

EXCERPT

Security and Vulnerability Management Software: Taking Control of the Security Environment

Charles J. Kolodgy

Rose Ryan

IN THIS EXCERPT

This excerpt is derived from the market analysis study *Worldwide Security and Vulnerability Management Software 2005–2009 Forecast and Analysis: Taking Control of the Security Environment* by Charles J. Kolodgy and Rose Ryan (IDC #34604, December 2005). It contains the IDC Opinion, Market Definitions, and Future Outlook sections, as well as a figure and a table.

IDC Opinion

The security market remains a high-growth one because it is always being renewed. New threats are created with the deployment of new information technologies, new hacker exploits, and government regulations that mandate better understanding about the integrity of the IT infrastructure. With these dynamics, the nature of the security markets must also be refreshed. IDC recognizes this need and has begun tracking the security management software market and the vulnerability assessment software market within a single security and vulnerability management (SVM) software market. The security management software market and the vulnerability assessment software market have been converging, and this coupling represents that change. Security and vulnerability management software revenue had a strong 22.4% growth rate from 2003 to 2004, which is rather impressive given that the total market exceeds \$1 billion. Revenue in the market was \$1.37 billion in 2004, compared with \$1.12 billion in 2003. For 2005, IDC believes the SVM market will generate approximately \$1.62 billion, a 17.9% increase. By 2009, the market should exceed revenue of \$3 billion with a surprisingly steady compound annual growth rate (CAGR) of 17.8%. Highlights are as follows:

- ☒ The growing reliance on IT for corporate operations and increasing government and industry regulation are elevating security policy, adherence to best practices, and measurement to a critical component of corporate governance. To meet these needs, SVM products are being released that can assist enterprises in handling policy creation, compliance measurements and audits, and reporting.
- ☒ Proactive security as embodied in security management will take a larger share of the market compared with reactive security, as represented by vulnerability scanning.
- ☒ Vendors have created or are moving to integrate vulnerability assessment with security management to provide enterprises with a comprehensive risk capability.

- ☒ By the end of the forecast period, the policy and compliance and the security information and event management submarkets will be the largest, both with more than \$600 million in vendor revenue.
- ☒ Software security vulnerability scanning products geared toward software developers and quality assurance are growing in popularity.

Security and Vulnerability Management Software Market Definitions

The security and vulnerability management software market is created by the merging of security management (SM), which was formerly part of the 3As market, with vulnerability assessment (VA), which was previously coupled with intrusion detection and prevention software. Although SVM is the overarching market, SM and VA remain distinct in their own right. With the creation of the security and vulnerability management software market, IDC has also expanded the subcategories within the market to include application protection. The submarkets are defined as follows:

- ☒ **Security management** software consists of a combination of tools that provide organizations with the ability to create security policy that drives other security initiatives, allows for measurement and reporting of the security posture, and ultimately provides methods for correcting security shortcomings. It also includes products that offer administration tools for security setting associated with security products, or any other network-attached devices. The security management market is divided into the following components:
 - ☐ **Patching and remediation** solutions automate or semiautomate the process of installing patches or correcting system misconfigurations across the enterprise immediately or on a scheduled basis. These products can include internal discovery systems to find network devices, identifying missing patches or misconfigurations, or they can interact with other SVM products to provide that knowledge. Automated patching systems respond to preset policy on how to respond to problems, and they also provide sourcing for patching content.
 - ☐ **Forensics and incident investigation** solutions capture and store real-time network and device data and identify how business assets are affected by network exploits, internal data theft, and security or HR policy violations.
 - ☐ **Policy and compliance** solutions allow organizations to create, measure, and report on security policy and regulatory compliance.
 - ☐ **Security information and event management (SIEM)** solutions include software designed to aggregate data from multiple sources to identify patterns of events that might signify attacks, intrusions, misuse, or failure. Event correlation simplifies and speeds the monitoring of network events by consolidating alerts and error logs into a short, easy-to-understand package. This market also includes activities that collect and disseminate threat intelligence, provide early warning threat services, and can provide information on countermeasures.

- ❑ **Security systems and configuration management (SSCM)** software is primarily systems management software that monitors and reports on the status of security solutions. It also is used to push security policy out to devices and to monitor the health of security systems.

- ☒ **Vulnerability assessment** products are batch-level products that determine the configuration, structure, security attributes, network user accounts, directories, servers, workstations, and other devices. This information is compared with a database of known security holes and best practices for security configuration management. More sophisticated VA products can test for unknown vulnerabilities by looking at the common attack profiles. Some products actually use penetration testing methods to determine the strength of various systems and networks. 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 is one way vulnerability scanners have become more efficient by eliminating false positives. Vulnerability assessment products are additionally segmented as defined below:
 - ❑ **Network-based** products use centralized scanners. These scanners simulate a hacker's view. They normally do not have credentialed access into devices or applications. These scanners search out and discover devices and try to find known vulnerabilities on target systems using techniques that are either inferential or similar to a hacker attack. They generally operate anonymously.

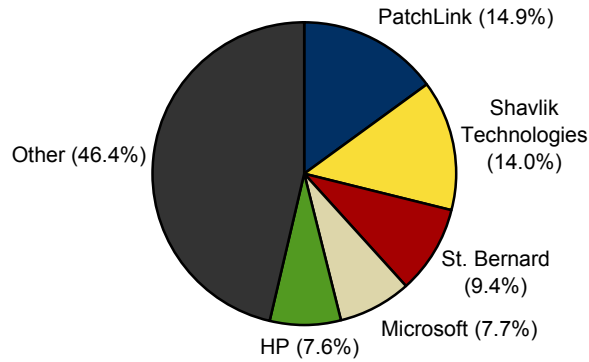
 - ❑ **Host-based** vulnerability assessment tools are generally considered to be a system administrator's look at devices and applications. These products typically use software agents placed on the device to provide privileged access (using usernames and passwords) to the managed system and report into a centralized management console. These host-based VA tools are normally used for analyzing internal security issues, including user security and system security.

 - ❑ **Application** scanners are products specifically designed to test the robustness of an application 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 in order to concentrate on vulnerabilities associated with direct interaction with applications. Application scanners include those products that look at deployed applications and those that can review source code.

Figure 1 displays 2004 market shares for leading patching and remediation software vendors.

FIGURE 1

Worldwide Patching and Remediation Software Revenue Share by Vendor, 2004



Total = \$117.3M

Source: IDC, 2005

FUTURE OUTLOOK

Forecast and Assumptions

Worldwide revenue for the SVM software market reached \$1.37 billion in 2004, representing 22.4% growth over 2003. IDC currently forecasts that the SVM software market will increase at a 17.8% CAGR and reach \$3.10 billion in 2009, as shown in Table 5.

TABLE 5

Worldwide Security and Vulnerability Management Software Revenue by Segment, 2004–2009 (\$M)

	2004	2005	2006	2007	2008	2009	2004–2009 CAGR (%)
Security management							
Security information and event management	209.9	266.6	335.7	419.5	520.9	635.5	24.8
Patching and remediation	117.3	150.5	192.7	246.2	305.8	370.0	25.8
Forensics and incident investigation	64.9	78.0	93.5	111.1	129.5	149.0	18.1
Policy and compliance	171.8	225.4	294.3	382.4	490.2	621.6	29.3
Security systems and configuration management	413.5	430.8	450.0	475.1	501.1	524.1	4.9
Subtotal	977.4	1,151.3	1,366.3	1,634.3	1,947.4	2,300.1	18.7
Vulnerability assessment							
Network based	147.7	175.6	206.8	240.9	272.2	304.9	15.6
Host based	198.5	227.3	258.6	292.0	322.4	354.6	12.3
Application	46.8	61.4	78.5	99.3	121.1	145.3	25.4
Subtotal	393.0	464.2	543.9	632.1	715.7	804.8	15.4
Total	1,370.4	1,615.5	1,910.2	2,266.4	2,663.1	3,104.9	17.8

Note: See Table 6 for the key forecast assumptions.

Source: IDC, 2005

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 2006 IDC. Reproduction is forbidden unless authorized. All rights reserved.