Magic Quadrant for Application Security Testing

Published 19 March 2018 - ID G00327353 - 50 min read

By Analysts Ayal Tirosh, Dionisio Zumerle, Mark Horvath

DevSecOps, modern web application design and high-profile breaches are affecting the growing application security testing market. Security and risk management leaders will need to meet tighter deadlines and test more-complex applications by integrating and automating AST in the software life cycle.

Strategic Planning Assumptions

By 2019, more than 50% of enterprise DevOps initiatives will have incorporated application security testing (AST) for custom code, an increase from fewer than 10% today.

By 2020, 60% of security vendors will claim machine-learning capabilities, an increase from fewer than 10% today.

Market Definition/Description

Gartner defines the AST market as the buyers and sellers of products and services designed to analyze and test applications for security vulnerabilities. Gartner identifies four 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 software life cycle (SLC) phases.
- 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), analyzes the application's reactions and, thus, determines whether it is vulnerable.

- Interactive AST (IAST) technology combines elements of SAST and DAST simultaneously. It is typically implemented as an agent in the test runtime environment (for example, instrumenting the Java Virtual Machine [JVM] or .NET CLR) that observes operation or attacks and identifies vulnerabilities.
- Mobile AST performs SAST, DAST, IAST and/or behavioral analysis on byte or binary code to identify vulnerabilities in mobile applications.

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 a product and service. Gartner's 2017 Survey on Security Buying Behavior showed nearly two-thirds of enterprises with more than 1,000 employees use some form of AST. However, the various technologies differ in adoption and maturity. [1] (#dv_1_the_results) DAST and SAST are the most widely adopted, whereas IAST adoption is still growing.

The 2018 Magic Quadrant will focus on a vendor's SAST, DAST, IAST and mobile AST offerings; maturity; and features as tools or as a service. AST vendors innovating, partnering and offering runtime application self-protection (RASP), which enables applications to protect themselves from vulnerability exploitation at runtime, were weighted heavily. This is also true of software composition analysis (SCA), which identifies open-source and third-party components in applications and their known security vulnerabilities.

Business-critical application security platforms incorporate AST for ERP platforms; however, they are not the focus of the 2018 Magic Quadrant. Although we took into account coverage of these platforms from broader AST solutions, specific solutions in the business-critical AST space typically focus on a single platform. They go beyond code analysis by incorporating modules, such as configuration checks, vulnerability management, and intrusion monitoring, which are all out of scope for this research.

Magic Quadrant

Figure 1. Magic Quadrant for Application Security Testing

Source: Gartner (March 2018)

Vendor Strengths and Cautions

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, and 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 Checkmarx Open Source Analysis for SCA (in partnership with WhiteSource), and Codebashing, which is a developer education platform for secure coding training. Checkmarx offers a managed service called AppSec Accelerator that offers SAST and DAST services (leveraging third-party DAST tools), as well as program support to help development organizations integrate AST in their software development life cycle (SDLC).

During the past 12 months, Checkmarx has acquired Codebashing and integrated it with its previous product, AppSec Coach, to deliver short, gamified training modules as an in-workflow developer education platform for secure coding training. The vendor has also begun offering DAST as a service through the AppSec Accelerator managed service. With the recent release of its IAST solution, Checkmarx now offers a full-suite of AST products and services.

Checkmarx's products will appeal to application development and security organizations that are seeking a comprehensive set of AST products and services with a strong set of enterprise-class capabilities and program support services.

Strengths

- Checkmarx offers strong SAST technologies that support a broad variety of programming languages and frameworks, scalability and quick turnaround times via incremental and parallel tests. The vendor's SAST gets high marks from customers for its depth of remediation guidance and context, such as highlighting optimal remediation points
- Checkmarx has complete integration in the SDLC. Integrations are provided for popular source code repositories, build systems, bug-tracking systems, integrated development environments (IDEs) and quality assurance (QA) testing tools.
- The addition of IAST in a passive testing model and DAST services to the portfolio enables Checkmarx to offer a comprehensive portfolio of AST tools and services that can adapt to most use cases.
- The acquisition and integration of Codebashing enables Checkmarx to deliver innovative training via short, interactive computer-based training models to developers about the vulnerabilities identified in their scans, providing "just in time" training when it's most relevant.
- Checkmarx gets high marks from users for user experience, ease of use and a generally low learning curve.

Cautions

- Checkmarx's IAST and DAST offerings are relatively new (IAST supports only Java and Node.js) and do not yet have the reputation of their SAST offering.
- For mobile testing, Checkmarx does not offer behavioral testing in a device or emulator, although CxIAST can be used to monitor and analyze data flow of instrumented Java apps during test execution.
- Although Checkmarx offers expanded, cloud-based services and a managed services offering, the client base still heavily skews toward on-premises SAST.
- Checkmarx's DAST offering is available only as a managed service.

CA Technologies (Veracode)

CA Technologies is an AST provider headquartered in the U.S., with a strong presence in the North American market, as well as a presence in the European market. CA Technologies' Veracode offering includes a family of products that provide SAST, DAST and SCA services, as well as IAST (and RASP). Veracode also provides mobile AST.

CA Technologies finalized the acquisition of Veracode in April 2017.

During the past 12 months, Veracode has further expanded its language and framework coverage, including Scala, TypeScript and Perl, as well as Play, ReactJS, Koa.js and support for single-page applications. Veracode has also made improvements to SDLC integrations. Veracode has also worked on improving the speed improvements in its static engine to reduce turnaround times.

Veracode will meet the requirements of organizations looking for complete portfolio of AST services, with broad language and framework coverage and ease of implementation and use.

Strengths

- Gartner clients rate the ease of use of the solution highly, as well as the vendor's support and willingness to work with customer requirements.
- Veracode provides a comprehensive and scalable AST-as-a-cloud service. 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.
- Veracode Greenlight, an IDE plug-in for the Eclipse, IntelliJ and Visual Studio IDEs, provides a

lightweight, faster-turnaround SAST that enables developers to test code for security defects, without the usual need to compile the full application.

- Veracode's mobile AST combines SAST, DAST and behavioral testing. Its behavioral testing statically identifies the possible states that the application can find itself in, which can identify certain events that emulation-based behavioral scanning may not.

Cautions

- Veracode does not offer AST tools, only AST as a service. However, it provides a virtual scan appliance that can be located on the client's network to support the discovery and testing of internal applications, with scanning configured and controlled via the cloud service.
- Although Veracode has a considerable reputation in the AST space, Gartner inquiries indicate that CA Technologies does not yet have brand recognition as an AST player.
- Veracode's IAST solution has limited language support and only supports Java. IAST does not support passive testing (as do some IAST competitors) and requires DAST as an inducer.
- Although Veracode has made improvements in its turnaround times, some organizations focusing on continuous integration/continuous deployment (CI/CD) integration express the need for shorter turnaround times to scanning cycles.
- For nonweb applications, application vulnerability correlation is not part of the AST platform, but rather the Runtime Protection platform.

Contrast Security

Contrast Security is an AST vendor based in the U.S. and present in North America, which also sells in the European and APAC regions. Contrast Security offers its IAST (Contrast Assess), which incorporates SCA. Contrast Security also offers RASP with its Contrast Protect product, which can be licensed independently or jointly with Assess. Contrast also offers a central management console, the Contrast TeamServer, which can be delivered as a service or on-premises. Testing does not require attack data to identify vulnerabilities; rather, it is driven by application test activity, such as QA, executed automatically or manually.

During the past 12 months, Contrast Security improved its native integration with development and bug-tracking environments, and added support for additional languages and platform as a service (PaaS). Contrast Security also added vulnerability autoremediation capabilities.

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

Strengths

- Contrast's testing approach is transparent to developers and security specialists, and does not require stand-alone testing or training. The solution does not require security specialists to run dedicated security tests; instead, the agent can identify vulnerabilities through normal application execution.
- Contrast Assess is one of the most broadly adopted IAST solutions and regularly competes in IAST shortlists.
- Clients highly rate the ease of use of the tool and the vendor's support.
- Contrast provides virtual patches of some identified vulnerabilities when licensed with Contrast Protect, for both in-house and third-party code, until the vulnerability is remediated in underlying code or server configuration.
- Contrast's solution enables customers to leverage the instrumentation agent to add or enhance security logging, delivering security analytics for production applications.

Cautions

- Contrast Security does not provide traditional SAST or DAST tools or services.
- Even though Contrast Security has expanded its language support, it still offers a limited spectrum, compared with other AST solutions.
- Contrast Security does not observe and analyze client-side logic executed in the browser only (for example, JavaScript or Java applets); therefore, it cannot identify client-side vulnerabilities, such as JavaScript-based Document Object Model (DOM) XSS.
- Contrast Security does not provide any human augmentation options, and the passive testing model means that proof of exploitation is not an option.
- Contrast can test mobile application back ends, but not the client-side code of the mobile app and does not conduct behavioral analysis.

IBM

IBM is a global vendor of IT services and products based in the U.S. IBM provides SAST and DAST desktop tools, including IBM Security AppScan Source, IBM Security AppScan Standard and an enterprise platform (AppScan Enterprise). This includes a centralized management console that enables users to import findings from third-party tools. IBM's cloud services for SAST and DAST (IBM Security Application Security on Cloud). IAST is delivered via the Glassbox agent in AppScan (AppScan Standard, Enterprise and Cloud), which is free to DAST customers, mobile AST (MAST; IBM Mobile Analyzer) and SCA offerings (IBM Security Open Source Analyzer [OSA]). For SCA, they license vulnerability and remediation databases from WhiteSource. IBM also has a partnership with Prevoty for RASP.

During the past 12 months, IBM made Open Source Analyzer (OSA) available as a cloud service. IBM improved the Intelligent Code Analysis (ICA) and expanded Intelligent Findings Analytics (IFA) to on-premises customers at no additional cost. Both improve the speed and accuracy of SAST scan results. ICA detects APIs in languages and frameworks and determines the security implications of those APIs to reduce false negatives. IBM IFA uses machine learning to significantly reduce the overall vulnerability count and the number of false positives, and to correlate results and suggest the smallest number of code changes to remediate vulnerabilities.

IBM has a considerable customer base, with an offering combining SAST, DAST and IAST in a single suite of products and services. 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 has been expanding functionality with an eye toward the needs of DevSecOps. This includes an expanded pallet of language support, splitting the DAST interface into a mode for developers and another for security experts, and running faster, lighter scans for quicker turnaround times.
- IBM is a large, stable provider of complete AST solutions (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 the IBM Security Framework and Risk Assessment, the underlying framework to manage business-impacting security risks in applications.
- IBM is one of the few vendors to allow importation into the reporting dashboard of third-party AST results, such as findings from manual code reviews, penetration testing, vulnerability

assessments and competitor AST solutions.

- IBM Mobile Analyzer offering combines SAST, DAST and IAST for iOS and Android apps, as well as malware analysis.

Cautions

- Some of IBM's newer functionality rests on partnerships, subject to a number of contingencies outside the company's direct control. For example, it was announced that HCL has licensed IBM's AST technology and will build new features. In addition, IBM partners with Prevoty for RASP and WhiteSource for SCA vulnerability and remediation data used by OSA.
- Gartner inquiry feedback indicates that IBM solutions are showing up in fewer competitive shortlists, especially in terms of static scanning, and a large percentage of AppScan clients leverage it as part of an existing relationship or spending with IBM.
- IBM's IAST has not earned brand recognition in this space, compared with its direct competitors. Its IAST technology is offered as an add-on to the DAST, but can't be delivered as a stand-alone product.
- IBM Mobile Analyzer does not offer behavioral analysis.
- ICA and SCA are available to IBM's SaaS customers only, as is IAST for mobile applications.

Micro Focus

Based in the U.K., Micro Focus is a global provider of AST products and services under the Fortify brand. On 1 September 2017, Micro Focus completed the spinoff/merger of Hewlett Packard Enterprise's (HPE's) software group, which included the Fortify portfolio, in addition to HPE's IT operations management, security, data analytics, and information management and governance software. Micro Focus sales has global reach, with a strong presence in North America, as well as the European and APAC region markets. Fortify offers Static Code Analyzer (SAST), WebInspect (DAST and IAST), Software Security Center (its console) and Application Defender (monitoring and RASP). Fortify provides its AST as a product, as well as in the cloud, with Fortify on Demand (FoD). Mobile AST is delivered via FoD. Fortify's SAST can leverage 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.

During the past year, Micro Focus Fortify has introduced incremental scanning capabilities for WebInspect to enable continuous testing on only changed content of web applications.

Multithreading capabilities were introduced to the SAST products to help improve scan times. In addition, improvements to vulnerability validation through machine-learning-assisted auditing have lowered SAST turnaround times.

Micro Focus Fortify'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

- Fortify is a well-known brand worldwide. It is a constant presence in customer shortlists for a wide range of AST use cases, particularly when multiple testing technologies are required. It has a historical reputation for delivering innovative products and services.
- Fortify has one of the most complete SDLC integrations — for example, by providing out-of-box integrations for popular IDEs and CI/CD tools.
- Fortify's SAST has the broadest language support and provides a range of deployment options making it a good fit for complex testing use cases. Its WebInspect IAST agent for Java and .NET is included at no cost for WebInspect DAST tool customers.
- Fortify continues to develop innovative automation and machine-learning-based features to support DevOps, such as real-time analysis in the Eclipse IDE, using Security Assistant. On-premises and Fortify on Demand customers can leverage machine-learning-based Audit Assistant for FP removal of SAST findings, and the SmartFix feature will suggest optimal fix locations.
- Fortify has a comprehensive set of enterprise capabilities, as well as integration with major SCA vendors. Sonatype assessments are included for all FoD SAST customers at no additional charge.

Cautions

- Customers are concerned that the recently completed spinoff and merger could threaten the future commitment of the merged company to the existing roadmap, as well as continued innovation and investment in AST solution R&D.
- Although the Fortify brand has a considerable reputation in the market, Gartner client interactions indicate that Micro Focus does not have brand recognition as an AST player.
- Customers report that getting the solution fully integrated and stable often requires extensive

configuration, which can lengthen the learning curve for clients new to AST and may require more dedicated staff to get tools operational and maintain them.

- Fortify IAST innovation and adoption continue to lag behind competitors. Support for PHP and Node.js is not yet available. Fortify's IAST can't be operated as a stand-alone product, but as an add-on to its DAST offering.

Positive Technologies

Positive Technologies is a security vendor co-headquartered in Moscow, and London, with a large presence in Russia, Italy and the Czech Republic. Positive Technologies offers PT Application Inspector (PT AI), which provides SAST and DAST. PT Application Inspector is available in a Desktop edition for security specialists and an enterprise offering (PT Application Inspector SSDL Edition) to support large development teams across the organization. Positive Technologies also provides SCA as part of PT Application Inspector, as well as a mobile AST service.

During the past 12 months, Positive Technologies has added incremental scanning, improved PT Application Inspector SDLC integration and extended its coverage to AST for mobile platforms and frameworks.

PT Application Inspector is a good fit for enterprises looking for large and especially midsize organizations in the European region that need integrated SAST and DAST with web application firewall (WAF) functionality.

Strengths

- PT Application InspectorSAST supports incremental scanning, which can help reduce turnaround times when there is a need to scan applications frequently.
- PT Application Inspectoris fully integrated with PT AF, the WAF offering from Positive Technologies. This can provide instant automated virtual patching for vulnerabilities that PT Application Inspectorhas identified.
- PT Application Inspectoruses a built-in abstract interpretation engine to improve accuracy and filter findings of vulnerabilities that are not applicable to specific contexts.
- Positive Technologies' customers praise the vendor's flexibility and support.
- PT Application Inspectorprovides support for SAST of iOS and Android mobile apps developed in C# on top of Xamarin. The vendor recently introduced support for Android Java.

Cautions

- Positive Technologies is rarely on North American shortlists and has a small presence in the region.
- Even though it supports mobile AST, PT Application Inspectordoes not support native iOS languages, such as Swift or Objective C.
- Relative to other SAST vendors, PT Application Inspector SAST supports a limited number of programming languages.
- PT Application Inspector's DAST has limited capabilities for testing the web services often required for dynamic security testing of modern web applications. It lacks support for Simple Object Access Protocol (SOAP), Web Services Description Language (WSDL) and JavaScript Object Notation (JSON) and for the testing of RESTful Services.
- PT Application Inspector's availability of scanning and reporting templates for compliance testing certification is limited.

Qualys

Based in Foster City, California, Qualys is a provider of cloud-based security services with a strong presence in North America and the APAC region, 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 at an affordable per year subscription, as well as pay-per-scan licensing.

During the past year, Qualys has focused on improving the DAST engine to support RESTful API testing, added form training to enhance crawling and introduced a partnership with Bugcrowd. WAS customers running a bug bounty program with Bugcrowd are now able to import and export results to and from Bugcrowd's Crowdcontrol platform,

Qualys is a visible DAST player with sizable market share, but does not provide SAST or IAST, and only provides DAST as a cloud service. Organizations looking for a lower-cost, automated DAST service that provides malware scanning should consider Qualys.

Strengths

- Qualys delivers highly scalable, low-cost, largely automated DAST services that will appeal to customers with large-enterprise application portfolios

- Qualys WAS is quite visible in the DAST market, and WAS is relatively straightforward to deploy and use.
- Qualys provides extensive, third-party WAF integration and one-click virtual patching with the Qualys WAF.
- Qualys partnership with Bugcrowd introduces an innovative approach to results analysis by providing the results of WAS analysis to joint customers via the Bugcrowd platform to enhance the efficacy of manual crowdsourced testing. WAS can also import Bugcrowd findings.

Cautions

- Qualys doesn't offer IAST, SAST or a dedicated SCA solution, and it has no partnership to offer them.
- Qualys WAS does not provide certain types of advanced DAST functionality, such as importation of Swagger/OpenAPI specifications to support automated API testing.
- Qualys WAS does not provide human augmentation options, beyond the Bug Crowd partnership.
- Qualys mobile AST is limited to dynamically assessing APIs and back-end services, and does not offer behavioral analysis.

Rapid7

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

During the past 12 months, Rapid7 launched InsightAppSec and InsightVM on its Insight platform to provide a cloud-based security analytics platform that combines application security data from InsightAppSec, with vulnerability information collected by InsightVM.

Rapid7 should be considered by organizations looking for a competitive alternative to the larger providers for DAST, delivered either as a product, service or fully managed service.

Strengths

- Rapid7 has a strong reputation for comprehensive DAST that can support in-depth manual assessments necessary for custom development use cases, as well as the more automated DAST required to support DevOps.
- Rapid7 is pursuing a vision of integrated AST and vulnerability management by extending its Insight platform to combine findings from AST with information such as IT log analytics, vulnerability management data and user-behavior analytics gathered from the Insight portfolio.
- AppSpider has good SDLC and enterprise integration capabilities for a DAST solution, including plug-ins with bug-tracking tools, WAF and IPS products. The vendor recently introduced a Chrome/WebKit integration to support integrated browser functionality with Chrome.
- Rapid7 gets mostly good marks from users for ease of use and reporting.

Cautions

- Rapid7 does not provide native SAST capabilities, although it provides SAST through its partnership with Checkmarx.
- Rapid7 does not support distributed scanning with its DAST offering.
- Despite industrywide trends toward increased adoption of services, most Rapid7 clients leverage the on-premises implementation, and Rapid7 struggles to be included on shortlists where services are a primary focus.
- Rapid7 does not provide IAST, nor does it provide behavioral testing. The vendor's mobile AST is limited to analyzing the traffic between the mobile app and the back-end services.
- Rapid7 does not provide a dedicated SCA solution.

SiteLock

SiteLock is a U.S.-based provider of AST with a strong presence in the North American market, as well as a presence in the European market. SiteLock offers 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 assessments of the web server, as well as SAST capabilities (SiteLock TrueCode) for web applications developed in Java or PHP. It sells its DAST with integrated SAST solutions as a service only.

During the past 12 months, SiteLock acquired and integrated Patchman into its offering. This provides real-time vulnerability detection and automatic patching of server-level vulnerabilities in commonly used Content Management Systems. SiteLock also made improvements in its malware detection, blacklisting and database cleaning capabilities, as well as its offline reporting.

SiteLock should be considered by midsize organizations looking for web AST that combines basic DAST and SAST, and includes network vulnerability assessments.

Strengths

- SiteLock product development continues to deliver features tuned to the needs of midsize customers, giving them significant visibility among small or midsize businesses (SMBs) that other AST players struggle to reach.
- SiteLock offers functionality that is not typically available from larger AST vendors in this Magic Quadrant. This includes automated malware detection and removal, as well as proactive risk scoring to predict a website's likelihood of compromise, based on comparisons with similar websites tested.
- SiteLock offers SCA, DAST and SAST.
- Customer's rate highly the ease of use and implementation of the service.

Cautions

- SiteLock does not have strong brand recognition as an AST vendor, and interactions with Gartner clients show that SiteLock rarely competes for the same large-enterprise clients with other AST vendors in this Magic Quadrant.
- SiteLock's SAST has limited programming language support, relative to other SAST vendors.
- 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 offers neither IAST, nor mobile AST, and it mainly focuses on web application testing.
- SiteLock has no support for testing web services, which is often required for testing modern web applications.

Synopsys

Based in Mountain View, California, Synopsys is a global-company with several offerings in the software and semiconductor areas. Synopsys has been expanding its application security portfolio during the past few years. In December 2017, during the creation of this research, Synopsys closed the acquisition of Black Duck. This acquisition follows a series of application security acquisitions — Cigital, Quotium's Seeker IAST, and Condenomicon, Protecode and Coverity, which provide Synopsys with IAST, SAST and SCA functionality.

Black Duck is a popular partner for SAST and DAST product companies that want to provide SCA functionality, but lack the personnel or expertise to create their own offerings. Black Duck partnerships have included other AST vendors, as well as Google.

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

Strengths

- Seeker continues to be one of the most broadly adopted IAST solutions, providing a wide range of language coverage and good SDLC integration. Synopsys introduced agent-only IAST for Seeker that does not require an inducer. This supports the passive testing model offered by some IAST competitors.
- SecureAssist is a good fit for DevOps shops, because it provides strong integration with IDEs to provide a SAST spellchecker early on in the development phase. Synopsys leveraged the Coverity engine to introduce support for JavaScript analysis within SecureAssist.
- Synopsys offers a comprehensive set of AST offerings suitable for a range of use cases and includes a variety of fuzzing capabilities (input fuzzing, protocol, etc.) delivered via Defensics, which is an unusual and often overlooked functionality that can complement AST initiatives.
- Synopsys is well-positioned in the IoT AST space, where it supports a broad range of protocols, such as XMPP, MQTT, CoAP and AMQP (via Defensics).

Cautions

- Gartner client feedback indicates that leveraging multiple solutions from Synopsys often requires extensive training and support services from the vendor to learn to integrate successfully.
- The solutions acquired by Synopsys require better integration and consolidation to offer a unified platform desired by customers. The acquisition of Black Duck, which overlaps some

Protecode functionality, further complicates this.

- Interaction with Gartner clients shows that Synopsys, contrary to its individual acquired AST players, is still not a well-recognized AST brand, especially outside North America.
- Synopsys does not offer a DAST on-premises product or an automated DAST offering, although it does offer DAST as a service.

Trustwave

Based in Chicago and owned by Singtel since 2015, Trustwave is a worldwide provider of security-related products and services. 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 (App Scanner Cloud). Its Managed Security Testing (MST) offering, which also delivers mobile AST, includes options for application penetration testing, managed application scanning and self-service application scanning.

During the past 12 months, Trustwave has developed an enhanced DAST scanning engine to better support single-page applications and modern application development. The vendor has also revamped the MST offering to improve the user experience, workflow and testing options.

Trustwave should be considered by organizations looking for an enterprise-class DAST solution with a varied level of 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 supports an expansive list of testing and reporting templates tailored to major regulatory requirements. This makes it a good fit for buyers in more-regulated industries.
- Trustwave provides a number of options for integration in the SDLC, including IDE, bug-tracking, quality testing and several WAF tools, including Trustwave's own WAF and the ModSecurity commercial ruleset.

- The portfolio of products and service options makes Trustwave suitable for clients with large, varied application portfolios requiring DAST testing.
- Trustwave client's praise the vendor's support and responsiveness and give high marks for the vendor's flexibility in meeting their requirements.

Cautions

- Trustwave struggles to be included on Gartner client shortlists, where PCI DSS compliance is not a main driver.
- Trustwave does not offer a SAST product or service, or application vulnerability correlation, nor does it partner to provide them.
- App Scanner does not provide SCA, nor does it partner for this, although the DAST solution can be used to identify well-known vulnerabilities and misconfigurations in the underlying web and application servers.
- Mobile AST, delivered via the Managed Security Testing offering, does not include automated static analysis of the code, but it does offer a manual code review service.
- Trustwave does not offer IAST capabilities, nor does it partner to provide this.

WhiteHat Security

Based in the U.S., WhiteHat Security is a global provider of DAST and SAST as a service. WhiteHat has a particularly strong presence in the North American AST services market. WhiteHat's AST suite, Sentinel, provides SAST (with integrated SCA) and DAST as a service, using an on-premises appliance to keep scanning local, when desired, as well as mobile testing delivered via partnership with NowSecure. Sentinel 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.

During the past 12 months, WhiteHat Security launched the Scout offering to provide fast-turnaround, fully automated SAST integrated into the IDE for developers engaged in fast-paced, iterative development.

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

- Among Gartner clients, WhiteHat Security has a strong reputation as a DAST as-a-service provider.
- WhiteHat's scalability and continuous testing offering scans web applications for changes and automatically initiates production-safe scanning of those changes. It appeals to organizations with large application portfolios in heavily regulated environments looking to support ongoing vulnerability assessments.
- WhiteHat's Scout is a fully automated SAST offering integrated into the IDE. It is tuned for high-assurance tests and quick turnaround, which will appeal to clients supporting DevOps use cases. Scout also provides open APIs for custom integrations.
- WhiteHat's customers continue to value the vendor's strong support services. These include vulnerability verification, manual business logic assessments, and its ability to leverage the vendor's Threat Research Center's engineers to discuss findings and get remediation support.
- WhiteHat SAST offers an innovative feature called Directed Remediation. This automatically provides custom code patches that can be copied and pasted into the code to fix identified vulnerabilities for a portion of findings (for example, roughly 30% of Java vulnerabilities). WhiteHat will use Attack Vector Intelligence to identify where a single fix can address multiple findings and will combine those findings for reporting and remediation purposes.

Cautions

- WhiteHat's introduction of new features and improvements tends to follow behind other similar features introduced previously by leaders in the market.
- WhiteHat Security does not sell DAST and SAST tools, it offers only testing services. However, its on-premises virtual appliance can test locally.
- The introduction of Scout affords improved time to results for SAST findings with Java; however, for languages not supported by Scout, clients in rapid development cycles still express the need for shorter turnaround times to scanning cycles.
- WhiteHat Security still struggles to compete for inclusion in shortlists, where SAST is the most heavily weighted component. In part, this is due to its limited number of supported languages, relative to other SAST vendors.
- WhiteHat security does not provide dedicated IAST, although it does offer application

vulnerability correlation (AVC) capabilities to correlate SAST and DAST findings.

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

Positive Technologies has been added.

Dropped

Acunetix, ERPScan, Fasoo, N-Stalker, NSFOCUS, PortSwigger and Virtual Forge were dropped, based on our inclusion and exclusion criteria.

Inclusion and Exclusion Criteria

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

- Provide a dedicated AST solution (product, service or both, with SAST, DAST or IAST capabilities)
- Provide an offering that identifies open-source components and known vulnerabilities in those components
- Have generated at least $20 million of AST revenue during the last four quarters (4Q16 and first three quarters of 2017), of which at least $16 million is from North America and/or Europe, the Middle East and Africa
- Provide a repeatable, consistent subscription-based engagement model (if the vendor provides AST as a service) using mainly its own testing tools to enable its testing capabilities
- Have a product or service that was generally available before 15 September 2017
- Be determined by Gartner to be significant players in the market because of their market presence or technology innovation

We will not include vendors in this research that:

- Focus only on mobile platforms or a single platform/language
- 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
- Provide network vulnerability scanning, but do not offer a stand-alone AST capability, or offer only limited web-application-layer dynamic scanning
- Offer only protocol testing and fuzzing solutions, debuggers, memory analyzers and/or attack generators
- Primarily focus on runtime protection
- Focus on application code quality and integrity-testing solutions or basic security-testing solutions, which have limited AST capabilities

Open-Source Software Considerations

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

Other Players

Several vendors that are not evaluated in this Magic Quadrant are present in the AST space or in markets that overlap with AST. These vendors do not currently meet our inclusion criteria; however, they either provide AST features or address specific AST requirements and use cases. These providers range from consultancies and professional services to related solution categories, including:

- SCA
- Business-critical application security
- Application security testing and orchestration solutions (ASTO)
- AVC

- Application security threats and requirements management (ASRTM)
- Crowdsourced security testing platforms (CSSTPs)

Gartner tracks and can discuss in inquiry specific additional AST vendors, including ERPScan, Virtual Forge, edgescan, Fasoo, PortSwigger, NSFOCUS, N-Stalker, Acunetix, Netsparker and High-Tech Bridge, as well as embedded functionality from major public cloud providers. In addition, we track and can discuss vendors in the listed adjacent markets (see "Hype Cycle for Application Security, 2017").

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, etc. This can be offered natively or through OEM agreements/partnerships, [2] (#dv_2_ibm_and) as defined in the market definition and detailed in the subcriteria. This criterion specifically evaluates current core AST product/service capabilities, quality and accuracy, and feature sets. Also, the efficacy and quality of ancillary capabilities and integration into the software development life cycle are valued.

Overall Viability: 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. Specifically looking for how the vendor supports proofs of concept (POCs) or pricing options for both simple and complex use cases. The evaluation will also include feedback received from clients on experiences with vendor sales support, pricing and negotiations.

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 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 that complement AST.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message 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 (SLAs), etc. 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 (March 2018)

Completeness of Vision

Market Understanding: The ability to understand customer needs and translate them into products and services. Vendors that show a clear vision of their market — listen, understand customer demands, and can shape or enhance market changes with their added vision. What we will be specifically looking for here is:

- The vendor's ability to understand buyers' needs and translate them into effective and usable AST (SAST, DAST, IAST and MAST) 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 and more-flexible approaches)
- Assessment of third-party and open-source components
- 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 are 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. Specifically, how a vendor reaches the market with its solution and sells it — for example, leveraging partners and resellers, security reports, or web channels.

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. Specifically, looking for 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 overall the security of applications.

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 and behavioral testing. We also value innovation in DAST to support modern web and infrastructural requirements such as single-page applications (SPA) 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 (March 2018)

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 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. Leaders should be able to support the testing of mobile applications.

Challengers

Challengers in this Magic Quadrant are vendors that have executed consistently, typically by focusing on a single technology (for example, SAST or DAST) 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 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 or delivery model, or a specific geographic region.

Context

The need for application security continues to grow, and vendors have sought to meet those needs by offering increasingly varied testing technologies and support offerings. The solutions in the market provide more SCA, security training services, program development services and remediation support. The growth in new business applications, as well as continued high-profile

breaches targeting the application layer, have put pressure on enterprises to adapt their application security programs and keep pace with the changes in their application development programs. DevOps, agile and a general demand for greater automation and speed has led to the emergence of technology categories that support or enhance AST efforts. ASRTM solutions now help automate threat-modeling and security requirements gathering.

Most AST organizations can export results for consumption to AVC solutions meant to correlate and deduplicate findings, while providing consolidated workflow for AST vulnerability management from multiple sources and remediation efforts. AST deployment and technology options have multiplied. Vendors have enhanced the accuracy of their solutions and the value of their remediation guidance through machine-learning approaches that help clients better focus on the most pertinent issues.

More is needed. Better accuracy, faster results, easier integrations and enhanced remediation guidance are top of mind for vendors in this market. It has become simpler for end users to find vulnerabilities. However, Gartner inquiry feedback indicates a need to improve remediation guidance, increase testing speed and accuracy, and simplify the operation of AST solutions to support clients adopting, integrating and scaling AST programs.

Furthermore, enterprises' ability to remediate vulnerabilities is challenged when faster and more-flexible development methodologies, such as DevOps, replace legacy approaches. This leads to large backlogs of unremediated findings that delay releases. They also result in applications being rushed into production with known vulnerabilities. In short, it leads to growing security debt for enterprises. AST vendors and those in related markets have focused on developing solutions to address these problems. However, development and security teams risk are being driven further apart, rather than becoming better collaborators. To cope with these challenges, organizations should:

- Require solutions that expose and integrate automated functionality through plug-ins (including IDE, build, repository, QA and preproduction) into the SDLC. This will enable developers to fix issues earlier in the process, and it will improve coordination between development and security.
- Require solutions that provide SCA, which is a critical or a mandatory feature of an overall approach to security testing of applications, because open-source and third-party components are proliferating in applications that enterprises build. Vendors in the industry are introducing their own SCA solutions, as well as partnering with specialized SCA vendors. Gartner clients should pay special attention to those SCA solutions that offer OSS governance capabilities to

enable the organization to proactively enforce its policy with respect to OSS when components are being onboarded.

- Favor AST solutions with lower turnaround times, while maintaining sufficient accuracy of results. Waiting for hours for a scan to complete does not scale where code changes are committed multiple times a day. To address this, AST 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. Passive IAST solutions are available that can identify vulnerabilities in applications during QA and functional testing, without requiring dedicated security tests. These solutions are transparent to security specialists and developers and require little to no training. Only a couple of vendors have lightweight SAST in the IDE that provides real-time feedback as a developer codes, much like a spell-checker.

- Press vendors for specifics on their roadmap with respect to machine-learning approaches to enhance their solutions. Gartner client's should weigh vendor plans with respect to machine-learning-based improvements, particularly when considering longer-term engagements, and consider the applicability of the proposed approaches. Artificial intelligence (AI) and machine learning are overloaded marketing terms, making it difficult to distinguish between hyperbole and genuine value, and should be evaluated closely (see "Artificial Intelligence and Application Security Vendors: Marketing Hype or Genuine Hope?"). Machine-learning-based approaches to improving the accuracy of AST solutions show promise and are already being used to considerable effect to sanitize reports of false positives.

Market Overview

Through 2021, the AST market is projected to have a 14% compound annual growth rate (CAGR). This continues to be the fastest growing of all tracked information security segments. The overall global information security market is forecast to grow at a CAGR of 7.6% through 2021. The AST market size is estimated to reach $775 million by the end of 2018. [3] (#dv_3_forecast_information)

In addition, 2017 saw a number of large acquisitions and developments with big effects on the AST landscape. On 1 September 2017, HPE and Micro Focus concluded the spinoff/merger announced in September of the previous year. [4] (#dv_4_micro_focus) In March 2017, CA Technologies announced plans to acquire Veracode for approximately $614 million. [5] (#dv_5_ca_technologies) In November 2017, Synopsys announced that it had come to a definitive agreement with Black Duck Software, a supplier of SCA, to acquire the latter for approximately $565 million. [6] (#dv_6_synopsys_to) Qualys entered into an agreement with Bugcrowd to bring

CSSTP capabilities to augment the automated testing they provide. [7] (#dv_7_qualys_and) When considering expected growth in the AST market and the opportunities this affords, as well as the space remaining for innovative solutions to disrupt the marketplace, Gartner expects 2018 to be another year of mergers, acquisitions and partnerships. Vendors are simultaneously trying enter the market, gain market share and keep pace with the competition.

Although not strictly a security testing solution, SCA solutions have become critical components of application security programs. SCA products analyze application composition to detect components known to have security and/or functionality vulnerabilities or that require proper licensing. It helps ensure that the enterprise software supply chain includes only components that have undergone security testing and, therefore, supports secure application development and assembly. Gartner clients are increasingly seeking these capabilities from AST vendors. As such, vendors in this Magic Quadrant deliver SCA through homegrown solutions or partnerships with leading SCA vendors to supply analysis and governance capabilities to their clients.

A distinct category exists in application security for solutions that are aimed at supporting security testing and vulnerability assessment for mission-critical, proprietary, commercial, off-the-shelf (COTS) applications. Business-critical application security is the set of processes and technologies that focus on the security, risk and compliance of business-critical applications, most notably ERP, but it can also be extended to human resources and other business-critical applications.

CSSTPs represent a significant deviation from traditional application and security penetration testing services, but have the potential to disrupt the traditional model and offer significant benefits. CSSTPs leverage a large pool of crowdsourced security testing practitioners to identify vulnerabilities through penetration testing and other techniques. CSSTPs also offer bug bounty program administration services, which often include options for vetting bounty seekers and payment processing, as well as options for full public or smaller private/invite-only bounty programs. CSSTP services enable organizations to leverage a diverse range of skills that might otherwise be difficult to replicate with traditional consulting services or AST. Thus, CSSTPs can augment an organization's application security expertise. Gartner has already observed partnerships between AST and CSSTP vendors.

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. Buyers are seeking accurate and fast SAST, integrated

into the developer's IDE to deploy early in the SDLC. Increasingly, Gartner sees clients investigating IAST solutions that can provide accurate vulnerability information during the course of QA and functional testing, without requiring DAST as an inducer.

- 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, SCA and supporting technologies, but not yet in RASP.
- Vendors are beginning to add or continuing to improve machine-learning-based enhancements to their offerings. They are used to filter out false positives postscan, helping organizations save time filtering through erroneous results. Increasingly, Gartner is seeing them being used to automate testing that previously would have required manual intervention.
- Increasingly, Gartner clients are seeking "one-stop shop" vendors that offer multiple technologies as part of a unified platform. To support this effort, buyers are prioritizing vendors that provide multiple technologies and deployment options, while pursuing aggressive roadmaps in innovative areas, such as IAST, SAST-lite, ML-based enhancements, embedded developer training and detailed remediation guidance. A best practice in AST is to use multiple technologies at different points in the SDLC.

  Using multiple vendors often requires learning different systems, as well as using separate dashboards to manage enterprisewide testing and application risk. As a result, many vendors have expanded their offerings through new development or acquisition to position themselves to these buyers. As an alternative to one-stop shops, Gartner has observed the emergence of ASTO solutions to orchestrate and integrate multiple testing solutions, as well as AVC solutions to consolidate findings and remediation workflows.

Evidence

Gartner used the following input to develop this Magic Quadrant:

- Results, observations and selections of AST solutions, as reported via multiple analyst inquiries with Gartner clients
- A formal survey of AST vendors
- Formal surveys of end-user references

[1] The results presented are based on a Gartner study conducted to understand end-user security spending behaviors — what they're investing in and why to determine trends. When asked what phase of adoption their organizations were in for technology products, 65% said that they were using or had deployed AST. Another 30% said that they planned to implement it during the next two years. The remaining 5% said that they had no plans to implement or deploy during the next two years.

The research was conducted online and via Computer Aided Telephonic Interviews (CATI) during September to October 2017. It involved 480 respondents in eight countries: Australia, Canada, France, Germany, India, Singapore, the U.K. and the U.S. All respondents were screened for active employment in organizations with more than 1,000 employees across a good representation of all industries. Respondents were required to have knowledge about their organization's security budget (current, planned and funding). Respondents were also required to have a high level of responsibility for security buying decisions across the several phases of the buying cycle.

Quotas were established by country and by company size to ensure a good representation in the sample. A good spread of industries was also required. The survey was developed collaboratively by a team of Gartner analysts who follow the market and was reviewed, tested and administered by Gartner's Research Data Analytics team. The results of this study are representative of the respondent base and not necessarily the business/market as a whole (see "Survey Analysis: Trends in End-User Security Spending, 2018").

[2] "IBM and HCL to Drive Growth and Innovation in Application Security Space" (https://securityintelligence.com/news/ibm-and-hcl-to-drive-growth-and-innovation-in-application-security-space/)

[3] "Forecast: Information Security, Worldwide, 2015-2021, 3Q17 Update"

[4] "Micro Focus Completes Merger With HPE Software Business, Creating One of World's Largest Pure-play Software Companies" (https://www.microfocus.com/about/press-room/article/2017/micro-focus-completes-merger-with-hpe-software/)

[5] "CA Technologies to Acquire Veracode, a Leading SaaS-based Secure DevOps Platform Provider" (https://www.ca.com/us/company/newsroom/press-releases/2017/ca-technologies-to-acquire-veracode-the-leading-saas-based-secure-devops-platform.html)

[6] "Synopsys to Enhance Software Integrity Platform With Acquisition of Black Duck Software" (https://news.synopsys.com/2017-11-02-Synopsys-to-Enhance-Software-Integrity-Platform-with-

Acquisition-of-Black-Duck-Software)

[7] "Qualys and Bugcrowd Bring the Power of Automation and Crowdsourcing to Web Application Security" (https://www.qualys.com/company/newsroom/news-releases/uk/2017-02-13-qualys-and-bugcrowd-bring-the-power-of-automation-and-crowdsourcing-to-web-application/)

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.

By Ayal Tirosh, Dionisio

Zumerle, Mark Horvath