Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

EXCERPT

Worldwide Security and Vulnerability Management 2009–2013 Forecast and 2008 Vendor Shares

IN THIS EXCERPT

The content for this excerpt was taken directly from the IDC Market Analysis Report, Worldwide Security and Vulnerability Management 2009-2013 Forecast and 2008 Vendor Shares, by Charles J. Kolodgy (Doc # 220283). All or part of the following sections are included in this excerpt: IDC Opinion, In This Study, Situation Overview, Market Trends, Essential Guidance. Also included are Tables 3 & 4 and Figures 6 & 7.

IDC OPINION

Enterprises and organizations continue to deploy security technologies to defend against ever-increasing threats. All of these security products add complexity to the security infrastructure. To manage the growth in security, organizations are turning to security and vulnerability management (SVM) solutions to provide the organization and intelligence to make security more effective. The growth in the SVM market also continued to be fed by the need to comply with government and industry regulations, and in 2008, the market was able to maintain growth even during volatile economic times. The SVM market provides a window into an organization's risk posture and allows for that risk position to be monitored and improved. Security and vulnerability management market revenue maintained growing at a double-digit growth rate. The market grew 17% in 2008 when compared with 2007. Revenue in the market was $2.6 billion in 2008 compared with $2.3 billion in 2007. IDC believes the SVM market will remain on a positive growth trajectory in 2009, with revenue anticipated to be $2.8 billion, but this is only a 5.6% increase. The slow growth in 2009 is attributed to reduced overall IT spending, but by the end of the forecast period (2013), the market should exceed revenue of $4.4 billion, with a climbing annual growth rate resulting in a compound annual growth rate (CAGR) of 10.8%. Highlights are as follows:

- The growing body of disclosure law governing security breaches and data loss incidents will result in ever-increasing usage of products that can create and enforce security policy and provide information required by auditors. It also requires that products that aggregate data and event management have the ability to identify and remediate internal threats based on user privileges.

- Security consists of products, people, and policy. SVM vendors are able to provide many policy solutions, which are used to supplement and validate other security defenses.

Filing Information: November 2009, IDC #220283, Volume: 1
Security Compliance and Vulnerability Management Software: Excerpt

- The SVM market continues to be extremely diverse, with no vendor having even an 8% share. IDC does not see this market becoming one dominated by a few players, so IDC would not expect any one company to exceed 12% in market share during this period. The market is too diverse for such a consolidation.

- SVM products will continue to benefit from increasing government regulations, which will result from the financial problems of 2008–2009. To maintain compliance, vendors will require products that can automate compliance functions.

IN THIS STUDY

This IDC study examines the security and vulnerability management market for the period 2008–2013, with vendor revenue trends and market growth forecasts. Worldwide market sizes and vendor revenue and market shares of the leading vendors are provided for 2008, and a five-year growth forecast for this market is shown for 2009–2013. This study concludes with market trends and IDC guidance for future success.

Vulnerability Management Market Definitions

- **Vulnerability assessment products.** These are batch-level products that scan servers, workstations, other devices, and applications to uncover security vulnerabilities. The scan information is compared with a database of known security holes (vulnerabilities) to determine the threat status of the device or application. More sophisticated VA products can test for unknown vulnerabilities by mimicking common attack profiles to see if a device or an application can be penetrated. The use of penetration testing is an advanced capability that allows you to safely exploit vulnerabilities by replicating the kinds of access an intruder could achieve and providing actual paths of attacks that must be eliminated. Penetration testing, when used in conjunction with vulnerability scanning, reduces the number of false positives. Vulnerability assessment products are additionally segmented as defined here:

  - **Device vulnerability assessment products.** Device vulnerability assessment products use either network- or host-based scanners to look into a device to determine the security vulnerabilities. These scanners search out and discover devices and try to find known vulnerabilities on target systems. They can both have credentialed access (using usernames and passwords) into devices and provide an uncredentialed (hacker's view) look at a device. Credentialed scanners can do a deep dive into the device to find known vulnerabilities, while the hacker view will simulate attacks to see if a device can actually be exploited. Device VA scanners generally operate anonymously.

 ©2009 IDC

- **Application scanners.** Application scanners are products specifically designed to test the robustness of an application or software to resist attacks — both specific attacks and attacks based on hacking techniques. Application scanners avoid doing general vulnerability checks, such as port scans, or patch checks to concentrate on vulnerabilities associated with direct interaction with applications. The application scanner market includes products that look at deployed applications and products that review source code.

SITUATION OVERVIEW

Security and Vulnerability Management Market in 2008

Products that fall within the security and vulnerability management market remain in high demand. The SVM market covers a wide area of solutions that are designed to provide the brains of the security organization. Organizations are looking for solutions to proactively mitigate risk, handle establishing and auditing security policy, consolidate risk management information, and, ultimately, provide some security peace of mind. As a result, the market had a 17% growth rate in 2008 when compared with 2007's results. The total market in 2008 was $2.6 billion. The SVM market is broken into two major components Security Management and Vulnerability Management. Table 3 provides the top 10 vendors in the Vulnerability Management market. Unlike some other security markets that are dominated by a handful of vendors, the leading vendor in this space does not exceed 13%. The market is very competitive with the ten vendors noted in the table only representing 54% of the total market.

The Vulnerability Management market is itself divided into two submarkets, Device vulnerability assessment and application scanners, as defined above. For 2008 the Device Vulnerability Assessment market generated $376.4 million in vendor revenue with Qualys being the leading vendor, as shown in Figure 6.

Table 4 provides the IDC forecast for the Vulnerability Management market. By the end of the forecast period, IDC expects this market to exceed a billion dollars.

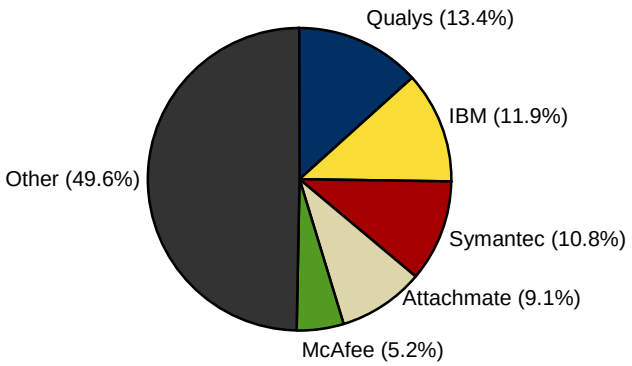
TABLE 3

Worldwide Vulnerability Revenue by Vendor, 2008

	Revenue ($M)	Share (%)
IBM	83.3	12.9
Qualys	50.3	7.8
Symantec	46.3	7.2
Attachmate	34.3	5.3
HP	29.0	4.5
Fortify	28.8	4.5
McAfee	21.1	3.3
Klocwork	18.8	2.9
nCircle	18.1	2.8
Imperva	18.0	2.8

FIGURE 6

Worldwide Device Vulnerability Assessment Revenue Share by Vendor, 2008



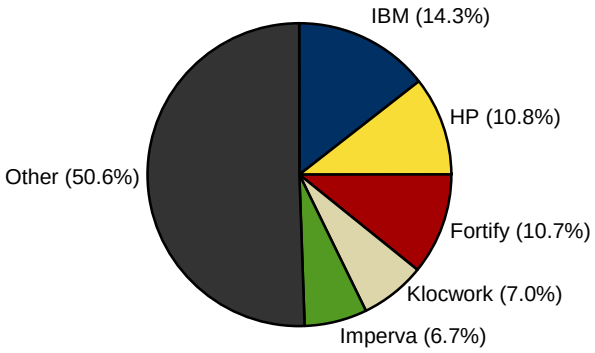
Total = $376.4M

Source: IDC, 2009

 ©2009 IDC

FIGURE 7

Worldwide Application Vulnerability Assessment Revenue Share by Vendor, 2008



Total = $269.5M

Source: IDC, 2009

TABLE 4

Worldwide Vulnerability Management Revenue by Segment, 2008–2013 ($M)

	2008	2009	2010	2011	2012	2013	2008–2013 CAGR (%)
Device Vulnerability Assessment	376.4	384.0	407.0	433.9	455.6	476.1	4.8
Application Scanners	269.5	307.6	341.0	400.4	467.8	542.2	15.0
Vulnerability Assessment Market Totall	645.9	691.6	748.0	834.2	923.4	1,018.2	9.5
SVM Total Market	2,634.5	2,780.9	3,048.4	3,432.1	3,880.0	4,393.4	10.8

Source: IDC, 2009

Market Trends

Given the importance of risk management, government regulations, and exposure through vulnerabilities, the security and vulnerability management market is full of opportunity. Developments that will shape this market in the future include the following:

- **Multiple delivery systems.** Vendors are providing SVM products using various delivery methods. These include software, hardware, software as a service, and virtualized software. The vulnerability assessment market has been available

through SaaS for many years. The use of SaaS for application testing continues to grow. SaaS is also growing in the SIEM market, and there is no reason SaaS can't be used in the policy and compliance market. Hardware products are most prominent in the SIEM and forensics and incident investigation submarkets because of the need to store vast amounts of log data. Virtualization is slowly becoming a part of the SVM market, and it is anticipated usage will grow quickly over the forecast period. Virtualization is required to ensure that the configuration and patch levels of virtual systems remain current. Virtual machines can be offline but can be activated at a moment's notice. It is important to keep those machines up to date. Additionally, nearly any of the SVM submarkets can also employ software appliances to run in a hypervisor-based environment. IDC would expect that SVM products will continue to be delivered in a diverse manner.

- **Application and software security vulnerability assessment.** As security becomes more important at the application level, new products will be introduced that are designed to assess the status of individual applications. There are tools that look at operational products such as databases and Web servers. The market has gained considerable visibility with the inclusion of software code scanning as a requirement within the payment card industry's Data Security Standard. The next step in this evolution is to utilize vulnerability discovery testing throughout the software development life cycle so that vulnerabilities can be eliminated before a program becomes operational. Organizations are going to demand software that is less vulnerable to attack; thus, application-level security needs to be a fundamental component for software development and quality assurance. Over the past year, the market grew 52%, and IDC forecasts that this segment will have solid growth during the forecast period (at 15% CAGR).

- **Unified security management.** Organizations depend on point security tools, including firewalls, VPNs, intrusion detection, and antivirus systems, for protection against attacks and malicious activity. The requirements for these products continue to grow. What organizations are looking for now are ways of optimizing their security infrastructure to cost effectively deal with real threats. Organizations are also seeking to extract more value out of regulatory compliance structure initially built for internal compliance and IT protection to use it for a basis of best practices to ratchet up not only enforcement but also auditing mechanisms. SVM technologies provide the knowledge and intelligence, allowing IT professionals to coordinate people, products, and policy. IDC will expect more vendors to discuss how their products can provide full risk management and regulatory compliance information.

ESSENTIAL GUIDANCE

Security is a value-add to many systems, not just a necessary evil or the purview of the paranoid. Companies understand that their systems, storage operations, network connectivity, and endpoints need to be inherently secure. Customers are demanding security, but they want it to be well integrated with the IT infrastructure and need it to be effective, manageable, and affordable. Security and vulnerability management is very important to meeting risk management goals because it provides policy and compliance context, vulnerability information, remediation, and, ultimately, a

comprehensive view of enterprise risk management. It offers organizations better ways to cost effectively provide risk management and automate the rising cost of compliance activities. SVM solutions can simplify the complexity associated with managing multiple security solutions while at the same time increasing the automation, effectiveness, and proactive nature of security. Vendors are growing the capabilities to provide comprehensive coverage within their security management offerings. The key to success in this space will be the ability to provide proactive security protection and the knowledge and intelligence to provide comprehensive security assessment data.

IDC believes vulnerabilities must be viewed as part of an overall security management infrastructure that takes into account security policy and compliance and risk management. SVM solutions will be expected to tell the enterprise why the vulnerability is a concern and how each specific vulnerability is ranked so that remediation can be performed in a consistent manner instead of handled in a chaotic manner. In general, SVM offerings must be able to provide a more aggressive, positive security model and not just respond to events.

Going forward, for the SVM market to return to double-digit growth rates, vendors must continue to make security smart. This includes providing proper policy management to automatically enforce the security policy. IDC also believes that vulnerability scanning, be it device or application based, white box or black box, credential or hacker view, provides critical information that allows organizations to adjust their security position to meet real security threats. IDC believes that products that can do real-time penetration testing will see considerable success over the next few years because they can pinpoint specific security gaps.

One area for the SVM market that has been underutilized is for solutions that handle small to medium-sized businesses. This group has been overlooked because the cost associated with vulnerability assessment and other SVM segments has been high in terms of both direct cost and overhead. However, as government requirements for security and privacy proliferate, all-sized organizations are beginning to be concerned about their ability to measure their compliance with security requirements. As these companies expand their use of additional security products and services, they will also be looking for ways to measure their risk. Vendors that can provide small and medium-sized enterprises with simple, easy-to-use, and affordable products for policy compliance and risk management should have considerable success.

Copyright Notice

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

Copyright 2009 IDC. Reproduction is forbidden unless authorized. All rights reserved.