease of DAST tools' native integration with multiple, popular SLC platforms — most notably in QA for DAST. 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 DAST product options and testing as a service with unified visibility and reporting across both.

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

Offering (Product) Strategy: We assess the vendor's approach to product development and delivery. This addresses the vendor's focus on security analysis; the optimal balance between satisfying the needs of leading-edge (that is, Type A) enterprises, and Type B (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 externally

accessible Web applications and embedded hardware devices with specialized protocol dynamic testing requirements).

Innovation: Here, we evaluate the vendor's development and delivery of a solution that is differentiated from the competition in a way that uniquely addresses critical customer requirements. We give a higher rating to vendors evolving toward ESI enablement 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). We give a higher rating to vendors that offer DAST and SAST, correlation of DAST and SAST, as well as offering IAST. DAST solutions should provide a variety of options for testing — stand-alone engines for security professionals, integration into development tools for developers, 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. 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'; and DAST for mobile and next-generation RIA platforms (see Table 2).

Table 2. Completeness of Vision Evaluation Criteria

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

Source: Gartner (December 2011)

Quadrant Descriptions

Leaders

Leaders demonstrate balanced progress in execution and vision. Their actions raise the competitive bar for all vendors and solutions in the market, and they tend to set the pace for the industry. A Leader's strategy is focused on the security of applications; its offering addresses the needs of application security specialists within the SLC, as well as the specific needs of information security professionals; and its brand is broadly recognized in the application security space. Leaders reach beyond DAST capabilities and encompass the broader application security discipline, including SAST and IAST capabilities offered as both a product and as a service. Leaders also understand the requirements of large application security programs with enterprise-class features such as application security governance, policy management, progress metrics, visibility across DAST and SAST testing on-premises and as a service, role-based access control via integration with enterprise directories, and the ability to view and prioritize vulnerabilities by risk and business impact. At the same time, Leaders are able to amass a relatively large clientele and revenue in this maturing market. A leading vendor is not a default choice for every buyer, and clients are warned not to assume that they should only buy from Leaders. Some clients may find that vendors in other quadrants better address their specific needs.

Challengers

Challengers typically offer DAST solutions, but haven't yet expanded into SAST, IAST or broader application security portfolio capabilities. They may offer DAST as a service or a product only instead of offering both. Their primary emphasis is on the dynamic testing of applications for security vulnerabilities, typically targeted at the information security professional. Challengers are able to sell application security to security professionals, yet they experience security brand recognition issues when reaching beyond their installed base into application development. Challengers have solid technologies that address the general needs of users. They are good at competing on foundational DAST capabilities, rather than on advanced features and/or broader ranges of application security products and services. Challengers are efficient and expedient choices to address narrowly defined problems.

Visionaries

Visionaries invest in the leading-/bleeding-edge features that will be significant in the next generation of DAST solutions and typically offer a broader range of application security solutions, and they will give buyers early access to greater security assurance and advanced capabilities. Visionaries can affect the course of technological developments in the market (for example, advanced testing of RIA, SAST capabilities or delivery of IAST), but they lack the ability to execute against their visions compared with the market leaders. Enterprises typically choose Visionaries for their best-of-breed, evolving features. Other vendors watch Visionaries as indicators of innovation and thought leadership, attempting to copy or acquire their technologies.

Niche Players

Niche Players offer viable, dependable solutions that meet the needs of specific buyers. Niche Players are less likely to appear on shortlists, but they fare well when considered for business and technical cases that match their focus. For example, some of the specialized vendors in this quadrant focus on dynamic testing of embedded applications using extensive protocol malformation and fuzz testing. Others in this category add Web application scanning as an upsell to their vulnerability management offerings for a straightforward way to meet compliance requirements. Others focus on technical capabilities and are designed for use by information security professionals and pen testers. Niche Players may address subsets of the overall market, and often can do so more efficiently and effectively than the Leaders. Enterprises tend to choose Niche Players when the focus is on a few important functions or on specific vendor expertise, or when they have an established relationship with the vendor.

Context

As organizations have improved the security of their network, desktop and server infrastructures, there has been a shift to application-level attacks as a way to gain access to the sensitive and valuable information they handle, or to use a breach of an application to gain access to the system underneath. In addition, there has been a shift in attacker focus from mass "noisy" attacks to financially motivated, targeted attacks. As a result of these trends, application security has become a top investment area for information security organizations, whether improving the security of applications developed in-house, procured from third parties or consumed as a service from cloud providers.

Application security testing solutions are designed to help organizations identify application-level vulnerabilities in all applications, whether developed in-house, outsourced or acquired. Their use should be considered mandatory by all organizations and all service providers. At a high level, application security testing tools fall into two broad categories: DAST and SAST solutions. DAST solutions are the focus of this Magic Quadrant. Originally designed for the detailed analysis of security vulnerabilities in running Web-based server applications, DAST solutions are increasingly being applied to testing client-side application logic within browsers and embedded applications. DAST contrasts with, and increasingly complements, SAST, a less mature security testing technology that examines the code of applications in a nonrunning state.

DAST market consolidation continues, and the market now offers DAST technologies from large application development platform vendors; point solutions from small, innovative startups; as well as a number of open-source DAST tools. Multiple providers offer dynamic-testing-as-a-service options, some exclusively. In addition, most of the larger providers offer DAST as well as SAST solutions for the broadest possible security testing of applications.

Market Overview

DAST solutions test applications in a running state from the "outside in." 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 — independent of the language or platform the application was developed on. This is in contrast to SAST solutions (see "Magic Quadrant for Static Application Security Testing"), which analyze the binary, byte or source code of an application from the "inside out" to identify coding conditions indicative of a security vulnerability.

Enterprises should understand the importance of application security vulnerability testing — dynamically and statically. All Web-enabled applications — whether internally developed, procured, outsourced or cloud-based — should be tested. As discussed in "Hype Cycle for Application Security, 2011," the adoption of DAST solutions, primarily in the form of Web application testing tools, has been rapid and is more mature than SAST.

Despite the widespread adoption of DAST solutions, the market continues to evolve, and new approaches are technologies are required for DAST solutions to test next-generation mobile, RIA and embedded applications (see "Key Trends in Application Security Testing"). The major trends shaping the market are discussed below.

Expansion of Dynamic Testing as a Service

Most of the larger vendors in this Magic Quadrant offer DAST as a service. In fact, several of the vendors (Qualys, Veracode and WhiteHat) offer only testing-as-a-service capabilities and do not offer their tools for sale independently. Increasingly, organizations tell us they prefer to use a product *and* a service from the DAST vendor — for example, testing their more-sensitive applications on-premises using a DAST product, and testing their less-sensitive applications via DAST 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 DAST products.

There are pros and cons with DAST testing as a service that must be fully considered. Testing-as-a-service offerings are appealing to enterprises for multiple reasons:

- Capital savings and savings on hiring, training and human resource management
- Pricing based on consumption
- Ease of trial and adoption
- Bridging dispersed business units and geographical locations
- Working through a backlog of deployed applications
- Options for less-expensive, more-frequent and less-intensive scans of applications
- Several DAST providers refine the results of their testing with skilled human analysis of the results to reduce the number of false positives associated with the technology
- Visibility across multiple enterprises to provide benchmarking metrics
- Pure cloud providers should have the potential to innovate and deliver enhancements more quickly

However, an exclusively service-based model for DAST poses a number of problems for organizations:

- They will likely require access the organization's internal network where more-sensitive applications reside.
- Enterprises may want more-comprehensive scans than the service provider offers.
- The service provider will have intimate knowledge of an application's vulnerabilities.
- Full testing of an application may require the disabling of security mechanisms — for example, two-factor authentication or enterprise directory integration.
- Information security specialists and penetration testers may find it difficult or impossible to perform customized inspections remotely.

Scans should be able to be submitted individually or in bulk, and scheduled so as to minimize the impact on production applications via a console interface or remotely automated via an API interface. Further, once a scan is submitted, the DAST service provider should provide some visibility as to the progress of a given scan or set of scans. Defining boundaries and establishing service-level agreements, feedback, handoffs and collaboration between the enterprise and the testing provider are essential, including how authentication, authorization and role-based access control will be handled as developers and other users consume the test results.

The Importance of Testing RIA and HTML5

The creators of client-side code have a responsibility to their users and customers and the Internet community to ensure that their code is adequately secure. Increasingly, Web-enabled applications involve rich client-side interfaces for end users. A hallmark of Web 2.0 applications is the use of RIA, mostly in the form of JavaScript (The "J" in Ajax) and Ajax frameworks. In addition, many applications include large amounts of client-side logic in the form of Adobe Flash, Flex, and Microsoft's Silverlight. More recently, interest has shifted to the use of HTML5 for RIA. In all cases, the use of client-side RIA logic complicates how traditional DAST testing is performed, since the JavaScript and other types of code are rendered at the client, not at the server.

Where the client-side logic is exercised, DAST solutions that use embedded attack browsers based on Mozilla or WebKit (in contrast to a pure proxy model) have an advantage as they are able to quickly adapt and support the testing of advanced JavaScript, HTML5 and so on as a direct benefit of using an open-source, third-party rendering engine (as the engine is updated, the DAST solution benefits). Because RIA platform vendors such as Adobe and Microsoft recently have favored HTLM5 over their proprietary platforms, the importance of understanding and testing HTML5-enabled applications will become a strategic differentiator for DAST solutions.

You cannot attack and assess what you cannot see and crawl. It is important that DAST solution providers also offer the ability to inventory and discover Web-enabled applications that the information security organization may not be aware of, including those inside of the perimeter firewall. Leading DAST 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 SSL certificates. Likewise, the DAST solution must be able to crawl complex Web applications,

which is increasingly challenging, because more and more Web navigation is driven by RIA constructs.

The Importance of Testing Mobile, Cloud and Web Services Applications

An emerging requirement for DAST solutions is the ability to test mobile applications. Ideally mobile applications would be tested with SAST and DAST; however, pure DAST testing can add value. Beyond the use of RIA and HTML5 discussed previously, 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. At a minimum, the exposed interfaces of the applications should be testable using DAST. Many of the mobile applications communicate with cloud-based applications on the back end, which must also be tested —by the enterprise contracting for the services or the cloud provider being required to show proof of dynamic (and ideally static) security testing of their services. The ability of a DAST testing tool to test RESTful HTTP interfaces is increasingly important, as well as the ability to monitor and observe an application in use so that intelligent protocol fuzzing can be performed. This becomes a key requirement as mobile users and applications access enterprise data and applications via these interfaces.

In addition to RESTful HTTP, advanced DAST tools 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.

For the testing of mobile applications, there is a requirement for DAST 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 different interfaces for different mobile clients to ensure the entire surface area of the application is tested for vulnerabilities.

SLC Integration and Alternative Interfaces for Developers

As responsibility for DAST testing expands from information security into the development organization, the importance of role-based views into testing results or, ideally, providing native integration into the development environment becomes increasingly important. The testing needs of an information security professional are quite different than someone in QA. Leading DAST solutions offer interfaces customized for each, or offer native integration into application development environments.

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 DAST tools as early in the development phase as possible when an application can be tested in its running state. When used during development, most often, DAST would take place in the QA process, where other types of black box testing are performed by QA testers or as part of a preproduction release process. In both cases, applications can be tested more thoroughly without the fear of impacting a production application. Most organizations will

prefer having DAST capabilities tightly integrated with their QA platforms, such as HP Quality Center, or at unit build via integration with build platforms such as Maven.

For complex navigation, many QA organizations already use tools — such as Selenium — to record and replay interactions. DAST tools need a similar capability and ideally would consume the navigation scripts generated by the same record/replay tools used by the QA organization. In addition, vulnerabilities found with DAST should be able to be placed into the organization's standard bug-tracking systems, such as Jira and Bugtraq. Even if DAST is procured via software as a service/cloud, having it tightly integrated with the SLC process/platform for remediation purposes is highly desirable.

Delivering Against the Vision of ESI

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

ESI enablement is based on two critical elements: (1) the interaction of technologies, and (2) the integration and correlation of information. When combined, these provide *contextual assessments* that enable *optimal security and risk management* The goal of delivering ESI becomes an important strategic criteria to evaluate DAST solutions in three important ways:

1. At a minimum, DAST solutions can improve the accuracy of their results by instrumenting the application under test delivering IAST (see "Evolution of Application Security Testing: From Silos to Correlation and Interaction"). Specifically, a software agent is deployed to the Web 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 — for example, identifying the specific line of code where a security vulnerability occurred, or providing detailed visibility into code coverage. However, IAST also requires that an agent be deployed on the application platform, which relegates the technique largely to QA and also requires that the vendor explicitly support the platform or language being instrumented (such as PHP, Java or .NET). Some of the vendors evolving their offerings in this direction and offering IAST include Acunetix, HP, IBM, NTO, Parasoft and Quotium. In addition to IAST, some vendors offer both DAST and SAST testing solutions — IBM, with its AppScan DAST and SAST technologies, HP, with the acquisition of SPI Dynamics for DAST and Fortify for SAST and Parasoft. Veracode offers both DAST and SAST as a service, and another DAST service provider, WhiteHat, acquired a SAST technology provider, Infrared, in 2011, but hasn't yet released its SAST capability.
2. In addition to the interaction of DAST/SAST, it is also valuable to have some level of interaction and integration of dynamic security testing tools and WAFs, and 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 DAST solutions) using runtime protection devices. 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. Leading DAST solutions offer this type of native WAF integration out

of the box, with predefined rule set creation specific to leading WAF platforms, such as Imperva, Citrix, F5 and others. For IPS integration, output to various Snort implementations is available. Once a WAF/IPS rule is in place, leading DAST solutions can replay the specific attack that identified the vulnerability to confirm that WAF/IPS is effective in blocking it.

3. Another foundational element of ESI is the integration and correlation of security information and contextual information into a queriable persistent repository. Security analysis results collected by DAST (and SAST) technologies, 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.

Recommended Reading

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

"Magic Quadrants and MarketScopes: How Gartner Evaluates Vendors Within a Market"

"Magic Quadrant for Static Application Security Testing"

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

"Prepare for the Emergence of Enterprise Security Intelligence"

"Application Security Technologies Enable Enterprise Security Intelligence"

"IBM Strengthens Its Application Security Testing Portfolio With Ounce Labs"

"HP's Acquisition of Fortify Confirms Trend Among SLC Vendors"

"Hype Cycle for Data and Application Security, 2010"

"The Future of Information Security Is Context Aware and Adaptive"

"Key Technology Trends in Application Security Testing Markets"

"Key Process Trends and Best Practices in Application Security Testing Markets"

"Toolkit: Checklist for 360-Degree Application Security Assessment"

"Toolkit: Best Practices Checklist for Secure Application Development"

"Toolkit: Checklist for Application Security Skill Management"

"Toolkit: Application Security Testing Checklist for Outsourced Application Development and Maintenance"

"Toolkit: Decision Frameworks in Application Security"

"Toolkit: Sample RFP for DAST Tool Selection"

Note 1 Example Open-Source DAST tools

- Nikto
- Open Web Application Security Project (OWASP) WebScarab
- Google ratproxy and skipfish
- w3af
- Websecurify

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

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

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

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

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

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

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen 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.

Regional Headquarters

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

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600