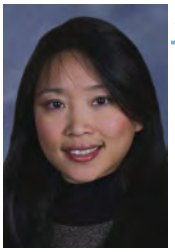
July 15, 2010

The Forrester Wave™: Vulnerability Management, Q2 2010

by Chenxi Wang, Ph.D.

for Security & Risk Professionals



July 15, 2010

The Forrester Wave™: Vulnerability Management, Q2 2010

Qualys Leads; Rapid7, nCircle, McAfee, And Lumension Follow

by Chenxi Wang, Ph.D.
with Stephanie Balaouras and Lindsey Coit

EXECUTIVE SUMMARY

In Forrester's 53-criteria evaluation of vulnerability management vendors, we found that the market is rife with mature products. Qualys led the pack because of its strong vulnerability assessment capability, forward-thinking strategy, and exceptional customer reviews. Rapid7, Lumension, McAfee, and nCircle are a notch down, but all turned in solid scores that landed them in the Leaders section. eEye Digital Security, Tenable Network Security, and Critical Watch are ranked as Strong Performers. These products may lack platform diversity, have slightly weaker application-level scanning capability, or do not support comprehensive policy compliance. However, all of the products we evaluated have mature vulnerability assessment functionality. Given this, IT security professionals should choose a vulnerability management product based on the more cutting-edge functionality, such as support for remediation and application-level scanning, rather than on traditional network and system vulnerability management functions.

TABLE OF CONTENTS

NOTES & RESOURCES

Forrester conducted product evaluations between March and May 2010 and interviewed more than 20 vendor and user companies, including Critical Watch, eEye Digital Security, IBM, Lumension, McAfee, Perimeter eSecurity, Qualys, Rapid7, Secunia, and Tenable Network Security.

Related Research Documents

"Market Overview: Client Management Suites"
July 29, 2009

"Market Overview: Security Information Management (SIM)"
April 30, 2009

"Operationalizing Application Vulnerability Management"
February 29, 2008

VULNERABILITY MANAGEMENT IS A CORE FUNCTION FOR IT SECURITY

Vulnerability management, comprised of vulnerability assessment, configuration compliance scanning, and remediation support, is an important IT security function. In Forrester's 2009 security survey, 42% of IT security professionals told us that they were fully responsible for vulnerability management, while another 29% said they were mostly responsible (see Figure 1).[1]

Forrester sees continued interest and a sustained level of investment in vulnerability management capabilities, because:

- **Threats do not let up.** Attacks exploiting security vulnerabilities for financial gain and criminal agendas continue to dominate headlines. Statistics from Microsoft bulletins and the National Vulnerability Database (NVD) suggest that the time it takes to release new exploits for a known vulnerability has decreased significantly in the past five years. This rapid release leaves more and more systems vulnerable to exploit attacks.

- **Regulations demand it.** Many government and industry regulations, such as PCI and Sarbanes-Oxley (SOX), mandate rigorous vulnerability management practices.[2] Insight into an organization's vulnerabilities is key to a proactive understanding of one's infrastructure risks. As a result, regulatory requirements will continue to drive demand for vulnerability management technologies.

- **Mature organizations treat it as a key risk management component.** Organizations that follow mature IT security principles understand the importance of risk management. Vulnerability assessment and management is an essential piece for managing overall IT risk. Beyond an established vulnerability management practice, a mature organization should employ advanced analytics and perform vulnerability trending and remediation tracking to further control and manage its infrastructure risks.

Figure 1 IT Security Professionals Are Responsible For Vulnerability Management

"To what extent is your firm's IT security group responsible for threat and vulnerability management?"

	Count	%
Security is fully responsible	400	42%
Security is mostly responsible	281	29%
Security is about half responsible	168	18%
Security is slightly responsible	70	7%
Security is not at all responsible	24	3%
Don't know/does not apply	10	1%

Base: 953 North American and European IT security decision-makers

Source: Enterprise And SMB Security Survey, North America And Europe, Q3 2009

56932 Source: Forrester Research, Inc.

Vulnerability Management Products Have Increasingly Broad Functionality

Vulnerability management products started out delivering pure network vulnerability assessment functionality. As the market matures, many vendors are looking to adjacent technology areas for additional growth. This has led to a number of market shifts, including:

- **Both vulnerability assessments and endpoint configuration are considered core functionality.** Almost every vulnerability management product today offers functionality. Some provide comprehensive mapping from a wide variety of regulations to specific vulnerability management and configuration controls.

- **Application-level scanning capabilities are now a table stake.** Application-level scanning, targeting Web applications and databases, is becoming a must-have item in RFPs for vulnerability management products. While some buyers are happy to procure pure-play application scanners, many customers look to a single vendor to provide consolidated vulnerability scanning capability and reports across network/system and applications.

- **Remediation and security analytics are fast becoming the newest differentiators.** As IT security organizations mature, buyers start to shift from assessment-only capabilities to advanced risk-based analytics and remediation management; both are somewhat newer functionalities for vulnerability management products.

VULNERABILITY MANAGEMENT VENDOR EVALUATION OVERVIEW

To assess the state of the vulnerability management market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of top vulnerability management vendors.

We Used Three Dimensions To Assess Vendors

After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of evaluation criteria. We evaluated vendors against 53 criteria, which we grouped into three high-level buckets:

- **Current offering.** We analyzed the vendor's capability on vulnerability assessment, both at the network/system level and at the application level; configuration compliance assessment; and any remediation capabilities (or support for remediation). We also looked at features such as reporting, performance, mode of delivery, and support for risk management.

- **Strategy.** Our analysis of each vendor's strategy included an assessment of the high-level company strategy, near-term product road map, and the company's plan for a partner ecosystem. In terms of company strategy, we looked at the vendor's vision and its value proposition, how well it is executing this vision and delivering on the value proposition, and whether the strategy demonstrates industry thought leadership.

- **Market presence.** We used traditional metrics, such as vendor revenues and customer numbers, to evaluate a vendor's market presence. Because this technology is often delivered via managed security services, we added criteria to measure each vendor's indirect customers from managed security services provider (MSSP) partners.

Our Evaluation Emphasized Comprehensive Capabilities

Forrester included eight vendors in the Forrester Wave assessment: Critical Watch, eEye Digital Security, Lumension, McAfee, nCircle, Qualys, Rapid7, and Tenable Network Security. Each of these vendors has (see Figure 2):

- **Both vulnerability and configuration compliance assessment capabilities.** Today's user organizations value vulnerability assessment as well as configuration scanning. Therefore, we consider both of these functions core to vulnerability management.

- **Support for remediation.** The product must either possess native remediation capability or offer tight integration with third-party remediation products.

- **Significant market presence or notable growth.** We focused on vendors that either have a notable market presence, evidenced by the number of customers or revenues, or ones that are up-and-coming with strong growth numbers.

We decided to focus our scope of evaluation on vulnerability assessment and configuration auditing products. Hence, we did not invite any pure-play Web application scanners, such as IBM and HP, or any vulnerability intelligence vendors, such as Symantec or 3Com, to participate in this evaluation.

EVALUATED VENDORS RENDER MATURE SOLUTIONS

The evaluation uncovered a market in which many mature solutions exist (see Figure 3):

- **Qualys leads the pack.** Qualys leads on its strategy as well as its execution. Not only did Qualys pioneer the SaaS hybrid model for vulnerability assessment, but today it is the largest vulnerability management vendor in terms of revenues. Its configuration compliance assessment functionality, also delivered via Qualys' in-the-cloud multitenant architecture, has since matured and is one of the most advanced in the market.

- **Rapid7, Lumension, McAfee, and nCircle offer competitive options.** These four vendors are a notch down from Qualys, but each offers strong vulnerability management functionality in one aspect or another. Lumension has the strongest strategy/vision due to its portfolio of endpoint remediation products, such as PatchLink. Straddling both assessment and remediation gives customers a one-stop shop for vulnerability management capabilities. Rapid7 receives

excellent scores for both its technologies and its risk-oriented strategy. nCircle's comprehensive functionality portfolio for vulnerability assessment and configuration compliance earned it a nod in the Leaders category. McAfee is an established vendor in this space, and its mature risk-based strategy is a unique differentiator.

- **eEye Digital Security, Tenable Network Security, and Critical Watch trail behind.** eEye has a solid vulnerability assessment product, but it is a bit weaker on application-level scanning and support for configuration compliance. Tenable's product has excellent technical functionality but lacks comprehensive enterprise support features. Critical Watch is the newcomer to the space. Its integration with TippingPoint is interesting, but the product doesn't have comprehensive platform support, and the company's long-term strategy lacks clear differentiation.

This evaluation of the vulnerability management market is intended to be a starting point only. We encourage readers to view detailed product evaluation spreadsheets and adapt the criteria weightings to fit their individual needs through the Forrester Wave Excel-based vendor comparison tool.

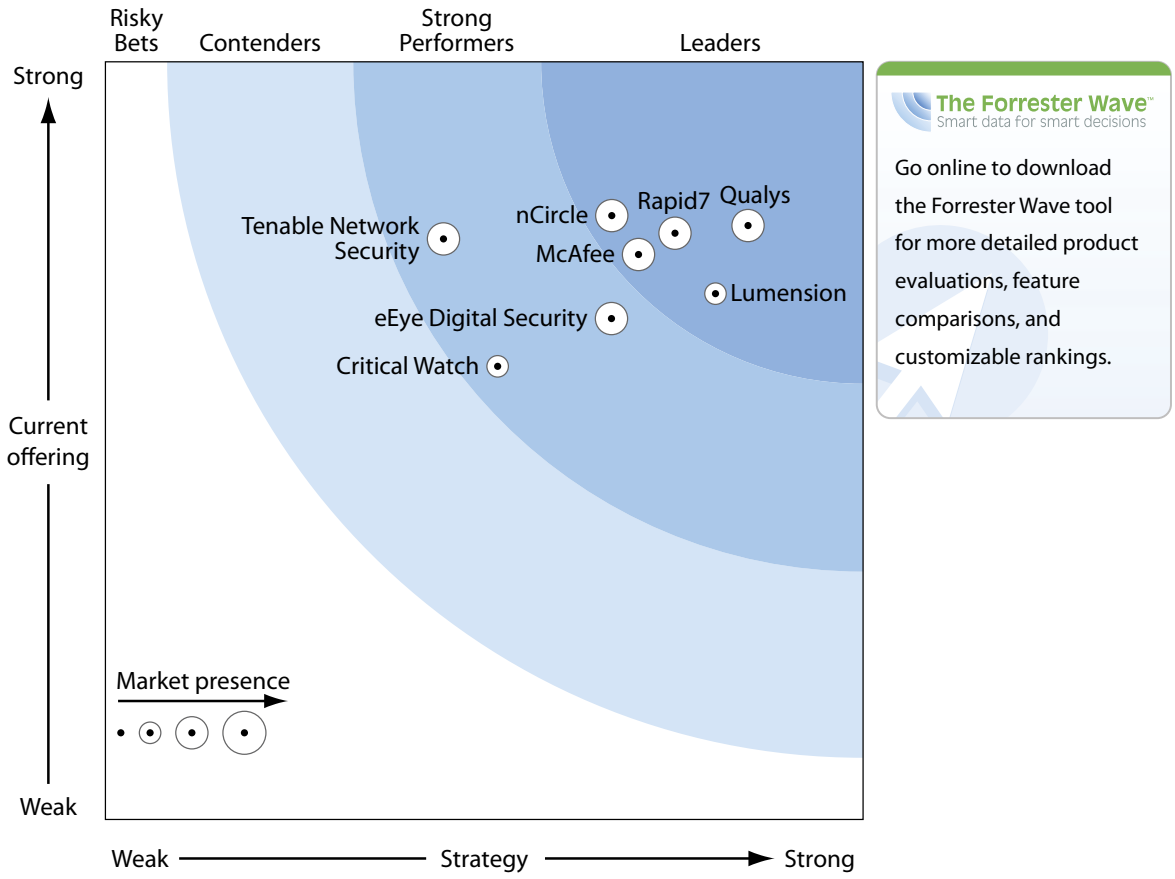
Figure 2 Evaluated Providers: Vendor Information And Selection Criteria

Vendor	Product evaluated	Product version evaluated	Date evaluated
Critical Watch	FusionVM	4.4.26	Q1 2010
eEye Digital Security	Retina CS	1.1.0	Q1 2010
	Retina Network Security Scanner	5.11.1	Q1 2010
Lumension Security	Lumension EndPoint Management and Security Suite	7.0	Q1 2010
McAfee	Foundstone McAfee Vulnerability Manager	6.8	Q1 2010
nCircle	nCircle Suite360	N/A	Q1 2010
Qualys	QualysGuard IT Security and Compliance Suite	6.10	Q1 2010
Rapid7	NeXpose Enterprise	4.8.0	Q1 2010
Tenable Network Security	Tenable Unified Security Monitoring	N/A	Q1 2010

Vendor selection criteria
Both vulnerability and configuration compliance assessment capabilities
Support for remediation
Significant market presence of notable growth

Source: Forrester Research, Inc.

Figure 3 Forrester Wave™: Vulnerability Management, Q2 '10



Source: Forrester Research, Inc.

Figure 3 Forrester Wave™: Vulnerability Management, Q2 '10 (Cont.)

	Forrester's Weighting	Critical Watch	eEye Digital Security	Lumension Security	McAfee	nCircle	Qualys	Rapid7	Tenable Network Security
CURRENT OFFERING	50%	2.99	3.31	3.47	3.73	3.98	3.92	3.87	3.83
Vulnerability assessment on the network/system level	25%	3.73	3.40	3.19	3.99	4.19	3.74	3.85	4.50
Application-level vulnerability management	15%	1.90	2.90	2.10	1.60	3.80	3.80	5.00	3.90
Compliance	25%	2.10	3.30	4.00	4.70	4.10	4.40	3.10	4.20
Take to market	5%	4.10	3.00	1.90	3.00	3.00	3.90	4.10	1.10
Remediation and integration with related functionality	8%	2.35	2.95	4.60	3.95	4.15	3.40	3.60	1.40
Administration and reporting	8%	4.00	3.60	4.40	4.30	4.20	3.10	3.80	3.70
Performance and operations	8%	3.45	3.85	4.05	3.35	3.50	4.05	4.10	4.35
Customer reference feedback	6%	4.33	3.66	3.67	3.99	4.00	4.67	4.33	4.34
STRATEGY	50%	2.59	3.34	4.03	3.52	3.34	4.24	3.76	2.23
Product strategy	70%	2.70	3.20	3.75	3.75	3.20	4.20	3.95	3.05
Partner strategy	30%	2.34	3.66	4.67	2.97	3.66	4.32	3.33	0.33
MARKET PRESENCE	0%	2.45	3.45	2.80	3.45	3.25	3.93	3.45	3.53
Customer base	50%	2.70	4.50	3.00	3.50	3.50	3.65	3.70	3.25
Revenues	50%	2.20	2.40	2.60	3.40	3.00	4.20	3.20	3.80

All scores are based on a scale of 0 (weak) to 5 (strong).

Source: Forrester Research, Inc.

VENDOR PROFILES

Leaders Offer Mature Solutions

- **Qualys leads in market share and innovation.** Qualys is the clear leader in this evaluation. Qualys pioneered the SaaS hybrid delivery model of vulnerability management: Fully managed scanner appliances are deployed on-premise, and the security console is hosted, in a multitenant fashion, in the Qualys cloud to drive scans, conduct analysis, and produce reports. Once viewed as radical, this service model now counts some of the largest organizations in the world as customers. Today, the QualysGuard cloud delivers vulnerability assessment, application-level scanning, and configuration compliance auditing, all from a centralized multitenant architecture. This architecture helps to deliver scalability and consolidated reporting. Qualys is also one of the few vendors in this evaluation that has a full-featured configuration compliance module that provides concrete mappings from a wide list of regulations to actual IT controls. Qualys has an extensive ecosystem of partners and is rounding out its service offerings by

adding a variety of new services, including malware scanning and the Qualys Go Secure trust seal. The company surpassed the $50 million mark in 2009, making it the largest market shareholder in the vulnerability management sector. As one IT security director we interviewed said, "While other products can be too expensive or too niche, it is hard to go wrong with Qualys." Who should buy Qualys? All but the most conservative organizations.

- **Rapid7 exhibits strong growth and clarity of vision.** Rapid7 is the up-and-coming vendor in this evaluation. The company experienced a dramatic surge in business in the past two years, rendering an impressive 50%-plus year-over-year growth. Rapid7 receives solid scores for its fundamental technology, which is built on top of an expert system that helps to deliver analysis accuracy. Rapid7 also leads on its strong application scanning capability — it's the only vendor in this evaluation whose scanning capabilities can handle Ajax and Web 2.0 technologies. Rapid7 delivers its functionality via a consolidated scanning and analysis architecture, which promises deployment efficiency and simplicity. The acquisition of Metasploit also helps to strengthen Rapid7's risk analytics and adds a penetration testing tool to its portfolio. The company has an ambitious vision — delivering unified vulnerability management across network, applications, and databases, with meaningful risk analytics. To execute this vision, Rapid7 needs to expand its policy compliance capability and strengthen its support for remediation. Today, Rapid7 is still a small company with revenues south of $20 million. But the company recently signed OEM deals with two of the largest security and service vendors in the industry. These partnerships will undoubtedly provide a further boost to the company's position in the market. Who should buy Rapid7? Organizations that seek a consolidated solution for network, system, and application-level vulnerability management.

- **nCircle has a comprehensive vulnerability auditing portfolio.** nCircle's vision is clear and well defined — to be the leader in vulnerability and configuration compliance auditing. To this end, the company has amassed one of the broadest capability portfolios in vulnerability auditing. In particular, nCircle's configuration compliance product is among the most sophisticated on the market today, and its topology analyzer is unique among vulnerability management vendors. Customers also reported positive reviews for its core vulnerability scanning product, IP360. For these reasons, nCircle received one of the highest "current offering" scores. However, some of nCircle's functionality came via acquisitions, and as a result, its vulnerability assessment product, IP360, its configuration compliance product, CCM, and its analytics product, the Suite360 Intelligence Hub, all have disparate code bases and there exists only sparse integration among the three. IP360 and CCM manage separate scanners, consoles, and databases. The Intelligence Hub, which pulls data from both IP360 and CCM, provides yet another management console and another database. Customers we interviewed reported a certain level of deployment complexity and challenges with nCircle's suite of products. Customers have also reported occasional accuracy problems with the company's Web application scanner. To eclipse its competition, nCircle needs to eliminate the architectural redundancy between its various modules, strengthen its application scanning capabilities, and further develop its value proposition for the Suite360 Intelligence Hub. Who should buy nCircle? Enterprises that have advanced compliance and risk analytics needs.

- **McAfee delivers strong risk management capabilities.** McAfee/Foundstone is an established vulnerability management vendor. Foundstone championed many early-day innovations in this space. The McAfee Vulnerability Management (MVM) product today boasts one of the most UI-conscious interface designs and solid support for translating vulnerability knowledge into meaningful risk metrics. In addition, MVM's integration with McAfee ePolicy Orchestrator is a nice feature and proves valuable to many ePO users. However, the product itself needs a bit of a tune-up: Customers we interviewed mentioned occasional accuracy problems with their scanners. The company's scan-based reporting is cumbersome to use. At the close of this evaluation —March 31, 2010 — McAfee had little in the way of application scanning capability. However, McAfee has alluded to the imminent release of new functionality to cover this void; prospective customers should investigate whether McAfee's new application scanner will suit their needs. Who should buy McAfee? Organizations with a mature risk management strategy and those that drive IT efficiency with ePO. Existing MVM customers who have a need to manage application-level vulnerabilities should also track McAfee's upcoming product releases.

- **Lumension has a unique product portfolio to deliver an "end-to-end" vision.** Lumension is the only vendor in this evaluation that has its own endpoint patch management functionality, Lumension Patch and Remediation (formerly Patchlink), and its own GRC product, Lumension Risk Management. Unlike the other vendors that may have a focus on assessment, Lumension's value proposition is much broader — instead of dealing with separate consoles from assessment, remediation, and compliance, Lumension aims to deliver a consolidated platform to manage the life cycle of vulnerabilities — from discovery to remediation to analytics. While this vision is unique, Lumension's vulnerability scanning product is clearly designed for technologists, with very few extra bells and whistles to boot. When used as a standalone product, it's not quite at par with its competition. Lumension's configuration compliance product, however, has much more sophisticated analytics and reporting capabilities. Compared with the other products, Lumension's strategies have a decidedly endpoint focus. Because of the expanse of its product portfolio, Lumension has a great deal of potential to challenge the top players in the vulnerability management market. Presently, however, the company should work on streamlining its various products to drive toward a consolidated platform as well as continue to invest in the research and development of its vulnerability assessment product. Who should buy Lumension? Organizations with a focus on consolidated assessment and remediation strategy.

Strong Performers Provide Robust Technical Alternatives

- **Tenable Network Security has a strong technology offering.** Tenable is the producer of the once open-source Nessus vulnerability scanner. Tenable's portfolio, including the Passive Vulnerability Scanner (PVS) and the Log Correlation Engine (LCE), renders strong vulnerability assessment capabilities. Many technologists we interviewed like what Tenable has to offer. What Tenable lacks are enterprise support features, such as executive reporting, advanced risk analytics, and integration with related products. Who should buy Tenable? Technology-minded buyers.

- **eEye Digital Security is evolving its product portfolio.** With a new management team in place, eEye is overhauling its products. eEye's vulnerability assessment product, Retina, has many desirable features, such as wireless scanning, diverse scan templates, and an extremely flexible reporting portal. The product is also attractively priced. eEye has a separate government-facing product, appropriately named Retina.GOV, which has specific SCAP-related functionality.[3] eEye's endpoint agent executes protection actions, such as application whitelisting, device control, and local scanning. eEye's high-level vision is similar to that of Lumension's — take the full life-cycle approach to vulnerability management. The value proposition of eEye's endpoint capabilities, however, is not as clearly defined. eEye needs to leverage on its strength — the vulnerability assessment product — and work on a few enhancements, including increasing the flexibility of the product, strengthening application-level scanning, and enhancing policy compliance. Who should buy eEye? Government clients, value-conscious organizations, and technology-minded buyers.

- **Critical Watch offers interesting new capabilities.** Critical Watch's FusionVM product has a number of distinct and innovative features, including the CEM structure that provides a flexible yet powerful organizational framework for managing scans, reports, and analysis. A key part of Critical Watch's positioning centers on its integration with TippingPoint's firewall product, which allows FusionVM a deeper insight into mitigation controls. Critical Watch has a relatively small market share, but the company has garnered a respectable customer base and has shown steady growth for the past two years. In terms of technology, what Critical Watch needs to work on is its breadth of platform support, application scanning capabilities, and support for endpoint remediation. In terms of company strategies, Critical Watch needs to expand the reach of its partner network and strive for a clearer value differentiation against its competitors. Who should buy Critical Watch? Organizations that have diverse reporting needs and value-conscious large enterprises.

Other Notable Vendors Round Out The Vulnerability Management Space

Before narrowing our evaluation to eight vendors, we studied a broader set of vendors — including vendors that fit squarely in the vulnerability management space and those that offer closely related functionality. For this evaluation, we chose to focus on vendors with a broad vulnerability management technology solution and those with a sizable market presence. A vendor's absence from this evaluation doesn't constitute any judgment as to the vendor's capabilities or viability.

Generally speaking, other products worth noting fall into these loosely defined categories:

- **Vulnerability assessment.** Other vendors in this space include Digital Defense, Perimeter E-Security, RandomStorm, Secunia, Trustwave, and IBM. These vendors either fail to meet the inclusion criteria or were omitted in favor of a vendor with a more significant market presence. IBM, in particular, is both a vulnerability management technology vendor and a significant

managed security service provider. IBM/ISS is traditionally an innovator in this space. However, at the time of evaluation, IBM was in the process of refreshing and upgrading its vulnerability management portfolio and will launch a new offering in Q3 2010. Because of the timing, it became difficult to include IBM for this evaluation. For that reason alone, IBM is not one of the vendors included in this Forrester Wave.

- **Vulnerability intelligence.** Vulnerability assessment technologies must update their knowledge of vulnerabilities to stay current, as new vulnerabilities surface constantly. Companies that provide vulnerability intelligence services include Symantec, Secunia, VeriSign, and 3Com. These vendors were not included in the evaluation because vulnerability intelligence, albeit important, is not the focus of this study.

- **Penetration testing and emulation.** Penetration testing or emulation products utilize the knowledge of existing vulnerabilities and demonstrate actual or virtual exploitation. With penetration testing or emulation, one can much more accurately assess the severity of certain vulnerabilities. Core Security Technologies and Metasploit (now a Rapid7 company) both provide automated penetration testing technologies. Core Security and Metasploit can leverage the output of a vulnerability scanner to craft a specific penetration test, and in turn, they may discover new vulnerabilities that are otherwise hidden from regular scanners. RedSeal Systems and Skybox Security, on the other hand, offer penetration emulation without actual tests on the system.

- **Remediation.** Endpoint patch management and configuration management products sit in this category. Remediation technologies must work hand-in-hand with assessment technologies to affect mitigation changes. Example products in this category include BigFix, IBM/Tivoli, McAfee, LANDesk Software, Shavlik Technologies, Symantec, and Trend Micro.

- **Web application scanners.** We made a conscious decision not to include pure-play Web application scanners because the technologies are very different. Vendors that have offerings in this space include Accunetix, Cenzic, HP (WebInspect), IBM (AppScan), and WhiteHat Security.

- **Managed security service providers.** We did not include any MSSPs in this evaluation, but MSSPs play an important role in this space and their involvement will be increasingly critical as more and more organizations procure vulnerability management functionality from MSSPs. Many MSSPs resell vulnerability management technologies and provide additional value-added services. Notable ones include IBM, Verizon Business, and SecureWorks.

SUPPLEMENTAL MATERIAL

Online Resource

The online version of Figure 3 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings.

Data Sources Used In This Forrester Wave

Forrester used a combination of three data sources to assess the strengths and weaknesses of each solution:

- **Vendor surveys.** Forrester surveyed vendors on their capabilities as they relate to the evaluation criteria. Once we analyzed the completed vendor surveys, we conducted vendor calls where necessary to gather details of vendor qualifications.
- **Product demos.** We asked vendors to conduct demonstrations of their product's functionality. We used findings from these product demos to validate details of each vendor's product capabilities.
- **Customer reference calls.** To validate product and vendor qualifications, Forrester also conducted reference calls with each vendor's customer references as well as other customers that we reached out to for reference information.

The Forrester Wave Methodology

We conduct primary research to develop a list of vendors that meet our criteria to be evaluated in this market. From that initial pool of vendors, we then narrow our final list. We choose these vendors based on: 1) product fit; 2) customer success; and 3) Forrester client demand. We eliminate vendors that have limited customer references and products that don't fit the scope of our evaluation.

After examining past research, user need assessments, and vendor and expert interviews, we develop the initial evaluation criteria. To evaluate the vendors and their products against our set of criteria, we gather details of product qualifications through a combination of lab evaluations, questionnaires, demos, and/or discussions with client references. We send evaluations to the vendors for their review, and we adjust the evaluations to provide the most accurate view of vendor offerings and strategies.

We set default weightings to reflect our analysis of the needs of large user companies — and/or other scenarios as outlined in the Forrester Wave document — and then score the vendors based on a clearly defined scale. These default weightings are intended only as a starting point, and we encourage readers to adapt the weightings to fit their individual needs through the Excel-based tool. The final scores generate the graphical depiction of the market based on current offering, strategy, and market presence. Forrester intends to update vendor evaluations regularly as product capabilities and vendor strategies evolve.

ENDNOTES

[1] Source: Enterprise And SMB Security Survey, North America And Europe, Q3 2009.

[2] PCI DSS has specific provisions for organizations to maintain an active vulnerability management program. Source: PCI Security Standards Council (https://www.pcisecuritystandards.org/).

[3] SCAP refers to the Security Content Automation Protocol. SCAP is a suite of specifications that standardize the format and nomenclature by which security software products communicate software flaw and security configuration information. SCAP is a multipurpose protocol that supports automated vulnerability and patch checking, technical control compliance activities, and security measurements. Goals for the development of SCAP include standardizing system security management, promoting interoperability of security products, and fostering the use of standard expressions of security content. The technical specification of SCAP is spearheaded by NIST. Source: Stephen Quinn, David Waltermire, Christopher Johnson, Karen Scarfone, and John Banghart, "The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.0," National Institute of Standards and Technology (http://csrc.nist.gov/publications/nistpubs/800-126/sp800-126.pdf).

FORRESTER®

Making Leaders Successful Every Day

Headquarters

Forrester Research, Inc.
400 Technology Square
Cambridge, MA 02139 USA
Tel: +1 617.613.6000
Fax: +1 617.613.5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices

Forrester has research centers and sales offices in more than 27 cities internationally, including Amsterdam; Cambridge, Mass.; Dallas; Dubai; Foster City, Calif.; Frankfurt; London; Madrid; Sydney; Tel Aviv; and Toronto.

For a complete list of worldwide locations visit www.forrester.com/about.

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com.
We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc. (Nasdaq: FORR) is an independent research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. Forrester works with professionals in 20 key roles at major companies providing proprietary research, customer insight, consulting, events, and peer-to-peer executive programs. For more than 26 years, Forrester has been making IT, marketing, and technology industry leaders successful every day. For more information, visit www.forrester.com.

FORRESTER®