G00270805

Critical Capabilities for Application Security Testing

Published: 17 August 2015

Analyst(s): Joseph Feiman, Neil MacDonald

Global-scale scandals around applications' breaches make application security testing mandatory to ensure that applications will resist attacks. This research, which targets CISOs and security managers, analyzes major AST providers' critical capabilities applied against most essential use cases.

Key Findings

- The majority of enterprises have come to the realization that security testing is a mandatory step in ensuring the security of their applications.
- Enterprises wish to ensure that application security testing (AST) is integrated into the overall software life cycle (SLC) and that it provides enterprise-class capabilities and yet enable capabilities for individual developers and security experts.
- Enterprises are searching for comprehensive solutions that combine multiple application testing technologies and that combine security detection (testing) with protection.

Recommendations

- Continue the use of mature static and dynamic AST technologies and services.
- Adopt innovative interactive AST technology, with its promise of increased accuracy of detection and an application self-testing delivery model.
- Begin adoption of emerging mobile AST technologies to address security, risk and compliance exposures of mobile apps.

Strategic Planning Assumption

By 2018, market penetration of interactive application security testing (AST) technology will reach nearly 35%, up from 10% in 2015.

What You Need to Know

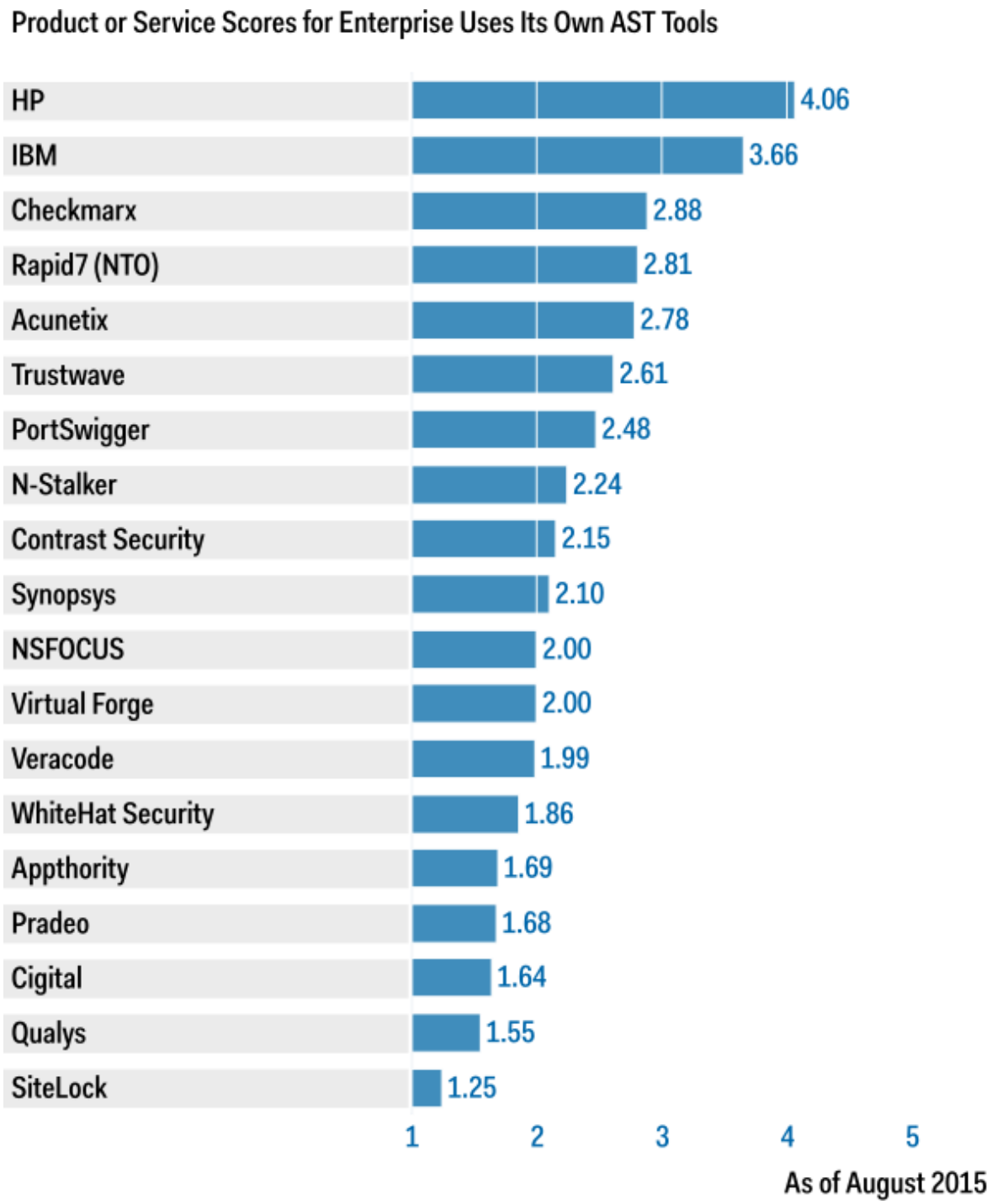
Chief information security officers (CISOs) and security and application development/operation managers should realize that applications are vulnerable to attacks. Teaching developers to program securely is insufficient to ensure application security; it still leaves numerous and serious vulnerabilities incorporated in the code and architecture. A critical and fundamental solution for ensuring application security is application security testing.

This research outlines the critical capabilities of AST technologies and ranks providers against most essential use cases, which include operating purchased AST tools, consuming AST as a vendor's service, manual Web penetration testing, Web application security testing, application code testing, Web application behavioral testing/self-testing and mobile app testing.

Analysis

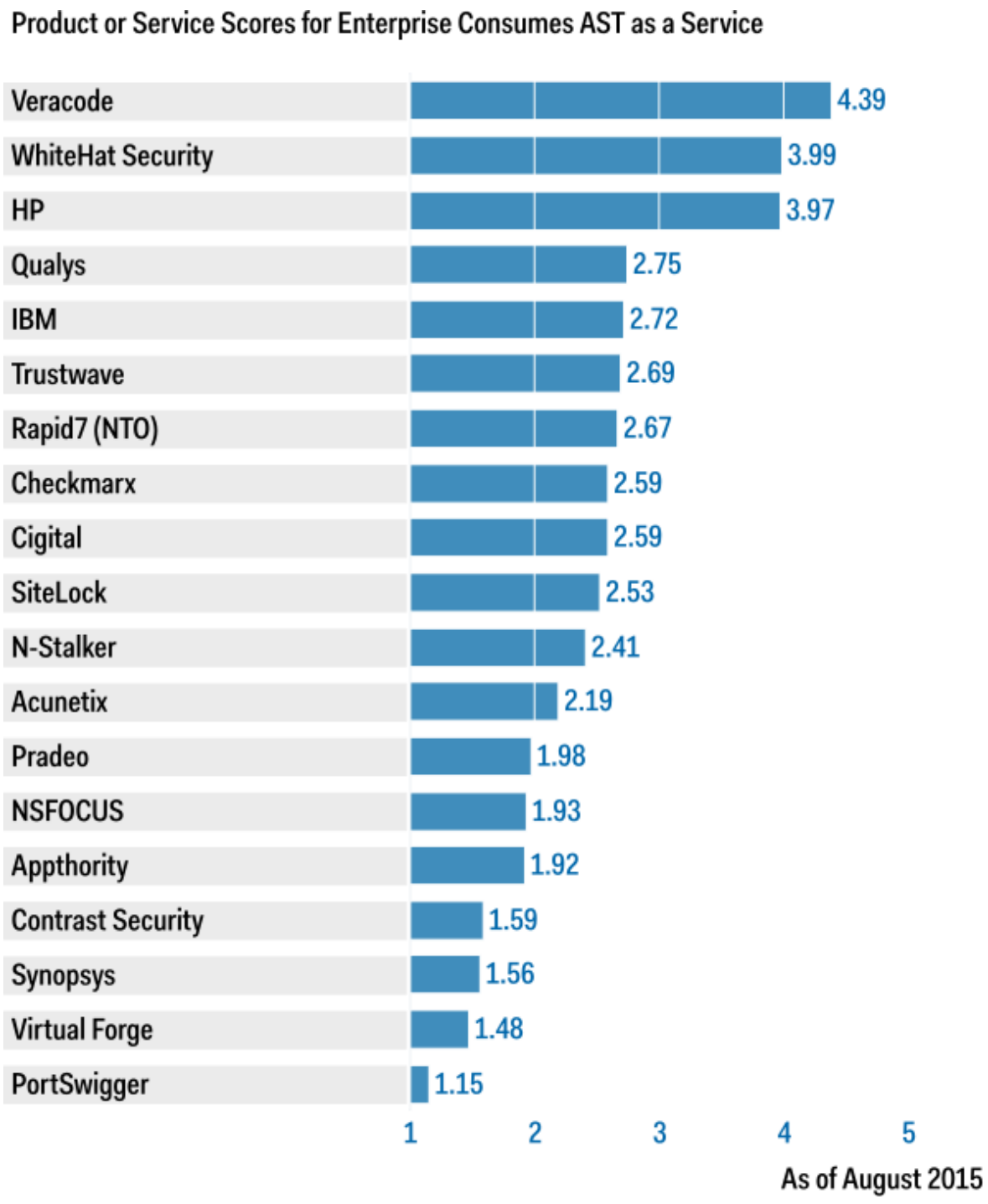
Critical Capabilities Use-Case Graphics

Figure 1. Vendors' Product Scores for "Enterprise Uses Its Own AST Tools" Use Case



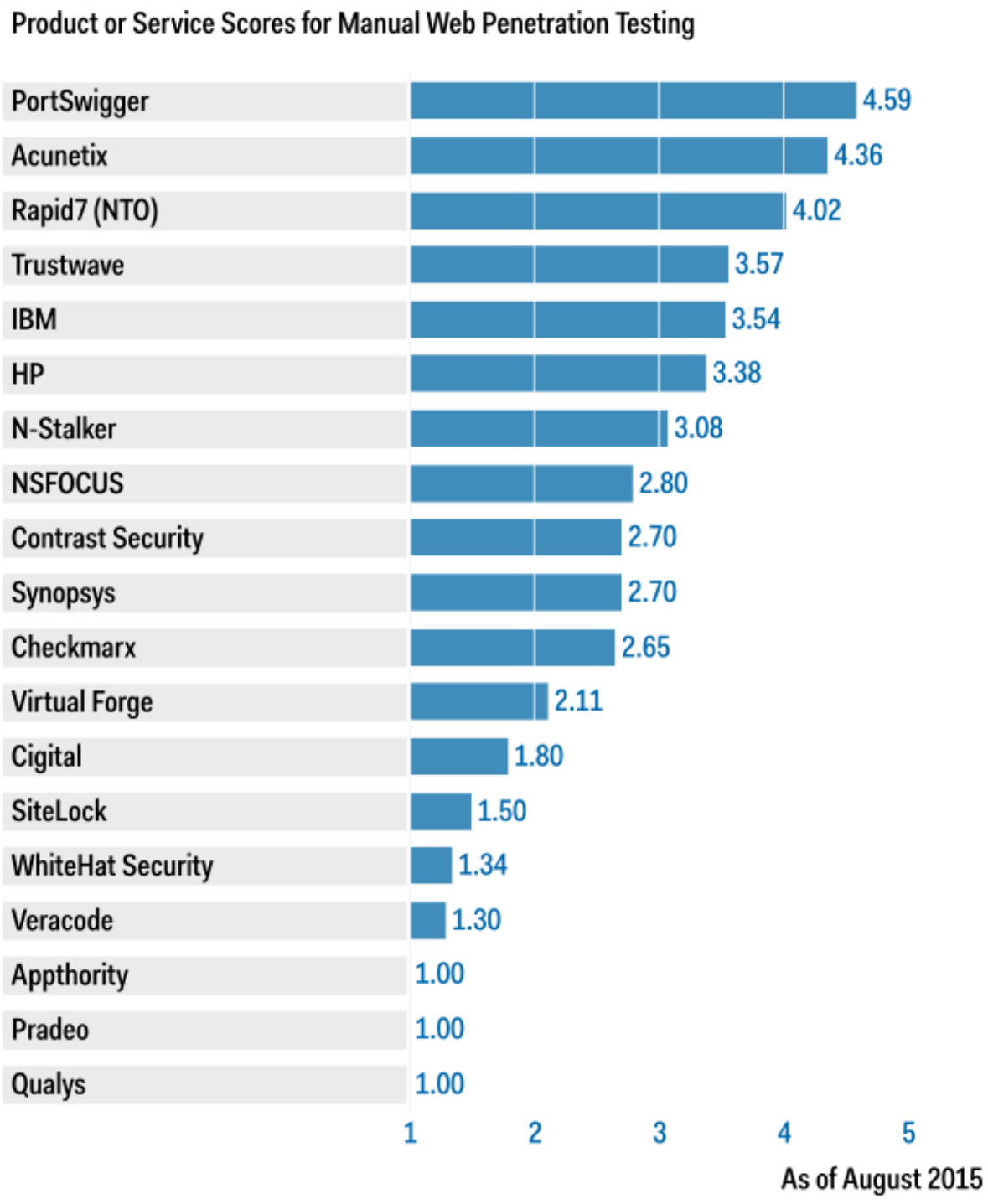
Source: Gartner (August 2015)

Figure 2. Vendors' Product Scores for "Enterprise Consumes AST as a Service" Use Case



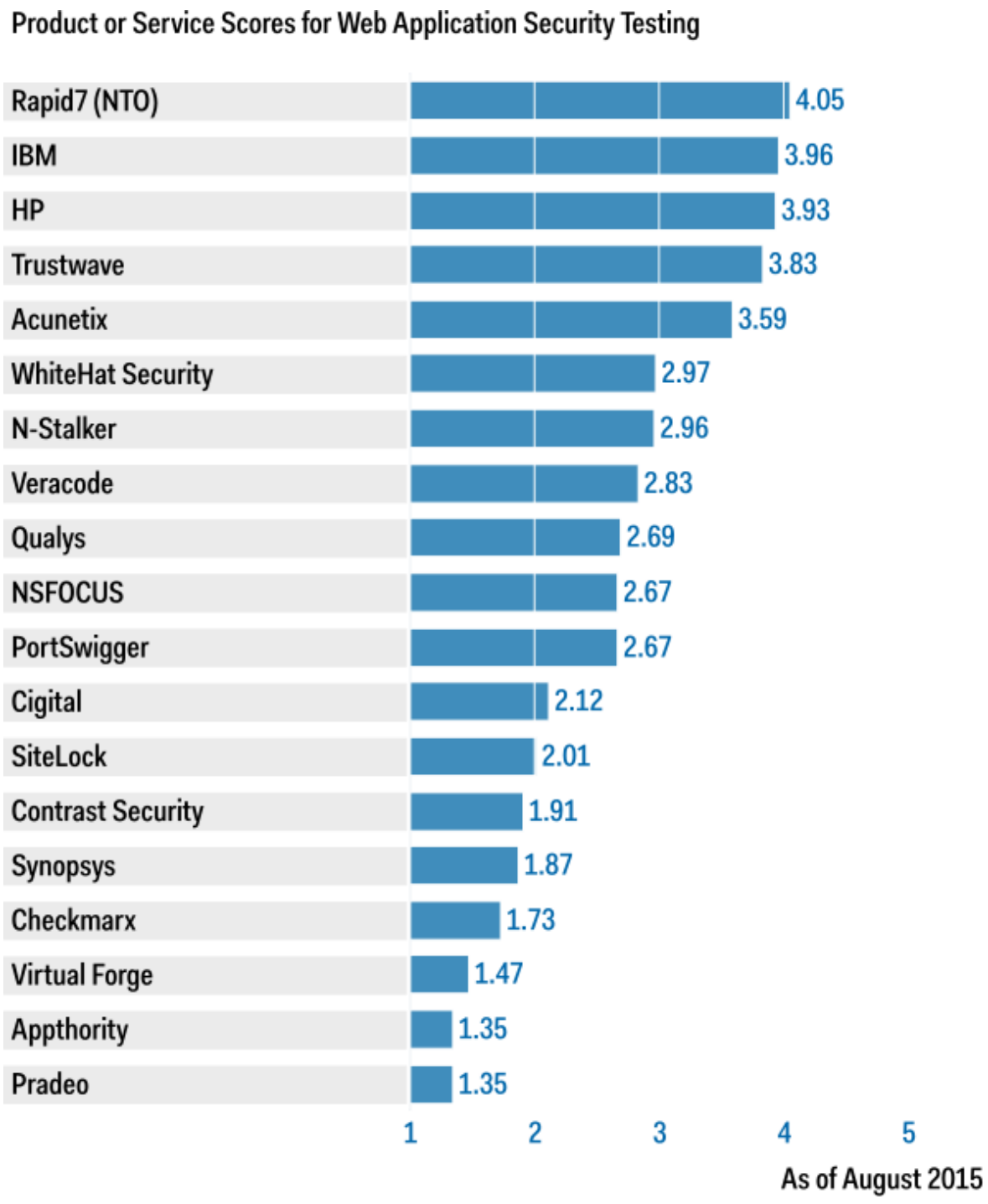
Source: Gartner (August 2015)

Figure 3. Vendors' Product Scores for Manual Web Penetration Testing Use Case



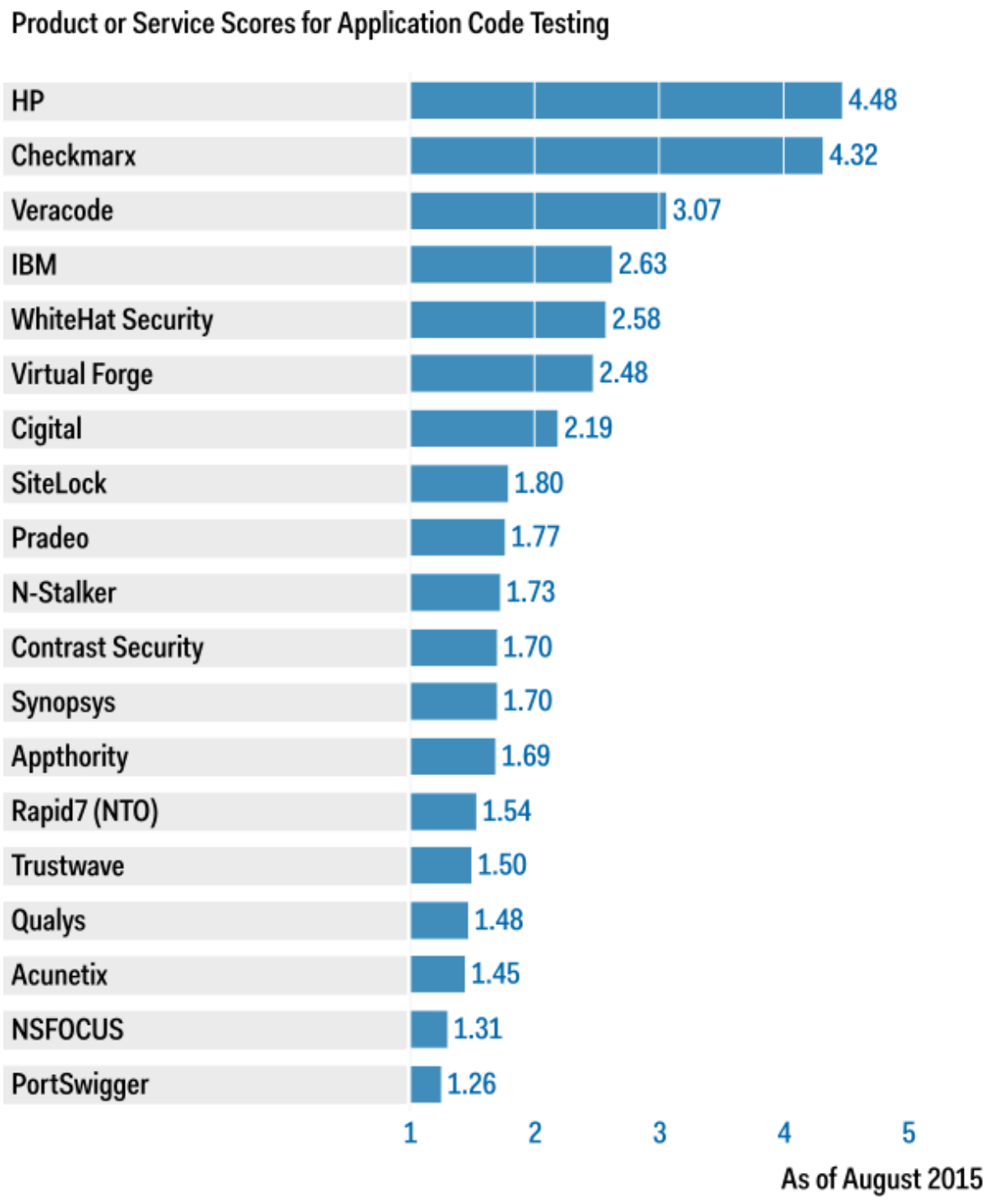
Source: Gartner (August 2015)

Figure 4. Vendors' Product Scores for Web Application Security Testing Use Case



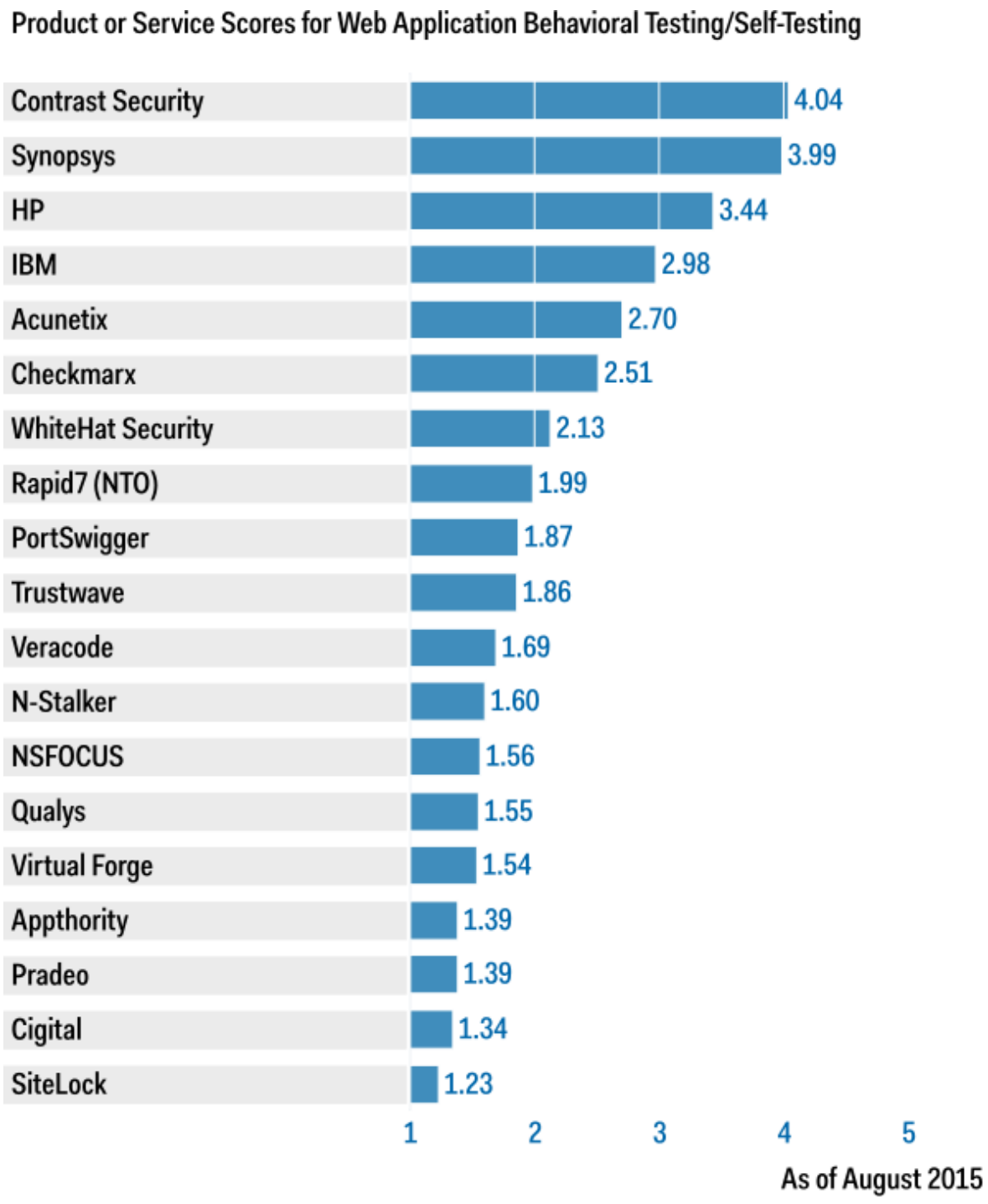
Source: Gartner (August 2015)

Figure 5. Vendors' Product Scores for Application Code Testing Use Case



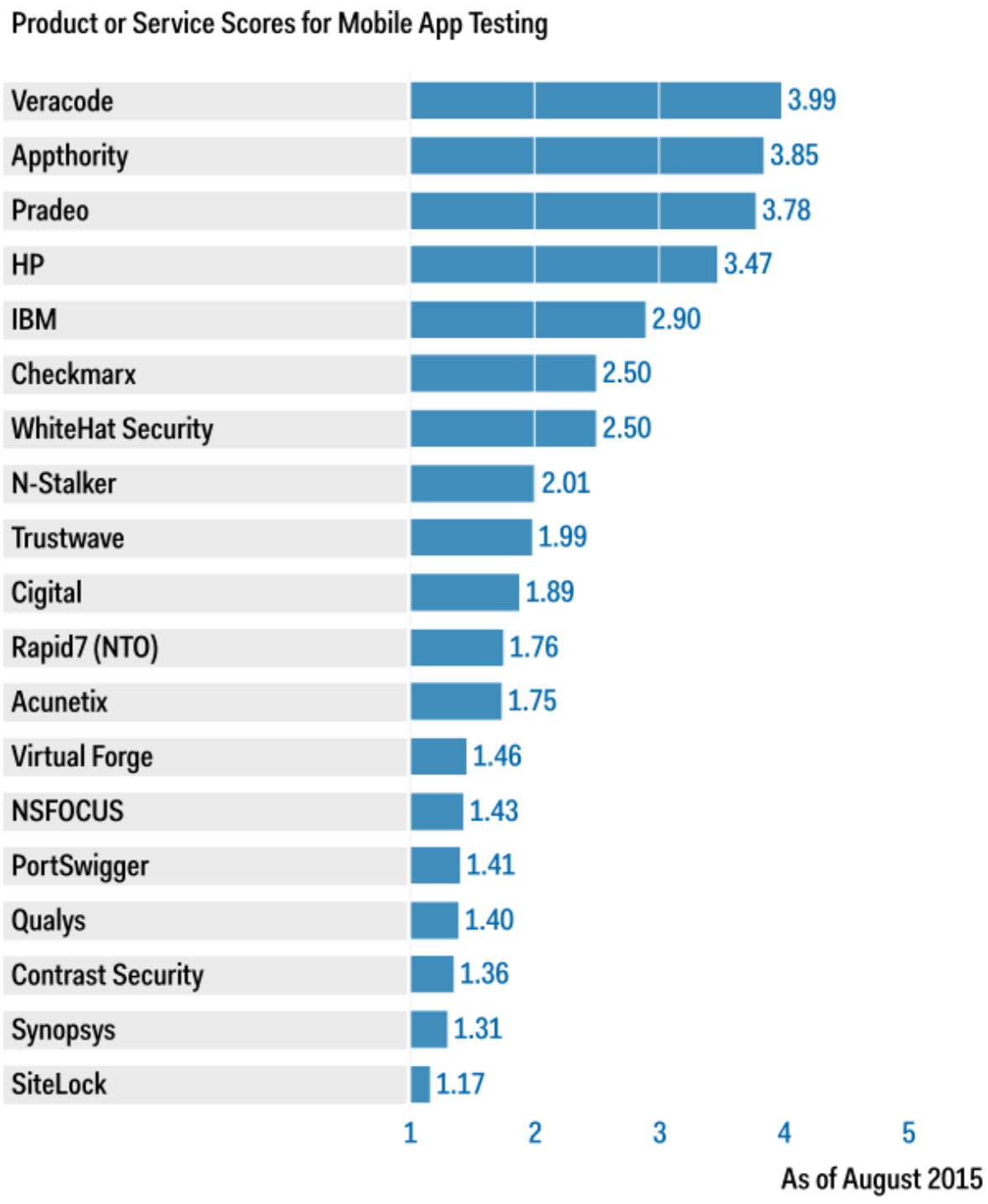
Source: Gartner (August 2015)

Figure 6. Vendors' Product Scores for Web Application Behavioral Testing/Self-Testing Use Case



Source: Gartner (August 2015)

Figure 7. Vendors' Product Scores for Mobile App Testing Use Case



Source: Gartner (August 2015)

Vendors

Acunetix

Acunetix is a Malta-based provider of dynamic application security testing (DAST) tools with advanced technical capabilities. Its Acunetix Web Vulnerability Scanner (WVS) can be run on-premises or from its console in the cloud service (built on Amazon Web Services [AWS]). It also offers a DAST service called Acunetix Online Vulnerability Scanner (OVS). Approximately 20% of its installed base utilizes Acunetix's integrated interactive application security testing (IAST) capability, called AcuSensor, which supports .NET and PHP. Acunetix should be considered by organizations looking for leading-edge Web application penetration testing capabilities conducted by security testing professionals.

Acunetix is one of the highest-rated vendors in the manual Web penetration testing use case. It is also highly rated in these use cases: "enterprise uses its own AST tools," Web AST and Web application behavioral testing/self-testing. This is due to its advanced Web application testing features, such as AcuSensor and AcuMonitor, which enable vulnerability detection with increased accuracy and JavaScript runtime testing. Due to its focus on DAST solutions with integrated IAST, Acunetix is rated lower in use cases such as application code testing and mobile app testing.

Appthority

Appthority is a U.S.-based vendor that was founded to provide mobile AST, risk analysis, behavioral assessment and policy management. It offers a stand-alone portal to upload private or public (third-party) apps for analysis, or to query its database (via a portal or API) for risk rating of more than 3 million analyzed public mobile apps. It can also automatically import apps for analysis from customers' enterprise mobility management (EMM) managed devices. It also provides an application URL analysis to detect connections to malicious or geographically unwanted locations. These processes are fully automated and use AWS to achieve the high scalability of Appthority's services. Appthority's technology is for organizations of all sizes concerned about the security of their own apps or purchased mobile apps, a reputation risk/security rating of mobile apps, and app policy enforcement on mobile devices. Appthority provides testing as a cloud service, with the ability to integrate into customers' on-premises EMM deployments.

Appthority is exclusively focused on mobile AST; it provides quite a full set of methods necessary to comprehensively test mobile apps for behavioral issues, and it earned one of the highest ratings in the mobile app testing use case. Although it provides static application security testing (SAST) and analysis for behavioral issues, it does not test for applications' source code vulnerabilities, such as buffer overflows. Instead, it focuses on identifying binary security vulnerabilities, such as compilation with position-independent executables (PIE), lack of encryption of sensitive data, and risky application behaviors (such as unexpected retrieval of the contact list and transmission of it to an outside IP address). The Appthority offering is only for mobile apps; its focuses on mobile app reputation analysis, and it cannot be used for testing Web applications. For this reason, it is not ranked high in nonmobile use cases.

Checkmarx

Checkmarx is a well-established AST vendor based in Israel that sells its technology in North America, Europe and Asia/Pacific. It has earned a strong reputation for the quality of its SAST tools and services. Checkmarx appeals to application development and security organizations that are seeking a comprehensive SAST tool for a variety of programming languages and frameworks. The SAST tool can test composite applications and provide scalability and quick turnaround times via incremental and parallel tests. The incremental scanning capabilities make the Checkmarx offering attractive to buyers concerned with testing tool impact on the duration of the test. Checkmarx is moving into new application security areas, specifically IAST and runtime application self-protection (RASP), where it currently has beta offerings for these technologies.

Checkmarx offers one of the strongest SAST technologies and earned one of the highest ratings in the application code testing use case. The offering tests a broad variety of programming languages and is well-integrated into the SLC. It is highly rated in the "enterprise uses its own AST tool" use case. Checkmarx offers SAST not only as a tool, but also as a cloud service, and the vendor earned a position in the upper half of the "enterprise consumes AST as a service" use case. It does not offer DAST and therefore does not rank well in the Web AST use case.

Cigital

Cigital, a U.S.-based application security consultancy, entered the DAST-as-a-subscription-service market with its October 2014 acquisition of India-based iViZ Security. Based on the iViZ platform, and using a combination of its own tools and commercial DAST tools, Cigital offers DAST as a service to its customers, which includes a human review of the results. It also offers several levels of SAST as a service. In April 2015, IBM announced that it was partnering with Cigital to deliver its human-augmented DAST-as-a-service capabilities. Cigital should be considered by organizations looking for human-augmented DAST or SAST as a service. Cigital also offers its own SAST tool, called SecureAssist, which is directly integrated with Visual Studio or Eclipse integrated development environments (IDEs) (much like a spell checker) and that can detect a limited number of security coding issues, which earned it a rating above the 50th percentile in the application code testing use case.

Cigital has limited brand recognition outside North America. It does not innovate in the IAST and RASP spaces, it is relatively new to the SAST-as-a-service market, and it does not integrate with Web application firewalls (WAFs). As a newer provider of AST as a subscription service (it is new to this 2015 Critical Capabilities research), and since it is best-known for testing Web applications as a service, Cigital doesn't score as well in cases where tools (not services) are weighted. Cigital's rating, in most use cases, is about at the 50th percentile or lower.

Contrast Security

Contrast Security, based in the U.S., is a startup focused on IAST and RASP. Its IAST aims to bring AST closer to developers and testers and to make AST transparent to them, with no need to buy, install and learn security testing tools, and to reach high scalability by introducing an application self-testing approach. Enterprises, especially Type A's (advanced IT adopters), should also start

evaluating Contrast Security's RASP offering, understanding the emerging phase of this transformational security technology (see "Hype Cycle for Application Security, 2015").

Contrast Security earned the highest ratings in the Web application behavioral testing/self-testing use case due to its execution in the IAST and RASP spaces. Due to its focusing exclusively on IAST technology, Contrast Security does not rank high in uses cases such as Web AST or mobile app testing.

HP

HP is a U.S.-based worldwide provider of SAST, DAST, IAST and RASP products and services. Its flagship Fortify SAST capabilities anchor its offerings, and the Fortify brand has been extended to its other capabilities, including WebInspect DAST and IAST. HP also offers all its AST products as services under Fortify on Demand branding. HP's AST solutions 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.

HP has high ratings for several reasons. First, it is the only AST vendor that provides capabilities in all four areas: SAST, DAST, IAST and RASP. Also, its SAST has the broadest language support of any SAST provider. In addition, HP has a comprehensive set of enterprise capabilities, such as full software development life cycle integration (IDE, quality assurance, bug tracking); Selenium support; role-based access control (RBAC); full authentication integration; SOAP, REST and JavaScript Object Notation (JSON) Web service testing; extensive WAF integration; EMM integration; and Sonatype integration for software composition analysis.

IBM

IBM Security is a dedicated business unit of IBM, a global IT vendor based in the U.S. IBM Security's solutions are primarily composed of tools from various vendor acquisitions (including SAST and DAST acquisitions). IBM has a large portfolio of security technologies, which, beyond application security, include security information and event management (SIEM), identity and access management, data masking, database activity monitoring, endpoint protection, EMM, intrusion prevention, vulnerability management, network forensics, and Web fraud prevention. IBM will appeal to enterprises seeking a single provider of AST technologies and technologies in adjacent security areas.

IBM offers SAST, DAST and IAST technologies, and it earned one of the highest ratings in the "enterprise uses its own AST tools" use case. It also earned a high rating in the "enterprise consumes AST as a service" use case, although, unlike its offering well-established DAST services, it has just started offering a fully automated SAST service. IBM is rated high in Web behavioral testing/self-testing due to its IAST offering. Its mobile AST does not include commercial application ratings, proactive testing or integration with EMM technologies. Its behavioral analysis is in beta testing now and only for the Android platform.

NSFOCUS

NSFOCUS, a China-based vendor, offers the NSFOCUS Web Vulnerability Scanning System (NSFOCUS WVSS) for DAST scanning of websites, as well as the NSFOCUS Web Security Monitoring system (NSFOCUS WSM) for the monitoring of website vulnerabilities, malicious content, defacement and sensitive content. It also offers a DAST service, WebSafe, a cloud-based service that combines these offerings: website vulnerability scanning, Web page malicious software (malware) monitoring, and Web page defacement monitoring on a monthly or weekly basis. NSFOCUS should be considered by organizations looking for basic, competitively priced Web AST products and services where a local-language console and support for Chinese and regional languages are desired, as well as full support for all mainland China.

NSFOCUS is not well-known outside China. The vendor offers no WAF integration other than its own WAF. It offers no capability to test Web services, REST, JSON or XML-based application interfaces for more advanced Web applications. It offers no SAST or mobile app security testing capabilities.

Since NSFOCUS currently tests only Web applications, it fares well only in use cases involving Web AST. For example, NSFOCUS is positioned at or above the 50th percentile in manual Web penetration testing and Web AST; a little lower than the 50th percentile in the "enterprise uses its own AST tools" use case; and low in the application code testing use case.

N-Stalker

N-Stalker, a Brazil-based regional provider of AST products and services, offers DAST as a tool and as a service. SAST capabilities are available only via its Cloud Web Scan platform and are limited to the context of testing Web applications. N-Stalker should be considered by organizations looking for easy-to-use, reasonably priced, enterprise-class Web AST in South America, seeking regional expertise and local-language support for Portuguese and Spanish languages. N-Stalker supports software composition analysis of many commercial off-the-shelf and open-source software products and packages. It has a reasonably broad array of enterprise features (not typically found in smaller providers), such as RBAC, Selenium support, IDE integration, OAuth and OpenID support, and SOAP- and REST-based Web service testing, as well as JSON-RPC and XMPP support. It does not innovate in the IAST or RASP spaces, and it has limited mobile AST capabilities.

Because of its focus on Web AST tools and services, N-Stalker fares better in these use cases. N-Stalker's rating is above or at the 50th percentile in use cases such as "enterprise uses its own AST tools," manual Web penetration testing and Web AST. It ranks lower in Web application behavioral testing/self-testing.

PortSwigger

PortSwigger is a U.K.-based privately owned vendor. It offers free editions of a DAST tool called Burp Suite and an aggressively priced (at approximately $300 per user per year) Burp Suite Professional edition. Burp Suite Professional should be considered by organizations seeking a

powerful DAST tool with advanced testing capabilities, which yet lacks enterprise-class features (such as SLC integration or RBAC console access and reporting).

PortSwigger's Burp Suite is one of the most widely adopted DAST tools in the DAST market, where it sees much adoption for its use as a desktop penetration testing suite. PortSwigger offers a proxy for the real-time capture of Web interactions, including back-end interfaces for dynamic testing. It introduced the Collaborator service component, which interacts with the running Burp DAST tool to improve detection of vulnerabilities such as blind cross-site scripting, XML external entity and server-side request forgery. PortSwigger is ranked the highest for the manual Web penetration testing use case. It ranks well (at about the upper 30th percentile) in use cases such as "enterprise uses its own AST tools," but it lags in other use cases where SAST capabilities, testing as a service, enterprise capabilities and mobile capabilities are important.

Pradeo

Pradeo is a privately held startup based in France. Its technology is delivered as three components: (1) AuditMyApps, a platform for AST; (2) CheckMyApps, a platform for mobile apps' security policy management; and (3) CheckMyApps API, a set of APIs. Pradeo's technology is for organizations looking to conduct comprehensive code and behavioral analysis of their mobile applications. Pradeo offers AST as a service for iOS, Android, and Windows 8 and Windows Phone platforms, and the vendor provides its technology as a cloud service or as an on-premises virtual appliance. Pradeo offers static code analysis (reverse-engineered bytecode or binary code analysis) and behavioral analysis of mobile applications. It also offers its own EMM agent, which can enforce policy on managed devices that use risky apps. It ranks one of the highest in the mobile app testing use case, but because mobile AST is its exclusive focus, it does not rank high in other use cases where Web application testing is required.

Qualys

Qualys is a U.S.-based provider of cloud-based security services. Its Web Application Scanning (WAS) DAST service offering is completely automated and integrated with the other Qualys services in its Web-based customer portal. The same portal is used to provide WAF and vulnerability management services. To access internal applications for testing, Qualys uses a physical or virtual appliance with the established secure VPN connectivity. Because of WAS's low cost, many enterprises use more expensive competitive offerings for their critical applications' testing, while they supplement testing the rest of the application portfolio with Qualys WAS. Qualys should be considered by any organization looking for basic Web AST as a service at an extremely competitive price.

Because Qualys offers only Web AST services, it fares well only in those use cases. Qualys is highly ranked in the "enterprise consumes AST as a service" use case. It is positioned at about the 50th percentile in Web AST because this use case also weights the availability of a tool (which Qualys lacks). Because Qualys does not offer tools but only services, does not offer SAST or IAST, and does not innovate in RASP or mobile AST, it is lagging in the other use cases.

Rapid7 (NTO)

NT OBJECTives (NTO) is a U.S.-based provider of DAST products and services. In 2015, NTO was acquired by Rapid7, which is best-known for its network vulnerability scanner capabilities. Rapid7's offerings include AppSpider Pro (renamed from NTOSpider, its completely automated Web app scanner), AppSpider Enterprise (enterprise portal), and AppSpider Enterprise OnDemand (DAST as a service, with five levels of testing). Rapid7 should be considered by organizations looking for enterprise-class DAST products and services as a competitive alternative to larger providers.

Rapid7's offering earned the highest rating for Web AST due to DAST features. These include its "universal translator," which enables testing of various types of exposed back-end interfaces, such as JSON, REST, SOAP, XML-RPC, Google Web Toolkit (GWT) RPC and Action Message Format (AMF). These features also include its enterprise capabilities — enterprise console, RBAC, one-click vulnerability verification, bug-tracking integration and extensive WAF integration. Rapid7 is well-positioned in many other use cases, but due to its focus on DAST, it lags in the application code testing use case.

SiteLock

SiteLock, a U.S.-based service provider, is a new entrant to the AST Magic Quadrant and Critical Capabilities research for 2015. SiteLock is best-known as a result of its partnership with Web hosting providers, such as GoDaddy. SiteLock offers three tiers of completely automated Web application scanning services (application scan, application pen testing and SecureVIP), using a combination of its own tools and commercial tools for Web hosting customers, as well as those that come to SiteLock directly. The vendor also has integrated network vulnerability scanning of the Web server, as well as integrated SAST capabilities specifically for Web applications developed in Java or PHP. It offers services beyond AST for Web applications, such as WAF and distributed denial-of-service protection and malware removal. It has no product offerings and sells its DAST and SAST solutions as a service only. SiteLock should be considered by midsize organizations seeking comprehensive Web AST with both DAST and SAST analysis. Because of its exclusive focus on Web AST services, SiteLock fares better in these uses cases.

Synopsys

Headquartered in France, with R&D in Israel, Quotium is a point solution vendor of an IAST product called Seeker. As the AST Magic Quadrant and Critical Capabilities research was coming to completion, Synopsys announced its acquisition of the Seeker technology from Quotium. Gartner will watch the progress of Seeker's integration into Synopsys' portfolio of quality and security testing technologies.

Seeker should be considered by enterprises' security and application development organizations that are seeking to adopt an innovative IAST technology that provides effective vulnerability detection and that can be reasonably easy to embed into SLC. Seeker is one of the most broadly adopted IAST technologies in the IAST market. It offers IAST for Java, .NET and PHP application server platforms, as well as support for PL/SQL and T-SQL, and includes JavaScript analysis. It ranks one of the highest in the Web application behavioral testing/self-testing use case. It ranks at

about the 50th percentile in the "enterprise uses its own AST tools" use case. But due to its focus on IAST technology only, it does not fare well in use cases such as "enterprise consumes AST as a service" or mobile app testing.

Trustwave

Trustwave is a U.S.-based worldwide provider of security-related products and services. Trustwave expanded its AST business with its 2014 acquisition of Cenzic. At the time of this writing, Trustwave was in the process of being acquired by Singtel, and it will remain a stand-alone security-focused business unit of the company. In its AST offerings, Trustwave is focused on offering DAST products (App Scanner Enterprise) and services. It offers mobile app security testing services with its Managed Security Testing (MST) offering. As part of its AST suite, Trustwave offers a manual application penetration testing service. Trustwave should be considered by organizations looking for an enterprise-class DAST solution with product and service options and competitive pricing, manual application penetration testing, or a "one-stop shop" for PCI-compliance-related products and services. For these reasons, it is highly positioned in manual Web penetration testing and Web AST. It is well-positioned at about the 30th percentile in the "enterprise uses its own AST tools" and "enterprise consumes AST as a service" use cases.

Veracode

Veracode is a U.S.-based well-established provider of SAST, DAST, software composition analysis (SCA) and mobile AST cloud services, and it is a provider of software supply chain testing. Veracode technology will meet the requirements of organizations that want to delegate their AST and SCA to a third-party expert with a strong reputation for the quality of its services and continuous innovation in application security. Veracode offers scalable AST as a service and tests tens of thousands of applications per year. It offers APIs for integrating its cloud-based services with multiple IDEs, code management and bug-tracking tools and build servers, thus making AST more seamless, expedient and better integrated with agile SLC processes. Veracode's Vendor Application Security Testing (VAST) program enables software composition and software supply chain analysis. Veracode offers comprehensive mobile AST as a cloud service, which includes static bytecode and binary code analysis, as well as behavioral analysis in the mobile device emulator or in a physical device. It also offers a mobile app reputation service for commercial application risk/security ratings for the most frequently downloaded apps from app stores. Veracode mobile testing supports iOS, Android, BlackBerry and Windows Mobile platforms.

Exclusively focusing on SAST, DAST and now IAST as a service, Veracode earned the highest rating in the "enterprise consumes AST as a service" and mobile app testing use cases. It is also highly rated in in the application code testing use case. Because Veracode does not offer AST tools, it is rated lower in the use cases that weight the availability of a tool.

Virtual Forge

Virtual Forge is a Germany-headquartered SAST solution provider, with a specific focus on and expertise in the security testing of SAP's ABAP programming language. Virtual Forge offers its solution CodeProfiler as a product or as a service. Virtual Forge can perform dynamic testing of the

secure configuration of the SAP environment with its SystemProfiler. Virtual Forge also offers SAP penetration testing services. IBM and Checkmarx resell Virtual Forge's ABAP testing capability as a part of IBM's AppScan and Checkmarx's SAST solutions. Virtual Forge should be considered by security-sensitive organizations that have extended and customized their SAP environment and that want to better understand their SAP security and risk posture.

Virtual Forge earned a high rating (about the 30th percentile) in the application code testing use case. Because it focuses on a single application ecosystem (SAP) and a single language (ABAP), it is positioned below the 50th percentile in the other use cases.

WhiteHat Security

WhiteHat Security, U.S.-based global company, is a well-established security-as-a-service provider of DAST and SAST. WhiteHat Security should be considered by organizations looking to delegate their DAST and (to a lesser degree) SAST and mobile AST to an expert third-party testing service provider. Those organizations will also benefit from WhiteHat Security's offering where all DAST and SAST services include a human-augmented review of the results to improve the accuracy of the tests. Its DAST service is highly scalable and is capable of testing tens of thousands applications per year. It offers correlation between SAST and DAST for improving accuracy of detection. Its SAST has one of the lowest adoption rates among SAST vendors. For mobile testing, WhiteHat Security provides automated source code analysis for Objective-C and Java, but it does not offer automated behavioral testing, a reputation service, or proactive testing and integration with EMM. Optionally, it offers a manual assessment service for mobile that covers behavioral testing at an extra cost.

Because of its focus on DAST and SAST as a service, with some mobile AST capabilities, WhiteHat Security earned one of the highest ratings in the "enterprise consumes AST as a service" use case, and it earned quite a high rating in the Web AST use case. Because WhiteHat Security does not offer tools but only services, it is rated lower in the use cases that account for tools.

Context

When selecting AST tools, enterprises should evaluate them in terms of different use cases, such as use as products or cloud services, or use for Web or mobile testing. Vendors differ in their ability to address different use cases. To help with vendor selection, Gartner offers this research, where it ranks vendors' technologies against typical, most essential use cases.

Product/Service Class Definition

We review nine classes of products and services: dynamic AST as a tool, dynamic AST as a service, static AST as a tool, static AST as a service, interactive AST, mobile AST, enterprise-class AST, stand-alone AST, and WAF/EMM integration or RASP.

Critical Capabilities Definition

Dynamic AST as a Tool

DAST technologies are designed to detect conditions indicative of a security vulnerability in an application in its running state. This critical capability focuses on DAST offered as a tool operated by the enterprise itself.

DAST technology analyzes applications in real or "almost" real life — that is, during operation or testing phases, which is an important advantage. DAST can often accurately identify the exploitability of the potential vulnerabilities it finds, because it analyzes application responses to the dynamic tests. However, even when a vulnerability is detected, DAST technology cannot point to the line of code where it originates, because DAST is a "black box" technology that does not have access to source code.

Most DAST solutions test only the exposed HTTP and HTML interfaces of Web-enabled applications. However, some solutions are designed specifically for testing non-Web protocol and data malformation (for example, RPC and Session Initiation Protocol [SIP]). DAST tool providers will vary on functionality, such as the ability to test complex JavaScript applications, HTML5 applications and other types of applications that involve the use of client-side code. Since most Web applications also use API calls (SOAP or RESTful based) to back-end applications, DAST tools should be able to discover, proxy and probe these interfaces for security vulnerabilities.

Dynamic AST as a Service

DAST-as-a-service capabilities encompass the same types of functional requirements as DAST tool capabilities. However, in this capability, the DAST functionality is delivered by providers as a service to enterprises over the Internet.

There are functional requirements and attributes that differentiate DAST as a service from DAST as a tool. Notably, DAST as a service should provide specific service levels for testing results and offer a variety of pricing options that are related to depth of analysis. It should also offer an option for human augmentation in the fully automated testing process to reduce false positives. Fully automated services will typically cost less, but there are limitations as to what vulnerabilities a fully automated scan can detect. There may also be issues with network connectivity and visibility for the testing of non-Internet-accessible applications requiring either an on-premises footprint to launch tests from, or VPN-level access to the applications to be tested. Likewise, comprehensive testing of the back end of Web-enabled applications requires visibility to the APIs and interfaces used to call out to other applications.

Static AST as a Tool

SAST tools are designed to analyze application source code, bytecode, and binaries for coding and design conditions that are indicative of security vulnerabilities. These solutions analyze applications in a nonrunning state.

We evaluate a tool's ability to analyze multiple programming languages; analyze source code and in addition or instead analyze bytecode and binary code; conduct software composition analysis; and assure security of the software supply chain. Ideally, the product should be tunable for an organization's specific coding practices and standard libraries, reducing the number of false positives that result from the testing. In addition, potential vulnerabilities should be categorized based on their severity and the confidence that they are real, providing enterprises a way to focus on the highest-confidence, most-severe vulnerabilities first. Since, ultimately, developers are needed to fix the vulnerabilities, there must be features for integration with bug-tracking and build management systems to help with security integration into the SLC.

Static AST as a Service

SAST-as-a-service capabilities encompass the same types of functional requirements as SAST tool capabilities. However, in this capability, the SAST functionality is delivered by providers as a service to enterprises over the Internet.

Just as in the SAST-as-a-tool space, vendors here differentiate on the breadth of languages and frameworks supported, as well as on their ability to perform security testing on source, byte and binary code. The testing of binary code or bytecode is a differentiator when testing third-party libraries and executables, where access to the source code is not possible. Because in the SAST-as-a-service category, a third party (that is, an AST service provider) is testing potentially sensitive intellectual property, some vendors minimize this risk by keeping the testing local, with a managed appliance. Others minimize the risk by testing binaries. In all cases, there must be an established reputation for trustworthiness from the providers and their architecture, people and processes, since they are dealing with sensitive intellectual property in the applications and dealing with sensitive information in the form of the vulnerabilities they discover. Service-level agreements become a differentiator as does human augmentation of the results to reduce false positives.

Interactive AST

IAST conducts behavioral analysis of applications, observing applications' input/output, logic, and data flow. An inducer feature executes test/attack scenarios. An agent residing inside an application server conducts runtime analysis of the application code, memory and data flow.

We evaluate vendors' degree of in-depth instrumentation of the runtime environment, which assures the degree of IAST accuracy. IAST technology is language/platform-dependent; that is, separate IAST tools are required for Java, .NET, PHP and other languages/platforms. Therefore, we evaluate vendors' breadth of language/platform coverage. An IAST inducer can be a typical DAST tool, a built-in attack generator, or any type of test, including quality assurance, user acceptance, performance and other tests. Therefore, we evaluate vendors' breadth of inducers. We also evaluate vendors' ability to analyze database access, including access authorization and data flow analysis. Finally, we value vendors' ability to effectively advise programmers and security specialists on the exploit path, which might include visualization and/or detailed explanation of the exploit path.

In this category, we also include capabilities that enable a product/service collaborative component to interact with a running AST tool to improve detection of some vulnerabilities.

Mobile AST

Mobile AST is designed to analyze mobile apps for coding, design, packaging, deployment and runtime conditions that indicate security vulnerabilities or risky behavior of mobile apps. Testing can also point to app functions that conflict with an enterprise's security policies.

We evaluate vendors' capability to analyze apps developed in-house, apps developed by third parties and commercial apps retrieved from public app stores. We evaluate vendors' capability to conduct a multistep testing process: the ability to analyze application code (source, byte and binary) for security vulnerabilities and undesirable behaviors; the ability to analyze application behavior at test runtime to detect malicious behaviors in the background while app performs expected legitimate functions in the foreground; the ability to test an app's communication with Web services and test Web services themselves; the ability to provide risk/reputation ratings of commercial apps; the ability to automatically submit apps for testing to ensure that no app is left untested; and the ability to integrate app testing and app protection. We also evaluate a product's architecture and how all tool components are integrated with each other in a comprehensive solution.

Enterprise-Class AST

This is a vendor's ability to support enterprise requirements with its AST solution. It includes AST tool/service integration into the SLC, enterprise-class management of the AST process, a reporting system and RBAC.

Most enterprises (especially larger ones) have numerous people involved in application security testing, and AST responsibilities may span several groups — for example, development and security. Therefore, enterprises need reporting and access controlled in a variety of ways (for example, by user, group and project) and overall application portfolio risk trending for the CIO/CISO. Enterprise integration capabilities should also include features such as integration points into the SLC, bug-tracking systems, quality assurance testing tools, build systems and IDEs. Multiple language support for the console and for services is another enterprise capability. Additionally, integration into other security systems, such as SIEM systems, are also desired.

Stand-Alone AST

This capability addresses those cases when penetration testers and other highly skilled security professionals use stand-alone tools to probe Web applications for vulnerabilities, requiring capabilities beyond the simple "point and shoot" design for broader enterprise users.

Stand-alone security testers may also expand their scope to look at operating system and network layer vulnerabilities. Some testers may sample areas of source code for analysis. One capability example is the ability to pause a security test in process to modify the testing parameters on the fly and resume the test. Another is the ability to capture traffic via a proxy, modify the traffic, and play it back to further probe vulnerabilities in Web-enabled APIs. Packaging and pricing targeted at individual professional testers is also an important capability.

WAF/EMM Integration or RASP

This critical capability addresses vendors' ability to offer either AST technology integration with protection technologies or its own RASP technology.

This capability addresses clients' needs to have means for both vulnerability detection and attack protection. This capability typically comes in two "flavors." The first is an integration between Web or mobile application security testing and protection technologies for the purpose of raising the accuracy of application protection. Typically, it is DAST that provides results of its vulnerability discoveries to the WAF technology, thus enabling WAF to act on specific vulnerabilities detected by DAST. In rare cases, AST vendors offer integration between SAST and WAF. For mobile app security testing, mobile AST and EMM tools are integrated. The second way of providing application security is when vendor offers its RASP technology, which enables application runtime environments to protect themselves and the application they execute.

Use Cases

We selected seven use cases for comparing AST solutions. We chose these use cases based on the most common inquiry requests from clients. They include use of AST as tools or services; use of different types of AST, such as static, dynamic and behavioral; manual Web penetration testing; and mobile app testing.

Enterprise Uses Its Own AST Tools

In this use case, an enterprise wants a comprehensive solution with DAST, SAST and IAST for Web apps and mobile AST for mobile apps.

It also wants to test with purchased tools operated by its own staff.

The typical situation is that the enterprise wants a single vendor for all aspects of security testing, and it doesn't want an outside service provider to perform the testing. In this use case, testing as a service is not a factor. Additional factors considered in this use case are the enterprise-class capabilities of the combined solution and, at a much lesser degree, AST integration with protection technologies and stand-alone AST capabilities.

Enterprise Consumes AST as a Service

In this use case, an enterprise wants a comprehensive solution with DAST, SAST and also mobile AST, but it wants to consume the testing entirely as a service.

The typical situation is that the enterprise wants a single vendor for all types of security testing. The reason is that the enterprise often doesn't have the resources to do it by itself, so tool capabilities are not considered. This use case incorporates a combination of DAST- and SAST-as-a-service capabilities, and enterprise-class capabilities with some mobile and IAST capabilities are factored in, as well.

Manual Web Penetration Testing

In this use case, technically advanced application security specialists use sophisticated stand-alone tools to probe Web applications for vulnerabilities.

Penetration testers may also expand their scope to look at operating system and network layer vulnerabilities. Some may sample areas of source code for analysis. Sophisticated tools with specific capabilities targeted at testing professionals are needed, such as the ability to pause a test in process, modify the testing parameters on the fly and resume the test, as well as the ability to capture traffic via a proxy, modify the traffic and play it back. Packing and pricing targeted at individual professional testers is also desirable. In this use case, we evaluate DAST tools' stand-alone capabilities and, at a much lesser degree, IAST and SAST capabilities.

Web Application Security Testing

For this use case, we evaluate vendors' ability to enable discovery of Web application vulnerabilities using mostly DAST solutions (products or services).

In addition to DAST tool and service capabilities, we evaluate, to a much lesser degree, IAST capabilities, because some DAST vendors have been offering DAST and IAST as a single-priced bundle. In that case, IAST uses DAST as attack inducer (simulator). We also evaluate the enterprise-class capabilities of DAST tool and service providers.

Application Code Testing

For this use case, we evaluate vendors' ability to enable discovery of vulnerabilities in an app's source, byte or binary code using SAST solutions (products or services).

In addition to SAST tool and service capabilities, we evaluate, to a lesser degree, IAST capabilities and the enterprise-class capabilities of SAST tool and service providers.

Web Application Behavioral Testing/Self-Testing

For this use case, we evaluate vendors' ability to enable discovery of vulnerabilities in the running application using IAST technology.

This test analyzes an application's behavior at test runtime.

We evaluate the accuracy of vulnerability detection enabled by the degree of the IAST's agent instrumentation into the application runtime environment and breadth of instrumented runtime environments (such as Java, .NET and PHP). We also evaluate, at a lesser degree, DAST capabilities, because DAST can be used as an IAST inducer in some vendors' implementations. We also evaluate, at a much lesser degree, SAST capabilities, because in some vendors' implementations, SAST can be used as a source of additional vulnerability information for IAST. Our evaluation includes IAST's enterprise-class capabilities necessary for reporting and analytics.

Mobile App Testing

For this use case, we evaluate vendors' ability to enable discovery of security vulnerabilities and to provide risk/reputation ratings for mobile apps.

For this use case, to achieve the most complete testing results, enterprises need to evaluate vendors' ability to test application code, conduct behavioral analysis at application test runtime, and analyze mobile app communication with enterprise assets, such as databases and Web applications. They also need to be able to get risk/reputation scores of mobile apps downloaded from public app stores. Another criterion includes the mobile AST's ability to integrate with protection technologies, such as EMM. Enterprise-class capabilities, enabling reporting and analytics, are also included in the list of evaluated parameters. This use case includes vendors' ability to test homegrown applications, as well as those purchased from third-party app vendors or retrieved from public app stores.

Vendors Added and Dropped

Added

In this year's Critical Capabilities and Magic Quadrant reports, we added the following AST vendors:

- Cigital
- NSFOCUS
- SiteLocker

In 2015, while we worked on this report:

- Quotium's Seeker product was acquired by Synopsys.
- NT OBJECTives was acquired by Rapid7, which we reflected in the name "Rapid7 (NTO)."
- Singtel entered into a definitive agreement to acquire Trustwave.

Dropped

We dropped Trend Micro because it did not meet the 2015 inclusion criteria.

Inclusion Criteria

We included in this Critical Capabilities report vendors that met the following criteria:

- Vendors that provide a dedicated application security testing solution (product, service or both; with SAST, DAST, IAST or mobile application security testing capabilities).
- Vendors that provide AST as a service using a repeatable, cookie-cutter subscription-based model using at least some of its own testing tools to enable its testing capabilities.

- Vendors that have 2014 revenue of at least $4 million specific to application security testing, or providers of a significant and new AST capability, such as mobile AST or IAST.

We did not include the following in this Critical Capabilities report:

- Vendors that provide services, but not on a repeatable, predefined subscription basis — for example, providers of custom consulting application testing services, contract pen testing, professional services and other nonsubscription services.
- Vendors that provide network vulnerability scanning, but do not offer a separately purchasable AST capability, or vendors that offer only some Web-application-layer dynamic scanning.
- Vendors that offer only penetration testing products and services.
- Vendors that offer network protocol testing and fuzzing solutions.
- Consultancies that offer AST services.
- Vendors that are focused on application code quality and integrity testing solutions, which have some limited AST capabilities.
- Open-source offerings, because they do not offer enterprise-class capabilities and security-as-a-service delivery.

Table 1. Weighting for Critical Capabilities in Use Cases

Critical Capabilities	Enterprise Uses Its Own AST Tools	Enterprise Consumes AST as a Service	Manual Web Penetration Testing	Web Application Security Testing	Application Code Testing	Web Application Behavioral Testing/Self-Testing	Mobile App Testing
Dynamic AST as a Tool	30%	0%	40%	35%	0%	10%	8%
Dynamic AST as a Service	0%	39%	0%	35%	0%	0%	0%
Static AST as a Tool	25%	0%	5%	0%	39%	5%	8%
Static AST as a Service	0%	33%	0%	0%	39%	0%	0%
Interactive AST	15%	5%	5%	9%	4%	65%	0%
Mobile AST	8%	8%	0%	0%	0%	0%	69%
Enterprise-Class AST	15%	12%	0%	14%	16%	15%	10%
Stand-Alone AST	2%	0%	50%	3%	2%	0%	0%
WAF/EMM Integration or RASP	5%	3%	0%	4%	0%	5%	5%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

As of August 2015

Source: Gartner (August 2015)

This methodology requires analysts to identify the critical capabilities for a class of products/services. Each capability is then weighed in terms of its relative importance for specific product/service use cases.

Critical Capabilities Rating

Each of the products/services has been evaluated on the critical capabilities on a scale of 1 to 5; a score of 1 = Poor (most or all defined requirements are not achieved), while 5 = Outstanding (significantly exceeds requirements).

Table 2. Product/Service Rating on Critical Capabilities

Critical Capabilities	Acunetix	Appthority	Checkmarx	Cigital	Contrast Security	HP	IBM	NSFOCUS	N-Stalker	PortSwigger	Pradeo	Qualys	Rapid7 (NTO)	SiteLock	Synopsys	Trustwave	Veracode	Virtual Forge	WhiteHat Security
Dynamic AST as a Tool	4.7	1.0	1.0	1.0	1.0	4.2	4.7	3.0	3.7	4.9	1.0	1.0	4.8	1.0	1.0	4.3	1.0	1.0	1.0
Dynamic AST as a Service	3.1	1.0	1.0	3.3	1.0	3.9	3.9	2.7	2.9	1.0	1.0	4.4	4.1	3.2	1.0	4.2	4.4	1.0	4.8
Static AST as a Tool	1.0	1.0	4.9	2.0	1.0	4.9	3.7	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	3.1	1.0
Static AST as a Service	1.0	2.0	4.0	2.2	1.0	4.3	1.0	1.0	2.1	1.0	2.2	1.0	1.0	2.5	1.0	1.0	4.8	1.4	3.7
Interactive AST	2.5	1.0	2.1	1.0	4.9	3.0	2.5	1.0	1.0	1.5	1.0	1.0	1.0	1.0	4.9	1.0	1.0	1.0	1.8
Mobile AST	1.3	4.7	2.1	1.9	1.0	3.1	2.5	1.0	1.8	1.0	4.6	1.0	1.0	1.0	1.0	1.5	4.6	1.0	2.5
Enterprise-Class AST	3.0	2.9	4.3	2.9	4.0	4.5	4.0	2.7	2.6	2.0	2.9	4.0	4.0	2.2	4.0	3.8	4.6	3.9	4.0
Stand-Alone AST	4.6	1.0	3.8	2.5	4.0	2.6	2.7	3.0	3.0	5.0	1.0	1.0	4.0	2.0	4.0	3.5	1.6	3.0	1.6
WAF/EMM Integration or RASP	2.0	3.1	3.0	1.0	2.1	3.0	2.0	3.0	2.7	1.0	3.1	3.0	4.2	2.0	1.1	3.1	4.0	1.0	4.2
																As of August 2015			

Source: Gartner (August 2015)

Table 3 shows the product/service scores for each use case. The scores, which are generated by multiplying the use-case weightings by the product/service ratings, summarize how well the critical capabilities are met for each use case.

Table 3. Product Score in Use Cases

Use Cases	Acunetix	Appthority	Checkmarx	Cigital	Contrast Security	HP	IBM	NSFOCUS	N-Stalker	PortSwigger	Pradeo	Qualys	Rapid7 (NTO)	SiteLock	Synopsys	Trustwave	Veracode	Virtual Forge	WhiteHat Security
Enterprise Uses Its Own AST Tools	2.78	1.69	2.88	1.64	2.15	4.06	3.66	2.00	2.24	2.48	1.68	1.55	2.81	1.25	2.10	2.61	1.99	2.00	1.86
Enterprise Consumes AST as a Service	2.19	1.92	2.59	2.59	1.59	3.97	2.72	1.93	2.41	1.15	1.98	2.75	2.67	2.53	1.56	2.69	4.39	1.48	3.99
Manual Web Penetration Testing	4.36	1.00	2.65	1.80	2.70	3.38	3.54	2.80	3.08	4.59	1.00	1.00	4.02	1.50	2.70	3.57	1.30	2.11	1.34
Web Application Security Testing	3.59	1.35	1.73	2.12	1.91	3.93	3.96	2.67	2.96	2.67	1.35	2.69	4.05	2.01	1.87	3.83	2.83	1.47	2.97
Application Code Testing	1.45	1.69	4.32	2.19	1.70	4.48	2.63	1.31	1.73	1.26	1.77	1.48	1.54	1.80	1.70	1.50	3.07	2.48	2.58
Web Application Behavioral Testing/ Self-Testing	2.70	1.39	2.51	1.34	4.04	3.44	2.98	1.56	1.60	1.87	1.39	1.55	1.99	1.23	3.99	1.86	1.69	1.54	2.13
Mobile App Testing	1.75	3.85	2.50	1.89	1.36	3.47	2.90	1.43	2.01	1.41	3.78	1.40	1.76	1.17	1.31	1.99	3.99	1.46	2.50
																			As of August 2015

Source: Gartner (August 2015)

To determine an overall score for each product/service in the use cases, multiply the ratings in Table 2 by the weightings shown in Table 1.

Gartner Recommended Reading

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

"Magic Quadrant for Application Security Testing"

"Application Security Detection and Protection Must Interact and Share Knowledge"

"Cost-Saving Tips for Acquisition and Implementation of Application Security Technologies"

"Hype Cycle for Application Security, 2015"

"Toolkit: Criteria for Selecting Application Security Testing Tools and Vendors"

"Six Principles of Mobile App Security Testing"

"How Products and Services Are Evaluated in Gartner Critical Capabilities"

Evidence

Gartner used the following input in developing this Critical Capabilities report:

- Analysis of approximately 200 inquiries that we received during the past year
- Vendors' responses to our detailed Magic Quadrant and Critical Capabilities survey
- Survey of approximately 150 enterprises that used AST technologies and services

Critical Capabilities Methodology

This methodology requires analysts to identify the critical capabilities for a class of products or services. Each capability is then weighted in terms of its relative importance for specific product or service use cases. Next, products/services are rated in terms of how well they achieve each of the critical capabilities. A score that summarizes how well they meet the critical capabilities for each use case is then calculated for each product/service.

"Critical capabilities" are attributes that differentiate products/services in a class in terms of their quality and performance. Gartner recommends that users consider the set of critical capabilities as some of the most important criteria for acquisition decisions.

In defining the product/service category for evaluation, the analyst first identifies the leading uses for the products/services in this market. What needs are end-users looking

to fulfill, when considering products/services in this market? Use cases should match common client deployment scenarios. These distinct client scenarios define the Use Cases.

The analyst then identifies the critical capabilities. These capabilities are generalized groups of features commonly required by this class of products/services. Each capability is assigned a level of importance in fulfilling that particular need; some sets of features are more important than others, depending on the use case being evaluated.

Each vendor's product or service is evaluated in terms of how well it delivers each capability, on a five-point scale. These ratings are displayed side-by-side for all vendors, allowing easy comparisons between the different sets of features.

Ratings and summary scores range from 1.0 to 5.0:

1 = Poor or Absent: most or all defined requirements for a capability are not achieved

2 = Fair: some requirements are not achieved

3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

To determine an overall score for each product in the use cases, the product ratings are multiplied by the weightings to come up with the product score in use cases.

The critical capabilities Gartner has selected do not represent all capabilities for any product; therefore, may not represent those most important for a specific use situation or business objective. Clients should use a critical capabilities analysis as one of several sources of input about a product before making a product/service decision.

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