

EXCERPT

MARKET ANALYSIS

Worldwide Security and Vulnerability Management 2013–2017 Forecast and 2012 Vendor Shares

Charles J. Kolodgy

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC Market Analysis: Worldwide Security and Vulnerability Management 2013-2017 Forecast and 2012 Vendor Shares by Charles J. Kolodgy (Doc # 242465). All or parts of the following sections are included in this excerpt: IDC Opinion, In This Study, Situation Overview, Future Outlook, and Essential Guidance. Also included is Table 1, Table 2, Table 4, Table 5, Table 8 and Figure 6 and Figure 8.

IDC OPINION

Economic growth and uncertainty have made for a difficult business environment for companies of all sizes and locales. What hasn't been slowing is the cyberthreats companies have been facing every day. As a result, the security and vulnerability management (SVM) market hasn't been experiencing a downturn. Enterprises and organizations continued to deploy technologies to improve their management of security operations. In response to sophisticated threats and privacy requirements, organizations turn to security and vulnerability management solutions to provide threat intelligence, security policy consistency, and risk management. 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 9.4% in 2012. This was down from a strong 13.9% rate from 2011. Revenue in the SVM market was \$4.2 billion in 2012 compared with \$3.8 billion in 2011. IDC believes the SVM market will remain on a positive growth trajectory in 2013, with revenue anticipated to be \$4.6 billion, which is a 9.8% increase. By the end of the forecast period (2017), the market should exceed revenue of \$6.4 billion with a steadily strong annual growth rate, resulting in a compound annual growth rate (CAGR) of 9.1%. Highlights are:

- ☒ The public disclosure of security breaches and data loss incidents results 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 is diverse. The top 10 vendors only command 44.5% of the overall market, with still only one vendor with a market share greater than 10%. Mergers and acquisitions (M&As) are slowly resulting in consolidation of the market; however, with multiple components, it will be difficult for a few vendors to dominate the market.
 - ☒ 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 2012–2017 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 2012, and a five-year growth forecast for this market is shown for 2013–2017. This study concludes with market trends and IDC's 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 have considerable overlap. There are seven subcategories divided between security management and vulnerability assessment. The markets and submarkets are defined as follows:

- ☒ **Security management products.** Security management products consist of products 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. The security management market is divided into the following components:
 - ☐ **Proactive endpoint risk management (PERM) solutions.** PERM solutions automate or semiautomate the *enforcement* of security policy and configuration management on endpoints. Proactive enforcement includes the setting, monitoring, and updating of system configuration settings and the installation of security patches. PERM can be done with or without agents. It also can internally discover systems to find network devices, identify system configuration, and determine patch status. A key feature of this category is the ability to *enforce* endpoint security policies, which include security configurations, patch levels, device controls, and application usage.

- ❑ **Forensics and incident investigation solutions.** 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. Products in this category also include those that can do historical recreations to find how an event occurred. The submarket is expanding to include malware forensics tools, used by researchers to deconstruct targeted and stealthy malware. Finally, this category also includes products that can be used by law enforcement to gather evidence associated with criminal activity.
- ❑ **Policy and compliance solutions.** Policy and compliance solutions allow organizations to create, measure, and report on security policy and regulatory compliance. This information is used to establish corporatwide policies, distribute them, and provide audit information for compliance measurement. Policy and compliance products do not directly enforce the security policies; that function is handled by PERM products. Products in this category are used to *establish* and *report* on enterprise security policy.
- ❑ **Security intelligence and event management (SIEM) solutions.** SIEM solutions include products 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. Many products in this category also consolidate and store the log data, which is processed by the SIEM. This market also includes activities that collect and disseminate threat intelligence, provide early warning threat services, and can provide information on countermeasures. Data from SIEM is provided to policy and compliance solutions for consistent reporting.
- ❑ **Security device systems management (SDSM) products.** SDSM products are primarily systems management products that monitor and report on the status of perimeter security products (e.g., firewalls, intrusion detection and prevention, and Web security). It can be used to manage device policy and monitor the health of security systems.
- ☒ **Vulnerability assessment (VA) products.** These are batch-level products that scan servers, workstations, other devices, and applications to uncover security vulnerabilities in the form of known security holes (vulnerabilities) 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. Specifications for application scanners include databases and Web software. The application scanner market could be segmented into products that look at deployed applications (dynamic testing) and products that review source code (static testing).

SITUATION OVERVIEW

Security and Vulnerability Management Market in 2012

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 9.4% growth rate in 2012 compared with 2011's results. The total market in 2012 was \$4.2 billion. With 40 named vendors, even following all of the merger and acquisition activity, the SVM market is large and competitive. Unlike some other security markets that are dominated by a handful of vendors, only one vendor exceeds 10% in market share. It takes 13 different vendors to accumulate 50% of the total market. This is up 1 vendor from what was required in 2011 to reach the same level.

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		RSA Security Analytics	RSA Archer eGRC Suite	RSA Security Analytics		
Enterasys Networks Inc.			NetSight	Security Information and Event Manager	Data Center Manager	
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 Monitor	QRadar		Rational AppScan; zSecure Audit; Guardium Database Vulnerability Assessment
Lumension Security Inc.	Lumension Endpoint Management and Security Suite		Lumension Compliance and IT Risk Management			Lumension Scan
McAfee	McAfee Total Protection for Compliance		Policy Auditor; ePolicy Orchestrator	McAfee Enterprise Security Manager; Risk Advisor		Vulnerability Manager; Vulnerability Assessment SaaS
Microsoft	Windows Server Update Services		System Center 2012 Configuration Manager			Baseline Security Analyzer; SCCM Vulnerability Assessment Configuration Pack
NetIQ	Change Guardian		NetIQ Secure Configuration Manager	NetIQ Security Manager; Sentinel		

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
Qualys			QualysGuard Policy Compliance			QualysGuard VM; QualysGuard Web Application Scanning
Rapid7						Nexpose; Metasploit
Symantec			Symantec Protection Center; Control Compliance Suite	Security Information Manager; DeepSight Early Warning		Risk Automation Suite
Tripwire Inc.	Tripwire Enterprise Remediation Manager		Tripwire Enterprise's Policy Manager	Tripwire Log Center		

Source: IDC, 2013

Table 2 provides worldwide SVM revenue and market shares

Table 4 displays 2012 worldwide revenue and market shares for the leading vulnerability assessment vendors.

Figure 6 displays 2012 market shares for the top 5 device vulnerability assessment vendors.

TABLE 2

Worldwide Security and Vulnerability Management Revenue by Vendor, 2011 and 2012 (\$M)

	2011	2012	2012 Share (%)	2011–2012 Growth (%)
IBM	424.4	477.8	11.4	12.6
HP	360.6	393.3	9.4	9.1
EMC	175.7	216.6	5.2	23.3
Symantec	122.3	129.4	3.1	5.8
McAfee (an Intel company)	82.6	127.0	3.0	53.8
NetIQ (an Attachmate company)	158.4	120.6	2.9	-23.9
Guidance Software	93.3	112.9	2.7	21.0
Microsoft	95.8	97.4	2.3	1.7
Tripwire Inc.	83.1	97.2	2.3	17.0
Qualys	76.0	91.4	2.2	20.3
Subtotal	1672.2	1863.6	44.5	11.4
Other	2160.6	2327.8	55.5	7.7
Total	3,832.6	4,191.5	100.0	9.4

Source: IDC, 2013

TABLE 4

Worldwide Vulnerability Assessment Revenue by Vendor, 2012

	Revenue (\$M)	Share (%)
IBM	102.1	11.1
Qualys	86.4	9.4
HP	60.4	6.6
McAfee (an Intel company)	55.1	6.0

TABLE 4

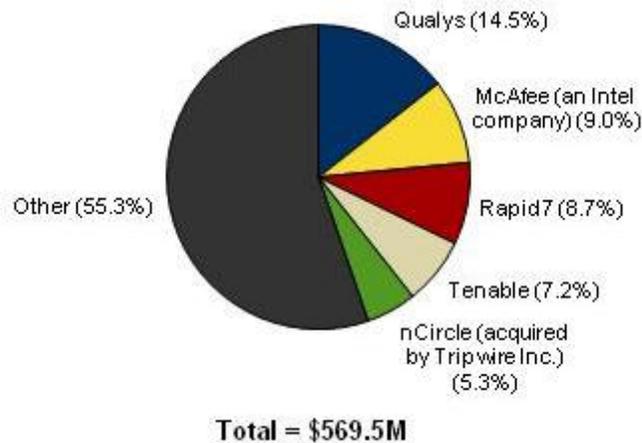
Worldwide Vulnerability Assessment Revenue by Vendor, 2012

	Revenue (\$M)	Share (%)
Rapid7	49.7	5.4
Subtotal	353.7	38.5
Other	562	61.5
Total	915.7	100.0

Source: IDC, 2013

FIGURE 6

Worldwide Device Vulnerability Assessment Revenue Share by Vendor, 2012



Source: IDC, 2013

FUTURE OUTLOOK**Forecast and Assumptions**

Worldwide revenue for the SVM market reached \$4.2 billion in 2012, representing 9.4% growth over 2011. IDC currently forecasts that the SVM market will increase at a 9.1% CAGR and reach \$6.5 billion in 2017, as shown in Table 5.

TABLE 5**Worldwide Security and Vulnerability Management Revenue by Segment,
2009–2017 (\$M)**

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2012–2017 CAGR (%)
Security management										
Security intelligence and event management	826.5	1,052.3	1,308.3	1,434.1	1,594.1	1,741.7	1,896.0	2,054.9	2,217.2	9.1
Proactive endpoint risk management	378.5	425.1	464.6	482.4	505.6	533.3	565.4	594.9	623.5	5.3
Forensics and incident investigation	136.6	188.7	221.0	305.0	368.7	436.4	507.5	581.6	657.7	16.6
Policy and compliance	587.6	694.2	800.5	875.3	961.9	1,049.1	1,141.8	1,238.4	1,336.4	8.8
Security device systems management	273.7	254.5	201.4	179.0	165.6	155.6	150.5	146.8	145.0	-4.1
Subtotal	2,202.9	2,614.7	2,995.9	3,275.9	3,595.8	3,916.0	4,261.2	4,616.5	4,979.9	8.7
Vulnerability assessment										
Device	428.3	474.7	522.0	569.5	617.4	666.2	717.7	771.2	825.6	7.7
Application	244.6	275.9	314.7	346.2	390.3	448.3	516.6	591.2	667.9	14.0
Subtotal	672.9	750.6	836.7	915.7	1,007.7	1,114.5	1,234.3	1,362.5	1,493.5	10.3
Total	2,875.8	3,365.3	3,832.6	4,191.5	4,603.5	5,030.6	5,495.5	5,979.0	6,473.4	9.1

Source: IDC, 2013

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 2012–2016 Forecast and 2011 Vendor Shares* (IDC #236065, July 2012). SVM continues to have strong growth, so the overall forecast is very similar to that published previously.

TABLE 8

Worldwide Security and Vulnerability Management Revenue, 2008–2017:
Comparison of July 2012 and August 2013 Forecasts (\$M)

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
August 2013 forecast	2,634.5	2,875.8	3,365.3	3,832.6	4,191.5	4,603.5	5,030.6	5,495.5	5,979.0	6,473.4
Growth (%)	NA	9.2	17.0	13.9	9.4	9.8	9.3	9.2	8.8	8.3
July 2012 forecast	2,634.5	2,875.8	3,365.3	3,832.6	4,295.6	4,796.5	5,314.4	5,817.4	6,221.7	NA
Growth (%)	NA	9.2	17.0	13.9	12.1	11.7	10.8	9.5	6.9	NA

Notes:

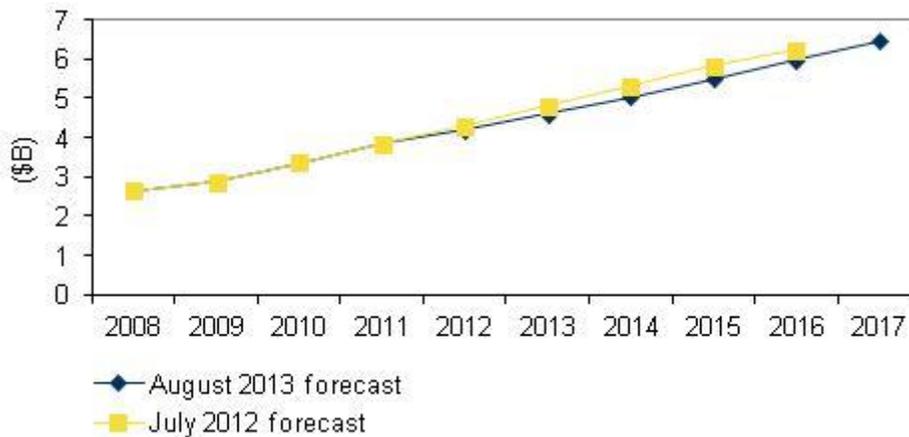
See *Worldwide Security and Vulnerability Management 2012–2016 Forecast and 2011 Vendor Shares* (IDC #236065, July 2012) for prior forecast.

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, 2013

FIGURE 8

Worldwide Security and Vulnerability Management Revenue, 2008–2017: Comparison of July 2012 and August 2013 Forecasts



Source: IDC, 2013

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:

- ☒ **Big Data analytics.** Organizations have a lot of data (various logs and other reporting data) associated with network devices, applications, and user activities. They have realized that to optimize their defenses, they need to effectively be able to not just collect all of this metadata, but also they must be able to process it. Combining Big Data with threat intelligence information, organizations can start using "situational awareness" to see the big picture of how their IT assets are working and how well they stack up to existing threats. SVM technologies provide the knowledge and intelligence to improve the overall security posture. SIEM technology does the heavy lifting of analyzing the data, but many of the other SVM technologies have a role to play. Vulnerability assessment data allows an organization to learn where risk resides, forensics provides historical data that can show how an attack proceeded, and policy and compliance provides data on devices but also is used to report many of the findings. By using advanced analytics to bring together threat intelligence, vulnerability information, security events, and protection profiles, it might be possible to predict what will be coming next. Both situational awareness and analytics are designed to facilitate better decision making by security professionals and executives and to help discover stealthy attacks.
- ☒ **Cloud.** Cloud infrastructures are growing in popularity, but organizations are concerned about the security of the devices that their data will be processed on and stored in. To deal with these fears, cloud providers are partnering 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.
- ☒ **Mobile devices.** Growth in corporate usage of smartphones and tablets, both enterprise owned and employee owned (bring your own device), is changing the risk posture of many organizations. The proliferation of these devices is requiring organizations to revamp some of their security policies, to improve their vulnerability management, and to bring security management into the mobile device management (MDM) systems. IDC expects that many MDM systems deployed by enterprises will come from security vendors that will be able to enforce unique security policies associated with mobile devices.
- ☒ **Application and software security vulnerability assessment.** As security becomes more important at the application level, especially with the proliferation of mobile applications, application-level security is becoming 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.

- ☒ **Multiple delivery systems.** Vendors are providing SVM products using various delivery methods, which include software, hardware, software as a service (SaaS), and virtualized appliances. 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 submarket, and there is no reason SaaS can't be used in the policy and compliance submarket. 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 expects that SVM products will continue to be delivered in a diverse manner.

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 and that is 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. 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. One 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 — whether it's device or application based, white box or black box, or 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.

LEARN MORE

Related Research

- ☒ *Worldwide Web Security 2013–2017 Forecast and 2012 Vendor Shares* (IDC #242033, July 2013)
- ☒ *Worldwide Network Security Forecast 2013–2017 and 2012 Vendor Shares* (IDC #241926, July 2013)
- ☒ *U.S. Mobile Security Survey, 2013* (IDC #240598, April 2013)
- ☒ *Worldwide Mobile Enterprise Security Software 2013–2017 Forecast and Analysis* (IDC #240014, March 2013)
- ☒ *Worldwide Security Software as a Service 2012–2016 Forecast: Delivering Security Through the Cloud* (IDC #238553, December 2012)
- ☒ *Worldwide IT Security Products 2012–2016 Forecast and 2011 Vendor Shares: Comprehensive Security Product Review* (IDC #237934, November 2012)
- ☒ *Worldwide Security and Vulnerability Management 2012–2016 Forecast and 2011 Vendor Shares* (IDC #236065, July 2012)

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 2013 IDC. Reproduction is forbidden unless authorized. All rights reserved.