MARKET SHARE

Worldwide Security and Vulnerability Management Market Shares, 2014: The Need for Improved Incident Response Driving Higher Growth Across the Market

Robert Ayoub
Elizabeth Corr
Christian A. Christiansen
Robert Westervelt

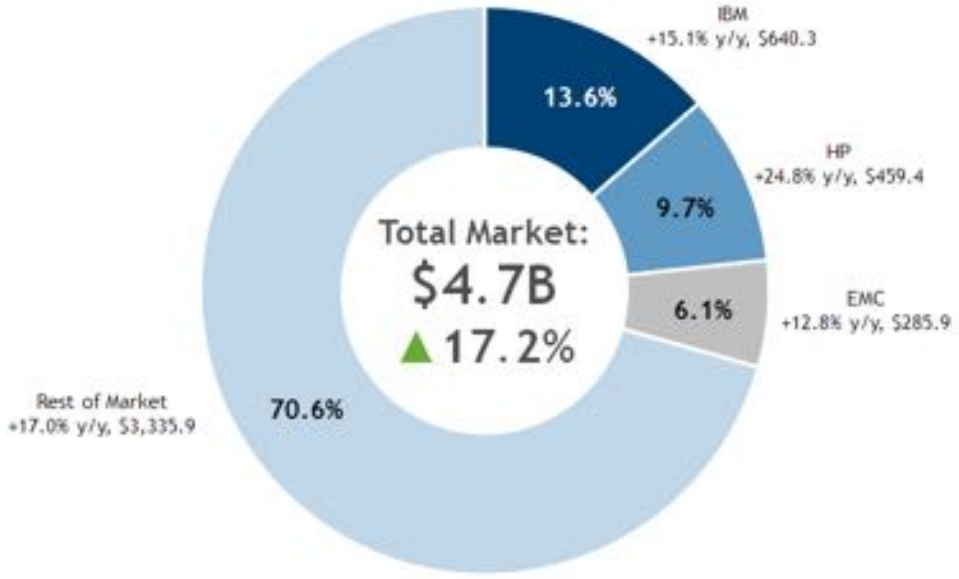
IN THIS EXCERPT

The content for this excerpt was taken directly from Worldwide Security and Vulnerability Management Market Shares, 2014: The Need for Improved Incident Response Driving Higher Growth Across the Market (Doc# 259864). All or parts of the following sections are included in this excerpt: Executive Summary, Advice for Technology Suppliers, Market Share, Who Shaped the Year, Market Context, Methodology, Market Definition, and Related Research sections that relate specifically to Qualys, and any figures and or tables relevant to Qualys.

IDC MARKET SHARE FIGURE

FIGURE 1

Worldwide Security and Vulnerability Management 2014 Share Snapshot



Note: 2014 Share (%), Growth (%), and Revenue ($M)

Source: IDC, 2015

November 2015, IDC #259864e

EXECUTIVE SUMMARY

Companies understand that their systems, storage operations, network connectivity, endpoints, and applications 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 (SVM) is very important to meeting risk management goals because it provides policy and compliance context, vulnerability information, 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 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 and its risk ranking as well as 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.

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 security information and event management (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.

This IDC study examines the market share of security and vulnerability management vendors in 2014 as well as the market forces that influenced their performances and the adoption of security and vulnerability management products.

"The incessant drumbeat of data breaches is driving a need for greater accountability among enterprises," says Rob Ayoub, research director, Security Products and Solutions at IDC. "Organizations need smarter tools to allow for the prevention, discovery, and remediation of attacks. As vendors have significantly improved security and vulnerability management products over the past few years, these tools are becoming an invaluable component in prioritization of threats and discovery of attacks."

MARKET SHARE

Table 1 provides worldwide SVM revenue and market shares.

TABLE 1

Worldwide Security and Vulnerability Management Revenue by Vendor, 2013 and 2014 ($M)

	2013	2014	2013 Share (%)	2014 Share (%)	2013–2014 Growth (%)
IBM	556.3	640.3	13.8	13.6	15.1
HP	368.0	459.4	9.1	9.7	24.8
EMC	253.5	285.9	6.3	6.1	12.8
Tripwire	150.0	166.9	3.7	3.5	11.3
McAfee, an Intel company	130.6	159.5	3.2	3.4	22.1
Qualys	102.6	124.6	2.5	2.6	21.5
Symantec	116.8	109.3	2.9	2.3	-6.4
Splunk	66.2	107.1	1.6	2.3	61.8
Trustwave	44.5	101.3	1.1	2.1	127.7
Good Technology	81.0	99.7	2.0	2.1	23.0
Subtotal	1,869.5	2,254.0	46.2	47.7	20.6
Other	2,159.4	2,467.5	53.8	52.3	14.3
Total	4,028.9	4,721.5	100.0	100.0	17.2

Source: IDC, 2015

Table 3 displays worldwide revenue and market shares for the leading vulnerability assessment vendors.

TABLE 3

Worldwide Vulnerability Assessment Revenue by Vendor, 2013 and 2014 ($M)

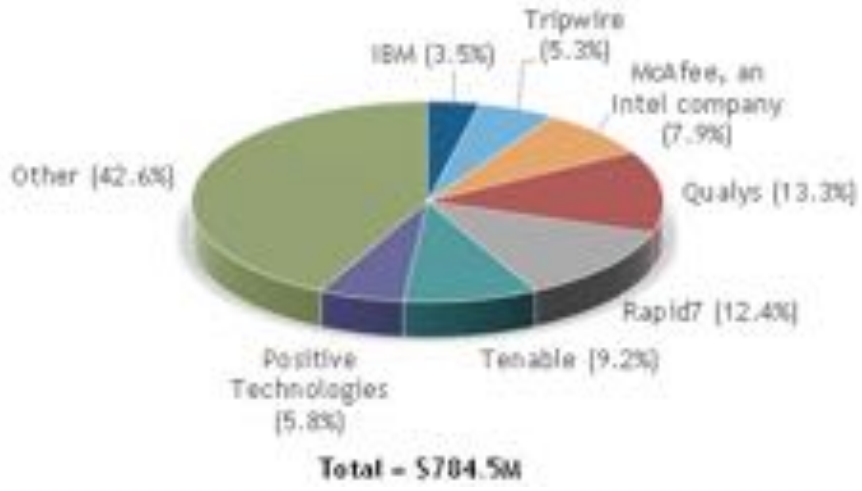
	2013	2014	2013 Share (%)	2014 Share (%)	2013–2014 Growth (%)
IBM	162.8	169.0	16.0	12.4	3.8
HP	94.2	141.7	9.3	10.4	50.4
Qualys	92.2	110.7	9.1	8.1	20.1
Rapid7	68.6	97.1	6.7	7.1	41.5
Tenable	49.4	71.8	4.9	5.2	45.3
Intel	59.3	68.2	5.8	5.0	15.0
Veracode	41.0	63.0	4.0	4.6	53.7
Trustwave	8.0	55.5	0.8	4.1	593.8
Positive Technologies	34.3	45.6	3.4	3.3	32.9
Tripwire	39.0	45.2	3.8	3.3	15.9
Subtotal	648.8	867.8	63.7	63.4	33.8
Other	369.2	500.6	36.3	36.6	35.6
Total	1,018.0	1,368.4	100.0	100.0	34.4

Source: IDC, 2015

Figure 1 illustrates the market share for the Worldwide Device Vulnerability Assessment submarket.

FIGURE 1

Worldwide Device Vulnerability Assessment Revenue Share by Vendor, 2014



Source: IDC, 2015

WHO SHAPED THE YEAR

EMC (RSA)

2014 saw the completion of RSA's pivot away from Envision toward the integrated security analytics platform. This new offering is built around the NetWitness acquisition and other components (ECAT) that are intended to bridge the gap between traditional SIEM and forensics and incident response. RSA has seen strong traction with positioning security analytics as a core security operations center (SOC) component, and IDC expects RSA to continue to have success with this offering.

IBM

IBM continues to have success with its strategy of positioning QRadar as a core component of its security offering. QRadar offers strong integration with IBM's other products (notably IPS), and customers are leveraging the integration to build smarter SOCs. IBM is also moving into the FII space with the release of QRadar's Incident Response module.

Qualys

Qualys, which has arguably been the pioneer in SaaS security software delivery, introduced continuous monitoring to its Qualys Cloud Platform in 2014. The move extends the company's specialization in vulnerability management to one that can provide cloud-based monitoring and threat detection over perimeter devices. In addition to identifying vulnerabilities and obtaining the available patches for applications running on hosts, initial functionality of continuous monitoring feature includes the ability to identify endpoint devices exposed to the Internet, track SSL certificates, detect unusual open ports and protocols being used, and spot the installation or removal of software. The move paves the way for Qualys to use endpoint agents more broadly in the future.

Rapid7

Rapid7 continued to drive toward tighter integration of its product suites in 2014. By combining traditional vulnerability management with incident tracking and security control testing, Rapid7 allows organizations a holistic view of their security posture. Rapid7 appears to target the c-suite with more focus on controls and overall risk management.

Splunk

Splunk has quickly gained traction in the SIEM market and is challenging the traditional leaders. In 2014, Splunk continued to develop partnerships with security device manufacturers in order to ensure easier integration of those products into Splunk. The flexibility of the product to support traditional IT operation in addition to security coupled with a focus on security-specific features will allow Splunk to continue to gain market share in the crowded SIEM space.

Tripwire

In late 2014, Belden announced its intentions to acquire Tripwire. This move brought a lot of questions around the integration of a technology company into a non-security business, along with concerns about the brand and future direction of Tripwire. While too early to see the impact of the acquisition, Belden does bring with it a vast set of new opportunities for Tripwire.

MARKET CONTEXT

The worldwide SVM market saw a significant uplift in 2014 as a result of high-profile data breaches in the retail and healthcare industries. Many organizations are finding that as they add more solutions to detect targeted and advanced threats, the ability to prioritize the most critical threats is getting lost in the noise of alerts.

Buyers of SVM products are also growing more concerned about the risks posed by a growing number of Internet-enabled devices attempting to connect to the corporate network. IDC expects the worldwide market for IoT solutions to grow at a 20% CAGR from $1.9 trillion in 2013 to $7.1 trillion in 2020. Network security vendors may be in a position to address many of the initial security requirements around access control, device inspection, and monitoring. Over time, security requirements will likely revolve around data protection and access to the back-end systems, collecting sensor-based information.

And increased interest in forensics and incident response is driving renewed interest in SIEM and FII products as enterprises are under increased pressure not just to report breaches but to identify how a breach occurred and exactly what data was leaked as a result. Cyberinsurance in particular will continue to drive this requirement forward.

Application security is also an area that is getting increased interest. As organizations look to continuously improve security, the need to tightly integrate the development process into the overall security life cycle is critical.

Significant Market Developments

The adoption of Splunk as part of analyzing and visualizing security threats is having an impact on the security information event management market. IDC has identified a broad number of large enterprises using Splunk Enterprise alongside existing SIEM investments and anticipates a long-term shift of

security resources away from legacy SIEM platforms to Splunk and other security analytics solutions. Big data projects, which are initially supporting business intelligence efforts, may also transition to increasingly provide security visibility and threat detection support.

FireEye's $1 billion acquisition of Mandiant shifted attention toward the opportunities around professional services. Attention is specifically being drawn to digital forensics and data breach support services. Managed security services providers, security consultancies, and resellers with strong security practices are beginning to play a role in this area, but security vendors are also bolstering their own incident response services. Cisco Systems acquired security advisory firm Neohapsis.

Manufacturers of networking appliances and gear were forced to respond to several high-profile open source vulnerabilities in 2014. Heartbleed, Poodle, and Shellshock highlighted the impact of widespread vulnerabilities on corporate networking infrastructure, including network security products. Attention was drawn to how well these products are being maintained as well as the strength of vulnerability and configuration management initiatives.

A record amount of venture capital (VC) funding, an estimated $2 billion or more in 2014, has caused the number of security start-ups to skyrocket. The rapid pace of innovative threat intelligence, analytics, and automated incident response solutions has forced security vendors in the SVM market to consider ways to adjust their portfolio to fulfill existing customer requirements and remain competitive against nimble start-ups.

METHODOLOGY

The purpose of this section is to provide an overview of the methodology employed by IDC's software analysts for collecting, analyzing, and reporting revenue data for the categories defined by the software taxonomy.

IDC's industry analysts have been measuring and forecasting IT markets for more than 40 years. IDC's software industry analysts have been delivering analysis and prognostications for commercial software markets for more than 25 years.

The market forecast and analysis methodology incorporates information from five different but interrelated sources, as follows:

- **Reported and observed trends and financial activity.** This includes reported revenue data for public companies.
- **IDC's software vendor interviews and surveys.** IDC interviews and/or surveys significant market participants to determine product revenue, revenue demographics, pricing, and other relevant information.
- **Product briefings, press releases, and other publicly available information.** IDC's software analysts around the world meet with hundreds of software vendors each year. These briefings provide an opportunity to review current and future business and product strategies, revenue, shipments, customer bases, target markets, and other key product and competitive information.
- **Vendor financial statements and related filings.** Although many software vendors are privately held and choose to limit financial disclosures, information from publicly held companies provides a significant benchmark for assessing informal market estimates from private companies. IDC also builds detailed information related to private companies through in-depth

analyst relationships and maintains an extensive library of financial and corporate information focused on the IT industry. We further maintain detailed revenue by product area model on more than 1,000 worldwide vendors.

- **IDC demand-side research.** This includes interviews with business users of software solutions annually and provides a fifth perspective for assessing competitive performance and market dynamics. Direct conversations with technology buyers provide an invaluable complement to the broader survey-based results.

Ultimately, the data presented in IDC's software studies and pivot tables represents our best estimates based on the previously mentioned data sources as well as reported and observed activity by vendors and further modeling of data that we believe to be true to fill in any information gaps.

Note: All numbers in this document may not be exact due to rounding.

Company Revenue Modeling

- Public company revenue models tie to SEC-reported revenue or other legal public agencies outside the United States (at least at the total company level and often at more granular levels when available). Note, however, that companies may report revenue that is allocated differently than the categorization employed in IDC's software revenue models. For example, portions of "services" or "maintenance" revenue reported by companies may be included as commercial software revenue by IDC's definitions.
- Further segmentations such as geographic region and operating environment distribution percentages are generally obtained from companies at a high level (e.g., the primary market level) and are prorated to individual markets. However, for large companies that have wide variations in geographic and/or operating environment allocations across different markets, these allocations are maintained at the secondary or functional market level whenever that level of detail can be obtained.

Revenue Recognition

Software companies and other companies with software revenue vary in the manner in which they recognize revenue from commercial software sales for reporting purposes, although U.S. public companies are constrained by U.S. accounting practice standards. This is important because IDC's revenue information for companies and for software markets is based on recognized revenue as defined in U.S. practice rather than on bookings, which is another measure. (In the case of private companies, IDC assumes they are using standards that are similar to public companies for their internal accounting.)

For accounting purposes, what matters is revenue, and this is what IDC uses as its metric for the software industry. One reason is that there is a reasonably consistent set of methodologies for determining what is revenue and what is not. These methodologies hinge on the issue of how bookings become "recognized" as revenue. In general, IDC bases its reporting of, and forecasts for, the software market based on revenue as defined by GAAP (to the extent that this is possible for non-U.S. companies).

The first requirement for the recognition of revenue for accounting purposes is whether the actual payment has been received (either directly from the customer or from a distributor or other agent) or whether a contract has been received that obligates the buyer to future payment. Once the booking has been deemed to be recognizable, the issue becomes one of how much may be recognized immediately and how much must or may be deferred and recognized in future periods. There are three

basic methods of recognizing revenue: immediate recognition, deferred recognition, and subscription revenue.

Immediate Recognition

Under this method, a company immediately recognizes all the value of a customer's purchase of software. In this case, a booking is turned almost immediately into recognized revenue. If a limited-term license is booked and there are no other contingencies or future deliverables (such as technical support) under the terms, then the total booking may also be recognized immediately.

Deferred Recognition

In practice, it is usual to negotiate mainframe and other large enterprise contracts as limited-term contracts with software "maintenance" and support provisions. Maintenance in the software sense means the right to "bug fixes," minor updates, and functionality improvements (what are called "point releases"), among other things. Here, the software company typically records the total value of the booking of a new or renewed long-term software right-to-use contract by amortizing the part associated with software maintenance over the life of the contract and then recognizing the remainder as immediate revenue.

A company may choose to report revenue recognized in the period as a total or may choose to break it out as license revenue versus maintenance revenue. Alternatively, a company may choose to report maintenance revenue together with revenue from other services, such as consulting services and implementation services, as one services figure. IDC attempts to determine in its data collection process the portion for license and for software maintenance.

Subscription Revenue

An alternative method of licensing software is via a subscription. In this case, the customer agrees to pay on a month-by-month basis (or some other period plan). Because the cancellation clauses of such contracts typically have a fairly small advance-notice requirement (usually between 30 and 90 days), there is no assurance of future revenue; therefore, revenue may be recognized only as it is billed under the terms of the contract.

There is no attempt to normalize revenue recognition across companies. For example, some companies may recognize revenue from long-term contracts over the life of the contract, others may only defer maintenance revenue, or others may apply some other model for revenue recognition. In all instances, IDC's software research reports revenue as it is recognized by a company regardless of the specific method the company uses for revenue recognition.

Mergers and Acquisitions: "Backstreaming"

To provide a true depiction of market (as opposed to individual vendor) changes over time, we "backstream" revenue when a company is acquired. That is, historical reports show revenue for the combined companies for previous years — independent of when the acquisition actually occurred. The specific rules for backstreaming are as follows:

- Revenue is backstreamed only when an entire company is acquired, not just a product line.
- Backstreaming occurs in the first full period (annual, semiannual, or quarterly) following the completion of a merger or acquisition depending on the historical data periods included in specific IDC products.

- Backstreaming is performed for all reported periods of history.

Calendar Versus Fiscal Years

All IDC software vendor revenue data is reported for calendar years regardless of the reporting cycles or fiscal years of specific vendors.

MARKET DEFINITION

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 six 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:
- **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. 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. Application scanners are primarily focused on finding database or Web application vulnerabilities. The application scanner market includes products that look at deployed applications (dynamic testing) and products that review source code (static testing).

Please note that proactive endpoint risk management (PERM) was previously included in the security and vulnerability management market but has now been incorporated in the endpoint security market.

RELATED RESEARCH

- *IDC's Forecast Scenario Assumptions for the ICT markets and Historical Market Values and Exchange Rates, Version 3, 2015* (IDC #259115, September 2015)
- *IDC's Software Taxonomy, 2015* (IDC #256767, June 2015)
- *Worldwide and U.S. Professional Security Services 2015-2019 Forecast: The Perfect Storm* (IDC #254562, March 2015)
- *Worldwide Security and Vulnerability Management 2014-2018 Forecast and 2013 Vendor Shares* (IDC #250223, August 2014)

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com