

MARKET ANALYSIS

Worldwide Security and Vulnerability Management 2011–2015 Forecast and 2010 Vendor Shares

Charles J. Kolodgy

IN THIS EXCERPT

The content for this excerpt was taken directly from the Worldwide Security and Vulnerability Management 2011–2015 Forecast and 2010 Vendor Shares by Charles Kolodgy (Doc # 231292). All or parts of the following sections are included in this excerpt: IDC Opinion, In This Study, Forecast and Assumptions, Market Context, Situation Overview, Future Outlook, Market Trends and Essential Guidance. Also included are Figure 1 and Tables 1, 2, 4, 5, 6 and 8

IDC OPINION

Recovery from recession and overall economic instability has been taxing on companies of all sizes and locales. However, while economic growth has been slow, and IT spending was primarily flat during 2010, enterprises and organizations continued to deploy technologies to improve their management of security operations. To respond to sophisticated threats and expanding government regulations, organizations turned to security and vulnerability management (SVM) solutions to provide intelligence, process consistency, and awareness to make security more effective, in terms of cost and improved security. 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 grew at a rate of 17.0% in 2010. This was up from the 9.0% in 2009, returning to the same growth rate as 2008. The 2010 results again exceeded the forecast rate. Revenue in the market was \$3.4 billion in 2010 compared with \$2.9 billion in 2009. IDC believes the SVM market will remain on a positive growth trajectory in 2011, with revenue anticipated to be \$3.8 billion, which is a 14.4% increase. By the end of the forecast period (2015), the market should exceed revenue of \$5.7 billion with a climbing annual growth rate, resulting in a compound annual growth rate (CAGR) of 11.3%. Highlights are:

- ☒ 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 that are used to supplement and validate other security defenses. SVM products can be considered the "brains" of an organization's security efforts.
- ☒ The SVM market continues to be extremely diverse with no vendor reaching 9% in market share. Although there have been some high-profile acquisitions within the market, IDC does not envision this market becoming one dominated by a few

players, so IDC would not expect any one company to exceed 13% in market share during this period. The market is too diverse for such a consolidation.

- ☒ SVM products will continue to benefit from increasing threats from organized attackers. SVM solutions help organizations identify weaknesses (vulnerabilities and policies), gain a full picture of what is going on (security intelligence and event management [SIEM] and forensics), and provide visibility of those issues to the executive team.
-

IN THIS STUDY

This IDC study examines the security and vulnerability management market for the 2010–2015 period, with vendor revenue trends and market growth forecasts. Worldwide market sizes and vendor revenue and market shares of the leading vendors are provided for 2010, and a five-year growth forecast for this market is shown for 2011–2015. This study concludes with market trends and IDC guidance for future success.

Security and Vulnerability Management Market Definitions

The security and vulnerability management market encompasses two separate but symbiotic markets — security management and vulnerability assessment. These two markets can stand alone, but they also have considerable overlap in how they are used by enterprises. There are seven subcategories divided between security management and vulnerability assessment. The markets and submarkets are defined as follows:

- ☒ **Vulnerability assessment products.** These are batch-level products that scan servers, workstations, other devices, and applications to uncover security vulnerabilities be they associated with known security holes (vulnerabilities) contained within a vulnerability database, or are configuration settings that can be exploited. These scans provide a view of the threat status of the device or an 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 have credentialed access (using usernames and passwords) into devices or 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.

- **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 2010

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 look for solutions to proactively mitigate risk, create and audit 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 2010 compared with 2009's results. The total market in 2010 was \$3.4 billion. With over 50 named vendors, even following all of the merger and acquisition (M&A) activity, the SVM market is large and competitive. Unlike some other security markets that are dominated by a handful of vendors, no single leading vendor reaches 9% in market share. It takes 14 different vendors to accumulate 50% of the total market. This is down one vendor from what was required in 2009 to reach the same number.

To illustrate the complexity and competitiveness of this market, Table 1 provides a collection of select vendors and their products as they fit into the market subcategories. Please understand this is a representative list and does not include every product a vendor has that falls within the SVM market.

TABLE 1

Representative SVM Vendor Products for Select Vendors

Company	Proactive Endpoint Risk Management	Forensics and Incident Investigation	Policy and Compliance	Security Intelligence and Event Management	Security Device Systems Management	Vulnerability Assessment
EMC		NetWitness Spectrum	Archer eGRC Suite	enVision		

TABLE 1

Representative SVM Vendor Products for Select Vendors

Company	Proactive Endpoint Risk Management	Forensics and Incident Investigation	Policy and Compliance	Security Intelligence and Event Management	Security Device Systems Management	Vulnerability Assessment
Enterasys Networks			NMS Policy Manager	Security Information and Event Manager	NMS Inventory Manager; NMS Console	
GFI				GFI EventsManager		GFI LANguard
Guidance Software	EnCase Cybersecurity	EnCase Forensic	EnCase Enterprise			
HP			Compliance Insight Packages	ArcSight ESM; ArcSight Logger		Fortify Real-Time Analyzer; Fortify Static Code Analyzer
IBM	Tivoli Endpoint Manager for Security and Compliance		Tivoli Security Compliance Manager; Tivoli Security Policy Manager; Guardium Database Activity Monitoring	Tivoli Security Information and Event Manager		Proventia Network Scanner; Rational AppScan; zSecure Audit; Guardium Database Vulnerability Assessment
Imperva			SecureSphere Database Activity Monitoring; File Activity Monitoring			SecureSphere Discovery and Assessment Server
Lumension Security	Lumension Patch and Remediation; Lumension Security Configuration Management		Lumension Risk Manager			Lumension Scan

TABLE 1

Representative SVM Vendor Products for Select Vendors

Company	Proactive Endpoint Risk Management	Forensics and Incident Investigation	Policy and Compliance	Security Intelligence and Event Management	Security Device Systems Management	Vulnerability Assessment
McAfee	McAfee Total Protection for Compliance; McAfee Configuration Control		Policy Auditor; Network User Behavior Analysis; ePolicy Orchestrator	Risk Advisor		Vulnerability Manager; Vulnerability Assessment SaaS
Microsoft	Windows Server Update Services		Systems Center Configuration Manager			Baseline Security Analyzer; SCCM Vulnerability Assessment Configuration Pack
NetIQ	Change Guardian		VigilEnt Policy Center	NetIQ Security Manager		NetIQ Secure Configuration Manager
NIKSUN		NetDetector; NetIntercept		NetOmni		
Q1 Labs (bought by IBM)				QRadar		
Qualys			QualysGuard PC			QualysGuard VM; QualysGuard WebApplication Scanning
Symantec	Critical System Protection; Altiris Client Management Suite		Control Compliance Suite	Security Information Manager; DeepSight Early Warning		Risk Automation Suite
Tripwire	Tripwire Enterprise Remediation Manager		Tripwire Enterprise Policy Manager	Tripwire Log Center		

Source: IDC, 2011

Table 4 displays 2010 worldwide revenue and market shares for vulnerability assessment vendors.

Figure 6 displays 2010 market shares for the top 5 device vulnerability assessment vendors and application vulnerability assessment vendors, respectively.

TABLE 2Worldwide Security and Vulnerability Management Revenue by Vendor,
2010 (\$M)

	2009	2010	2010 Share (%)	2009–2010 Growth (%)
IBM	212.4	286.5	8.5	34.9
HP	219.5	280.1	8.3	27.6
Symantec	195.0	207.2	6.2	6.3
EMC	125.4	135.2	4.0	7.8
Microsoft	90.0	92.0	2.7	2.2
NetIQ (an Attachmate company)	81.8	88.7	2.6	8.4
McAfee	93.2	88.5	2.6	-5.1
Guidance	65.9	80.0	2.4	21.5
Fujitsu	63.9	78.5	2.3	22.9
Lumension	71.4	76.4	2.3	7.0
Q1 Labs (bought by IBM)	48.5	76.1	2.3	56.9
Enterasys	64.4	73.2	2.2	13.6
Tripwire	60.0	66.0	2.0	10.0
Qualys	57.6	65.4	1.9	13.5
Cisco	94.4	61.1	1.8	-35.3
LogLogic	41.0	53.3	1.6	30.0
NIKSUN	39.4	41.8	1.2	6.1
Check Point	32.3	41.2	1.2	27.6
GFI	34.0	37.4	1.1	10.0
Imperva	27.0	35.8	1.1	32.6
LANDesk	23.1	34.6	1.0	49.6
SecureWorks (bought by Dell)	31.8	33.9	1.0	6.6
Trustwave	17.2	33.4	1.0	94.2
Shavlik (bought by VMware)	46.1	32.0	1.0	-30.6
Hitachi	29.0	31.6	0.9	8.9
Application Security	25.4	29.2	0.9	15.0
Cenzic	18.0	28.6	0.8	58.9
CA Technologies	29.4	28.1	0.8	-4.6
Nitro Security (bought by McAfee)	16.8	27.6	0.8	64.3

TABLE 2Worldwide Security and Vulnerability Management Revenue by Vendor,
2010 (\$M)

	2009	2010	2010 Share (%)	2009–2010 Growth (%)
NetWitness (bought by EMC)	19.7	26.2	0.8	33.0
nCircle	21.9	25.8	0.8	17.8
Core Security	20.0	25.2	0.7	26.0
Tenable Network Security	18.0	24.3	0.7	35.0
Novell (bought by Attachmate)	29.9	23.8	0.7	-20.4
Rapid7	11.2	19.0	0.6	69.6
eEye	8.0	18.2	0.5	127.5
Accuvant	13.0	18.0	0.5	38.5
Kaseya	14.0	17.8	0.5	27.1
NEC	13.1	16.8	0.5	28.6
NGS Secure	12.0	16.5	0.5	37.5
Tufin	12.7	16.1	0.5	26.8
LogRhythm	11.0	16.0	0.5	45.5
AccessData	11.0	15.0	0.4	36.4
eIQnetworks Inc.	14.5	15.0	0.4	3.4
Solera Networks	4.0	15.0	0.4	275.0
netForensics	19.5	14.8	0.4	-24.1
WhiteHat	6.1	9.5	0.3	55.7
TriGeo (bought by SolarWinds)	11.0	9.0	0.3	-18.2
SenSage	6.0	8.0	0.2	33.3
CSC	7.0	7.5	0.2	7.1
Secunia	11.9	7.2	0.2	-39.5
MANDIANT	5.0	7.0	0.2	40.0
RedSeal	6.0	7.0	0.2	16.7
Dell	6.4	6.7	0.2	4.7
Intrusion.com	4.9	5.6	0.2	14.3
Entrust Inc.	4.5	5.3	0.2	17.8
Acunetix	4.0	5.0	0.1	25.0
Blue Lance	4.0	5.0	0.1	25.0

TABLE 2Worldwide Security and Vulnerability Management Revenue by Vendor,
2010 (\$M)

	2009	2010	2010 Share (%)	2009–2010 Growth (%)
Subtotal	2,284.2	2,649.7	78.7	16.0
Other	591.6	715.5	21.3	20.9
Total	2,875.8	3,365.2	100.0	17.0

Source: IDC, 2011

TABLE 4

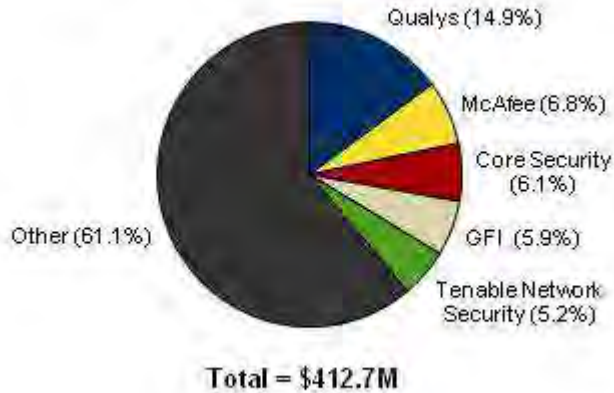
Worldwide Vulnerability Assessment Revenue by Vendor, 2010

	Revenue (\$M)	Share (%)
IBM	86.5	11.4
Qualys	62.8	8.3
HP	55.0	7.2
McAfee	33.1	4.4
Cenzic	28.6	3.8
Symantec	26.9	3.5
Core Security	25.2	3.3
GFI	24.3	3.2
nCircle	22.4	2.9
Tenable Network Security	21.4	2.8
Microsoft	20.3	2.7
Rapid7	19.0	2.5
Lumension	18.7	2.5
eEye	15.0	2.0
Imperva	14.4	1.9
NGS Secure	13.5	1.8
Application Security	12.2	1.6
WhiteHat	9.5	1.2
Trustwave	9.1	1.2
CSC	7.5	1.0
Secunia	7.2	0.9
Shavlik (bought by VMware)	6.0	0.8
Acunetix	5.0	0.7
NetIQ (an Attachmate company)	4.2	0.6
CA Technologies	4.1	0.5
Blue Lance	0.5	0.1
Subtotal	552.4	72.6
Other	208.2	27.4
Total	760.6	100.0

Source: IDC, 2011

FIGURE 6

Worldwide Device Vulnerability Assessment Revenue Share by Vendor, 2010



Source: IDC, 2011

FUTURE OUTLOOK

Forecast and Assumptions

Worldwide revenue for the SVM market reached \$3.4 billion in 2010, representing 17.0% growth over 2009. IDC currently forecasts that the SVM market will increase at an 11.3% CAGR and reach \$5.7 billion in 2015, as shown in Table 5.

TABLE 5

Worldwide Security and Vulnerability Management Revenue by Segment, 2009–2015 (\$M)

	2009	2010	2011	2012	2013	2014	2015	2010–2015 CAGR (%)
Security management								
Security intelligence and event management	826.2	1,056.8	1,281.1	1,515.4	1,757.5	1,971.7	2,153.0	15.3
Proactive endpoint risk management	384.5	415.1	449.5	484.1	517.6	548.5	576.4	6.8
Forensics and incident investigation	142.0	188.7	234.1	276.6	322.2	366.5	410.5	16.8

TABLE 5

Worldwide Security and Vulnerability Management Revenue by Segment,
2009–2015 (\$M)

	2009	2010	2011	2012	2013	2014	2015	2010–2015 CAGR (%)
Policy and compliance	536.1	688.5	802.9	906.6	1,008.6	1,098.4	1,179.8	11.4
Security device systems management	295.1	255.6	238.1	225.1	217.1	214.9	214.9	-3.4
Subtotal	2,183.9	2,604.7	3,005.8	3,407.7	3,822.9	4,199.9	4,534.5	11.7
Vulnerability assessment								
Device	398.3	412.7	433.3	460.2	491.0	525.9	554.8	6.1
Application	293.6	347.9	410.6	472.9	533.7	594.0	655.3	13.5
Subtotal	691.9	760.6	843.9	933.1	1,024.8	1,119.9	1,210.2	9.7
Total	2,875.8	3,365.3	3,849.7	4,340.9	4,847.7	5,319.8	5,744.7	11.3

Note: See Table 6 for top 3 assumptions and Table 7 for key forecast assumptions.

Source: IDC, 2011

Tables 6 and 7 show the top 3 assumptions and the key forecast assumptions, respectively, which provide the basis for the worldwide security and vulnerability market forecast for 2011–2015.

Market Context

Table 8 and Figure 8 show a comparison of IDC's current forecast with the forecast published in *Worldwide Security and Vulnerability Management 2010–2014 Forecast and 2009 Vendor Shares* (IDC #225988, December 2010). SVM has withstood the economic downturn better than expected, so the forecast is slightly higher than that published previously. Growth for submarkets that can demonstrate definitive value to the organization and provides regulatory compliance will be strong. Products that reduce costs through automation will also see strong investment.

TABLE 8

Worldwide Security and Vulnerability Management Revenue, 2006–2015:
Comparison of December 2010 and November 2011 Forecasts (\$M)

	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
November 2011 forecast	1,885.9	2,251.6	2,634.5	2,875.8	3,365.3	3,849.7	4,340.9	4,847.7	5,319.8	5,744.7
Growth (%)	NA	19.4	17.0	9.2	17.0	14.4	12.8	11.7	9.7	8.0
December 2010 forecast	1,885.9	2,251.6	2,634.5	2,875.8	3,158.9	3,553.6	4,020.7	4,554.2	5,168.5	NA
Growth (%)	NA	19.4	17.0	9.2	9.8	12.5	13.1	13.3	13.5	NA

Notes:

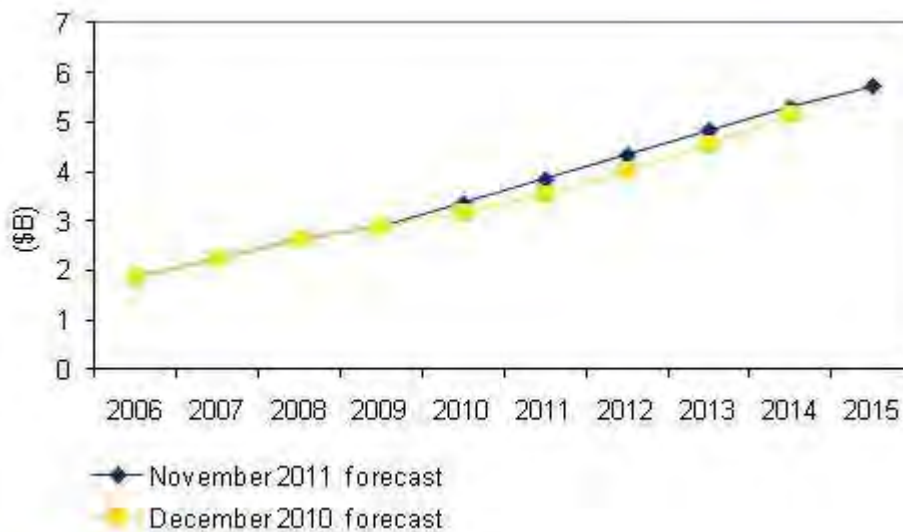
See *Worldwide Security and Vulnerability Management 2010–2014 Forecast and 2009 Vendor Shares* (IDC #225988, December 2010) for prior forecast.

Historical market values presented here are as published in prior IDC documents based on the market taxonomies and current U.S. dollar exchange rates existing at the time the data was originally published. For more details, see the Methodology in the Learn More section.

Source: IDC, 2011

FIGURE 8

Worldwide Security and Vulnerability Management Revenue,
2006–2015: Comparison of December 2010 and November 2011 Forecasts



Source: IDC, 2011

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. 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.
- ☒ **Cloud.** Cloud infrastructures are growing in popularity, but one of the things holding more deployment is security concerns. Organizations are concerned about the security of the devices that their material will be processed on and stored in. To deal with these fears, cloud providers are beginning to work with SVM vendors to allow customers to assess the security posture of the cloud infrastructure they will be utilizing. For ease of use, the cloud infrastructure vendors are turning to cloud security providers so that there is consistency regarding the scans, assessments, and reporting. In this way, they are using the cloud to protect the cloud.
- ☒ **Application and software security vulnerability assessment.** As security becomes more important at the application level, organizations are demanding software that is less vulnerable to attack; thus, application-level security needs to be a fundamental component for software development and quality assurance. There are application scanning tools that look at operational products such as databases and Web servers, and in the future, there will be code scanning of individual mobile apps. The market has been moving from individual static and dynamic testing products to hybrid solutions that can offer both capabilities. IDC refers to this as "measuring twice and cutting once." Products within this market will continue to evolve to the point where they will be used throughout the software development life cycle so that vulnerabilities can be eliminated before a program becomes operational.
- ☒ **Situational awareness and analytics.** Organizations are looking for 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. There has been a growing movement toward using SIEM technology to provide organizations with

"situational awareness," that is to bring information together in order to understand how information, events, and your own actions will impact your goals and objectives. Many SIEM vendors, such as eIQnetworks, NitroSecurity, and EMC, state how their products put security events into context, thus being able to better find real problems. Both IBM and HP are pushing analytics to take security events and start to predict what will be coming next. Both situational awareness and analytics are designed to facilitate better decision making by security professionals and executives.

☒ **Acquisitions.** In most markets, smaller vendors with interesting technology will be purchased by larger players. This has been happening with regularity over the past few years within the SVM market. Recent acquisitions include EMC's purchases of Archer and NetWitness, IBM's purchases of BigFix and Q1 Labs, HP's purchases of Fortify and ArcSight, Dell's purchases of KACE and SecureWorks, Attachmate's deal for Novell, and Trustwave's purchase of Intellitactics. Most of the purchases are to provide the acquiring vendor products that they did not have. However, part of the reason for consolidation is that customers are reducing the number of vendors they purchase from and are looking for solutions that work together. Even with this consolidation, IDC does not expect the market to have just a few dominant players. The market is too diverse, has too many needs, and is always evolving along with the threat landscape. Over the years the number of vendors will shrink and a few vendors will gain larger portions of the market, but in the short term this will not drastically change the diversity within the market. It will take time for this consolidation.

ESSENTIAL GUIDANCE

Security is a value-add, 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 demand security management that is well integrated with the IT infrastructure, effective, usable, 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 vendors should develop tools that bring together event records, efficiently prioritize incidents, separate real security violations from false alarms, and aggregate security events from different locations, devices, and manufacturers. Moreover, vulnerabilities must be viewed as part of an overall security management infrastructure that takes into account security policy, compliance, and risk management. SVM solutions should tell the enterprise why the vulnerability is a

concern, its risk ranking, and how to remediate. SVM offerings must be able to provide a more aggressive, positive security model and not just respond to events in a chaotic manner. In many cases, SVM solutions, especially in the proactive endpoint risk management category, are moving to the point where the product will automatically remediate any security problems that should develop. Over time, SVM vendors need to combine their SVM agent with their own endpoint security solutions to provide all endpoint security capabilities, or the SVM vendor will need to partner with an endpoint security vendor that does not have SVM capabilities itself.

For the SVM market to maintain its strong growth rates, vendors must continue to make security smart. This includes providing proper policy management to automatically enforce the security policy. IDC sees the PERM market as a market that can bring considerable positive security value to enterprises. Another area where SVM makes security smart is in the SIEM market, where an ever-growing set of security data has to be processed to find the critical information among a huge set of data and to put that intelligence into its proper context. The SIEM market is important for providing audit information and ensuring proper utilization of security technologies. 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.

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 2011 IDC. Reproduction is forbidden unless authorized. All rights reserved.