The evolution of the vulnerability assessment market has slowed as vendors have focused on incremental improvements for deployment, assessments and compliance reporting. Buyers must consider how VA will fit with overall security process requirements when evaluating VA technologies.

What You Need to Know

Enterprises should define the scope and frequency of vulnerability scanning and the integration requirements first, and then select the best mix of delivery mechanisms (software, appliance, service, mix) before evaluating vulnerability assessment (VA) products.

These products focus on discovering network nodes and identifying network-level vulnerabilities. While some vendors include some capabilities for discovering application-level vulnerabilities, network VA products are not substitutes for application-level vulnerability analysis products.

Enterprises that cannot devote the staff resources to regularly use network VA products should focus on service offerings.

MarketScope

VA products are basic tools used by security groups to support vulnerability management activities that find and fix security weaknesses. Although VA is a fundamental security capability, the strongest driver for project funding is compliance, including prescriptive compliance regimes such as Payment Card Industry (PCI) Data Security Standards, and the U.S. Federal Information Security Management Act (FISMA) and Federal Desktop Core Configuration (FDCC) requirements. In addition to supporting basic security activities and formal compliance regimes, VA tools are used by security groups to support vulnerability management activities that business partners and customers require of an enterprise.

The VA market is settled, with a relatively stable set of technology providers. Since the last VA MarketScope, Symantec acquired Gideon to gain Security Content Automation Protocol capabilities, and Fortinet acquired Secure Elements for similar reasons. Feature and function improvements have been incremental, with emphasis on adding scanning targets, improving integration with adjacent technologies and increasing delivery options. The products mostly differentiate on scale, overall price and manageability.

Some VA vendors have broadened the scope of scanning to include applications and database management systems (DBMSs), and a growing number also provide security configuration assessment. However, the primary driver for deployment of these VA products is scanning at the network level, and most enterprises use other dedicated products when application and database vulnerability scanning is required.

VA tools also support other security operations. VA scanning discovers unmanaged devices on the network so that those devices can be brought under management or removed from the network. Scanning provides baseline vulnerability status, and trending provides evidence of the effectiveness of vulnerability management activities. Vulnerability reports that include recommendations for mitigation or remediation of vulnerable assets can improve the efficiency of IT operations, and risk-rated reports can help measure security effectiveness.

Integration of VA scanning with protective technologies, such as intrusion protection systems (IPSes) or Web application firewalls (WAFs), provides targeted mitigation capabilities that security operations can use to shield vulnerable systems while those systems are being updated. Scanning tools that provide configuration assessment can be used drive policy enforcement.

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).
VA scanning is available in several delivery formats: as software, as appliances and as a service. Hybrid delivery options that include one or more of the delivery formats are becoming available. For example, an enterprise may deploy software or appliances inside its network perimeter and use a scanning service to assess the perimeter from the outside. Buyers should match the deployment options to their specific requirements. VA software provides the flexibility to deploy VA on enterprise-standard platforms. Appliances offer easy deployment without the need to procure and manage additional hardware. Services offer acquisition benefits (typically, services are paid from operations budgets rather than capital budgets) and easy service startup. When considering a deployment that includes more than one delivery option, take into consideration the vendor’s ability to provide unified management and reporting across the different delivery modes.

Market inhibitors include the complexity of the tools, the performance and management requirements of large-scale deployments, the continued availability of vulnerability assessment scanning from periodic engagements with security consultancies, and the availability of VA delivered as a service directly by vendors or from managed security service providers (MSSPs). Gartner expects that VA products will continue to be available as point solution offerings for those enterprises able to deploy and run them in-house, but we expect the growth of VA services to be higher than the growth of product sales.

**MarketScope for Vulnerability Assessment**

---

### MarketScope Rating Framework

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

---

### Inclusion and Exclusion Criteria

Vendors were included based on these criteria:

- They use their own VA engines.
- They perform active network VA.
- They provide vulnerability information and reference multiple vulnerability IDs, including common vulnerabilities and exposures, SANS Top-20, Bugtraq ID and vendor-specific IDs.
- They provide remediation guidance.
- They offer an enterprise-level product that supports central administration of multiple distributed scanners and consolidated reporting.
- They focus on the security organization.
- They provide asset classification capabilities.

Gideon Technologies, acquired by Symantec in January 2010, met our inclusion criteria, but was not evaluated in the MarketScope based on its publication schedule. Gideon Technologies’ Secure Fusion product provides discovery, configuration and VA scanning, and has been sold into commercial and federal government markets.

Vendors were excluded based on these criteria:

---

**Inclusion and Exclusion Criteria**

---

http://www.gartner.com/technology/media-products/reprints/rapid7/173772.html

5/15/2010
MarketScope for Vulnerability Assessment

- They redistribute a third-party VA scanner or rely on one to be enterprise-deployed
- They sell primarily to the operations group or lack security context
- They embed VA function in broader products and suites

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

- Symantec. The company currently sells Control Compliance Suite for Internet Security (the VA technology that it gained from its 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 Network Access Control [NAC] offering). Symantec Control Compliance Suite customers that wish to implement VA technology should evaluate the Internet security component. Symantec also provides SecurityExpressions (from its 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), it 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.

- Secunia. The company is best known for vulnerability research and information feeds, and added agent-based and credential-based vulnerability assessment in 2008. Secunia's approach, Corporate Software Inspector (CSI), provides useful detail on installed software and matches installed software with known vulnerabilities and remediation advice. CSI provides limited functionality, such as assessment of port, service and registry settings, compared with competitor offerings. Because Secunia does not support active network scanning, it was not included in the MarketScope.

- Sourcefire. The company'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.

- Secure Elements. This company, which was acquired by Fortinet in September 2008, 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 Elements' 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, its C5 Compliance Platform and Auditor Pro products began providing discovery and scanning capabilities and integration with security policy management products, such as FISMA, 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.

Vendors Added to the MarketScope

Trustwave has been added to this MarketScope based on the availability of its TrustKeeper scanning technology.

Vendors Dropped From This MarketScope

Criston Software does not appear in this MarketScope, because it no longer meets the inclusion criterion for a stand-alone VA offering.

Rating for Overall Market/Market Segment

Overall Market Rating: Positive

VA remains a steady growth market, with revenue estimated at $320 million in 2009 and an expected $400 million in 2010. The market 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. There will be stable, long-term demand for security VA 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 and FDCC.

Evaluation Criteria

Table 1. Evaluation Criteria

---

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 sales, and client feedback on the product and vendor support has been positive, but the relative size and growth rate of Beyond Security in this market segment continues to be the primary challenge.

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

Rating: Promising
Critical Watch

Critical Watch delivers its FusionVM vulnerability management solution as an appliance, as a virtual appliance or as a managed service. The company also has partnerships with service providers, such as ACS (Xerox), Jefferson Wells and Perot Systems (now Dell), which use Critical Watch technology and services in their outsourcing businesses or in projects to implement vulnerability management capabilities. During 2009, Critical Watch engaged TippingPoint Technologies in an active partnership based on integration of Critical Watch Vulnerability Management and TippingPoint IPS technology.

Strengths: In addition to providing security-oriented reporting, FusionVM also provides reports and strong workflow capabilities that are oriented to remediation activity — for use by operations areas that are assigned remediation tasks. FusionVM also provides security configuration assessment capabilities.

Challenges: Although Critical Watch grew revenue at a healthy pace during 2009, it remains one of the smaller vendors in the market. The company's challenge is allocating limited resources to continue to add functionality while maintaining core capability.

Optimal use case: Organizations with limited deployment and support resources, and organizations that have engaged a Critical Watch consulting or outsourcing partner, should evaluate Critical Watch scanning services. Organizations that wish to deploy an appliance and require remediation-oriented reporting and workflow, as well as those that also need security configuration assessment functions, should evaluate the FusionVM appliance.

Rating: Promising

eEye Digital Security

eEye Digital Security provides Retina Network Security Scanner as a software image, as an appliance and as a managed service based on the Retina 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, the best fit is in Microsoft Windows-centric environments.

Strengths: eEye's security research team continues to provide good Windows vulnerability coverage and mitigation advice for zero-day vulnerabilities. REM supports PCI and SCAP reporting and maps reports to FDCC and Defense Information System Agency (DISA) Security Technical Implementation Guide (STIG). REM provides integration with several security information and event management (SIEM), WAF, NAC and patch management products.

Challenges: eEye must continue to improve database and application scanning capabilities of Retina, and add additional compliance and control reporting and mapping options to REM.

Optimal use case: Companies considering or committed to Blink endpoint protection, and those looking for Windows-centric scanning with easy deployment requirements, should evaluate REM.

Rating: Positive

IBM Internet Security Systems

The IBM ISS VA offering is composed of Internet scanner software, the Proventia Network Enterprise Scanner appliance and the Vulnerability Management Service.

Since ISS was one of the original vendors of network vulnerability scanning software, IBM ISS has the largest market penetration. Enterprises that have deployed other ISS security products can use the IBM SiteProtector to provide centralized management of deployed VA systems. IBM recently announced that ISS products would be integrated into the Tivoli business unit. The Vulnerability Management Service remains in IBM's Global Services unit.

Strengths: IBM's Network Scanner products are widely supported by third-party vendors, and there is a large base of security personnel with experience using IBM's product. IBM's X-Force is one of the industry's strongest vulnerability research labs.

Challenges: Since acquiring ISS, IBM has been slow to add competitive features to its Network Scanners. The movement of the ISS business unit into Tivoli may result in more resources leaving ISS or being diverted to other, faster-growth areas.

Optimal use case: Current IBM SiteProtector and Proventia customers that require VA technology should evaluate Network Enterprise Scanner. Enterprises seeking scanning as a service should evaluate IBM's Vulnerability Management Service.

Rating: Caution
Lumension Security

Lumension’s VA scanning roots include the acquisition of Harris Security Threat Avoidance Technology (STAT) Guardian Vulnerability Management Suite, which had recognition and market share among government buyers. Although Lumension still offers the Scan product as a stand-alone offering (and thus meets the inclusion criteria for this MarketScope), Lumension Scan is typically deployed as part of Lumension Vulnerability Management suite.

Strengths: The Lumension Scan product has achieved Common Criteria certification, and Lumension recently added SCAP support, giving Lumension the ability to address government and high-security markets that require such certification. The Lumension vulnerability database and remediation information provide a strong basis for detailed vulnerability assessment.

Challenges: Lumension has a higher profile for its patch management offerings than for its VA product. The STAT technology had limited coverage outside of Windows and Linux/Unix systems, compared with other offerings.

Optimal use case: Current users of Lumension Patch and Remediation and Lumension Security Configuration Management products, as well as government agencies that have contract vehicle access to the STAT scanner, should consider this vendor.

Rating: Promising

McAfee

McAfee Vulnerability Manager is available as software, an appliance or a managed service. Since McAfee sells a wide range of security products, its VA strategy has been focused on integrating Vulnerability Manager into McAfee’s ePolicy Orchestrator (ePO) management console, and with other McAfee products with intrusion prevention, reporting, risk assessment and remediation functions.

McAfee’s development strategy has been to improve stand-alone VA capabilities while also developing integrations with related technologies that provide risk management and remediation functions. Integration with Remediation Manager provides the capability to generate remediation actions from the VA. Integration with Risk Advisor allows users to correlate threats with vulnerabilities and deployed countermeasures. McAfee’s acquisition of Solidcore provides file integrity monitoring and application "whitelist" capability to the McAfee portfolio of products.

Strengths: Vulnerability Manager is SCAP and Common Criteria certified, and it provides templates and reports for support for multiple compliance regimes. Vulnerability Manager integrates with ePO, which provides endpoint configuration information that improves scanning efficiency and accuracy. Vulnerability Manager is also integrated with McAfee’s risk assessment, policy audit and network IPS technologies. McAfee provides an API for integration with third-party products.

Challenges: McAfee needs to maintain its balanced positioning of Vulnerability Manager 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 Vulnerability Manager. Organizations that have deployed ePO and deployed or plan to deploy McAfee’s intrusion prevention, policy management or remediation technologies will benefit from the cross-product integration initiatives that the company has executed.

Rating: Positive

nCircle

nCircle’s IP360 product line provides vulnerability scanning, Web application scanning, security configuration assessment, file integrity monitoring and topology-based risk assessment. All nCircle products are available as appliances or as virtual images, and the Suite360 Intelligence Hub reporting facility is available as a software image. nCircle also provides a PCI scanning service, and nCircle products are the foundation of the Hitrust Security and Configuration Auditing SaaS solution and other SaaS services from managed services provider partners.

Strengths: Suite360 Intelligence Hub provides flexible risk-rating capabilities and extensive compliance reporting, and IP360 and the Configuration Compliance Manager are SCAP-certified. nCircle provides integration with a number of SIEM vendors and adjacent technologies.

Challenges: nCircle should continue to expand delivery options, and tailor management requirements and pricing for buyers that lack the resources of a large enterprise security staff. nCircle is launching vertically focused compliance SaaS solutions during the first half of 2010. Its competitors are also targeting the managed security service provider channel, or have started their own service delivery capabilities, to deliver VA as a service with features and pricing attractive to the midmarket.
Optimal use case: Organizations that require a VA product with extensive reporting, flexibility and extensibility for configuration assessment, and file integrity monitoring.

Rating: Strong Positive

Qualys

Qualys entered the VA market with a service-based offering, and has expanded delivery options to encompass remote scanning as well as appliance-based scanning. The company has expanded the scope of its offering to include security configuration assessment and Web application scanning. This range of offerings, along with flexible pricing, enables Qualys and its channel partners to address a wide range of enterprise sizes and operational demands.

Strengths: The company’s early implementation of VA as a service has enabled it to capture many channel partners that resell Qualys’ capability, rather than build their own or acquire competing products. Qualys typically gets excellent grades from customers for ease of deployment, and on its level of support and responsiveness. Qualys is the largest company in this market, has the broadest and deepest channel support, and is most frequently seen on Gartner client shortlists.

Challenges: Qualys must improve the flexibility of its reporting capabilities to allow more customization by users. As other VA vendors add or augment their service-based delivery, Qualys’ service-based approach will provide less differentiation to customers and channel partners.

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

Rating: Strong Positive

Rapid7

Rapid7 has gained visibility among VA buyers, and has added significant channel partners to supplement its direct sales operation. Rapid7 also closed OEM deals with managed security provider SecureWorks and with another MSSP that will use Rapid7 technology to deliver VA as a service to its managed security customers. Rapid7’s NeXpose capability is available as software, as an appliance, and as a security-as-a-service and managed service offering. NeXpose provides a broader range of vulnerability analysis compared with many other offerings. Rapid7 has added engineering, enterprise support, product management and business development capabilities, and continues to be one of the first VA vendors to offer new checks for emerging complex vulnerabilities.

Strengths: Rapid7 has improved scanning performance, and NeXpose provides strong remediation reporting. NeXpose’s penetration-testing-oriented approach to vulnerability validation should be further strengthened by the recently acquired Metasploit technology. Rapid7 has added a large number of channel partners and two OEM services deals, and maintains a strong inside sales force and aggressive pricing posture.

Challenges: Rapid7 must ensure that it can manage the growth in its customer base and business partner relationships. Postsales technical support must be able to meet the demands of the growth in its customer base, and the sales force must be more conscious of some buyers’ preferences for less-aggressive sales techniques.

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

Rating: Strong Positive

Saint

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

Strengths: Saint consistently receives good marks for operation-focused 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 roadmap to ensure 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.
**StillSecure**

StillSecure's VA capability is available as a software image, as an appliance and, since mid-2009, as a managed service through its ProtectPoint MSS offering. In addition to scanning, the vulnerability management product suite includes workflow, remediation and risk reporting. StillSecure offers Safe Access for NAC and the Strata Guard IDS/IPS products.

**Strengths:** VAM's appliance and managed services deployment options and integrated remediation workflow for suite buyers looking for low resource deployment and operations are strengths. The product's Nessus roots offer staff with Nessus experience a short learning curve for VAM. In addition, StillSecure provides APIs to enable integration and data import from IT operations and security products (including other VA scanning products). StillSecure gets high marks for responsive technical support and strong customer care.

**Challenges:** VAM's compliance reporting is not as well developed as that of competing products. The add-on Security POV module provides richer reporting capabilities for additional cost. As a relatively small vendor supporting several products and services, StillSecure must balance the requirements of point solution buyers with those seeking more-integrated suites.

**Optimal use case:** Organizations that require a suite that supports the vulnerability management life cycle should evaluate StillSecure, as should organizations that want to leverage Nessus expertise.

**Rating: Promising**

**Tenable Network Security**

Tenable's enterprise VA solution is composed of three components: the Nessus 4 Vulnerability Scanner, which provides active scanning; the Passive Vulnerability Scanner; and Security Center, which provides consolidated reporting and management. The Nessus vulnerability scanner also provides compliance and security configuration assessment. Although Tenable changed the licensing model for the Nessus scanner from open-source to proprietary in 2005, which implemented Nessus restrictions that restricted 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. Tenable provides updates for the research content/vulnerability checks via a home use (free) and commercial use (fee) subscription model.

**Strengths:** Tenable's VA and security event management technologies are tightly integrated within Security Center, and the customer base tends to use both capabilities.

**Challenges:** Tenable needs to maintain its recent focus on sales and marketing to support continued growth.

**Optimal use case:** Organizations that want a common reporting and administrative interface for VA, security configuration assessment and SIEM should consider Tenable. Organizations that want to continue the use of Nessus scanners, but require consolidated management and improved reporting, should evaluate Tenable.

**Rating: Positive**

**Trustwave**

Trustwave offers TrustKeeper capability as a service for external scanning, and as an appliance for internal scanning, with a Web-based portal for scan management and reporting. TrustKeeper is part of a suite of PCI compliance services, including enterprise governance risk and compliance, offered by Trustwave. The VA capability is built around assessing PCI compliance, although Trustwave plans on adding other compliance reporting capabilities.

**Strengths:** Trustwave has strong market visibility awareness as a PCI compliance assessor. The TrustKeeper portal features flexible scheduling and role-based administration, and Trustwave receives good marks for responsive technical support.

**Challenges:** Trustwave must add reporting and mapping for other compliance regimes and controls standards to move beyond PCI-specific deployments.

**Optimal use case:** Organizations requiring VA of their PCI environments should consider Trustwave.

**Rating: Promising**