Gartner

Market Guide for Mobile Application Security Testing

Published: 24 April 2017 **ID:** G00317559

Analyst(s): Dionisio Zumerle, Ayal Tirosh

Mobile AST is different from traditional AST and is pervading the enterprise. Security and risk management leaders responsible for application security must accommodate mobile AST and treat it as a precursor to their future AST endeavors.

Key Findings

- Mobile application security testing (AST) is a growing market and technology space that is bound to merge with the broader AST market as the technologies mature, and as the evolution of mobile platforms slows down as they converge with PC platforms.
- Mobile AST leverages the static application security testing (SAST) and dynamic application security testing (DAST) techniques used in the broader AST space, but these techniques are adapted to mobile platforms.
- The main innovation brought with mobile AST, compared to broader AST, is the introduction of behavioral analysis as a complement to DAST and SAST.
- The use cases and enterprise needs for mobile AST are often different from the ones for the broader AST market in terms of speed and agility of development and the budget allocated.

Recommendations

Security and risk management leaders responsible for application security:

- Integrate mobile AST with your broader AST program and use it as a trial or precursor for enterprisewide DevOps.
- Accommodate more fragmented and agile development processes, with multiple sources of development and multiple users (workforce, consumers, partners) by using mobile AST solutions that allow for frequent, automated testing.
- Test not only the code that resides on the device, but also its interaction with the enterprise back end.

- Include behavior-based solutions to test coming third-party libraries, but require traditional AST to be included to test in-house developed code.

Strategic Planning Assumption

By 2020, up to 90% of enterprises will test mobile application for security vulnerabilities, with more than half of them using the same vendor they use for web application security testing.

Market Definition

The mobile AST market is composed of buyers and sellers of products and services that analyze and identify vulnerabilities in applications used with mobile platforms (iOS, Android and Windows 10 Mobile) during or postdevelopment.

Many variations and flavors of techniques exist, but fundamentally mobile AST solutions test applications in three main ways:

- **SAST:** These solutions statically analyze the source, binary or bytecode of an application to identify vulnerabilities. This technique is very similar to the SAST performed on more traditional applications, such as web apps, and is performed at the programming and/or testing phases of the software development life cycle (SDLC). SAST can analyze the code of the portion of the app residing on the device, as well on the server side.
- **Behavioral testing:** Mobile AST solutions use behavioral analysis to observe the behavior of the app during runtime and identify actions that could be exploited by an attacker. Behavioral testing is usually conducted by running the app in a mobile device emulator, simulator or on an actual mobile device.
- **DAST:** These solutions also use dynamic analysis to test the app in its runtime state. DAST simulates attacks against an application and analyzes the application's reactions, determining whether it is vulnerable. DAST is typically performed in the testing, the preproduction and sometimes the production phases. Traditional DAST is designed to test the server-side of an application, but not the code of the app residing on the mobile device, which is typically addressed by static analysis.

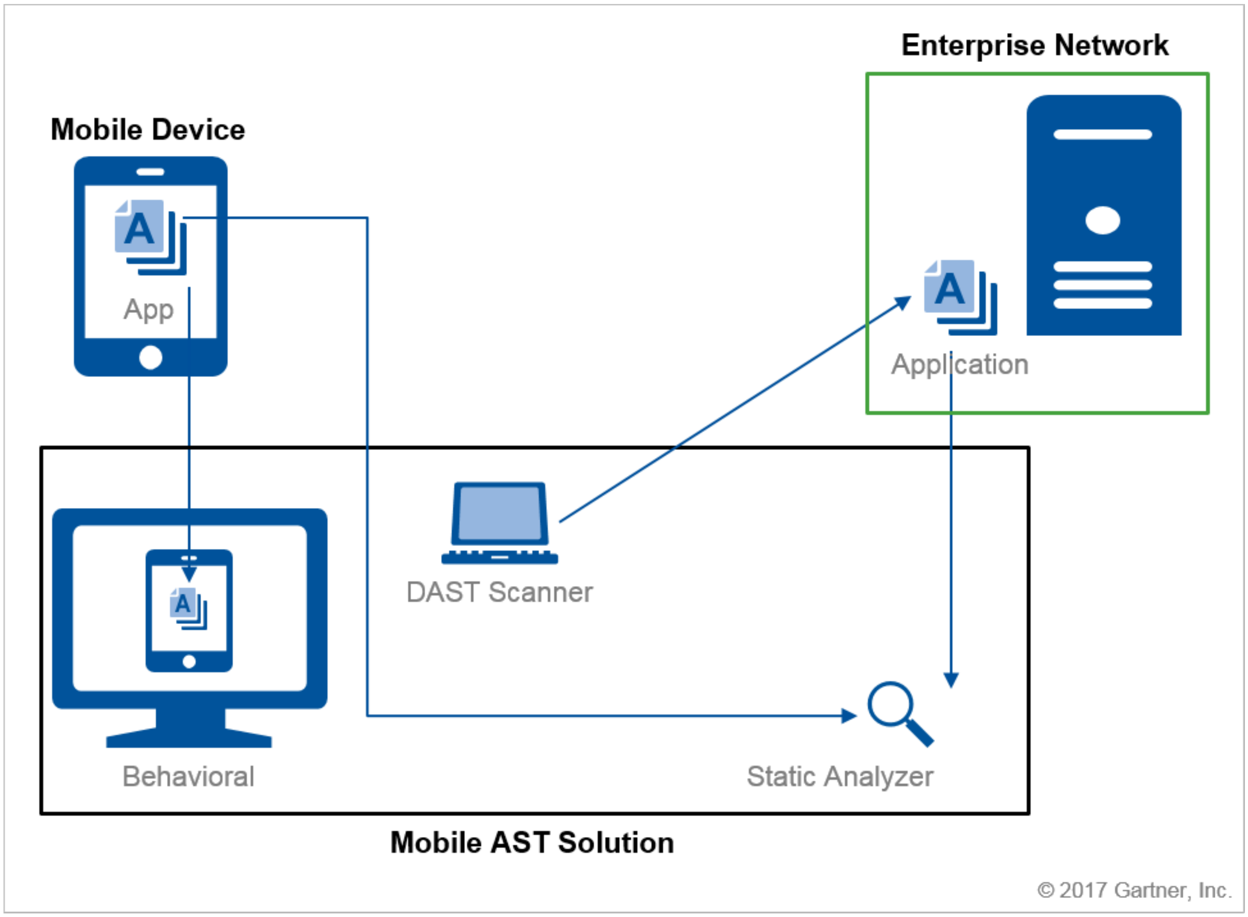
The delivery of the technology can be as-a-service, with some vendors also providing an on-premises option. In this Market Guide, we focus on automated solutions, used by enterprises to conduct security testing on apps they develop, rather than on the multitude of providers that conduct manual security testing, or penetration testing of apps using professional services.

Mobile AST leverages the SAST and DAST techniques used in the broader AST space, with behavioral testing being an innovation. However, these techniques are adapted to mobile platforms. Static analysis has to support different languages (for example, Swift and Objective-C), as well as the iOS and Android platforms.

Some of the code may reside and run on the mobile device, rather than just the web app server, which has multiple implications. SAST now needs to test the code on the device as well as the back-end code. DAST needs to adapt to interactions between the mobile app and the back end. Behavioral analysis can help identify and map these interactions.

Figure 1 shows a model of a mobile AST solution. There are more components used to analyze, correlate and report the findings, but the figure provides an overview of the points of intervention of the solution on the app that is being tested.

Figure 1. Model of a Mobile AST Solution



Source: Gartner (April 2017)

Behavioral Analysis

A main innovation with mobile AST is behavioral analysis. Running the mobile app in an emulator, a simulator or a mobile device, it intercepts the traffic generated so that the mobile AST solution can map the interactions of the app with various other components, such as back ends.

While this mapping can be then used to feed a DAST tool and carry out dynamic analysis, behavioral analysis is also used to observe the behavior of an app during runtime and identify risky, dangerous or malicious actions. For example, it can identify whether the application requests to access the contacts list, but it can also see during runtime whether this list is sent and if so where. This will mainly serve in two cases:

- When testing external components used in the enterprise's apps (for example, third-party libraries that have been added when writing an app). Because in mobile app development, reusing third-party APIs is a very common practice,[1] behavioral analysis is a fundamental component of mobile AST. In this use case, behavioral analysis can be compared to software composition analysis in broader AST, as it identifies vulnerabilities in third-party code, although using a very different technique.
- When performing AST on the mobile app, behavioral analysis uncovers some developer errors, such as sending credentials in clear or unsecure storage.

What behavioral analysis lacks is the ability to identify typical vulnerabilities introduced during development, such as SQL injection or XSS. Mobile AST solutions need to combine other forms of testing, such as DAST and SAST.

Behavioral analysis is often used with apps that are obfuscated, such as commercial apps retrieved from public app stores. Behavioral analysis will compensate, in part, for the lack of static analysis, which cannot be performed because of the obfuscation.

Mobile app reputation solution (MARS; see "Market Guide for Mobile Threat Defense Solutions") offerings leverage this to scan and assess the riskiness of commercial apps, and provide an indication to the enterprise of whether the apps are fit for enterprise use. For example, behavioral analysis can identify whether an app accesses the device contact list and whether it forwards that list to a third party.

Market Direction

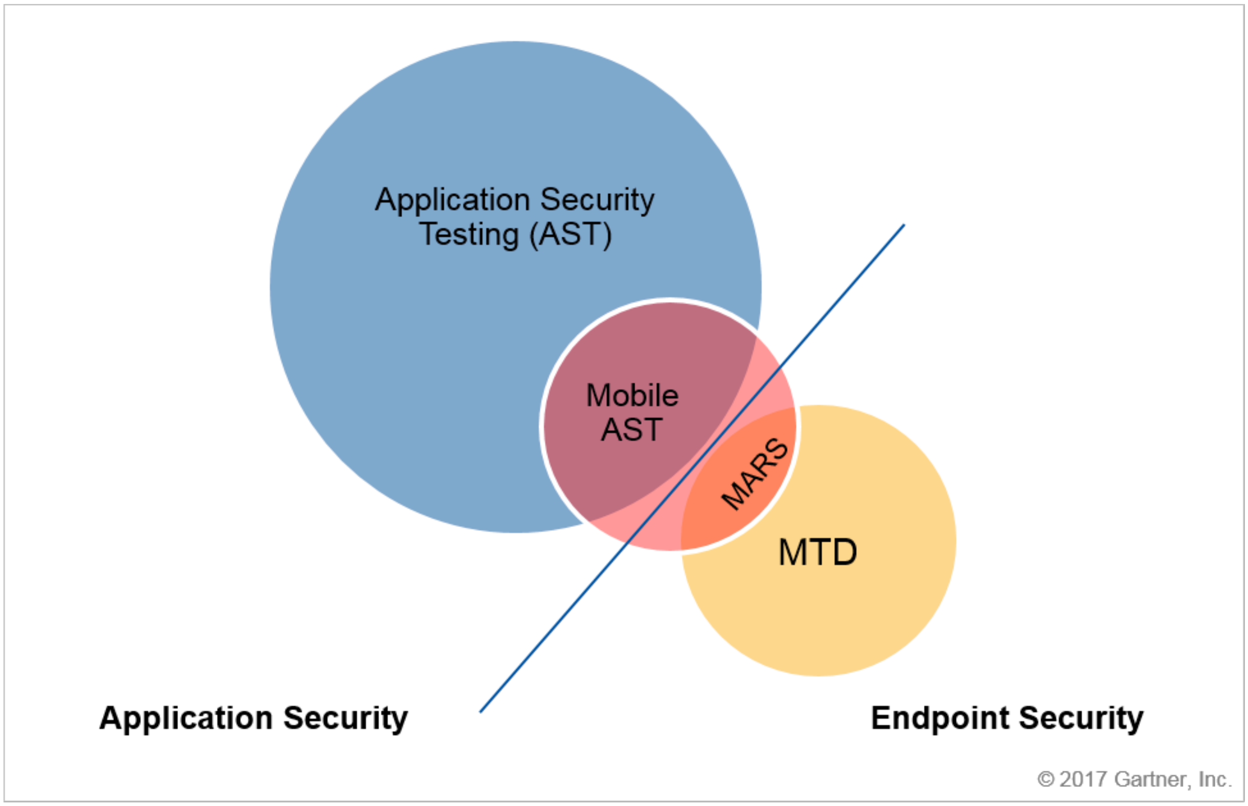
The underlying technologies may be similar, but the use cases and enterprise needs for mobile AST are often different from the ones for the broader AST market. The need to identify vulnerabilities in the code produced and used by an enterprise is still there, but the speed of development, the development processes and the budget allocated for this are very different from traditional AST. Many companies are much closer to a true DevOps approach in mobile than in their other software development activities.[2] The development activities are numerous, fragmented and often do not come from the core team of software development (for example, when coming from citizen IT or business-unit-led initiatives; see "Good Citizen IT App Development Security Depends on Good IT Citizenship"). In many of these scenarios, the need then becomes for a quick, automated, frequent and less detailed testing, opening the door to small newer vendors that can accommodate these requirements.

Mobile applications are growing, and security testing has been following this trend. In a recent Gartner survey, 53% of respondents suggested that they already have mobile apps in their enterprise, while 40% stated they have plans to deploy mobile apps in the future.[2] The landscape is composed of a multitude of new, small vendors with dedicated and innovative solutions, and many well-known AST vendors that have expanded their solutions to address mobile use cases. The evolution of the market will inevitably see smaller mobile vendors merge with larger vendors, but so far there has been little consolidation activity, with only a few acquisitions.[3] and partnerships taking place.[4]

The market adoption for the primary use case of mobile AST on in-house-developed apps is growing, even though it is still only a fragment of the AST market. Some adoption exists also for the MARS use case, but the two are difficult to compare. The buying center for the first is usually the security or application development department, while IT operations governs the second one. The licensing models are also different. Mobile AST follows the AST model with per-app, per-year or per-scan licenses. Indeed, some of the larger vendors include mobile AST in their ordinary AST licensing. MARS, on the other hand, follows the enterprise mobility management (EMM) model, which typically licenses per user per month or year.

Figure 2 illustrates the relationship between AST and mobile AST, as well as its overlap with MARS, in addition to the relationship with mobile threat defense (MTD) solutions.

Figure 2. Relationship and Overlap Between AST, Mobile AST, MARS and MTD



Source: Gartner (April 2017)

From a technology standpoint, the market is in evolution to keep up the pace with the changes in mobile platforms. One example was Apple's introduction of the Swift programming language. Another example is Android's Instant Apps,[5] or the ephemeral apps that WeChat[6] allows to install inside its app, which also show how fast-paced the evolution of mobile AST is, and especially MARS in such situations.

Some vendors are introducing interactive application security testing (IAST) for mobile,[7] to overcome technological challenges. Indeed, behavioral analysis might not detect disguised time bombs that are activated after a long period of time. Additionally, behavioral analysis and DAST will have difficulties in analyzing applications that require authentication with private credentials, and when testing an application as a black box, they will not identify the specific line or portion of code that introduces the vulnerability.

A fundamental component of IAST is the ability to observe the application from the inside while conducting attacks. This is achieved by leveraging the instrumentation that many frameworks and languages support natively (e.g., PHP or .NET). In mobile, part of the app resides in the device however. In this case, instrumentation requires introducing an agent that observes the application and requires running the app on a physical device or an emulator. Because of the rigidity of iOS, that might mean having to use a jailbroken iPhone.

In addition to IAST, some vendors are working on innovations involving runtime application security protection (RASP) for mobile, which we did not consider in this Market Guide.

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

App-Ray

http://app-ray.co

App-Ray is a company based in Austria, founded in 2015 based on an application scanning technology developed by Fraunhofer. App-Ray provides fully automated application scanning with static analysis for iOS and a combination of static and dynamic analysis for Android. Its scanning addresses the OWASP Mobile Top 10 and mainly focuses on privacy breaches and data leaking potentials for apps, while it can also determine certain developer-induced vulnerabilities. App-Ray can scan obfuscated apps and provides MARS. It can be delivered as a service, but also has an on-premises option. App-Ray offers both a-per scan license as well as a subscription package.

Appknox

www.appknox.com

Appknox is a Singapore-based company founded in 2014 that provides mobile AST through a single dashboard delivered in a SaaS model. Appknox provides SAST, DAST and manual testing. It supports apps built on Android, iOS and Windows 10 Mobile platforms. Appknox provides compliance reporting for OWASP Top 10, PCI DSS and HIPAA, as well as other regulations and use cases. Appknox provides an API that allows the solution to integrate in the software development life cycle (SDLC). The company offers its mobile AST solutions under various subscription plans, which cover single platform (either iOS or Android), dual platform (both iOS and Android) or multiple platform (iOS, Android and Windows 10 Mobile) support.

Appthority

www.appthority.com

Appthority is a San Francisco, U.S.-based company founded in 2011 that provides a MTD solution. Appthority's solution, Appthority MTP, provides automated binary scans of iOS and Android applications to identify indicators of risk in the code, such as malicious intent, data leakage capabilities and exploitable vulnerabilities such as unsecure storage or privacy-invasive third-party libraries. Appthority's solution is primarily used as a cloud-based solution. Appthority can also be used as a MARS solution, in which case it can be integrated with existing on-premises EMM systems. Appthority provides per-year licensing that varies depending on the number of mobile apps being scanned and analyzed on an ongoing basis.

Checkmarx

www.checkmarx.com

Checkmarx is an Israel-based company established in 2006. The company offers both web application as well as mobile AST. For mobile, Checkmarx's CxSAST provides static source code analysis for Android and iOS apps. Checkmarx has a broad language and framework support, being able to test Objective-C, C#, Swift, Apache Cordova and Java (Android) apps. Checkmarx also provides a variety of SDLC integration and automation options, such as multiple integrated development environments (IDEs), source code repositories, build servers and bug tracking platforms, as well as incremental scanning. Checkmarx provides mobile AST as part of its broader AST offering, which licenses on a per-user or per-project basis.

Codified Security

https://codifiedsecurity.com

Codified Security is a U.K.-based company founded in 2015. Codified Security's mobile AST product uses static analysis to test the mobile client for iOS and Android, as well as manual analysis to reduce false positives. The product provides a dashboard and reporting on mobile app security issues, including OWASP Mobile Top 10, PCI DSS, GDPR and HIPAA, with remediation advice for each vulnerability. Codified Security supports Objective-C, Swift, Java (Android) and Xamarin. The product provides an API to integrate into the SDLC. Codified Security does not require access to source code. The solution is hosted on Google Cloud Platform. Codified Security licenses its solution on a per-scan basis, as well as with enterprise packages for higher volumes.

Data Theorem

www.datatheorem.com

Data Theorem is a Palo Alto, U.S.-based company founded in 2013. Data Theorem performs static analysis, runtime scanning (dynamic and app logic analysis), as well as server-side and API scanning. Data Theorem's solution scans apps, including third-party SDKs, in production or preproduction. It can constantly monitor customer apps on the major app stores (iOS App Store, Google Play and Windows Store), as well as enterprise app stores, to identify security flaws and data privacy issues. Data Theorem can scan iOS, Android and Windows 10 Mobile applications. Data Theorem's solution integrates into the SDLC with a variety of quality assurance and bug tracking tools, and also provides code remediation. In addition to the mobile AST offering, Data Theorem offers MARS. Data Theorem provides daily alerts on severe security issues, and unlimited scans for its Baseline and Enterprise monthly subscriptions.

Hewlett Packard Enterprise (HPE)

www.hpe.com/us/en/home.html

HPE is a Palo Alto, U.S.-based software and service company that was founded in 2015 when it was split from parent company HP. In September 2016, HPE announced that it would split off and merge its software group with Micro Focus, a U.K.-based software vendor, with the deal set to close in 3Q17. HPE provides SAST, DAST for iOS, Android and Windows 10 Mobile via its on-premises broader AST Fortify offering and the Fortify on Demand (FoD) cloud service. FoD mobile assessments also offer behavioral analysis, and HPE's mobile reputation database is provided free to FoD customers. Behavioral testing is conducted in a real device where permissions, data protection settings and file systems are analyzed for risk. FoD is licensed per scan or as a single app subscription for unlimited scans per year. The on-premises solution is licensed by user.

IBM

www.ibm.com/us-en

IBM is an Armonk, U.S.-based vendor of IT services and products that was founded in 1911. IBM provides a range of AST solutions. IBM's on-premises solution, AppScan, provides SAST of mobile applications, and both SAST and DAST for mobile back-end servers. IBM Application Security on Cloud provides an automated SaaS offering for IAST of iOS and Android mobile apps via an agent that observes app execution to detect vulnerabilities and the presence of embedded malware. Application Security on Cloud is licensed either per scan or as a subscription for unlimited scans for one app for a year. The on-premises solutions are licensed per user.

Kryptowire

www.kryptowire.com

Kryptowire is a U.S.-based company Virginia that was founded in 2011, initially funded by the Defense Advanced Research Projects Agency (DARPA) and the Department of Homeland Security (DHS Science and Technolog [S&T]) to provide mobile application security analysis technologies and solutions. Kryptowire offers Software Assurance as a mobile AST product that performs security and compliance (producing compliance reports for assurance standards such as NIAP) analysis on iOS, Android, and Windows 10 Mobile apps. Kryptowire also provides a MARS product. Kryptowire Software Assurance is available as both on-premises and cloud services, and is licensed on a per-scan or unlimited scan basis.

NowSecure

www.nowsecure.com

NowSecure, formerly known as viaForensics, is based in Oak Park, Illinois, and was founded in 2009. NowSecure provides a cloud-based mobile AST solution that conducts fully automated static and dynamic analysis on iOS and Android. NowSecure uses its own proprietary technology for its mobile AST solution, in addition to leveraging open-source tools, such as Frida and Radare, to which the development of it also actively contributes. The solution integrates in the SDLC at various points, such as bug tracking tools and code repositories, but not the IDE. NowSecure provides vulnerability reports that link to Common Vulnerability Scoring System (CVSS), National Information Assurance Partnership (NIAP), Common Weakness Enumeration (CWE) and OWASP Mobile Top 10, and offers remediation expertise. NowSecure offers annual term licensing with a range of tiers ranging from a limit on apps to fully unlimited usage.

Pradeo

www.pradeo.com/en-US

Pradeo is a mobile application security company based in Montpellier, France, and founded in 2010. Pradeo's mobile AST offering is cloud-based and analyzes binary code rather than source code. Pradeo's automatic behavioral analysis solution includes elements of static and dynamic analysis to determine behaviors as well as vulnerabilities in apps. Pradeo also provides suggested corrective actions, as well as automatic remediation for unwanted behavior. Pradeo supports iOS, Android and Windows 10 Mobile apps, and is available both on-premises as well as in the cloud. Pradeo licenses the solution with an unlimited testing per-app per-year model and applies a decreasing rate based on the total number of apps.

Synopsys

www.synopsys.com

Synopsys is a company with offerings in the software and semiconductor areas founded in 1986 and based in Mountain View, California. Synopsys offers mobile AST as a service via its acquisition of Cigital in November 2016. Synopsys mobile AST combines manual and tool-based SAST and DAST assessments, human-assisted analysis of results, and detailed reporting and actionable remediation guidance. The offering combines automated scanning with manual testing to find vulnerabilities including client-side code, server-side code, third-party libraries and underlying mobile platforms, and provides training in penetration testing and defensive programming for iOS and Android. Synopsys also provides mobile SAST through its Coverity tool, which scans the source code of Android and iOS mobile applications written in Java and Objective-C, respectively. Synopsys provides mobile AST as part of its broader AST offering.

Varutra Consulting

www.varutra.com

Varutra Consulting is based in Pune, India, and was founded in 2013. Varutra's Mobile Application Security Testing Suite (MASTS) uses a combination of source code SAST and DAST, as well as a MASTS Agent to install on the mobile device that facilitates DAST by supporting app authentication where needed. Varutra also provides some behavioral testing functionality, by employing a sniffer that captures the actions of the app over the network to analyze it. MASTS supports test cases from OWASP Top 10 for mobile, and also provides custom test cases. Varutra can test native Android applications, mobile-browser-based and hybrid applications. MASTS includes Snapshot Utility for Android (SAND), which provides details for various phases before, during and after application deployment, such as files and databases created by the application on the device. Varutra MASTS comes in two variants: a trial edition with limited vulnerability test cases and five scans, and the professional edition, which provides unlimited scans.

Veracode

www.veracode.com

Veracode is a U.S.-based application security service vendor in Burlington, Vermont, and founded in 2006. In March 2017, CA Technologies finalized the acquisition of Veracode. Veracode provides its automated cloud services for statically scanning iOS and Android binaries, including those built with cross-platform frameworks including PhoneGap, Titanium and Xamarin, to identify vulnerabilities in the code, as well as DAST for web applications rendering on mobile browsers. Veracode provides a range of SDLC integrations (such as IDEs and bug-tracking tools) and detailed reporting to aid in remediation, and also offers behavioral analysis integrated in its static scanning technology for iOS and Android. Veracode licenses cloud services as a subscription per app.

WhiteHat Security

www.whitehatsec.com

WhiteHat Security is Santa Clara, California, U.S.-based application security service company founded in 2001. WhiteHat Security's Sentinel Mobile offering combines automated and manual SAST and DAST for iOS and Android apps. WhiteHat conducts both source code and binary analysis, and it will perform SAST on the back-end app server if the source code is available. All vulnerabilities are verified by Threat Research Center engineers. Behavioral analysis is conducted in an emulator or real device. WhiteHat also offers mobile business logic assessments, which cover client/server interactions and business logic testing for complex workflows. WhiteHat clients can choose between an express and more comprehensive dynamic analysis.

Other Vendors

There are a number of additional vendors that are active in the mobile AST market that were not profiled in this research but that we can discuss in Gartner client inquiries, including AppSecTest, Entersoft, Foregenix, High-Tech Bridge's ImmuniWeb, MediaTest's Appvisory, Netcraft, NSFOCUS, Shearwater, Tech Mahindra's mobiVIGIL and Verify.ly.

Market Recommendations

Mobile AST is an evolving market and technology space. Gartner expects the market to eventually merge with the broader AST market as the technologies mature, the evolution of mobile platforms slows down and the Windows platform further resembles a mobile platform.

Perform security testing on the mobile applications you develop, but take into account the peculiarities of mobile AST. Integrate mobile AST into your AST program, and use as a precursor or trial of enterprisewide DevSecOps.

Accommodate more fragmented and agile development processes, with multiple sources of development and multiple users (workforce, customers and partners), by using tools that can allow for frequent, automated testing. Ensure to test not just the code on the device, but also its interaction with the back end.

Include behavior-based solutions to test coming third-party libraries, but require traditional AST to be included to test in-house-developed code.

If you are focused on app vetting to identify leaky third-party apps rather than scanning your own in-house apps, select solutions that scan apps as part of a larger MTD offering (see "Market Guide for Mobile Threat Defense Solutions").

Additional research contribution and review was provided by Manish Ranjan.

Gartner Recommended Reading

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

"Avoiding Mobile App Development Security Pitfalls"

"Toolkit: Security Checklist for Mobile App Developers"

"Securing Mobile App Back Ends"

"Good Citizen IT App Development Security Depends on Good IT Citizenship"

"Hype Cycle for Mobile Security, 2016"

"Market Guide for Mobile Threat Defense Solutions"

"Magic Quadrant for Application Security Testing"

"Critical Capabilities for Application Security Testing"

Evidence

[1] Mario Linares-Vásquez, Andrew Holtzhauer, Carlos Bernal-Cárdenas and Denys Poshyvanyk. "Revisiting Android Reuse Studies in the Context of Code Obfuscation and Library Usages." The College of William and Mary, Williamsburg, Virginia and Universidad Nacional de Colombia, Bogotá, Colombia.

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

[3] "Bulking Up for BYOD: Veracode Acquires Marvin Mobile Security," Veracode, and "Proofpoint Buys Mobile App Threat Identification Assets," CRN.

[4] "WhiteHat Security Partners With NowSecure to Deliver the Industry's Fastest, Most Accurate Mobile Application Security Testing Solution," WhiteHat Security, and "Zimperium Boosts Visibility Into Mobile Threat Detection and Remediation Landscape With New Product Features," Zimperium.

[5] "Android Instant Apps," Android developers.

[6] "How Chinese Super App WeChat Plans to Lock out Foreign App Stores in China," Forbes.

[7] "Building the Best Open-Source Mobile App Security Testing Tool: Q&A With the Creators of Frida and Radare," NowSecure.

GARTNER HEADQUARTERS

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

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

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

The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity."