Market Share

Worldwide Security and Vulnerability Management Market Shares, 2016: Top Vendors Expand Through Nontraditional Feature Additions

Robert Ayoub Sean Pike Pete Finalle

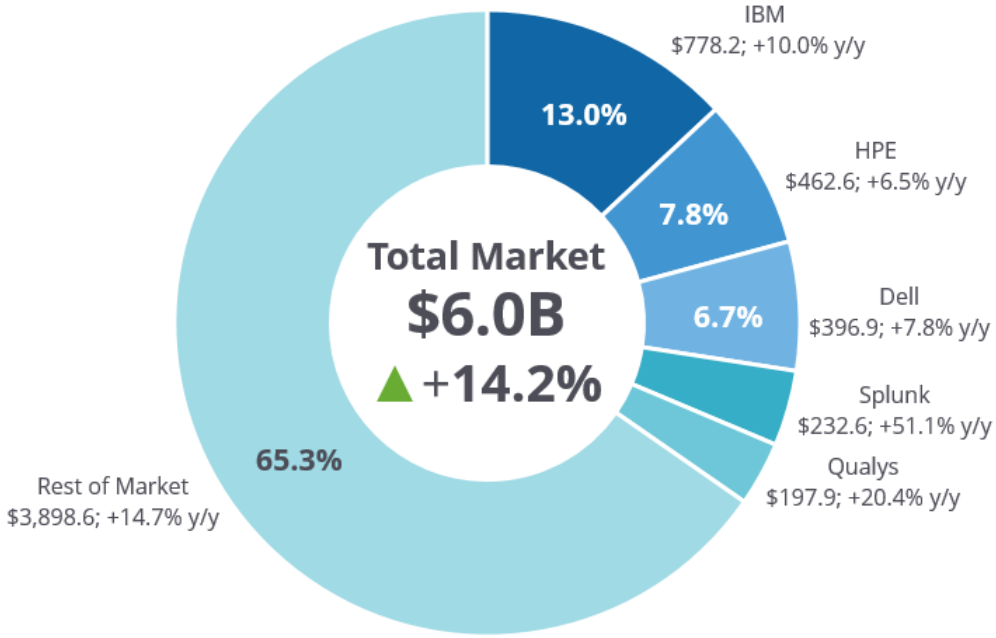
IN THIS EXCERPT

The content for this excerpt was taken directly from Worldwide Security and Vulnerability Management Market Shares, 2016: Top Vendors Expand Through Nontraditional Feature Additions (Doc# US43497916). 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 2016 Share Snapshot



Note: 2016 Share (%), Growth (%), and Revenue ($M)

Source: IDC, 2018

EXECUTIVE SUMMARY

Security management has gone from being something that only the largest organizations do to an increasingly important part of the security function. There are many reasons for this: the adoption of cloud, the explosion of devices interacting with data, the ever-increasing threat of data exfiltration, and regulatory requirements affecting companies of all sizes, just to name a few. As a result of companies being held liable for the data they are charged with protecting, as well as the increasing number of vendors being employed for security functions, it should be no surprise that security management is growing in importance.

IDC believes vendors should develop platforms 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. Security and vulnerability 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 systems that are intuitive and effective. While all vendors have begun touting the integration of machine learning and artificial intelligence into their solutions, customers have high expectations for these systems. Enterprises want tools to augment their existing staff and help address the widespread talent shortage that exists. IDC also believes that vulnerability scanning — whether it's device or application based, white box or black box, or a 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 2016 as well as the market forces that influenced their performances and the adoption of security and vulnerability management products.

"The effectiveness of attackers and the constant drumbeat of breaches continue to drive the SVM market," says Rob Ayoub, research director for Security Products at IDC. "Organizations are demanding better tools to allow for the prevention, discovery, and remediation of attacks. Vendors continue to not only improve the efficacy of current products but also add even more features in order to drive solution sales. This combination of more user-friendly products and broader solutions looks to drive healthy growth in this space for the foreseeable future."

ADVICE FOR TECHNOLOGY SUPPLIERS

SVM technology suppliers face an increasingly challenging market, and vendors much respond accordingly to continue to grow. Enterprises face an increasingly challenging threat landscape, and even though investment in security products continues, the challenge of continually managing those products and the overall risk posture of the organization are key challenges that point products cannot solve.

A primary consideration and challenge for SVM vendors moving forward will be integration and compatibility, especially across adjacent technologies. Enterprises have a myriad of applications and devices — cloud and on-premises, employee owned, and company owned — that all must be managed

and continuously assessed for risk. SVM vendors must continue to partner across the board – devices and applications – in order to ensure that they can provide the appropriate controls and altering for the enterprise.

The strongest SVM solutions appear to come from vendors that have created strong technology partnerships, and IDC has determined that a security vendor's technology partner ecosystem is being examined thoroughly in product evaluations. To remain competitive, SVM vendors should also consider the following recommendations:

- **Focus on prescription, not just alerting.** Many of the large breaches that continue to plague the industry could have been prevented. Enterprises are finding that their existing security products are flagging events that are real. The challenge is that the number of alerts coming from the security stack is unmanageable. SVM products must improve the ability of the user to react to events in a timely manner. SVM vendors must leverage threat intelligence and their understanding of user behavior to provide a complete picture of the most pressing risks.
- **Expand deployment options.** A key buying requirement is the ability to integrate products with existing security infrastructure. This requirement may result in the need for full SaaS or on-premises or a mixture of SaaS and on-premises solutions. Buyers are choosing SVM solutions with flexible deployment models as they work to address an expanding infrastructure and the shortage of trained security workers.
- **Create more streamlined and managed services offerings.** SVM products have traditionally required significant professional services engagements because of the complexity of the products. While the products have become more efficient, most enterprises simply do not have the staff to support the tuning requirements of most SVM products. As the need for advanced capabilities moves downstream, vendors that offer their own managed services or partner to provide those services will be in a stronger position moving forward.
- **Support the forensics and incident investigation (FII) process.** Forensics and incident investigation are quickly becoming a requirement for the enterprise. While many SVM products already provide a great deal of pertinent information, the integration with dedicated forensics and incident investigation tools will be a key requirement for the future.

MARKET SHARE

Table 1 provides worldwide SVM revenue and market shares for 2015 and 2016.

Table 3 displays worldwide revenue and market shares for the leading vulnerability assessment (VA) vendors for 2015 and 2016.

Figure 5 illustrates the market share for an individual submarket that IDC tracks.

TABLE 1

Worldwide Security and Vulnerability Management Revenue by Vendor, 2015 and 2016

	2015		2016		
Vendor	Revenue ($M)	Share (%)	Revenue ($M)	Share (%)	2015–2016 Growth (%)
IBM	707.6	13.5	778.2	13.0	10.0
HPE	434.4	8.3	462.6	7.8	6.5
Dell	368.0	7.0	396.9	6.7	7.8
Splunk	153.9	2.9	232.6	3.9	51.1
Qualys	164.3	3.1	197.9	3.3	20.4
Subtotal	1828.3	35	2068.2	34.7	95.9
Other	3398.1	65	3898.6	65.3	69.1
Total	5,226.4	100.0	5,966.8	100.0	14.2

Source: IDC, 2018

TABLE 3

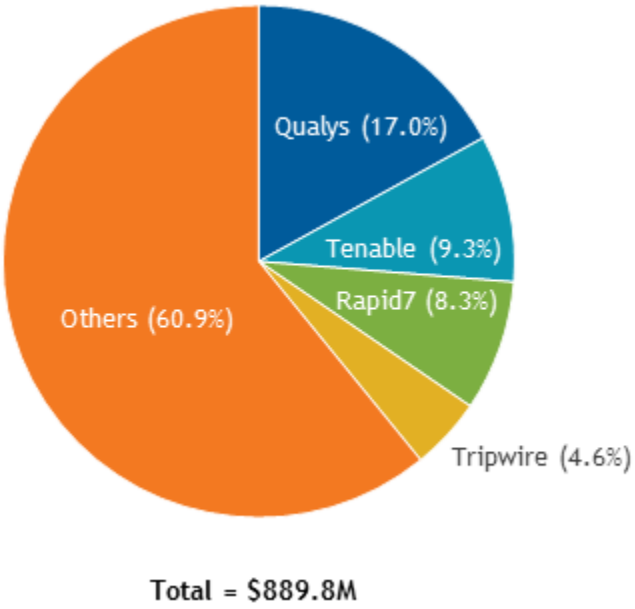
Worldwide Vulnerability Assessment Revenue by Vendor, 2015 and 2016

	2015		2016		
Vendor	Revenue ($M)	Share (%)	Revenue ($M)	Share (%)	2015–2016 Growth (%)
Qualys	144.2	9.6	173.5	10.1	20.3
IBM	137.7	9.0	151.0	8.7	9.7
HPE	134.0	8.8	142.7	8.2	6.5
Veracode	87.7	5.7	105.8	6.1	20.7
Tenable	77.4	5.1	82.5	4.7	6.6
Subtotal	581	38.1	655.5	37.7	63.9
Other	944.1	61.9	1084.7	45.6	23.8
Total	1,525.1	100.0	1,740.2	100.0	14.1

Source: IDC, 2018

FIGURE 5

Worldwide Device Vulnerability Assessment Revenue Share by Vendor, 2016



Source: IDC, 2018

WHO SHAPED THE YEAR

Qualys

Qualys continued to drive hybrid environment security forward in 2016. The move extends the company's specialization in vulnerability management to one that can provide cloud-based monitoring and threat detection over the entire enterprise – regardless of the type or location of the device. 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. These updates put Qualys in the enviable position of providing scanning, compliance reporting, and protection of assets no matter where they are deployed.

MARKET CONTEXT

The worldwide SVM market saw a significant uplift in 2015 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. 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.

An increased interest in forensics and incident response is driving renewed interest in SIEM and FII products as enterprises are under increased pressure not to just 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

2016 saw the acquisition of HPE by Micro Focus and the acquisition of EMC/RSA by Dell, both moves that could strongly disrupt the SVM market. Another development has been a greater interest in the handling of PII by end users and a greater interest in businesses taking accountability for PII and its protection. This is different from traditional compliance reporting in the case of a breach. As consumers are more concerned about the security of their data, there had been a demand for organizations to illustrate what they are doing to protect data and to explain how a breach was executed.

This increased interest in forensics is driving organizations to build their own internal FII capabilities. While an actual breach may require a third party to mitigate, the cost for these services is so high that many organizations see the benefits associated with establishing forensics and IR practices upfront. In addition, the increase in the adoption of cyberinsurance will force many organizations to show exact losses in the case of a data breach. Getting to this level of granularity requires dedicated staff and specialized tools.

The completion of many major firewall upgrade projects has occurred. In many cases, these infrastructure upgrades allowed organizations to gain additional security-related staff and budgets. As infrastructure projects have been completed, SVM is the next step for many organizations looking to build out their security infrastructure.

Finally, the consolidation of many companies that have SVM products offers the potential for significant shifts in the market as new companies may increase/decrease their level of investment in SVM products.

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.

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 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 immediate recognition 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 (which are called "point releases"). 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 30–90 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 an 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.

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

MARKET DEFINITION

The security and vulnerability management market encompasses two separate but symbiotic markets: security management and vulnerability assessment (VA). These two markets can stand alone, but they have considerable overlap. There are five 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:
  - **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 submarket 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.
  - **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 also includes malware forensics tools, used by researchers to deconstruct targeted and stealthy malware. Finally, this category 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 corporatewide policies and distribute them and provide audit information for compliance measurement. Products in this area can be used to establish and measure baseline configurations that devices (desktops, laptops, servers, smartphones, and tablets) should be adhering to. They can monitor and report on when devices fall outside of policy norms. Policy and compliance products do not directly enforce the security policies; that function is handled by endpoint security products.

- **Vulnerability assessment products.** These are batch-level products that scan servers, workstations, applications, and other devices 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 further segmented as follows:
  - **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 (a 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 submarket 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 4, 2017* (IDC #US43531218, January 2018)
- *Worldwide Security and Vulnerability Management Forecast, 2016-2020: Enterprises Continue Focus on Security Operations* (IDC #US41943616, December 2016)
- *Worldwide Security and Vulnerability Management Market Shares, 2015: Top Vendors Acquire and Integrate to Deliver Powerful, Flexible Platforms* (IDC #US42068716, December 2016)

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-community.com
www.idc.com

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 2018 IDC. Reproduction is forbidden unless authorized. All rights reserved.