Magic Quadrant for Application Security Testing

Published: 28 February 2017 **ID:** G00290926
Analyst(s): Dionisio Zumerle, Ayal Tirosh

Summary

Security testing is growing faster than any other security market, as AST solutions adapt to new development methodologies and increased application complexity. Security and risk management leaders must integrate AST into their application security programs.

Strategic Planning Assumptions

By 2019, 80% of application security testing vendors will include software composition analysis in their offerings, up from 40% today.

By 2019, enterprise IAST adoption will have exceeded 30%; however, runtime application self-protection (RASP) adoption will be no more than 10%.

Market Definition/Description

Gartner defines the application security testing (AST) market as the buyers and sellers of products and services designed to analyze and test applications for security vulnerabilities. Gartner identifies three main styles of AST:

Static AST (SAST) technology analyzes an application's source, bytecode or binary code for security vulnerabilities, typically at the programming and/or testing phases of the software development life cycle (SDLC).

Dynamic AST (DAST) technology analyzes applications in their dynamic running state during testing or operational phases. It simulates attacks against an application (typically web-enabled applications and services) and analyzes the application's reactions to determine whether it is vulnerable.

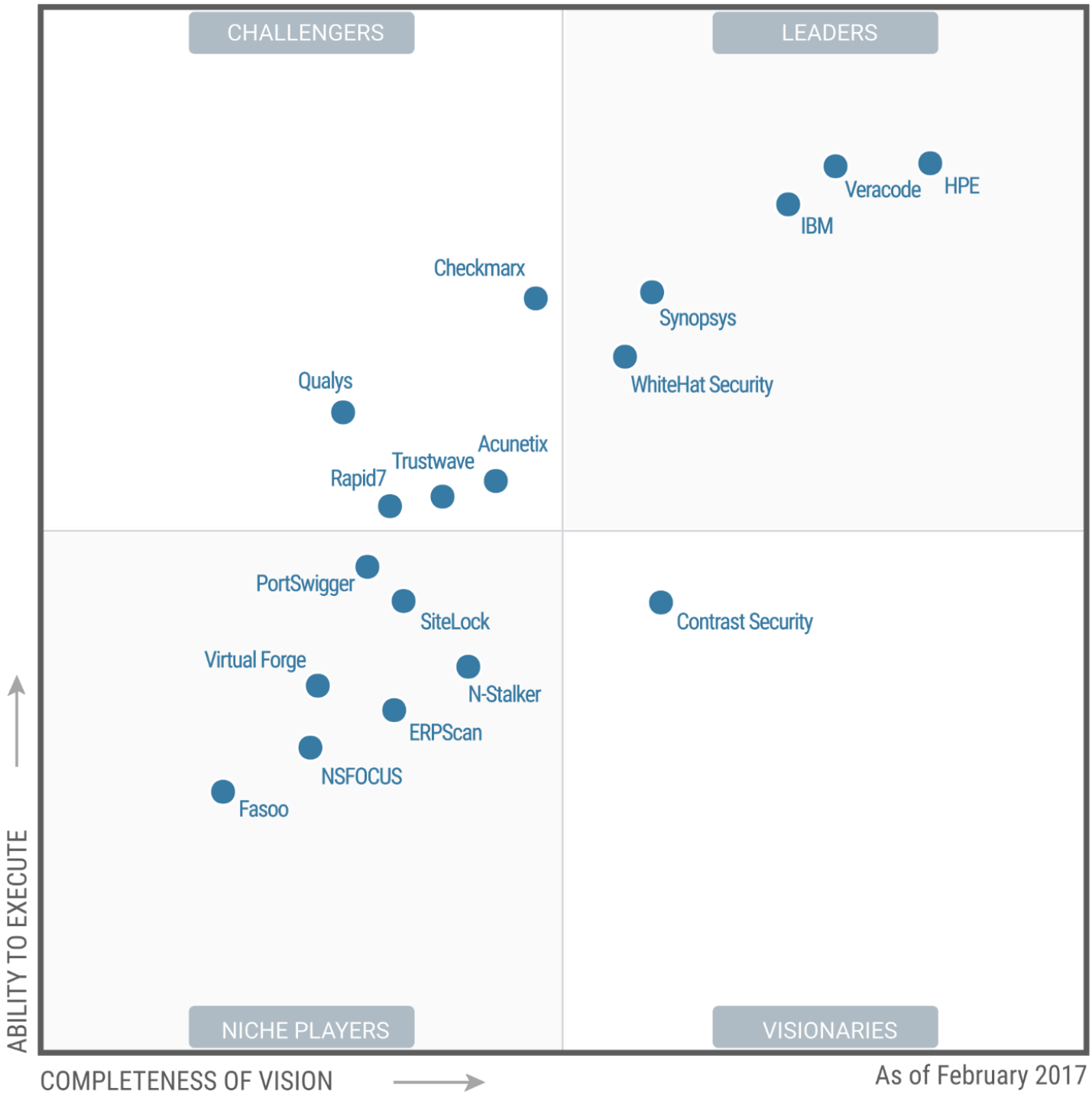
Interactive AST (IAST) technology combines inside-out observation of a running application being tested with DAST simultaneously. It is typically implemented as an agent within the test runtime environment (for example, instrumenting the Java Virtual Machine [JVM] or .NET CLR) that observes operation or attacks from within the application and identifies vulnerabilities.

All of the above technology approaches can be delivered as a tool or as a subscription service. Many vendors offer both options to reflect enterprise requirements for both a product and service. The majority of enterprises that develop applications employ some form of AST, but the various technologies differ in adoption and maturity. DAST and SAST are the most widely adopted, while IAST adoption is still growing.

This Magic Quadrant focuses on a vendor's SAST, DAST and IAST offering, maturity and features as tools or as a service. AST vendors innovating, partnering, and offering RASP (a technology for allowing applications to protect themselves from vulnerability exploitation at runtime) or software composition analysis (SCA; a technology used to identify open-source and third-party components in use in an application and their known security vulnerabilities) were weighted more heavily. Also, although mobile application security testing, intended as AST for applications that run on mobile platforms (such as iOS and Android), was kept out of the scope of the Magic Quadrant for this year, vendors that provide mobile AST were valued in terms of their AST innovation.

Magic Quadrant

Figure 1. Magic Quadrant for Application Security Testing



Source: Gartner (February 2017)

Vendor Strengths and Cautions

Acunetix

Acunetix is a Malta-based provider of DAST and IAST with a strong presence in the North American and European markets. Its primary offering is an on-premises vulnerability scanner (formerly referred to as Web Vulnerability Scanner [WVS] and now called Acunetix). Its Acunetix Online service delivers Acunetix as a service (formerly referred to as Online Vulnerability Scanner [OVS]). Acunetix provides integrated IAST via AcuSensor for PHP and .NET. Acunetix also provides a free suite of manual tools that includes an HTTP Fuzzer and HTTP Sniffer.

Over the last 12 months, Acunetix has centered its efforts on providing a new dashboard, improving reporting and management of vulnerabilities, as well as improving multiuser and multirole capabilities. Acunetix has also added SDLC and web application firewall (WAF) integration options.

Acunetix should be considered by organizations looking for DAST with advanced functionality and integrated IAST, as well as organizations seeking a tool for manual web penetration testing.

STRENGTHS

Acunetix has a strong reputation for its extensive DAST capabilities, such as being able to parse complex client-side JavaScript applications to test for vulnerabilities via its DeepScan crawling technology.

Acunetix's AcuMonitor can identify vulnerabilities that do not provide any response to a scanner (for example, blind cross-site scripting [XSS]) by providing the scanner with access to an intermediary service that monitors the application over time for vulnerabilities.

Acunetix offers integrated IAST included at no additional cost with both of its offerings.

CAUTIONS

Acunetix does not have SAST capabilities, nor does it partner to offer these.

Acunetix and Acunetix Online do not share policies and configurations for organizations that may use both.

Checkmarx

Checkmarx is an AST vendor based in Israel with a strong reputation for its SAST solution. Checkmarx has significant presence in North America and Europe, while it also serves the Asia/Pacific (APAC) region. Checkmarx provides CxSAST, which is a SAST product with broad language coverage that provides a variety of options to customize it for specific applications. Checkmarx also provides SCA under the name of Checkmarx Open Source Analysis, and AppSec Coach, which is a developer education platform for secure coding. Checkmarx Managed Services provide services to help development organizations integrate application security testing within their SDLC.

Over the last 12 months, Checkmarx has introduced AppSec Coach as an in-workflow developer education platform for application security and secure coding training. It has added analysis of open-source components via its Checkmarx Open Source Analysis offering as a result of its partnership with WhiteSource. Checkmarx has also experienced significant growth and has obtained substantial market share in the SAST space.

Checkmarx appeals to application development and security organizations that are seeking a comprehensive SAST tool for a variety of programming languages and frameworks, with advanced customization possibilities, low turnaround times and a full set of options for integration in the SDLC.

STRENGTHS

Checkmarx offers one of the strongest SAST technologies, which supports a broad variety of programming languages and frameworks beyond only the most common ones, such as Java and .NET.

Checkmarx has one of the most complete integrations in the SDLC, including source code repositories, build systems, bug-tracking systems, integrated development environments (IDEs) and quality assurance (QA) testing tools.

The SAST tool can test composite applications, and provide scalability and quick turnaround times via incremental and parallel tests, as well as the ability to write custom queries to discover vulnerabilities or check for code adherence to secure programming best practices.

Checkmarx gets very good marks from users for ease of use and low learning curve.

CAUTIONS

Even though Checkmarx partners with Rapid7 for DAST, Checkmarx's focus on SAST makes them less suitable for situations where an all-in-one suite is desired.

Checkmarx's IAST solution is in beta, while its RASP technology did not come out of beta.

While Checkmarx offers a cloud-based version of its SAST product, the majority of clients use the on-premises tool.

Its SAST integration with WAFs supports only ModSecurity, and not popular commercial WAFs.

Contrast Security

Contrast Security is an AST vendor based in the U.S. It has presence in the North American market while also serving the European and APAC regions. Contrast Security offers its IAST (Contrast Assess), RASP functionality (Contrast Protect) and SCA from a single platform. Contrast Assess and Contrast Protect can be licensed independently, while SCA is part of Contrast Assess. Contrast also offers a central management console, the Contrast TeamServer, which can be delivered as a service or on-premises.

Over the last 12 months, Contrast Security added SDLC integration options and support for Node.js, and made efforts to increase the scalability of its solution. Also, Contrast Security showed strong growth and closed another round of funding in September 2016.

Contrast is a good fit for organizations pursuing a DevOps methodology and looking for innovative approaches to insert automated, continuous security testing that is transparent to developers and testers.

STRENGTHS

Contrast Security offers a self-testing model, where security testing is driven by any application test (typically QA) that is executed automatically or manually, and well suits rapid DevOps-style development. This process is transparent to developers and security specialists, and does not require training.

Contrast Security has a strong presence on IAST shortlists. Clients highly rate the vendor's support, responsiveness and ease of use.

Contrast's solution allows customers to leverage the instrumented agent to add or enhance security logging, delivering security analytics for production applications.

CAUTIONS

Contrast Security does not provide SAST or DAST tools or services.

Contrast Security is currently limited to testing of applications written in Java, .NET, ColdFusion and Node.js.

Contrast Security does not observe and analyze client-side logic executed in the browser only (for example, JavaScript or Java applets), and therefore cannot identify vulnerabilities such as JavaScript-based Document Object Model (DOM) XSS.

Contrast does not integrate out of the box with popular WAFs.

ERPScan

ERPScan is an AST vendor headquartered in the Netherlands with a platform for the security of ERP systems. ERPScan has a strong presence in the European and North American markets, while also serving the Asia/Pacific region. The ERPScan Security Monitoring Suite is available on-premises for detecting vulnerabilities and misconfigurations in SAP and Oracle PeopleSoft applications. The vendor also offers services for code reviews, SAP penetration tests and audits. It has a strong background in security research of SAP systems and a recently introduced SAP Cyber Threat Intelligence report.

ERPScan is a new addition to the Magic Quadrant. ERPScan will appeal to security teams trying to assess the security of their large-scale SAP and PeopleSoft applications, particularly in organizations that have extended and customized their environments.

STRENGTHS

ERPScan offers SAST for Advanced Business Application Programming (ABAP), PeopleCode and Java applications over ERP frameworks. It is the only vendor in the Magic Quadrant to include specialized tests for PeopleCode, and one of the very few to test ABAP code. ERPScan offers automated code corrections that can be applied to a large percentage of detected vulnerabilities.

The ERPScan Security Monitoring Suite offers vulnerability management capabilities such as secure configuration, checks for missing security patches and vulnerable programs (delivering SCA functionality), and segregation of duties (SOD) checks, frequently requested alongside security testing of SAP and PeopleSoft code. ERPScan can correlate findings from static analysis with the results of configuration management and access control checks.

Clients highly rate the vendor's strong support and comprehensive expertise with SAP and PeopleSoft applications.

CAUTIONS

ERPScan's SAST support is limited to ABAP, Java and PeopleCode. ERPScan does not partner for SAST for other programming languages, and lacks out-of-the-box integration with popular IDE and bug-tracking tools. However, it does integrate with ThreadFix, which can import and aggregate results from other SAST tools.

Although ERPScan offers penetration testing services and dynamically analyzes secure configuration, it does not offer DAST within its product offering.

ERPScan does not offer IAST.

Fasoo

Fasoo is a provider of data and software security solutions, with global headquarters in South Korea and North American headquarters in New Jersey. Fasoo's SAST solution, Sparrow SCE, launched in 2009. Fasoo also provides Sparrow QCE, which is focused on quality assurance. Sparrow SCE is generally offered as an on-premises solution; however, Fasoo also provides Sparrow on Cloud.

Fasoo is a new addition to the Magic Quadrant and is one of the few solutions to support South Korean government requirements for AST products. Fasoo Sparrow SCE is a good option for APAC-based enterprises that need an on-premises SAST solution.

STRENGTHS

Fasoo is very visible in the APAC region and especially South Korea, where its compliance to local regulatory requirements gives a competitive advantage compared to external players.

Fasoo receives praise from its customers for its ability to customize and its support for complex enterprise systems.

Sparrow's Active Suggestion provides sample code to fix identified vulnerabilities.

CAUTIONS

Fasoo has no AST presence outside the APAC region, and very limited presence outside South Korea.

Fasoo does not have a DAST or IAST solution.

Fasoo customers advocate for UI improvements in the solution.

Fasoo has limited integration with SDLC and infrastructure, such as WAF.

HPE

Hewlett Packard Enterprise (HPE) is a U.S.-based global provider of AST products and services under the Fortify brand. HPE offers Static Code Analyzer (SAST), WebInspect (DAST and IAST), Software Security Center (its console) and Application Defender (monitoring and RASP). HPE provides its AST as a product as well as in the cloud, with Fortify on Demand. DevInspect combines HPE's SAST with real-time, in-line vulnerability detection via a spell-checker (called Security Assistant) in the Eclipse IDE. Security Assistant highlights vulnerable code as the developer programs. It is also available in other versions and license models of the SAST solution.

In September 2016, HPE announced that it would be spinning off its software group to Micro Focus, including the Fortify portfolio, in addition to its IT operations management, security, data analytics, and information management and governance software. The deal is expected to finalize during mid-2017 and the Fortify brand is expected to be maintained.

On the product side, HPE's efforts have included employing machine learning with crowdsourced and customer historical results data to reduce false positives, as well as integration of Swagger-supported REST APIs to support security testing.

HPE's AST offerings should be considered by enterprises looking for a comprehensive set of AST capabilities, either as a product or service, or both combined, with enterprise-class reporting and integration capabilities.

STRENGTHS

HPE Fortify is a well-known brand worldwide. It very frequently appears on clients' shortlists, particularly where multiple testing technologies are desired, and was the first AST vendor to provide capabilities in SAST, DAST and IAST.

HPE's SAST has the broadest language support of any of the SAST providers, and its WebInspect IAST agent for Java and .NET is included at no cost for WebInspect DAST tool customers.

HPE has one of the strongest SDLC integrations and includes innovative features in this space, such as DevInspect and Security Assistant.

HPE has a comprehensive set of enterprise capabilities, such as role-based access control (RBAC), full authentication integration, extensive WAF integration and its own SCA capabilities, as well as integration with Sonatype and Black Duck.

CAUTIONS

The spinoff and merger of HPE's software group with Micro Focus raises concerns for clients about how the newly expanded company will integrate and support the Fortify brand and its customers, and the future commitment of the merged company to the existing roadmap as well as continued innovation and investment in research and development of the AST solutions.

Some AST capabilities, such as malware detection, are only available with the Fortify on Demand offering.

Clients have frequently mentioned that the on-premises Fortify AST solutions can have a steep learning curve and require extensive configuration to properly integrate and run.

IAST support for PHP and Node.js is not yet available.

IBM

IBM is a global vendor of IT services and products based in the USA. IBM provides a desktop DAST tool (AppScan Standard), a management console and enterprise DAST tool (AppScan Enterprise), and a SAST tool (AppScan Source). IBM also provides IAST in AppScan Standard and Enterprise, via a functionality called glass box. IBM Application Security on Cloud (ASoC) is its SaaS offering.

IBM provides Intelligent Code Analytics (ICA) and Intelligent Finding Analytics (IFA), which improve the speed and accuracy of scan results. ICA detects APIs in languages and frameworks, and determines the security implications of those APIs to reduce false negatives. IFA provides automated analysis of scan findings to reduce false positives and provide recommendations to optimize vulnerability remediation.

In the last 12 months, IBM has worked on making features of its on-premises offerings available to its ASoC offering (for example, adding SAST-as-a-service offering for Java and .NET).

IBM will appeal to enterprises seeking a single provider of AST technologies, with IBM offerings in adjacent security areas, looking for an AST solution that can provide risk-based management and a full set of enterprise-class capabilities.

STRENGTHS

IBM is a large provider of a complete AST solution (SAST, DAST and IAST) and other security products/services with multiregional presence and delivery capabilities.

IBM's Application Security Management provides risk-centric unified reporting and dashboard functionality and an underlying framework to manage business-impacting security risks in applications.

IBM has added innovative SAST functionality to improve accuracy, namely Intelligent Code Analysis (ICA) and Intelligent Findings Analytics (IFA), both of which are delivered via the cloud to on-premises and cloud clients.

CAUTIONS

Gartner inquiry feedback indicates IBM solutions are showing up in fewer competitive shortlists than other Leaders, and that a large percentage of AppScan clients leverage it as part of an existing relationship or spend with IBM.

The stability and evolution of IBM's partnership with Cigital to deliver managed, human-augmented DAST services is unclear with the recent acquisition of Cigital by Synopsys.

IBM does not have its own SCA, and its integration with partner Black Duck is limited to AppScan Enterprise.

IBM's IAST has not earned brand recognition in this space compared to its direct competitors.

NSFOCUS

NSFOCUS is an AST vendor based in China, serving the Asia/Pacific region with a strong presence in the Chinese market. NSFOCUS offers a variety of security solutions, including intrusion prevention systems (IPS), next-generation firewalls, distributed denial of service (DDoS) protection and vulnerability assessment.

For AST, NSFOCUS offers NSFOCUS Web Vulnerability Scanning System (WVSS) for DAST scanning of websites, as well as Web Security Monitoring System (WSM) for the monitoring of website vulnerabilities, malicious content, defacement and sensitive content. NSFocus also offers WebSafe, a cloud-based service that combines WVSS and WSM.

NSFOCUS has introduced IAST, and has focused on expanding its geographic region beyond China with new offices in North America.

NSFOCUS should be considered by organizations looking for competitively priced web application security testing tools and services, with extensive support in China and local language support and console.

STRENGTHS

NSFOCUS is a well-known security provider with good visibility in China and an integrated set of security products.

NSFOCUS includes capabilities for the detection of well-known vulnerabilities in commercial off-the-shelf (COTS) or open-source software (OSS) components and applications, delivering SCA capabilities for DAST.

NSFOCUS recently introduced an instrumentation agent for PHP to provide IAST capability for WVSS. The agent monitors the running application and reflects relevant data back to the WVSS scanner.

CAUTIONS

NSFOCUS rarely appears on client shortlists outside of China.

NSFOCUS provides limited capabilities for testing web services, and currently lacks the ability to test REST- or XML-based application interfaces for more advanced web applications.

NSFOCUS does not offer a SAST tool, but rather a manual service.

NSFOCUS does not offer enterprise class capabilities, such as SDLC and WAF integrations, outside of integrating with its own WAF.

N-Stalker

N-Stalker, based in Brazil, is a regionally known provider of AST products and services. N-Stalker primarily serves the South American market, with presence in the European and Asia/Pacific markets, and a smaller presence in the U.S. market. N-Stalker provides a DAST tool, Web Application Security Scanner, and a SaaS-based offering (Cloud Web Scan Platform) that includes DAST and SAST.

Over the last 12 months, the vendor has focused on improving WAF integration (Exceda and Akamai), partnering with Dognaedis to provide cloud-based SAST via Code V, and providing application vulnerability correlation.

N-Stalker should be considered by organizations looking for easy-to-use, reasonably priced, enterprise-class web application security testing in South America and Latin America, and that prefer both the regional expertise that N-Stalker provides as well as local language support for Portuguese and Spanish.

STRENGTHS

N-Stalker has a broad array of enterprise features not typically offered by smaller providers, such as RBAC, Selenium support, IDE integration, OAuth and OpenID support, SOAP- and REST-based web service testing, as well as JavaScript Object Notation (JSON) remote procedure call (RPC) and Extensible Messaging and Presence Protocol (XMPP) support.

N-Stalker is well-known in Brazil and neighboring countries in South America, with local language support and consoles in Spanish and Portuguese.

N-Stalker provides its own software composition analysis capabilities to support the identification and scanning of more than 2,000 third-party COTS and OSS components and platforms for Common Vulnerabilities and Exposures (CVEs) related to those packages.

CAUTIONS

N-Stalker has limited brand awareness outside of South America.

N-Stalker's integrated SAST capabilities are only available via its Cloud Web Scan platform, are limited to web applications and provide no support for dynamic programming languages, such as Ruby.

N-Stalker has no IAST capabilities.

PortSwigger

PortSwigger is a U.K.-based DAST provider serving primarily the North American and European markets. Its offering, called Burp Suite, is a set of integrated tools that includes Burp Scanner, and together provides advanced DAST, client-side SAST and as of recent IAST (Burp Infiltrator). PortSwigger offers free editions of Burp Suite and an aggressively priced Burp Suite Professional edition that includes DAST, IAST and client-side SAST capabilities. Burp Collaborator is a cloud-based component that communicates with the DAST solution to support out-of-band detection techniques. PortSwigger offers a proxy for the real-time capture of web interactions, including back-end interfaces for dynamic testing.

Over the last 12 months, PortSwigger introduced an IAST capability, called Burp Infiltrator, currently supporting Java and .NET platforms, as well as innovations for the DAST solution. Infiltrator instruments the application bytecode, fingerprints Burp payloads that reach potentially dangerous API calls and communicates back to the DAST component via the Burp Collaborator server.

PortSwigger should be considered by organizations seeking a powerful DAST tool with advanced testing capabilities to be used by a security professional, but that do not require enterprise-class features such as deep SDLC integration out of the box.

STRENGTHS

PortSwigger's Burp Suite is one of the most widely adopted tools in the DAST market, with a strong reputation and popularity among professional security testers.

PortSwigger's products are highly customizable and extensible, and can be API-driven. The community of Burp users has developed a number of useful extensions/additions to Burp that are available to Burp users.

PortSwigger's offering provides innovative and advanced DAST capabilities, such as the Burp Collaborator service, which supports deferred interactions, allowing for the identification of vulnerabilities that are triggered after the scan is completed.

PortSwigger's IAST Burp Infiltrator is available at no additional cost as part of DAST scanning using the Burp Suite Professional edition.

CAUTIONS

PortSwigger is rarely included in shortlists where enterprise-class integrations are a critical requirement.

Burp Suite does not offer software composition analysis or SAST.

PortSwigger does not offer DAST as a service.

PortSwigger does not offer integration with WAFs, IDEs or QA systems.

Qualys

Qualys, based in Redwood City, California, is a provider of cloud-based security services. It has a strong presence in North America and APAC, as well as a presence in the European market. Qualys offers Web Application Scanning (WAS), which is a DAST service that is completely automated and

integrates with the other Qualys security services in the Qualys Cloud Platform. Qualys provides WAS through an affordable yearly subscription, as well as pay-per-scan licensing.

In the last 12 months, Qualys has focused on improving DAST scanning for modern web applications, introducing SmartScan for testing web applications leveraging Ajax and new frameworks, and enhancing testing for DOM-based XSS.

Organizations looking for a lower-cost automated DAST service that provides WAF integration and malware scanning should consider Qualys.

STRENGTHS

Qualys WAS is quite visible in the DAST market, and customer feedback indicates that WAS is relatively straightforward to deploy and use.

Qualys provides extensive WAF integration, including its own WAF-as-a-service offering.

Qualys WAS provides malware scanning at no additional cost.

CAUTIONS

Qualys offers no IAST, SAST or SCA capabilities, nor does it partner to offer these.

Qualys WAS does not provide certain types of authentication options, such as OAuth.

Qualys WAS does not provide any human augmentation options.

Rapid7

Rapid7 is a provider of security, data and analytics software and IT services based in Boston, Massachusetts. It has a strong presence in the North American market, as well as a presence in the European market. In the AST space, Rapid7 provides DAST. Its offering consists of an automated web app scanner called AppSpider Pro, an enterprise portal called AppSpider Enterprise and DAST as a service under the name of AppSpider Enterprise OnDemand. In addition, Rapid7 provides AppSpider Managed Services, which offer the same on-demand DAST in a completely outsourced fashion.

In the past 12 months, Rapid7 has focused on improving DAST scanning for modern web applications, including support for automated testing of Swagger-enabled REST APIs and supporting frameworks used in single-page web applications.

Rapid7 should be considered by organizations looking for DAST as a competitive alternative to the larger providers.

STRENGTHS

Rapid7's "universal translator" technology allows its DAST solution to adapt to, parse and attack new and complex web applications, involving REST, JSON, JavaScript and other technologies.

AppSpider has good SDLC and enterprise integration capabilities, including plug-ins with bug-tracking tools, WAF and IPS products.

Rapid7 gets mostly good marks from users for ease of use and reporting.

CAUTIONS

Rapid7 does not provide any SAST capabilities, even though it provides SAST through its partnership with Checkmarx.

Rapid7 does not provide any SCA functionality.

Rapid7 does not support distributed scanning with its DAST offering.

Rapid7 does not provide IAST, nor does it partner to provide it.

SiteLock

SiteLock is a U.S.-based provider of AST with a strong presence in the North American market, as well as presence in the European market. SiteLock offers multiple tiers of completely automated web application scanning services (SiteLock Application Scan) using a combination of its own tools and commercial tools for web hosting customers. SiteLock has integrated network vulnerability scanning of the web server, as well as SAST capabilities (SiteLock TrueCode) specifically for web applications developed in Java or PHP. It has no tool offerings, and sells its DAST with integrated SAST solutions as a service only.

Over the last 12 months, SiteLock introduced an innovative proactive risk score analysis to help prioritize applications before scanning, by highlighting a potential risk score for an application based on the similarity to other websites or applications that have recently undergone compromise. SiteLock has expanded its go-to-market strategy to target customers directly, instead of focusing entirely on growing sales through partner channels.

SiteLock should be considered by midsize organizations seeking comprehensive web application security testing that combine basic DAST and SAST, and includes network vulnerability scanning.

STRENGTHS

SiteLock has gained significant visibility among midsize customers by using web hosters as one of its channels.

SiteLock includes offerings geared toward website security needs of small and midsize businesses, offering functionality such as automated malware detection and removal and its proactive risk scoring.

SiteLock has a comprehensive offering, providing SCA in addition to DAST and SAST.

CAUTIONS

SiteLock does not yet have a strong brand recognition as an AST vendor. SiteLock is rarely included in shortlists for large-enterprise use cases.

SiteLock lacks many of the advanced testing capabilities and enterprise-class integration options (such as IDE, bug-tracking system and QA integration) available from other vendors.

SiteLock does not offer IAST.

SiteLock has no support for testing web services and integrates only with its own WAF.

Synopsys

Synopsys is a global company based in Mountain View, California that has a number of diverse offerings in the software and semiconductor areas. Synopsys has been expanding its application security portfolio in the last few years. In November 2016, during the creation of this research, Synopsys closed the acquisition of Cigital and Codiscope. This acquisition follows a series of application security acquisitions, namely Quotium's Seeker IAST, Codenomicon, Protecode and Coverity, which provided Synopsys with IAST, SAST and SCA functionalities.

With the acquisition of Cigital, Synopsys integrates DAST as a service and SAST as a service in its offering, while via Codiscope's SecureAssist, Synopsys integrates a lightweight SAST tool in its offering. Gartner will be closely following the integration of Cigital into Synopsys's portfolio of security testing technologies.

Synopsys is well-positioned in the Internet of Things (IoT) AST space, where it supports a broad range of protocols, such as XMPP, Message Queuing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP) and Advanced Messaging Queuing Protocol (AMQP) via Defensics.

Synopsys should be considered by organizations looking for a complete AST offering, and wanting variety in terms of AST depth capabilities, deployment options and licensing.

STRENGTHS

Synopsys's Seeker continues to be one of the most broadly adopted IAST solutions, providing a wide range of language coverage and good SDLC integration.

Cigital 3D licensing provides flexible options for organizations to choose among three levels of SAST and DAST testing for any application, for a fixed yearly cost.

Codiscope's SecureAssist provides strong integration with IDEs to provide a SAST spellchecker early on in the development phase.

CAUTIONS

Interaction with Gartner clients shows that Synopsys, contrary to its individually acquired AST players, is not yet a well-recognized AST brand, especially outside North America.

Even though Synopsys has a positive track record in handling acquisitions, it remains to be seen how it will manage to integrate all the Cigital AST offerings with the ones from its previous acquisitions.

Synopsys does not offer a DAST on-premises product or an automated DAST offering.

Trustwave

Trustwave is a worldwide provider of security-related products and services, based in Chicago and owned by Singtel since 2015. Trustwave offers a portfolio of application-layer products and services, including web application firewalling, web application vulnerability assessment, network vulnerability scanning and database activity monitoring. Trustwave is a well-known player in the managed security services and Payment Card Industry Data Security Standard (PCI DSS) assessment markets.

Trustwave is focused on offering DAST products (App Scanner Enterprise) and cloud-based services. In its Managed Security Testing (MST) offering, there are options for application penetration testing, managed application scanning and self-service application scanning.

In the last 12 months, Trustwave has focused on expanding DAST attack capabilities, such as enhancing support for testing of REST services, handling scans that were affected by account lockout and verifying XSS vulnerabilities.

Trustwave should be considered by organizations looking for an enterprise-class DAST solution with product and service options at competitive pricing, or a "one-stop shop" for PCI-compliance-related products and services.

STRENGTHS

Trustwave's comprehensive portfolio of technologies and managed security services remains well-known for its support of PCI DSS.

Trustwave provides a number of options for integration in the SDLC, including IDE, bug-tracking, quality testing and a number of WAF tools, including Trustwave's own WAF and the ModSecurity commercial ruleset.

Trustwave's proprietary Hailstorm Application Risk Metric (HARM) risk scoring provides high-level management, customization and view of risks across the portfolio, helping organizations prioritize remediation and testing by risk.

CAUTIONS

Trustwave does not offer a SAST product or service, or application vulnerability correlation, nor does it partner to provide these.

Trustwave does not offer IAST capabilities, nor does it partner to provide this.

Trustwave rarely appears in Gartner client inquiries where PCI DSS compliance is not a main driver.

Veracode

Veracode is a well-established global AST provider with a strong presence in the North American market as well as presence in the European market. Veracode's offering includes SAST, DAST and SCA cloud services, as well as IAST (and RASP).

In the last 12 months, Veracode launched Greenlight, a SAST service to be used early on in the development process by integrating into the IDE to scan an individual class or file. In addition to Greenlight, Veracode provides the Developer Sandbox, which can statically scan an application or component and measure results without impacting or penalizing developer metrics. Veracode focused some of its recent efforts on extending its language and framework support, as well as SDLC integration, and most recently it announced a single instrumentation agent to provide IAST and RASP capabilities.

Veracode will meet the requirements of organizations looking for a broad set of AST services and that want support for their AST and SCA from a third-party expert with a comprehensive AST solution.

STRENGTHS

Gartner clients highly rate the ease of use of the solution, as well as the vendor's support and willingness to work with customer requirements.

Veracode provides a comprehensive AST-as-a-cloud service. The results of all types of testing can be integrated into a single dashboard to simplify vulnerability management and remediation.

For integration into SDLC processes, Veracode offers built-in integration with multiple IDEs, bug-tracking systems and build servers, as well as APIs for integration, Greenlight and the Developer Sandbox.

CAUTIONS

Veracode does not offer AST tools, only AST as a service, though it provides a virtual scan appliance that can be located on the client's network to support discovery and testing of internal applications, with scanning configured and controlled via the cloud service.

Veracode SAST requires byte/binary code for analysis of compiled languages, such as Java, C/C# and Objective-C. This requires the application to be compiled before being shipped to Veracode for analysis.

Veracode's IAST is still on early availability and needs to establish itself in the market.

Virtual Forge

Virtual Forge is a Germany-based provider of SAST for SAP-related programming languages such as Advanced Business Application Programming (ABAP), XS JavaScript (XSJS) and SQLScript. Virtual Forge has a strong presence in the European market, with a presence also in North America and APAC. It offers its solution, CodeProfiler, as a product or service for ABAP analysis. Virtual Forge can perform dynamic testing of the secure configuration of the SAP environment with its SystemProfiler. Virtual Forge also offers penetration testing services for SAP environments.

Over the last 12 months, Virtual Forge has focused on improving its customization and reporting capabilities, adding multilanguage support, as well as enhancing support for the SAP Hana platform.

Checkmarx resells Virtual Forge's ABAP testing in its solutions. Virtual Forge should be considered by organizations that want to test the security of their SAP system, and that have extended and customized their SAP environments.

STRENGTHS

Virtual Forge appears frequently on client shortlists where ABAP security testing is the primary requirement, and is one of only four vendors in this research to provide SAST of ABAP code. Virtual Forge has deep SAP expertise, is SAP-certified, and leverages the native SAP ticketing workflow in SAP's Solution Manager, SIEM systems and other environments.

CodeProfiler for ABAP and for Hana are integrated into the SAP development environment (ABAP Workbench, Eclipse and Web IDE); and it includes automated code correction capabilities (a capability it refers to as "quick fix") within SAP's IDE, as well as bulk corrections.

Virtual Forge's SystemProfiler can scan the SAP environment for secure configuration and up-to-date patching, a capability frequently requested alongside SAST of ABAP. Output from CodeProfiler and SystemProfiler is integrated to improve the efficacy of CodeProfiler's findings.

Virtual Forge provides real-time feedback to developers via spell-checker SAST in the Eclipse IDE, as well as near-real-time feedback in the SAP ABAP development environment.

CAUTIONS

Virtual Forge provides SAST only for SAP-related programming languages, which limits its inclusion in shortlists where additional language support is required. Java, a language often used in SAP environments, is not supported. Virtual Forge partners with Checkmarx for SAST of other programming languages.

Virtual Forge provides no IAST capabilities.

Virtual Forge provides no software composition analysis and does not partner for it, though it will report on known vulnerabilities in SAP modules. It does not offer DAST, but SystemProfiler will dynamically analyze SAP for secure configurations.

WhiteHat Security

WhiteHat Security, based in the U.S., is a global provider of DAST and SAST as a service. It was one of the pioneers for DAST as a service. WhiteHat's AST suite, Sentinel, also provides SAST as a service, using an on-premises appliance to keep scanning local. Its SAST solution can scan both binaries and source code. The results of all of WhiteHat's DAST and SAST scans are reviewed by an expert in WhiteHat's Threat Research Center before delivery to the customer.

WhiteHat Security provides risk management capabilities, such as Factor Analysis of Information Risk (FAIR)-based quantification of application risk, the WhiteHat Security Index (WSI) for comparisons with peers and a dedicated customer success manager. WhiteHat focused in the last 12 months on adding binary analysis and additional languages to its offering, as well as expanding its SDLC integration options .

WhiteHat Security should be considered by organizations looking to outsource their DAST and (to a lesser degree) SAST practices to an expert third-party testing service provider with a scalable solution.

STRENGTHS

WhiteHat Security is widely visible and has a very strong reputation as a DAST as-a-service provider among Gartner clients.

WhiteHat Security offers the ability to interact via chat with a security engineer from the Threat Research Center to answer questions and offer remediation guidance on demand through the UI.

The WSI provides a visual overview of the robustness of the website and scores the overall application security posture, and also allows for comparison of metrics with peers via the Peer Benchmarking dashboard.

CAUTIONS

WhiteHat Security does not sell DAST and SAST tools, only testing services. However, its on-premises virtual appliance can keep scanning locally, including SAST.

WhiteHat Security provides SAST for a limited number of programming languages, despite having recently added languages to its offering, and is not frequently included in shortlists where SAST is the primary requirement.

WhiteHat does not provide IAST.

Vendors Added and Dropped

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

Added

We added ERPScan and Fasoo.

Dropped

Appthority and Pradeo were dropped, as we moved the focus of this Magic Quadrant away from mobile application security testing.

Cigital was dropped, as it was acquired by Synopsys.

Inclusion and Exclusion Criteria

To qualify for inclusion in this research, vendors need to:

- Provide a dedicated application security testing solution (product, service or both; with SAST, DAST or IAST capabilities)
- Have generated at least $10 million revenue in the last four quarters specific to AST (4Q15 and three first quarters of 2016); or have generated at least $6 million revenue in the last four quarters (4Q15 and three first quarters of 2016) specific to AST and year-on-year growth of at least 100%; or have at least 5,000 distinct enterprise AST customers under active management
- Provide a repeatable, consistent subscription-based model (if the vendor provides AST as a service) using mainly its own testing tools to enable its testing capabilities
- Be capable of providing at least seven production references that can be surveyed
- Have a product or service that was generally available before 1 September 2016
- Be determined by Gartner to be significant players in the market because of their market presence or technology innovation

We did not include in this research:

- Vendors that focus on mobile application security testing
- Vendors that provide services, but not on a repeatable, predefined subscription basis — for example, providers of custom consulting application testing services, contract pen testing or professional services
- Vendors that provide network vulnerability scanning, but either do not offer a stand-alone AST capability, or offer only some web-application-layer dynamic scanning
- Vendors that offer only penetration testing products and services.
- Vendors that offer network protocol testing and fuzzing solutions

Consultancies that offer AST services

Vendors that are focused on application code quality and integrity testing solutions, which have some limited AST capabilities

Open-Source Software Considerations

Magic Quadrants are used to evaluate the commercial offering, sales execution, vision, marketing and support of products within markets, which excludes evaluation of raw open-source software (OSS).

Other Players

Several vendors that are not present in this Magic Quadrant are either present in the AST space or in markets that overlap with AST. These vendors do not currently meet our inclusion criteria, but they either provide AST features or address specific AST requirements and use cases.

Specific additional AST vendors we track and can discuss in Gartner inquiry include edgescan, Netsparker, Onapsis, Positive Technologies and Security Innovation, as well as embedded functionality from major public cloud providers and vendors that provide SCA, such as Black Duck and Sonatype.

Evaluation Criteria

Ability to Execute

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

This criterion specifically evaluates current core AST product/service capabilities, quality, accuracy and feature sets. Also, the efficacy and quality of ancillary capabilities and integration into the software development life cycle are valued.

Overall Viability (Business Unit, Financial, Strategy and Organization): Viability includes an assessment of the organization's overall financial health as well as the financial and practical success of the business unit. Views the likelihood of the organization to continue to offer and invest in the product, as well as the product position in the current portfolio.

Specifically, we look at the vendor's focus on AST, its growth and estimated AST market share, as well as customer base.

Sales Execution/Pricing: The organization'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, and customer needs evolve, and market dynamics change. This criterion also considers the vendor's history of responsiveness to changing market demands.

We evaluate the match of the vendor's broader application security capabilities with enterprises' functional requirements, and the vendor's track record in delivering innovative features when the market demands them. We also account for vendors' appeal with security technologies complementary to AST.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message in order to influence the market, promote the brand, increase awareness of products and establish a positive identification in the minds of customers. This "mind share" can be driven by a combination of publicity, promotional, thought leadership, social media, referrals and sales activities.

We evaluate elements such as the vendor's reputation and credibility among security specialists.

Customer Experience: Products and services and/or programs that enable customers to achieve anticipated results with the products evaluated. Specifically, this includes quality supplier/buyer interactions, technical support or account support. This may also include ancillary tools, customer support programs, availability of user groups, service-level agreements and so on.

We evaluate elements such as the ease of use of the tool as perceived by end users and customers.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product or Service	High
Overall Viability	High
Sales Execution/Pricing	Medium
Market Responsiveness/Record	High
Marketing Execution	High
Customer Experience	High
Operations	Not Rated

Source: Gartner (February 2017)

Completeness of Vision

Market Understanding: Ability to understand customer needs and translate them into products and services. Vendors that show a clear vision of their market — that listen, understand customer demands, and can shape or enhance market changes with their added vision.

What we specifically look for is the vendor's ability to understand buyers' needs and translate them into effective and usable AST (SAST, DAST and IAST) products and services.

In addition to examining a vendor's key competencies in this market, we assess its awareness of the importance of integration with the SDLC (including emerging more flexible approaches, such as agile and DevOps), assessment of third-party and open-source components, and the tool's ease of use and integration with the enterprise infrastructure and processes.

We also assess how this awareness translates into its AST products and services.

Marketing Strategy: Clear, differentiated messaging consistently communicated internally, externalized through social media, advertising, customer programs and positioning statements.

The visibility and credibility of the vendor's security research labs is also a consideration.

Sales Strategy: A sound strategy for selling that uses the appropriate networks, including direct and indirect sales, marketing, service, and communication. Partners that extend the scope and depth of market reach, expertise, technologies, services and their customer base.

Offering (Product) Strategy: An approach to product development and delivery that emphasizes market differentiation, functionality, methodology and features as they map to current and future requirements.

What we specifically look for is the product and service AST offering, and how its extent and modularity can meet different customer requirements and testing program maturity levels.

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 also look at how offerings can integrate relevant non-AST functionality that can enhance the security of applications overall.

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

Specifically, we look at how vendors are innovating to support enterprise security intelligence, as well as developing methods to make security testing more accurate. We value innovations in IAST, but also in areas such as SCA, RASP, mobile application security testing and behavioral testing.

We also value innovation in DAST to support modern web and infrastructural requirements, such as rich internet application (RIA) and cloud platforms.

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.

We evaluate the worldwide availability and support for the offering, including local language support for tools, consoles and customer service.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	**Weighting**

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

Source: Gartner (February 2017)

Quadrant Descriptions

Leaders

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

Challengers

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

Visionaries

Visionaries in this Magic Quadrant are vendors that are particularly innovative in AST. Vendors that provide innovative capabilities to accommodate DevOps, to integrate in the SDLC, or to identify vulnerabilities with alternative technologies to established SAST and DAST, such as IAST. Visionaries may not execute as consistently as Leaders or Challengers, and may not have comprehensive offerings in terms of SAST, DAST and IAST.

Niche Players

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

Context

The need for application security has grown among organizations since the last Magic Quadrant, due to a growth in new business applications [1] as well as continued high profile breaches targeting the application layer. [2] AST deployment and technology options have multiplied. The task of finding vulnerabilities has gotten simpler for end users. However, Gartner inquiry feedback suggests clients still struggle with fully adopting, integrating and effectively scaling application security testing solutions. In a recent Gartner study, 71% of respondents replied that increased usage of automated and integrated app testing before production will be among their top-three critical security measures to be adopted by the end of 2019. [3] Furthermore, enterprises' ability to remediate vulnerabilities is challenged when faster and more flexible development methodologies, such as DevOps, [4] replace legacy approaches. This leads to large backlogs of unremediated findings, delaying releases or leading to applications that are rushed into production with known vulnerabilities — in short, it leads to growing security debt for enterprises. Ultimately, development and security are driven further apart, rather than becoming better collaborators. To cope with these challenges, organizations should:

- Require solutions which expose and integrate automated functionality through plug-ins (including IDE, build, repository, QA and preproduction) into the SDLC. This will not only allow developers to fix issues earlier in the process, but it will also improve coordination between development and security.
- Favor AST solutions with lower turnaround times. Waiting for hours for a scan to complete does not scale where code changes are committed multiple times a day. To address this, application security testing vendors have adapted existing solutions and introduced new ones. For example, many vendors now have options for "incremental scanning," where only the portion of new or changed code is scanned. A few vendors also have lightweight SAST within the IDE that provides real-time feedback as a developer codes, much like a spell-checker.
- Require solutions that provide software composition analysis. SCA is becoming a critical or a mandatory feature of AST solutions, as open-source and third-party components are proliferating in applications that enterprises build. [5] In a recent Gartner survey, approximately 40% of respondents claimed to use commercial off-the-shelf software. [3] Vendors in the industry are introducing their own SCA solutions, as well as partnering with specialized SCA vendors.

Market Overview

The application security testing market is growing rapidly, with a projected 14.2% compound annual growth rate (CAGR) through 2020. This is the highest growth of all tracked information security segments, as well as the overall global information security market, which is forecast to grow at a CAGR of 7.8% through 2020. The AST market size is estimated to have reached $719 million at the conclusion of 2016. [6]

The market sees vendors adapting their solutions to the changing landscape. Four main technology trends are observed:

AST solutions are adapting to Agile and DevOps methodologies by integrating deeply into the SDLC and providing faster turnaround.

AST vendors are adapting their solutions to address newer and more complex applications. In DAST, that may mean crawling "single-page applications," or applications requiring complex authentication flows. In SAST, it may mean keeping up with the proliferation of languages, frameworks and libraries. To cope with some of the challenges Gartner has observed a growth in IAST adoption, but not yet in RASP.

Vendors are beginning to add machine-learning-based enhancements to their offerings. These are used to filter out false positives postscan, helping organizations save time on filtering through erroneous results.

While most mainstream AST vendors are not yet focused on IoT security testing, mobile AST is growing quickly. The maturity, sales volumes and even some of the fundamental technologies used for mobile AST require a separate focus, and we did not include mobile AST in this research.

Evidence

[1] R. Shapiro, "The U.S. Software Industry: An Engine for Economic Growth and Employment," Sonecon, September 2014.

[2] Verizon's 2016 Data Breach Investigations Report (http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/)

[3] Gartner Application Security Trends Study 2017. Gartner's Application Security Trends Study was fielded online with 108 IT leaders in January 2017 in order to understand the enterprise web application security landscape and identify the trends organizations face in meeting their digital business objectives. Participants are members of Gartner's proprietary Research Circle panel of experts.

[4] See "Predicts 2017: Application Development." (../../../Users/dzumerle/AppData/Local/Temp/notesAF3A78/%22Predicts 2017/ Application Development.%22)

[5] Black Duck Application Security Report (https://www.blackducksoftware.com/application-security-report) ; Sonatype Releases 2016 State of the Software Supply Chain Report (https://www.sonatype.com/ssc-press-release)

[6] "Forecast: Information Security, Worldwide, 2014-2020, 4Q16 Update"

Evaluation Criteria Definitions

Ability to Execute

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

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

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

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

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

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

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

Completeness of Vision

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

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

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

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

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

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

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

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

these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity. (/technology/about/ombudsman/omb_guide2.jsp)"
