IDC MarketScape

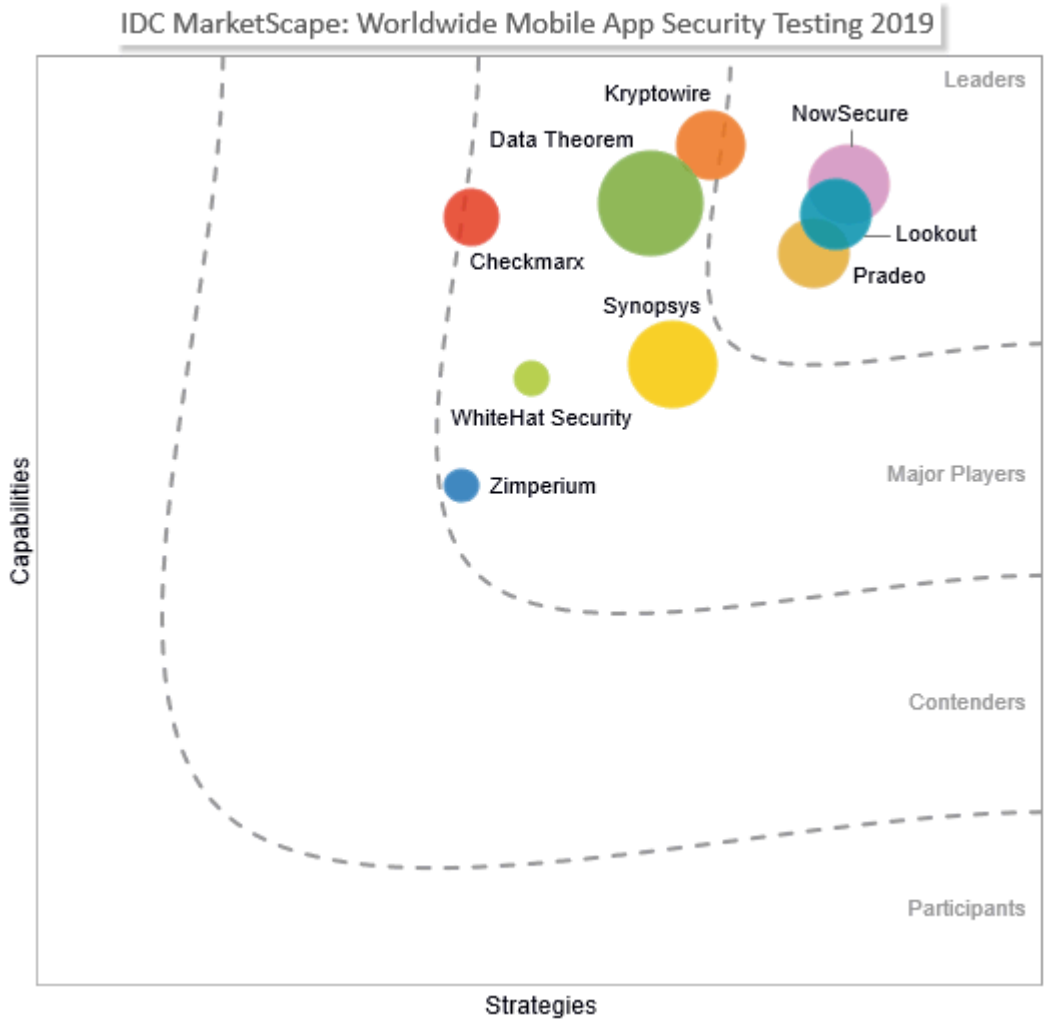
IDC MarketScape: Worldwide Mobile App Security Testing 2019 Vendor Assessment — InfoSec Emphasis

Denise Lund

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Mobile App Security Testing Vendor Assessment



Source: IDC, 2019

September 2019, IDC #US45459219

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

IDC OPINION

Mobile apps are prevalent in organizations today and with this come too many security incidents, including leaked or exposed sensitive data because of mobile app usage by employees or malicious apps installed on workers' devices intended to steal data or spy on user activity. Whether developed in-house or by a third party, the apps are installed and running on employees' mobile devices, thereby bringing with them the mounting security risks to businesses, employees, and consumers. Information security (InfoSec) practitioners are tasked with helping secure massive amounts of data coming and going from these mobile apps that have become increasingly core to workflows in businesses. While an organization's developers are expected to continue to incorporate mobile app security testing (MAST) into the DevOps process as a way to identify and fix risky mobile app code before it is deployed, IT is left to address the host of problems that can come from mobile apps that have already been deployed and are running on employees' mobile devices. The mobile apps in these cases may have been developed by a third party rather than in-house developers, developed using low-code/no-code tools by nontechnical developers in the line of business, or simply developed within an organization, but one that has not implemented an integrated DevSecOps process to catch risky mobile app code early on in the life cycle. Regardless, the opportunity to detect risky mobile app behaviors and the associated problematic code when the app is running, sending data, and integrated with the cloud is significant and touches nearly every organization.

MAST software can give InfoSec practitioners the opportunity to discover mobile app security threats and vulnerabilities before it is too late. The MAST software inspects mobile apps through a variety of analyses looking for risky behaviors, including problematic data sends and risky mobile client-to-cloud integrations. Detailed reports and analyses on the problematic mobile app code and behaviors are provided to the IT department, as well as are made available to be fed into an organization's mobility management solution. This means that security risks such as man-in-the-middle attacks and unnecessary transmissions of location or unencrypted passcode data can be prevented by catching the problematic code and having the mobile app fixed. Blacklisting of problematic mobile apps can be set up with mobility management solution integration. MAST vendors with an InfoSec emphasis often bring key advantages in depth of code tested (source or binary) or in integrations with not only CI/CD processes but also mobile app development platforms. Some MAST vendors have further aligned their software to test with key industry and/or government standards, again helping developers efficiently see problems that require fixes early on in the development life cycle. All MAST vendors, as in many early stage markets, continue to work to build out their road map and ecosystem strategies to include their role in the testing of low-code/no-code mobile apps. Use of mobile apps in workplace is growing.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

To be included in this assessment, vendors must offer MAST software that has capabilities that improve the security of mobile apps for information security-focused professionals. This software must inspect and analyze the mobile app's data usage and behaviors (e.g., connections with back-end/cloud data, network, and services), with the test results benefactor being InfoSec practitioners. The software may or may not have a focus on testing of mobile app code for risks during the development process, as it is not a requirement for this assessment. While we realize that pen testing services often accompany a vendor's MAST software offering, vendors that *only* offer mobile app pen testing services without any MAST software product sales are not included in this study. Other inclusion factors are:

- MAST software offering must be a distinct product offering, rather than just a one-off feature of an offering.
- Offering must, at a minimum, support Android- and/or iOS-based smartphones or tablets.
- Offering must have been available for at least one year.
- Vendors must have a minimum of $1 million in revenue for 2018 in MAST software.
- Offering must have at least two verifiable customers.

ADVICE FOR TECHNOLOGY BUYERS

This study analyzes and rates vendors that have MAST software focused on discovering security risks in mobile apps with the benefactor being information security-focused practitioners in organizations. MAST software must inspect and analyze mobile app behaviors and integrations to identify risky behaviors so that problems can be stopped ideally before they occur. Organizations may choose to blacklist mobile apps until the app code is fixed. Vendors are assessed on a broad range of capability- and strategy-focused criteria. As with many early stage markets, vendors largely have a foundational level of MAST capabilities available. Differentiation opportunities exist with regard to integrations with mobile app deployment and management software, marketing and road map emphasis on modern app development, and a strategic plan that includes attention to how employees and organizations will use mobile apps for work in the coming years. When considering MAST solutions, buyers must take into account that their development approaches will change over time and that vendors have a vision and plan that supports the approach, with progress toward it. Specifically, buyers with information security goals should consider vendors with MAST solutions:

- Vendors must be keenly aware of how the use of mobile apps is evolving in organizations. MAST vendors that show a clear understanding of and priority on keeping their intelligence thorough and up to date on the latest security risks for mobile apps that leverage containers, cloud services, integrations, and third-party components are most likely to have the awareness because of extensive exposure of their analytical tools to mobile apps in use in organizations.
- Vendors should have a vision and road map capabilities for the security testing of low-code/no-code approaches to app development. This is a mobile app development approach that is increasingly common yet carries as much opportunity for security risks as native mobile app development, yet rather nascent in many MAST solutions today. Security testing of mobile apps post deployment is critical to organizations given the growing presence of nontechnical developers in the lines of business who are quickly dragging and dropping components together for mobile apps that address their workflow needs (financial approval workflows, inventory management, etc.).

- Vendors must be forward thinking when it comes to MAST integration strategy. The type of integrations that the MAST vendor has and plans to pursue according to its strategic plan is critical to how well risky mobile apps and app behaviors can be dealt with in any organization. Integration of the breadth of MAST findings with key mobility management software is critical and allows organizations to mitigate security disasters, thereby helping ensure that the MAST findings are used to benefit organizations' mobile usage.

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

Checkmarx

Checkmarx is positioned as a Major Player in the 2019 IDC MarketScape for MAST.

Checkmarx was founded in 2006, with a continued focus on offering a suite of MAST software and services since its inception. Checkmarx's CxSAST is a solution for the inspection of app source code, CxOSA is an offering for open source code analysis, and CxIAST is an offering that monitors app behavior on running apps. Checkmarx rounds out its portfolio of MAST software with the option for a software managed service called AppSec Accelerator, a training platform to improve secure design of apps branded CxCodebashing, and a platform that pulls together all security testing results and analysis for the client into one interface, as well as provides integrations to software development life-cycle (SDLC) processes and IDEs, called the Checkmarx Software Exposure Platform.

The Checkmarx MAST software lets clients apply user-defined rules to testing using the query language provided, as well as tests against industry and government standards (such as MITRE CWE, HIPAA, FISMA, MISRA, and PCI-DSS) and against common vulnerabilities as per OWASP Top 10 and SANS Top 10. According to Checkmarx, the results from the MAST testing are provided with a "Best Fix Location" algorithm, which points a developer to the optimal place in the app to start remedy the identified app security problems. The Checkmarx MAST software can be deployed onsite or hosted in the cloud.

Strengths

Checkmarx has established partnerships in the industry to help round out its MAST portfolio so that organizations that want both a DevSecOps solution and an InfoSec solution can use Checkmarx as a one-stop shop.

Challenges

Checkmarx is missing a strong message around the magnitude of its testing of mobile apps in app stores. While this missing emphasis does not change its MAST value to organizations when it comes to SAST and IAST/DAST capabilities, it does leave prospective clients, particularly those with an InfoSec objective, curious as to how Checkmarx builds its MAST testing backdrop on an ongoing basis beyond what standards are set by industry and government associations or defined by a given client. It also leaves the question open as to in what capacity Checkmarx may or may not incorporate machine intelligence into its MAST approach in the future.

The Checkmarx IAST and DAST solutions, those solutions that are core to MAST with an InfoSec emphasis, are offered as a managed service only, which may cause some organizations to look elsewhere for automated software solutions that do not rely on partner solutions and/or managed services arrangements. Further, the strong product emphasis that Checkmarx has on its MAST DevSecOps value overshadows the benefits it brings to InfoSec practitioners.

Consider Checkmarx When

Organizations should consider Checkmarx when they are looking for an established MAST vendor that can offer both a DevSecOps benefit and an InfoSec benefit to an organization with its portfolio of SAST, IAST, and DAST solutions and are open to a managed services approach.

Data Theorem

Data Theorem is positioned as a Major Player in the 2019 IDC MarketScape for MAST.

Founded in 2013, Data Theorem has established a suite of mobile app security products that use SAST, BAST, and DAST approaches to securing modern apps. Data Theorem offers App Secure, a SaaS offering that automates the inspection of iOS and Android mobile apps, looking for vulnerabilities and data privacy issues. More specifically, App Secure automatically discovers and downloads all the mobile apps associated with a customer's publisher identity on the Apple App Store and Google Play Store, and through the Data Theorem Analyzer Engine, the solution regularly scans for vulnerabilities, prioritizing inspection for those issues that make a mobile app vulnerable to a remote attacker with the goal of data extraction, technical blockers, and other security or privacy concerns that can cause brand damage. Data Theorem also offers Brand Protect, which is a MAST product that automatically crawls the web to find unauthorized, fraudulent, and/or maliciously cloned mobile apps. Core to Data Theorem's MAST for modern apps value proposition is API Discover automated SaaS, a solution that looks for new APIs, any changes to known APIs, and other related cloud-based API services. These APIs are discovered via dynamic runtime testing performed by the Data Theorem Analyzer Engine.

Data Theorem's API Discover service provides an analytic dashboard to track the APIs, informing the client's administrator of suspicious APIs with alerts. These APIs are immediately sent to the API Inspect service for deeper security analysis and compliance policy violations. Data Theorem offers its solutions neither as managed services nor with onsite consulting and professional services, preferring to invest in the scalability of its SaaS suite of MAST offerings for clients. Data Theorem MAST solutions test against government and industry security and privacy standards, including MITRE ATT&CK Mobile, GDPR, HIPAA, PCI, OWASP, and other industry-specific standards.

Strengths

Data Theorem has a visible priority focus on applying MAST to microservices and serverless mobile apps, positioning its solutions as highly relevant to modern app development in organizations today. Data Theorem's commitment to MAST for modern app development is evidenced in the vendor's clear understanding of its target market of InfoSec practitioners and its product capabilities and their treatment of APIs and mobile apps in third-party app stores to this end goal.

While not overly emphasized in its marketing of its value proposition, Data Theorem MAST services automatically test against industry security and privacy standards (i.e., MITRE ATT&CK Mobile, GDPR, HIPAA, OWASP, PCI). By meeting high standards for security and also GDPR and privacy, Data Theorem results are suitable for vulnerability assessments in businesses as well as government and healthcare institutions.

Challenges

Data Theorem's ecosystem strategy would benefit from expansion to include partnerships that will help drive awareness and further adoption by InfoSec practitioners, ecosystem partners in the mobile OS space, and mobile app development platform vendors, including low-code app development platform vendors.

While Data Theorem will complete enterprise mobility management (EMM)/MDM integrations where needed by a client, a priority on proactively incorporating such integrations with its MAST products will take client's ability to efficiently take action among its employee mobile users to mitigate a security risk to a new level.

Consider Data Theorem When

Organizations should consider Data Theorem when they are looking for a MAST vendor that has a major emphasis on integrated MAST solutions with a heavy emphasis on actionable feedback loops driven by the discovery of mobile security risks due to mobile app behaviors and related third-party APIs, services, and mimicked/cloned apps. DevOps teams who are interested in automated security solutions that accelerate their ability to ship secure applications on modern technology stacks should also consider Data Theorem's offerings.

Kryptowire

Kryptowire is positioned as a Major Player in the 2019 IDC MarketScape for MAST.

Founded in 2011, Kryptowire has established itself as a vendor with software-based security testing capabilities that help companies achieve government and industry mobile app security standards. Kryptowire's MAST software automatically tests against internationally recognized security and privacy standards, including NIAP, NIST, OWASP, GDPR, and other industry-specific standards. Kryptowire software performs automated testing of app binaries and every library included in the mobile app, including fully automated dynamic analysis, which uses proprietary forced-path execution to examine every branch of code. Kryptowire provides automated BAST that inspects behaviors of the mobile app user interface (UI) and supports the custom test scenarios. Kryptowire does not have a formal pen testing service to supplement its automated MAST software tests, given its commitment to its MAST software quality and remediation options for problematic mobile apps.

Kryptowire software automatically tests in-house-developed and third-party Android and iOS mobile apps for security vulnerabilities. Kryptowire separates the testing results for all customers for privacy and security reasons. Kryptowire leverages its corpus of pre-analyzed apps as a database in an agnostic, referential sense only to find and use comparable nonclient-specific results. Kryptowire MAST software can be deployed on site or hosted in the cloud and integrates with every major MDM to test every app on every employee mobile device across the enterprise. In addition, Kryptowire can be used at any stage of the SDLC for both developers and IT professionals to perform scans for security risks device assets. In a related but different part of Kryptowire's portfolio, the vendor performs device-specific vulnerability scans of OEM over-the-air (OTA) system app updates.

Strengths

Kryptowire automated mobile app and device security testing technology gives clients mobile app analysis results that are in accordance with internationally recognized software assurance standards (NIST, NSA, OWASP, HIPAA, GDPR, and PCI). By meeting high standards for security and also GDPR and privacy, Kryptowire results are suitable for vulnerability assessments in businesses as well as government and healthcare institutions.

Kryptowire's adjacent offering, namely device-specific vulnerability scans of OEM OTA system app updates, provides an unique context to the testing of mobile apps for security risks. While this is a separately procurable offering to Kryptowire's MAST offering, the vendor can help round out the picture of what security risks appear during a mobile app's behavior.

Challenges

Ecosystem partnerships that will increasingly get Kryptowire in front of organizations that should be thinking about MAST will be advantageous. Partnerships with ecosystem vendors that are complementary in the mobile security software space will facilitate organizations' familiarity with Kryptowire.

Organizations are increasingly exposing their nontechnical employees to rapid mobile app development techniques that will benefit from testing to industry and government standards (i.e., healthcare, financial). Kryptowire should take its marketing messaging to the next level by highlighting its mobile app's testing approach as aligned with mobile apps that have been developed using low-code/no-code tools. Marketing of Kryptowire's solution is holistic, and as such, the company can inadvertently downplay its DAST and BAST capabilities to organizations with a high need for MAST on low-code/no-code mobile apps. Organizations should also consider Kryptowire when they are looking for a vendor that has a holistic integrated MAST offering, including focus on DevSecOps integration.

Consider Kryptowire When

Organizations should consider Kryptowire when they are looking for a MAST vendor that has a major emphasis on testing mobile apps for alignment and compliance with government and industry standards, particularly when organizations are in key security- and privacy-conscious vertical industries such as banking, finance, healthcare, and government.

Lookout

Lookout is positioned as a Leader in the 2019 IDC MarketScape for MAST.

Founded in 2007, Lookout has established a suite of solutions to help organizations with mobile protection against security risks. Core to the suite is Lookout Mobile Endpoint Security (MES) offering, available in two products: Mobile Endpoint Security for Threats and Mobile Endpoint Security Comprehensive. Comprehensive adds data leakage controls, device risks, and customizable app risk policies, as well as the mobile app security testing solution. Lookout has architected its solutions to leverage intelligence informed by over 170 million devices in its global installed base of personal and enterprise devices and over 70 million applications are inspected for security risks and problems. The scale of its security testing and analysis brings to bear over a thousand malicious apps on public app stores and thousands malicious apps per day from other sources. Core to Lookout's Mobile Endpoint Security offerings are Lookout artificial intelligence (AI) tools to analyze data in its cloud, allowing analysis and detection of new and unknown threats such as malware/malicious app variants, phishing attacks, and other sophisticated network-based attacks. Lookout offers optional professional services, including a service that provides manual app pen testing.

Lookout supports integrations into all major third-party MDMs to pull data, produce reports, scale, and enable deployment in organizations. For mobile devices that are unmanaged, Lookout can determine device health (including malware or apps blacklisted by an enterprise or rooted/jailbroken or other device anomalies), making it a simple one-step process to disallow that device to access corporate resources. Last, the Lookout Mobile Endpoint Security Console presents to administrators the app analysis and app risk details in a user interface that allows administrators to enable enterprise policies. Further, Lookout has built numerous partnerships in the ecosystem with mobile carriers, such as AT&T, Verizon, T-Mobile, Sprint, Orange, EE, Deutsche Telekom, KDDI, and NTT DOCOMO, to make the deployment and use of MAST and Mobile Threat Management offerings pervasive in the market.

Strengths

Lookout's use of telemetry to inform AI engine ongoing mobile security risks brings a unique level of app risk knowledge to the company's MAST and other Mobile Endpoint Security capabilities. Lookout's distribution partnerships with many of the world's largest mobile network operators, including AT&T, Verizon, Vodafone, T-Mobile, Sprint, Orange, EE, Deutsche Telekom, KDDI, and NTT DOCOMO, contribute to the vendor's growing base of Android and iOS mobile device and app security knowledge. This growing base of knowledge feeds the Lookout AI engine and includes the growing knowledge set from MAST deployments and use among Global 2000 Enterprises and SMBs in the Americas, EMEA, and APAC regions.

Lookout's console and administrative functionality complements the vendor's MDM integrations, making it possible for Android-using organizations with and without EMM software and iOS-using organizations with MDM software to implement mitigations to mobile app security risks, such as blacklisting of apps and end-user warning notifications. For organizations that decide to blacklist an app that violates a policy in the Lookout system, Lookout informs EMM and SIEM/analytics systems of that event through integrations it has.

Challenges

Lookout's MAST solution is not designed with the goal of mitigating mobile app security risks early in the app development process. While this is not a core requirement for MAST solutions that are focused on the InfoSec practitioner in an organization, it can be a beneficial set of capabilities for an organization to have access to from a single MAST vendor. Lookout could accommodate the need for these capabilities by expanding its ecosystem partnerships.

Lookout does not test mobile apps against government standards automatically, but standards can be customized by clients. The lack of marketing of this capability may inadvertently cause some organizations to look elsewhere if government standards is core to their MAST goals.

Consider Lookout When

Organizations should consider Lookout when they are looking for a MAST vendor that brings an extensive knowledge set and AI to identifying security risks of mobile apps in use in the employee base and an interactive console that affords administrators the ability to apply mitigation policies. Organizations that also plan to deploy Mobile Threat Management tools should consider Lookout as a single integrated offering providing threat detection capabilities and application security testing.

NowSecure

NowSecure is positioned as a Leader in the 2019 IDC MarketScape for MAST.

Founded in 2009, NowSecure is known for its focus on the automated testing enabled by its breadth of SAST, DAST, and BAST solutions. The NowSecure automated binary SAST, DAST, and deep, customizable BAST testing is performed on real devices, not emulators, to help minimize both false-negative and false-positive test results. NowSecure continuously monitors and tests mobile apps in production app stores. NowSecure also offers the Workstation as an option for customers that want to enable security analysts to do deeper interactive testing and certifications with auto-generation of reports. Workstation is a preconfigured hardware and software kit for security vulnerability assessment and penetration testing, testing for complex configurations, and use cases such as IoT, two-factor authentication, and device touch interactions. NowSecure also recognizes that mobile app development takes place with low-code/no-code development tools today and offers its binary testing as a way for clients to test these apps as well. Further, NowSecure integrates with popular CI/CD tools and issue ticketing systems to automate MAST for apps currently in development.

The NowSecure MAST software automatically maps test results against internationally recognized security and privacy standards, including GDPR, NIAP, FISMA, FFIEC, HIPPA, and PCI, as well as industry standards such as AT&T's FirstNet and OWASP Top 10. NowSecure offers manual pen testing services as an option for clients that want it for additional risk mitigation, but as a rule, NowSecure believes that its automated MAST solution with its breadth of testing with low false positives meets most client needs.

Strengths

The NowSecure MAST solution includes deep automated dynamic testing on iOS, in addition to Android and full test coverage of code written by the organization's own developers and in third-party libraries. NowSecure software tests the OS interaction and offers behavioral testing via its NowSecure "Attacker Point of View" approach focused on helping ensure high code coverage, allowing for rigorous API connection behavior testing and ultimately useful in helping organizations flag its risky mobile apps with low false positives and false negatives.

NowSecure has established a varied set of partnerships in the enterprise mobility ecosystem. These relationships not only help ensure that the NowSecure MAST solution is available to potential clients through VARs, resellers, and embedded partner clients that are accustomed to working with but also give NowSecure ongoing access to a pipeline of MAST results that continue to inform its testing intelligence.

Challenges

NowSecure's messaging that speaks to developers is not as targeted to InfoSec practitioners as it could be. NowSecure's detailed discussion of the vendor's value to developers inadvertently overshadows its MAST value to organizations' IT security professionals tasked with finding solutions to help mitigate risks of mobile apps deployed and in use across the employee base.

NowSecure does not have its own portfolio of complementary mobile threat management software. MAST solutions that are integrated with other mobile app-related security software with analysis in one customer interface platform will be increasingly useful and common among security software vendors. This is a challenge that can be solved through ecosystem partnerships or by organically growing one's security software product set.

Consider NowSecure When

Organizations should consider NowSecure when they are looking for a MAST vendor that offers an automated interactive testing solution for mobile apps that have been deployed or provided by a third party and are in use by the employee base in addition to the opportunity to utilize MAST test results on apps in the SDLC process.

Pradeo

Pradeo is positioned as a Leader in the 2019 IDC MarketScape for MAST.

Pradeo was founded in 2010 and offers the breadth of MAST solutions including SAST, DAST, and BAST, delivering app binary inspection results and data and runtime app security test results to its clients. Pradeo's MAST API enables integration within the existing environment to automate security tests and ensure security levels along development cycle, ultimately helping improve the "shift left in DevOps" desired in many organizations. Pradeo also offers automated testing of third-party apps in app stores, which gives the vendor and clients access to a multitude of public applications security reports.

Pradeo provides integrations to SDLC processes and a wide range of enterprise managed mobility (EMM) solutions. It addresses both iOS and Android apps and is available onsite or hosted in the cloud.

Strengths

Pradeo maintains as part of its focus a priority on automatic scanning of third-party apps in app stores as well as an intelligence center that serves as part of the information feedback loop with its AI machine. This investment and priority help put context to Pradeo's MAST results for clients.

Pradeo makes integration of its MAST solution with enterprise software that enables InfoSec practitioners to take action on the results of MAST testing. Pradeo has established integrations with all major EMM/MDM solutions, including Microsoft, VMware, MobileIron, BlackBerry, IBM, SOTI, 42Gears, and FancyFon. In addition, Pradeo has completed advanced integration between its MAST solution and IBM MaaS360 App Exchange.

Challenges

Pradeo does not automatically test mobile apps against government or industry standards. Testing against industry standards can be done on a custom basis if an organization chooses to pursue this with Pradeo. The lack of this capability as part of the standard MAST functionality may cause some organizations to look elsewhere if testing against these is core to their MAST goals, despite the option being available for a custom engagement.

Pradeo's MAST solution does not allow for users' custom testing scenarios, flexibility that can be beneficial to organizations with specific risky security and privacy scenarios in mind.

Consider Pradeo When

Organizations should consider Pradeo when they are looking for a MAST vendor that has a major emphasis on app security test results being part of a virtuous circle of information and action with integrated managed mobility and threat management solutions.

Synopsys

Synopsys is positioned as a Major Player in the 2019 IDC MarketScape for MAST.

Synopsys was founded in 1986 and has made numerous acquisitions over the past few years to build out a portfolio of MAST capabilities to accompany its legacy play in SDLC and app quality testing. Synopsys offers a broad set of MAST solutions, namely Coverity SAST, Black Duck SCA for open source security testing, Defensics Fuzz Testing, and Seeker IAST. Polaris is Synopsys' central management console for the vendor's MAST products. For organizations that do not want to run their own MAST solutions using Synopsys' suite of MAST solutions, Synopsys offers its MAST solution as a managed service, including both automated software security testing managed on behalf of the client and two levels of manual pen testing services. Synopsys tests mobile apps against government on request and against industry standards regularly, including OWASP Top 10, PCI DSS, GDPR, and CWE/SANS Top 25.

Strengths

Synopsys leverages its investments in its CyberSecurity Research Center across its MAST mobile app security analyses, bringing a unique level and nature of thought leadership to the vendors' MAST solutions and analyses.

Synopsys brings together a wide range of MAST technologies from its various acquisitions, enabling it to offer clients solutions that meet their both DevSecOps needs and InfoSec needs.

Challenges

Synopsys emphasizes its MAST benefits to the shortening and improvement of mobile apps that are in the development life cycle but can appeal to more organizations if it increased its emphasis on the value of its dynamic and behavioral app testing for mobile apps in use by organizations.

Synopsys will integrate with EMM software as needed for a client, but not as a standard part of its process for analyzing and managing apps and their security for clients. Synopsys has the capability to integrate, hence it should take this to the next level as part of its standard offering.

Consider Synopsys When

Organizations should consider Synopsys when they are looking for a MAST vendor that has a wide range of MAST products with not only a priority on app security testing results integration with SLDC processes but also testing approaches that will meet InfoSec needs.

WhiteHat Security

WhiteHat Security is positioned as a Major Player in the 2019 IDC MarketScape for MAST.

WhiteHat Security was founded in 2001 and was recently acquired by NTT Security Corporation. As part of NTT, it will operate as an independent, wholly owned subsidiary. WhiteHat Security offers a portfolio of web and app security testing products and for mobile apps specifically, a variety of options. Its security test results are assessed against the variety of AI, machine intelligence, and human manual testing approaches in its Threat Research Center (TRC). WhiteHat's Mobile Bundle for Android and iOS is source code scanning with a manual assessment of the app review by its TRC. Sentinel Mobile SE (Standard Edition) is WhiteHat's automated mobile SAST/BAST/DAST software solution providing unlimited scans using NowSecure's software. The WhiteHat Security Mobile BLA is a manual pen testing-based source code analysis by the security team in the TRC. WhiteHat's MAST

results are integrated into the WhiteHat Security Sentinel dashboard, along with any of the client's WhiteHat web app and website security testing results. In addition, WhiteHat offers a software composition analysis (SCA) solution for clients that want to test third-party elements and integrate this with their other test results, as well as tests against industry standards.

WhiteHat Security integrates with the software development life cycle, ultimately helping improve the "shift left in DevOps" desired in many organizations with its source and manual binary code inspection. WhiteHat also places a product and marketing emphasis on its mobile app behavior testing offering via its solution partnership with NowSecure.

WhiteHat Security integrates with enterprise mobility management solutions if desired, is available as a managed service if desired, and is available onsite or hosted in the cloud.

Strengths

WhiteHat Security offers a broad range of app and website security testing beyond just MAST. The centralization of this into its Sentinel dashboard is valuable to organizations in today's market as they often have a variety of digital apps and sites to test.

WhiteHat Security maintains a TRC that it uses to enhance the accuracy of its MAST results, incorporating AI and machine learning (ML). This investment and priority help put context to WhiteHat's MAST results for clients.

Challenges

WhiteHat's automated MAST solution relies on the direction of its vendor partner offering. By not being able to control a road map of its own for this automated software, it risks not being differentiated enough.

While manual penetration testing can help minimize the chance of false-positive test results that are largely advantageous, WhiteHat's Sentinel Mobile SE relies on this testing by personnel in its TRC, potentially adding time to a client's MAST testing process.

Consider WhiteHat Security When

Organizations should consider WhiteHat Security when they are looking for a MAST vendor that has a major emphasis on app security test results being part of a broader set of app and web security testing offerings with all results available in a centralized dashboard.

Zimperium

Zimperium is positioned as a Major Player in the 2019 IDC MarketScape for MAST.

Zimperium was incorporated in 2013 and offers mobile enterprise security products including mobile threat management and MAST and protection software. Zimperium's MAST offering is z3A, a SaaS solution that analyzes mobile apps for risky, insecure app behaviors. For mobile apps deemed risky by z3A's analysis, the app is flagged, may even be blacklisted according to the client's policy settings, and the app code, behavior, and context as well as the app's privacy and risk scores are provided in the zConsole. zConsole is Zimperium's dashboard that provides role-based access with the client's product subscription capabilities tightly integrated and most notably providing role-based access at the user, team, management, and policy administration levels. MAST results context provided in the zConsole includes domain certificates, shared code, and network communications that are relevant, in addition to privacy and security ratings. Zimperium's zConsole is integrated with major EMM solutions

in the market, including Microsoft Intune, MobileIron, VMware Workspace ONE, IBM MaaS360, Citrix, and SOTI. The z3A MAST technology analyzes apps on employee devices via the inventories pulled by an EMM solution on iOS devices and can access the apps directly or from an EMM solution on Android devices.

In addition to the z3A MAST solution, Zimperium offers zIPS mobile device threat protection software and a mobile application security tool, zIAP, which is used to build security features into mobile apps via an SDK for third-party software developers. The zIAP product has been deployed in mobile apps, protecting over 25 million users. All of Zimperium's solutions leverage the vendor's ML-based engine, z9.

Strengths

Zimperium offers a broad range of threat detection and management software beyond just MAST, so it can be a single provider for a number of security related needs within an organization. The opportunity for clients to integrate MAST results with other threat management and detection results in a centralized dashboard, Zimperium's zConsole, that is set up to give different views and information based on the dashboard user's role is valuable to organizations in today's market.

Zimperium's solutions leverage the vendor's patented ML-based engine, z9. This brings intelligence to bear on MAST results as to risky behaviors and integrations from a variety of access points. The z9 machine intelligence–based engine is continuously detecting static and behavioral states and actions that can create unnecessary security risk to a client through their mobile apps and devices.

Challenges

Zimperium does not test mobile apps against government standards, and it only tests against industry standards if clients specifically request this of Zimperium. By not testing mobile apps against government and industry standards automatically as a regular part of its z3A testing solution, this can cause some organizations to look elsewhere if testing to such standards is critical to their MAST goals.

While Zimperium markets its strength in mobile security threat detection, its MAST solution and value may be overshadowed and missed by clients looking for a vendor to help them first and foremost with MAST.

Consider Zimperium When

Organizations should consider Zimperium when they are looking for a MAST vendor that has a major emphasis on MAST results that are integrated with other mobile threat detection and management solutions and role-based views of results available in a centralized dashboard.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

Mobile app security testing (MAST) software products inspect mobile app code, app behavior, and mobile app client-to-cloud communications for vulnerabilities to a variety of security compromises. IDC defines mobile app security testing approaches according to three major categories:

- **Static app security testing (SAST):** This mobile app testing includes pen testing, which inspects the binary, and sometimes source, code for known vulnerabilities. Note that, for the purposes of this document, pen testing services revenue is excluded, but the rest of SAST revenue is included.
- **Dynamic app security testing (DAST):** This mobile app testing looks for known vulnerabilities or weaknesses in the collection and transmission of personal or business-sensitive data and whether the app's integrations are working as planned (e.g., while the app is running). DAST looks for the vulnerabilities on the mobile device client side of the app as well as the integration with databases and services in the cloud and enterprise software.
- **Behavioral app security testing (BAST):** This testing inspects the mobile client side and back-end integrations for risky behaviors performed by the mobile app. For example, BAST looks for location data and contextual data that would suggest that the app is acting in a risky manner about the network integrations, cloud integrations, and so forth.

All three MAST approaches can be conducted in a manual or automated manner. Manual testing involves dedicated staff that visually inspect and physically test for known vulnerabilities. Automated testing involves the use of analytical software technologies and, in several cases, machine and predictive intelligence algorithms embedded in the testing software.

MAST solutions are part of a larger family of security products defined in *IDC's Worldwide Cybersecurity Products Taxonomy, 2019* (IDC #US44382318, November 2018) as AppSec and DevSecOps. These include secure code analysis and runtime application self-protection tools, which address broader code security and behavioral testing, such as software developed for other endpoint computing platforms (e.g., Windows, Mac) or server-side applications and code in web infrastructure. Penetration testing tools and services are also included in this category.

Strategies and Capabilities Criteria

Tables 1 and 2 provide key strategy and capability measures, respectively, for the success of MAST vendors when it comes to emphasis on InfoSec.

TABLE 1

Key Strategy Measures for Success: Worldwide Mobile App Security Testing

Strategies Criteria	Definition	Weight (%)
Customer acquisition	The vendor has strong direct industry partnerships/access that helps support adoption and use of mobile app security testing (MAST) software.	3.0
Delivery	The vendor shows understanding of how security market is evolving to address mobile app security testing market needs (i.e., approaches and methodologies to test for new types of security risks).	10.0
Financial/funding	There is growth in vendor's revenue.	5.0
Functionality or offering strategy	There is a road map based on customer and partner input that covers core and differentiated MAST software capabilities and demonstrates product growth and expansion to meet current and future market needs.	33.0
	The vendor product is designed to be flexible to accommodate MAST outcomes and actions appropriate to client needs.	
	The vendor can articulate strong differentiation aspects of its MAST offering relative to competition.	
	The vendor's offering demonstrates ongoing suitability and priority to modern app development, including container-based and microservice-oriented mobile app development.	
Growth	The vendor has a proven history of growing its customer base with high focus on mobile apps.	42.0
	The vendor has the agility and the means/ability to make innovation and competitive response happen.	
	There is a strategic plan to penetrate enterprise mobile app development and deployment processes with mobile app security testing and intelligence related to this to make apps in the enterprise less risky.	
	The vendor has a strong strategy to build an ecosystem around MAST products.	
Marketing strategy	The vendor has strong customer segmentation and targeted marketing and sales efforts for its MAST solution.	5.0
R&D pace/productivity	Innovation, proven best-of-breed security criteria, and road map show ongoing attention to this status.	2.0
Total		100.0

Source: IDC, 2019

TABLE 2

Key Capability Measures for Success: Worldwide Mobile App Security Testing

Capabilities Criteria	Definition	Weight (%)
Customer satisfaction	Customers are satisfied with the vendor's current MAST capabilities.	2.0
Functionality or offering	Software ingests high-volume and a variety of mobile apps as part of its app testing foundation.	73.0
	Option for manual pen testing is available.	
	Key capabilities match the market needs for the following items: degree of automation; network-based testing (commonly referred to as testing of data in motion); app scanning of open source elements; third-party library testing; testing of API connection behaviors in mobile app runtime; mapping issues to privacy and compliance regimes like GDPR, PIC, FFIEC, and NIAP; capture and test endpoint connections; and analyzing apps in app stores.	
	Key capabilities balance emulators and/or real mobile devices to optimize results and market needs.	
	Key capabilities run at the speed of customer requirements.	
	Key capabilities match the market need for reducing false positives.	
	Key capabilities match the market need for usability and user experience by key stakeholders.	
	Key capabilities enable blacklisting of mobile apps with risk score presence.	
	Key capabilities provide both pass and fail evidence.	
Range of services	Essential capabilities include DAST.	6.0
	Essential capabilities include BAST.	
Integration capabilities	Capabilities are designed and successful as part of SDLC process/vulnerability tracking systems.	6.0
	Integration is proven with enterprise mobility management (EMM) systems to analyze apps on devices.	
Portfolio benefits	Related software portfolio includes intellectual property that addresses mobile threat management solution or other proven and available solution that assigns and manages risk levels to mobile devices.	1.0

TABLE 2

Key Capability Measures for Success: Worldwide Mobile App Security Testing

Capabilities Criteria	Definition	Weight (%)
Pricing model or structure of product/offering	How cost effective are the purchase options (scalability for price)/price performance?	4.0
	Differentiated messaging and positioning are communicated through various direct, indirect, and social channels.	
Range of services	Configuration of results is customizable to client needs.	2.0
	Managed services are available and optional.	
Testing standards	A vendor tests against government standards (NIASP).	6.0
	A vendor tests against industry standards (OWASP, NIST, etc.).	
	User can create custom test scenarios.	
Total		100.0

Source: IDC, 2019

LEARN MORE

Related Research

- *IDC MarketScape: Worldwide Mobile App Security Testing 2019 Vendor Assessment — DevSecOps Emphasis* (IDC #US45388519, August 2019)
- *IDC TechScape: Worldwide Mobile App Security Testing Technologies, 2019* (IDC #US45182719, June 2019)
- *Mobile App Security Testing Gains Attention Heading into 2019* (IDC #US44521918, December 2018)
- *IDC Innovators: Mobile App Security Testing, 2018* (IDC #US44506918, December 2018)
- *2018 Enterprise Mobility Decision Maker Survey: Software, Management, and Security Highlights* (IDC #US44434018, November 2018)
- *Worldwide Mobile Enterprise Security Software Forecast, 2017 – 2021* (IDC #US43311217, December 2017)

Synopsis

This IDC study uses the IDC MarketScape model to provide an assessment of vendors participating in the mobile app security testing (MAST) market. This study specifically analyzed MAST software offerings from MAST vendors that have a strong emphasis on InfoSec.

"Mobile app security testing software that is well aligned with the future mobile app deployments and usage by employees is an invaluable tool for InfoSec practitioners," says Denise Lund, research director, Enterprise Mobility, IDC. "Third-party mobile apps, apps that have been developed by nontechnical developers with drag-and-drop tools, and even apps built by in-house developers can be addressed quickly by organizations once the risky behaviors are discovered by up-to-date MAST software."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright and Trademark Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights. IDC and IDC MarketScape are trademarks of International Data Group, Inc.

Copyright 2019 IDC. Reproduction is forbidden unless authorized. All rights reserved.