

MarketScope for Vulnerability Assessment

Kelly M. Kavanagh, Mark Nicolett, John Pescatore

The vulnerability assessment market is changing as vendors try to evolve to address functional and market challenges. Although VA is an important aspect of an organization's security program, technical and process challenges must be considered when evaluating and deploying VA technologies.

WHAT YOU NEED TO KNOW

Network vulnerability scanning products are mature but require frequent use by trained staff to be an effective element of security operations. All the vendors in this segment provide active network scanning, but there are significant differences in delivery (software, appliance and/or managed service), scope (network, system, Web server and/or database) and vendor size. Vendors with multiple security products are incorporating vulnerability assessment (VA) data into their vulnerability management, intrusion prevention system (IPS) and network access control (NAC) offerings. One vendor is successfully building a business around a service-based model, and many other point solution vendors provide VA as a product (software or appliance) and as a service.

IBM Internet Security Systems (ISS) and McAfee are good choices for companies that are already using related security products from these vendors, and for companies that favor larger, stable vendors. Companies that want VA as a service and those that need VA from a third party for compliance or audit requirements would likely be satisfied with vendors such as Qualys, Beyond Security or Critical Watch. Qualys is the most successful provider of VA scanning and appliances as a service, and Beyond Security and Critical Watch provide VA appliances as a product offering as well as a service. Companies that are Windows-centric would likely value eEye Digital Security's strong security research resources, while nCircle is a good choice for large organizations that want an appliance-based solution and the ability to baseline against configuration standards. Tenable Network Security and StillSecure are good options for organizations that have Nessus expertise but also require centralized administration and reporting. StillSecure also is an option for companies that want vulnerability management support. Organizations that require strong remediation-oriented reporting and assessment that includes database and Web server scanning should consider Rapid7. The VA market has a group of vendors (Beyond Security, Criston, Critical Watch, StillSecure, Saint, Rapid7 and Tenable Network Security) with unique capabilities and good customer references, but that also carries some viability risk because of the vendors' small size.

MARKETSCOPE

VA is an essential component of an effective security program. VA initially provides discovery and security baseline data, and periodic rescanning provides updated data for vulnerability management, trending and compliance reporting. VA tools provide a bottom-up security baseline for the IT environment from a database of known vulnerabilities. There are three approaches to VA: active network scanning, passive observation of network traffic and persistent agents. The most-accurate scanning requires credentialed access (over the network or via an agent).

IT security organizations require a network-based approach that can accurately discover and evaluate vulnerabilities on managed and unmanaged systems. However, for VA data to be used to improve security and satisfy audit requirements, there must be strong prioritization capabilities and reporting with three orientations: security (vulnerability and threat-focused), operations (remediation-focused) and audit (risk and remediation trending). Organizations also will need to implement the vulnerability management life cycle if they want to use VA to make the environment more secure.

The VA market is mature, and it has traditionally satisfied a long-standing requirement for external assessment of security weakness as part of annual audits. In the early phases of this market, security consultancies were prominent users of VA tools, often homegrown or open-source utilities (Nessus). The vulnerability-seeking worm attacks of 2001, 2003 and 2004 drove more enterprises to deploy VA products and services, and to use them more frequently, as

components of the enterprise security infrastructure. As was common with many security segments, the increase in demand caused a large number of startup vendors to enter the market.

The strongest driver of the current VA market is compliance, including Payment Card Industry (PCI) Data Security Standard specification for VA. Deploying VA to meet the continuing need for effective vulnerability management remains a driver. Market inhibitors include the complexity of the tools and the ability of tools to fit large-scale deployments, the continued availability of VA from periodic engagements with security consultancies, the availability of VA from managed security service providers (MSSPs), and the continued use of Nessus by enterprises. VA capabilities are migrating into broader security offerings by larger vendors. Stand-alone VA products will be primarily niche offerings for enterprises able to do VA scanning themselves with vendor-supported products rather than open-source tools.

Market/Market Segment Description

This MarketScope focuses on vendors that provide active network scanning capabilities to the security buying center. VA comprises three basic approaches:

- **Active network scanning**, also referred to as network VA, will remotely scan devices over the network without requiring agents; deeper inspection of endpoints can be performed through credentialed access.
- **Passive observation of network traffic** does not actively scan endpoints, but it captures traffic between endpoints to determine their state based on those traffic patterns. Although passive observation can provide information about endpoints that cannot be actively scanned (for example, systems with personal firewalls), this technique alone does not provide sufficient data to support remediation activity.
- **Persistent agents** reside on the endpoints, collecting state information in real time. They can determine aspects of the endpoint that cannot be determined remotely, such as applications or services that are installed but not running. Agent-based approaches must be augmented with discovery and baseline functions that can be applied to unmanaged endpoints.

All the vendors in this MarketScope provide active network scanning. Gartner has focused on this functional area because most product purchase decisions for VA technology require this capability, and there is little demand for stand-alone VA products that are solely agent-based or passive.

The VA market is a mature segment that includes:

- Two large vendors (IBM ISS and McAfee) that sell VA technology and also integrate it with related security products
- One vendor (Qualys) that is focused primarily on delivering VA as a service
- Ten smaller point solution vendors that provide a mix of software-, appliance- and/or service-based offerings

Revenue in the VA market is spread thinly across these 13 vendors, and all must compete with each other, as well as with Nessus and professional service offerings from consultancies. This situation introduces a viability risk for the smaller vendors in the market.

Inclusion and Exclusion Criteria

Vendors are included based on the following criteria:

- Use their own VA engine
- Perform active network VA
- Provide vulnerability information and reference multiple vulnerability IDs, including Common Vulnerabilities and Exposures, SANS Top-20, Bugtraq ID and vendor-specific IDs
- Provide remediation guidance
- Offer enterprise-level product that supports central administration of multiple distributed scanners and consolidated reporting
- Focus on the security organization
- Provide asset classification capabilities

Vendors are excluded based on the following criteria:

- Redistribute a third-party VA scanner or rely on one to be enterprise-deployed
- Sell primarily to the operations group or lack security context
- Embed VA function in broader products and suites

The following three vendors do not fully meet our market inclusion criteria, but should be evaluated in some cases:

- Symantec currently sells Control Compliance Suite for Internet Security (the VA technology that it gained from the BindView acquisition), but provides VA technology only as a function in the suite and does not sell VA as a stand-alone offering. Symantec also will use VA technology in other products (such as an agentless scanner for its NAC offering). Symantec Control Compliance Suite customers that wish to implement VA technology should evaluate the Internet security component. Symantec also provides SecurityExpressions (from the Altiris acquisition), an agentless security configuration policy compliance product within a security configuration policy audit and remediation product that includes agentless VA as a function. Although SecurityExpressions meets many of our VA market inclusion criteria (because of the capability to do agentless scanning against a database of approximately 600 known vulnerabilities), SecurityExpressions is not sold as (or priced like) a VA product, and its network-oriented discovery capabilities are limited. Organizations that are deploying SecurityExpressions for security configuration policy compliance should evaluate the VA function for managed systems, but they will still need to deploy a network-oriented VA product for discovery and assessment of unmanaged systems.
- Sourcefire's Real-time Network Awareness (RNA) technology uses passive discovery methods to provide an analysis of network flows and host characteristics. RNA can be used as a stand-alone discovery and analysis method that complements an active VA scanner. Data gathered by RNA also is consumed in Sourcefire's intrusion detection system and vulnerability management products. Because Sourcefire does not have a stand-alone scanner product, the company is not included in this MarketScope. Gartner included Sourcefire in "MarketScope for Network Behavior Analysis, 2H06."
- Secure Elements provides a compliance and vulnerability management platform that includes network node discovery and agent-based VA. The platform also supports the integration of third-party VA data. Because Secure Elements does not have a network-

based active scanner, it is not included in this MarketScope. Organizations that are implementing Secure Element's vulnerability management offering should evaluate its agent-based VA technology, but may also need to deploy a network-based scanner to cover unmanaged nodes. Secure Elements has primarily been focused on the federal government and the critical infrastructure market. In 2007, the C5 Compliance Platform and Auditor Pro products began providing discovery and scanning capabilities and reporting against regulatory requirements, such as the Federal Information Security Management Act, PCI, Federal Energy Regulatory Commission-North American Electric Reliability Corporation and others. Secure Elements has been very strong in Common Vulnerability Scoring System, Security Content Automation Protocol (SCAP) and Extensible Configuration Checklist Description Format XML-based standards efforts, and has achieved National Institute of Standards and Technology SCAP compliance.

Rating for Overall Market/Market Segment

Overall Market Rating: Positive

VA remains a steady growth market, with revenue of \$200 million in 2007 and an expected \$240 million in 2008, and is characterized by a large number of vendors competing for available business, the existence of multiple alternative forms of delivery and a longer-term trend of incorporating VA functions into broader technology. Viable alternatives to direct spending on commercial VA tools include open-source tools (Nessus), services from security consultants and offerings from numerous external service (including nonsecurity) providers. VA also is being integrated into other, broader offerings (such as vulnerability management products from Symantec and Altiris, and threat protection products from IBM ISS); thus, it is available to buyers of those broader offerings. However, there will be stable, long-term demand for narrower assessment capabilities, and the effect of the incorporation of the VA function into broader offerings will be to mute, but not eliminate, the demand for stand-alone VA functions. Nonetheless, VA capabilities will continue to evolve, driven by requirements such as the extension of PCI assessments to include Web application scanning.

Evaluation Criteria

Table 1. Evaluation Criteria

Evaluation Criteria	Comment	Weighting
Market Responsiveness and Track Record	Market responsiveness and track record evaluate the match of the VA offering to the functional requirements stated by buyers at acquisition time, and the vendor's track record in delivering new functionality when it is needed by the market. Also considered is how the vendor differentiates its offerings from those of its major competitors.	high

Evaluation Criteria	Comment	Weighting
Sales Execution/Pricing	Sales execution focuses on the success and "mind share" of the product or service in the VA market. The evaluation includes revenue and installed base for VA products and services. The maturity and breadth of the organization's distribution channels and the level of interest from Gartner clients are also considered.	standard
Offering (Product) Strategy	An offering (product) strategy is the vendor's approach to product development and delivery that emphasizes differentiation, functionality and feature set as they map to current and future requirements. Development plans during the next 12 to 18 months are evaluated.	standard
Product/Service	Product or service evaluates current product function in areas such as base scanning methods, scope of VA, workflow and remediation support, and reporting capabilities.	high
Overall Viability (Business Unit, Financial, Strategy, Organization)	Overall viability includes an assessment of the overall financial health of the organization, along with the financial and practical success of the business unit. Also evaluated is the ability of the organization/business unit to continue investing in the VA market and to continue developing innovative products to meet the requirements of several different types of customers.	standard

Evaluation Criteria	Comment	Weighting
Customer Experience	Customer experience is an evaluation of product function or service in production environments. The evaluation includes ease of deployment, operation, administration, stability, scalability and vendor support capabilities. This criterion was assessed by conducting qualitative interviews of vendor-provided reference customers and feedback from Gartner clients that are currently using or have completed competitive evaluations of the VA offering.	high

Source: Gartner

Figure 1. MarketScope for Vulnerability Assessment

	RATING				
	Strong Negative	Caution	Promising	Positive	Strong Positive
Beyond Security		x			
Criston		x			
Critical Watch		x			
eEye Digital Security				x	
IBM ISS			x		
Lumension Security		x			
McAfee				x	
nCircle					x
Qualys					x
Rapid7				x	
Saint		x			
StillSecure			x		
Tenable Network Security			x		

As of 19 May 2008

Source: Gartner (May 2008)

Vendor Product/Service Analysis

Beyond Security

Beyond Security is a relatively small provider of hosted external scanning services and VA appliances. The company's Automated Vulnerability Detection System integrates with the assessment appliance and adds vulnerability scoring, asset management and integrated ticketing. The assessment appliance includes Web application and database assessment functions. The company also operates the SecuriTeam security portal.

Strengths: Beyond Security has focused on scalable and accurate scanning, as well as ease of deployment. Customer feedback has been positive in all these areas.

Challenges: Achieving growth remains Beyond Security's primary challenge. Alcatel-Lucent cobrands Beyond Security's appliance for worldwide sale. Client feedback on the product and vendor support have been positive, but a Caution rating is based on the relative size and growth rate of Beyond Security in this market segment.

Optimal-use case: Organizations that want an appliance-based scanner or an external scanning service should evaluate Beyond Security.

Rating: Caution

Criston

Criston, a French company, provides VA and PC life cycle management software to its European and Asian customer base. Vulnerability Management is a network-oriented VA scanner. The Vulnerability Management scanning agent provides scanner server functions. The agent also can be installed on target systems to do host-level scans. Criston has implemented common agent and policy management, and a common inventory and reporting infrastructure for Vulnerability Management and PC life cycle management.

Strengths: The primary differentiator for Criston's VA technology is the tight integration with mitigation functions provided by the PC life cycle management suite.

Challenges: Criston is a small vendor with a broad product suite that has large, established competitors in the VA and PC life cycle management segments.

Optimal-use case: Organizations that can implement the security and operations technologies provided by Criston will benefit from the remediation capabilities that are enabled through cross-product integration.

Rating: Caution

Critical Watch

Critical Watch provides its FusionVM product in appliance form and as a managed service hosted by Critical Watch. Critical Watch sells directly to end users and also has partnerships with service providers, such as ACS, Jefferson Wells and Perot Systems, which use Critical Watch technology and services in their outsourcing businesses or in projects to implement vulnerability management capabilities.

Strengths: The combination of scanning services and scanning technology that can be deployed effectively without extensive tuning enables rapid deployment and use by end-user organizations, managed service providers and consultants. The company has developed remediation tracking capabilities that are designed for use in an overall vulnerability management process. Customer feedback on product/service function, scalability and support has been positive.

Challenges: Although Critical Watch has provided VA services since 2000 and VA products since 2004, it has not achieved the visibility or customer base of service provider competitors, such as Qualys, or appliance providers, such as nCircle. In the absence of venture capital funding, Critical Watch depends on maintaining profitability rather than on rapid expansion. The Caution rating is not based on the quality of the technology or customer feedback, but rather on Critical Watch's ability to grow in this market, and the burden of a small company providing VA as a product and a service.

Optimal-use case: Organizations with limited support resources that want VA scanning services should evaluate Critical Watch, as should organizations that have engaged one of the partner consultancy or outsourcing companies for a vulnerability management deployment, and organizations that wish to deploy an appliance and require strong role-based access and workflow support.

Rating: Caution

eEye Digital Security

eEye Digital Security provides Retina Network Security Scanner as software or an appliance. Retina Enterprise Manager (REM) provides centralized administration and reporting. Host-based Blink provides VA and intrusion prevention functions. Although the Retina products provide multiplatform VA, eEye is rated Positive because of the fit of the solution to the needs of midsize Windows-centric enterprises.

Strengths: The company maintains a strong security research team, which has helped it provide a breadth and depth of Windows vulnerability coverage. Reporting includes PCI and scoring that is specific to the U.S. Department of Defense.

Challenges: REM is not widely deployed in eEye's installed base, and it lacks some of the compliance and control standards reporting and configuration options offered by vendors that are best in class in this area. Also, eEye has ambitious plans for expansion to additional areas, which is risky for a small vendor.

Optimal-use case: The company offers a software solution that is optimal for Windows-centric midsize enterprises that value ease of deployment over advanced compliance and configuration reporting.

Rating: Positive

IBM ISS

IBM ISS provides two VA products: the software-based Internet Scanner and the appliance-based Proventia Network Enterprise Scanner. IBM's SiteProtector system can provide centralized management of Internet Scanner and Network Enterprise Scanner deployments. IBM also offers VA as a managed service.

Strengths: Network Enterprise Scanner offers scan control and reporting improvements over Internet Scanner. Enterprises that already have investments in other IBM Internet Security System products, such as Proventia IPS, SiteProtector and RealSecure, should realize added benefits from Network Enterprise Scanner's capability to integrate with those products to improve the accuracy of intrusion prevention and detection.

Challenges: IBM ISS has yet to demonstrate that it can deliver added VA functionality for applications and databases, and reporting that would bring Network Enterprise Scanner into closer competition with other VA products. Non-IBM ISS customers should evaluate competing products.

Optimal-use case: Current IBM RealSecure, SiteProtector and Proventia customers that require VA technology should evaluate Network Enterprise Scanner, as should organizations that wish to minimize their viability risks.

Rating: Promising

Lumension Security

Lumension was formerly known as PatchLink. In February 2007, PatchLink (which had been known mainly for patch management capabilities) acquired the Harris Security Threat Avoidance Technology (STAT) Guardian Vulnerability Management Suite — including the STAT Command Center, Report Center, Analyzer and Scanner products. PatchLink already had integrated these products as part of an established original equipment manufacturer partnership with Harris. The STAT scanner primarily is used for credentialed VA, but also supports remote scanning. The Harris acquisition gave PatchLink the ability to do agentless VA and gained them market share in the government vertical market, where STAT had primarily been used. Later in 2007, PatchLink acquired SecureWave, an endpoint security company, and PatchLink changed its name to Lumension. Lumension's Vulnerability Assessment Solution now consists of the PatchLink Scan network vulnerability scanner and the PatchLink Security Management Console.

Strengths: The Harris STAT product had achieved Common Criteria certification, and Lumension recently added Security Content Automation Protocol support, giving Lumension a strong position in government and high-security markets that require such certification. The PatchLink vulnerability database and remediation information provide a strong basis for detailed vulnerability assessment. Lumension has been aggressive in partnering with NAC vendors.

Challenges: Lumension does not have high visibility outside of its patch management roots. The STAT technology had limited coverage outside of Windows and Unix systems, compared with other offerings.

Optimal-use case: Current users of PatchLink patch/configuration management products and government agencies that have contract vehicle access to the STAT scanner.

Rating: Caution

McAfee

McAfee's Foundstone VA is available as software, an appliance or a managed service. McAfee's development strategy has been to improve stand-alone VA capabilities while also developing integrations with related technologies that improve assessment and remediation functions. An integration with Remediation Manager provides the capability to generate remediation actions from the VA.

Strengths: Although the Foundstone technology is not dependent on McAfee's ePolicy Orchestrator (ePO) infrastructure, the integration with ePO provides endpoint configuration information that improves scanning efficiency and accuracy. During the past year, McAfee has expanded the scope of scanning to include security configuration assessment. Foundstone VA also provides network scanning for McAfee's NAC solution, and is integrated with McAfee's risk assessment, policy audit and network IPS technologies.

Challenges: McAfee needs to maintain its balanced positioning of Foundstone as a competitive stand-alone assessment technology as it continues its cross-product integration efforts.

Optimal-use case: Organizations that want effective scanning technology with minimal provider viability risk should evaluate McAfee's offerings. Organizations that have deployed ePO and plan to deploy McAfee's security, policy management or remediation technologies will benefit from the cross-product integration initiatives that the company has executed.

Rating: Positive

nCircle

nCircle's IP360 Vulnerability Management System is an appliance-based VA offering that can be extended with add-on products that provide additional capabilities in areas such as security configuration policy compliance and topology-based risk assessment. nCircle VA also is available as a service through service provider partners. nCircle's Configuration Compliance Manager provides security configuration policy compliance and incorporates technology from the Cambia Security acquisition in May 2007.

Strengths: The company's VA appliance solutions can be extended with ancillary products that provide risk assessment, security configuration policy assessment and file integrity monitoring. The integration of Configuration Compliance Manager and IP360 has begun, and integrated VA and security configuration reporting is provided through nCircle's Security Intelligence Hub.

Challenges: Although nCircle provides a broad set of advanced assessment capabilities, its VA product's features are oriented toward large enterprises that can dedicate staff to run the product and analyze results. To maintain growth, nCircle must penetrate the broader market of enterprises at lower price points and with simplified offerings. The company has begun to reach the broader market indirectly through its MSSP partners.

Optimal-use case: Organizations that require a VA appliance that is delivered as a product, or those that want to extend VA scanning to include security configuration policy compliance, should evaluate nCircle.

Rating: Strong Positive

Qualys

Qualys has focused from the start on delivering VA as a service offering. Service offerings have evolved from simple Internet-based scanning (QualysGuard Express) to internal scanning via a customer premises appliance (QualysGuard Enterprise), with vulnerability data sent back to the Qualys security operations center, to the latest offering, QualysGuard @Customer, with all sensitive data stored on the customer premises appliance. This range of offerings, along with flexible pricing, enables Qualys and its channel partners to address a wide range of enterprises sizes and operational demands.

Strengths: The company's focus on security as a service has enabled it to capture many channel partners who resell Qualys' capability, rather than build their own or acquire competing products. Qualys continually receives best-in-class grades from customers for ease of deployment and on its level of support and responsiveness.

Challenges: Qualys did not make the expected move into application vulnerability testing services, which has provided openings for other scanning service vendors (such as WhiteHat Security and Rapid7) to gain traction.

Optimal-use case: Organizations that need VA, but do not want to invest in the internal resources needed to support a product deployment, should evaluate Qualys.

Rating: Strong Positive

Rapid7

Rapid7 increased its installed base and channel strength in 2007, adding several large accounts to its customer mix. Rapid7's NeXpose capability is available as software, an appliance, and as a security-as-a-service and managed service offering. NeXpose provides a deeper range of vulnerability analysis compared with many other offerings, which caused some users to report

difficulty in use and interpretation of results; however, improvements in the management interface have alleviated those concerns. Rapid7 has added engineering, product management and business development expertise capabilities and continues to be one of the first VA vendors to offer new checks for emerging complex vulnerabilities. Also, the demand for PCI-specific vulnerability testing has worked to Rapid7's benefit.

Strengths: Broad coverage of complex vulnerabilities, strong remediation reporting and a penetration-testing-oriented approach are Rapid7's primary technical strengths. A strong inside sales force and aggressive pricing are its business strengths.

Challenges: Although some users report slow service response, the majority was satisfied; however, Rapid7 will need to ensure that post-sales support keeps up with an expanding installed base. As a small company competing with many larger, publicly held companies, Rapid7 must continue to show growth in channel strength and integration partners to address long-term viability concerns.

Optimal-use case: Organizations that want broad VA capabilities that go beyond one-pass scanning and a variety of delivery options should evaluate Rapid7.

Rating: Positive

Saint

Saint offers VA through software, an appliance and a managed service since 2001. The product offers limited Web application and database assessment. Saint includes a limited penetration testing component with VA.

Strengths: Saint gets good feedback for operational remediation support and technical-support responsiveness.

Challenges: Saint's biggest challenges are related to its small size, relative to competitors. Secondary challenges include a feature set that is not as rich as those of many competitors, such as more-limited compliance-specific and control-standards-based reporting compared with other products. Saint will need to show sufficient financial depth and demonstrate that it is meeting its development road map to assure its enterprise customers of long-term viability.

Optimal-use case: Organizations looking for remediation-focused VA through software, a managed service or an appliance should evaluate Saint.

Rating: Caution

StillSecure

The distinguishing characteristic of StillSecure's VAM is that it is a component of a vulnerability management suite that includes assessment, workflow, remediation and risk reporting. The VA scanner also is used to baseline endpoints within the Safe Access NAC component. StillSecure initially derived its VA scanning engine from Nessus, but it has made extensive enhancements that have resulted in scanning technology that is now independent of Nessus. Although the scanning engine is not Nessus, users that are familiar with the Nessus scanner will recognize its Nessus roots.

Strengths: VAM's strengths include the capability to apply existing Nessus expertise to an enterprise VA deployment, as well as the integration of VA with StillSecure's vulnerability management functions. StillSecure has received good marks for the accessibility and responsiveness of its technical support.

Challenges: There are some limitations in the area of vulnerability reporting in the base VAM product. The Security POV option remedies those shortcomings; however, because StillSecure licenses technology from an OEM, Security POV requires an additional license fee. StillSecure is a relatively small vendor spreading its resources across intrusion prevention, NAC and vulnerability management. This makes competitive differentiation difficult in cases in which the security buying center just wants VA technology.

Optimal-use case: Organizations that require a suite that supports the vulnerability management life cycle should evaluate StillSecure, as should organizations that are comfortable with Nessus but require centralized administration and management.

Rating: Promising

Tenable Network Security

Tenable Network Security's enterprise VA solution is comprised of Nessus 3 scanners in combination with Security Center, which provides consolidated reporting and management. The solution also provides security configuration policy compliance functions. Tenable also provides passive vulnerability scanning, and security event management and IDS technologies, which are all integrated through Security Center. Although Tenable has implemented Nessus restrictions that prevent its use in commercial products, Nessus is one of the most widely used VA tools and is still offered to the general public as a free download.

Strengths: Recent improvements in Security Center consolidated management and reporting capabilities have resulted in a level of function that is competitive in the market segment. Tenable's VA, intrusion detection and security event management technologies are tightly integrated, and the customer base tends to use all the capabilities. The company has achieved SCAP certification, which makes it easier to sell to the federal government market.

Challenges: Now that Tenable has competitive consolidated management and reporting, the company needs to become more visible in competitive evaluations and to expand its support options.

Optimal-use case: Organizations that want to continue the use of Nessus scanners, but require consolidated management and improved reporting, should evaluate Tenable.

Rating: Promising

RECOMMENDED READING

"Magic Quadrants and MarketScopes: How Gartner Evaluates Vendors Within a Market"

"Defining the Security-as-a-Service Market"

"Selecting the Right Targets for Security as a Service"

"The Future of Vulnerability Assessment Faces Functional and Market Challenges"

"Best Practices for Network Vulnerability Assessment"

"Responsible Vulnerability Disclosure: Guidance for Researchers, Vendors and End Users"

"Improve IT Security With Vulnerability Management"

"Identifying and Solving Vulnerability Management Weak Spots"

"Visibility and Control Are Key to Managing IT Security Vulnerabilities"

"Penetration Testing Augments Vulnerability Management to Deal With Changing Threats"

"Ten Recommendations to Prevent a Successful Attack"

Acronym Key and Glossary Terms

ePO	ePolicy Orchestrator
IPS	intrusion prevention system
MSSP	managed security service provider
NAC	network access control
VA	vulnerability assessment
PCI	Payment Card Industry
REM	Retina Enterprise Manager
RNA	Real-time Network Awareness
SCAP	Security Content Automation Protocol
STAT	Security Threat Avoidance Technology

Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Gartner MarketScope Defined

Gartner's MarketScope provides specific guidance for users who are deploying, or have deployed, products or services. A Gartner MarketScope rating does not imply that the vendor meets all, few or none of the evaluation criteria. The Gartner MarketScope evaluation is based on a weighted evaluation of a vendor's products in comparison with the evaluation criteria. Consider Gartner's criteria as they apply to your specific requirements. Contact Gartner to discuss how this evaluation may affect your specific needs.

In the below table, the various ratings are defined:

MarketScope Rating Framework

Strong Positive

Is viewed as a provider of strategic products, services or solutions:

- *Customers:* Continue with planned investments.
- *Potential customers:* Consider this vendor a strong choice for strategic investments.

Positive

Demonstrates strength in specific areas, but execution in one or more areas may still be developing or inconsistent with other areas of performance:

- *Customers:* Continue planned investments.
- *Potential customers:* Consider this vendor a viable choice for strategic or tactical investments, while planning for known limitations.

Promising

Shows potential in specific areas; however, execution is inconsistent:

- *Customers:* Consider the short- and long-term impact of possible changes in status.
- *Potential customers:* Plan for and be aware of issues and opportunities related to the evolution and maturity of this vendor.

Caution

Faces challenges in one or more areas.

- *Customers:* Understand challenges in relevant areas, and develop contingency plans based on risk tolerance and possible business impact.
- *Potential customers:* Account for the vendor's challenges as part of due diligence.

Strong Negative

Has difficulty responding to problems in multiple areas.

- *Customers:* Execute risk mitigation plans and contingency options.
- *Potential customers:* Consider this vendor only for tactical investment with short-term, rapid payback.

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509