[illegible]ET [illegible]LYSIS

Worl[illegible]e Endpoint S[illegible]urit[illegible] 201[illegible]–2[illegible]4 [illegible]recast and 2[illegible] Vendor Sha[illegible]

Charle[illegible]olo[illegible]

IDC OPINION

Endpoint security is the final line of defense in the battle with malware. Survey after survey confirms that some form of desktop security (e.g., antivirus, threat management, encryption, or a suite with multiple solutions) resides on the vast majority of machines. The market for these products continues to grow, even during a weak economy. With more endpoints being mobile, and thus out of the di[illegible] control of the enterprise, endpoint security requi[illegible] increase as [illegible] endpo[illegible] cannot [illegible] on the n[illegible]ecurity infr[illegible]ucture[illegible]cause ma[illegible]s the endp[illegible] will be[illegible]necti[illegible] the[illegible]ternet u[illegible]sted net[illegible]k [illegible]nection[illegible]e [illegible]ion tha[illegible] be acq[illegible] from [illegible]p machine[illegible]sumer[illegible]nd corporations [illegible]nt s[illegible]ity at[illegible]ec[illegible]ce. In [illegible], this ma[illegible]t was [illegible] billion, whi[illegible]epresents 3.3% g[illegible]h when comp[illegible]d with 2008's revenue of $6.4 billion. IDC expects the market to grow at a compound annual growth rate (CAGR) of 8.3% between 2009 and 2014, reaching a total revenue of nearly $10 billion ($9.9 billion) by the end of the forecast period. Key trends in the endpoint security software market include:

- The purchasing of multiple security tools (antivirus, antispyware, firewall, intrusion detection) continues to be popular with consumers and is increasing with enterprise customers. IDC believes that through the use of security suites, new security technologies can be implemented without degrading existing security capabilities. This trend will only continue as people search for more complete security that is also manageable.

- As the network perimeter becomes more difficult to control, endpoint security designed to protect mobile and remote workers by enforcing security policy prior to a network connection, will increase. This will require improved enterprise management capabilities associated with the endpoints.

- In addition to endpoint security used to enhance Internet security, there will be a growing need for the use of endpoint security to protect corporate information from unauthorized disclosure. This is performed by full-disk and file encryption and desktop data loss prevention.

- Consumers continue to be a huge part of the endpoint security market. The majority of endpoint security revenue is associated with consumers, and that will continue throughout the forecast period.

Filing Information: November 2010, IDC #225759, Volume: 1
Security Products: Market Analysis

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

IN THIS STUDY

This study examines the endpoint security market for the period from 2009 to 2014, with vendor revenue trends and market growth forecasts. Worldwide market sizing is provided for 2009. A five-year growth forecast for this market is shown for 2010–2014. Revenue and market share of the leading vendors are provided for 2009. This study concludes with market trends and IDC guidance for future success.

Methodology

See the Learn More section for a description of the forecasting and analysis methodology employed in this study.

In addition, please note the following:

- The information contained in this study was derived from the IDC Software Market Forecaster database as of May 14, 2010.
- All numbers in this document may not be exact due to rounding.
- For more information on IDC's software definitions and methodology, see *IDC's Software Taxonomy, 2010* (IDC #222023, February 2010).

Endpoint Security Market Definitions

The endpoint security market encompasses products that are designed to protect endpoints from attack or to directly protect information residing on endpoints. At the macrolevel, the market is segmented into those products that are purchased by consumers and those that are acquired by corporations and other organizations. For this research, the corporate endpoint security market is additionally segmented into the following four subcategories:

- **Antimalware** software consists of products that provide antivirus and antispyware protection. It includes both products that are signature based and those that use other technologies, such as white listing, to prevent the installation or execution of malicious software.
- **Server security** solutions include antimalware, desktop firewall, and host intrusion detection and prevention software that is designed to maintain the integrity of servers. These products primarily protect the operating system of servers to ensure that the systems do not run malicious software that can compromise the business applications and data on the servers. These products are generally more robust than desktop endpoint security and are available for a much wider set of operating systems (Windows, Unix, and Linux). This category also includes products that are designed to protect hypervisors and virtual servers.
- **Security suites** include multiple endpoint security tools in a single, centrally managed package. Endpoint security suites normally contain antivirus, antispyware, desktop firewall, and host intrusion prevention. As endpoint security

solutions evolve, additional features, such as antiphishing, encryption, device control, patching, and network access, are being incorporated.

- **Access and information protection** products perform one or more of the following: encryption (full disk, file, and folder), device control, data leak prevention, or network access control.

SITUATION OVERVIEW

Endpoint security has long been a component in the IT security arsenal. It has been used to detect and remove computer viruses, prevent the implanting of spyware, protect the computer from hacking attacks while connected to the Internet, and provide data protection with encryption. With each defense, attackers would expand their abilities, which required more security. The proliferation of security products placed on a single device has become daunting to acquire and manage and equally expensive. In response, many organizations now purchase a single product that can handle multiple security requirements. Security suites have the advantage of being easier to install than multiple applications, and easier to manage, provided they can be managed with a single console. Consumers have been more apt to adopt security suites, but many corporate customers have been moving in this direction as vendors have improved the ability of enterprises to centrally manage the products.

Endpoint security remains a prominent security solution. The growth in the market can be attributed to a number of factors. First is the increasing usage by consumers. As consumers expand their day-to-day interaction on the Internet, they are realizing they need to protect the critical data that now resides on their home systems. Another key factor in the growth of endpoint security is the number of attacks that are now directed toward the endpoint. Most of these attacks come via Web interactions and are difficult to defeat at a network level and must be halted at the endpoint. Last is the ever-expanding perimeter. As mobile computing devices become an island onto themselves, they must have robust security capabilities because they can't rely on network security features when they aren't connected to the corporate network.

The Endpoint Security Market in 2009

Performance of Leading Vendors in 2009

Table 1 displays 2009 worldwide revenue and market share for endpoint security vendors. Worldwide revenue for endpoint security vendors reached $6.6 billion in 2009. Seven endpoint security vendors have revenue that exceeded $150 million in 2009. These vendors, mentioned below, captured 77% of the market's total revenue:

- Symantec led the endpoint security market with 35.8% of the market on revenue of $2.4 billion. This represented a 2.2% growth when compared with 2008.
- McAfee generated $1.2 billion in endpoint security revenue and was the only other vendor with a double-digit market share (18.1%).
- Trend Micro generated $596 million in endpoint security revenue with a growth rate of 3.8%. It accounted for 9% of the total worldwide market.

- Kaspersky Lab held the fourth position with revenue of 380.1 million. It grew at a rate of 44.5% and captured a 5.8% share of the market.
- Sophos generated $203.1 million in endpoint security revenue and accounted for a 3.1% share of the worldwide market.
- AVG Technologies, another fast-growing endpoint security vendor, generated revenue of $190.1 million. It had a growth rate of 23.4% and had a 2.9% market share.
- ESET, the fastest-growing vendor among those companies with over $50 million in revenue, reached $159.2 million in revenue, good enough for a 2.4% share.

TABLE 1

Worldwide Endpoint Security Revenue by Vendor, 2008 and 2009

	Revenue ($M)			
	2008	2009	2009 Share (%)	2008–2009 Growth (%)
Symantec	2,309.2	2,359.8	35.8	2.2
McAfee	1,130.0	1,191.1	18.1	5.4
Trend Micro	574.2	596.0	9.0	3.8
Kaspersky Lab	263.0	380.1	5.8	44.5
Sophos	209.0	203.1	3.1	-2.8
AVG Technologies	154.0	190.1	2.9	23.4
ESET	99.9	159.2	2.4	59.4
F-Secure Corp.	141.3	148.7	2.3	5.2
BitDefender	135.0	139.1	2.1	3.0
Panda Software	131.1	132.1	2.0	0.8
Webroot	119.9	124.5	1.9	3.9
Check Point	129.0	122.8	1.9	-4.8
CA	91.2	99.8	1.5	9.5
IBM	88.0	99.1	1.5	12.6
Cisco	100.0	95.1	1.4	-4.9

TABLE 1

Worldwide Endpoint Security Revenue by Vendor, 2008 and 2009

	Revenue ($M)			
PGP (bought by Symantec)	51.5	45.0	0.7	-12.6
SafeNet Inc.	41.0	42.2	0.6	2.8
Avast	10.0	29.0	0.4	190.0
Norman ASA	25.9	28.5	0.4	10.2
PKWARE	25.0	25.0	0.4	–
CREDANT Technologies	23.0	23.0	0.3	–
Workshare	23.0	20.9	0.3	-9.1
GuardianEdge (bought by Symantec)	19.0	16.0	0.2	-15.8
Agnitum	12.0	14.0	0.2	16.7
Becrypt	9.0	14.0	0.2	55.6
InfoExpress	12.0	13.4	0.2	11.7
WinMagic	9.0	10.1	0.2	12.2
Adobe	12.0	9.8	0.1	-18.3
SoftCamp	13.8	9.3	0.1	-32.3
eEye	7.0	7.0	0.1	–
AhnLhab Inc.	4.5	4.3	0.1	-4.8
Subtotal	5,972.6	6,352.2	96.3	6.4
Other	412.6	245.7	3.7	-40.5
Total	6,385.2	6,597.9	100.0	3.3

Source: IDC, 2010

Table 2 displays 2009 worldwide revenue and market shares for corporate endpoint security vendors.

TABLE 2

Worldwide Corporate Endpoint Security Revenue by Vendor, 2008 and 2009

	Revenue ($M)			
	2008	2009	2009 Share (%)	2008–2009 Growth (%)
Symantec	642.0	610.8	22.1	-4.9
McAfee	508.5	501.5	18.2	-1.4
Trend Micro	279.9	274.4	9.9	-2.0
Sophos	205.9	203.1	7.4	-1.4
Kaspersky Lab	97.3	121.2	4.4	24.6
IBM	86.2	99.1	3.6	14.9
Cisco	100.0	95.1	3.4	-4.9
Check Point	78.7	79.1	2.9	0.6
CA	71.1	74.9	2.7	5.3
Panda Software	68.2	67.4	2.4	-1.2
ESET	40.0	63.7	2.3	59.2
F-Secure	55.8	56.5	2.0	1.2
AVG	41.6	50.7	1.8	21.9
PGP (bought by Symantec)	49.4	45.0	1.6	-9.0
SafeNet	41.0	42.2	1.5	2.8
Webroot	34.4	34.9	1.3	1.3
PKWARE	25.0	25.0	0.9	–
CREDANT Technologies	23.0	23.0	0.8	–
Workshare	23.0	20.9	0.8	-9.1
BitDefender	24.3	19.5	0.7	-19.9
GuardianEdge (bought by Symantec)	19.0	16.0	0.6	-15.8
Becrypt	9.0	14.0	0.5	55.6
InfoExpress	12.0	13.4	0.5	11.7
Norman ASA	16.8	10.8	0.4	-35.6
WinMagic	9.0	10.1	0.4	11.9
Adobe	12.0	9.8	0.4	-18.3
SoftCamp	13.8	9.3	0.3	-32.3

TABLE 2

Worldwide Corporate Endpoint Security Revenue by Vendor, 2008 and 2009

	Revenue ($M)			
eEye	5.3	7.0	0.3	33.3
Avast	6.0	6.1	0.2	1.7
Agnitum	6.7	6.0	0.2	-10.7
AhnLab	4.5	4.3	0.2	-4.8
Subtotal	2,609.5	2,614.6	94.7	0.2
Other	264.7	145.0	5.3	-45.2
Total	2,874.2	2,759.6	100.0	-4.0

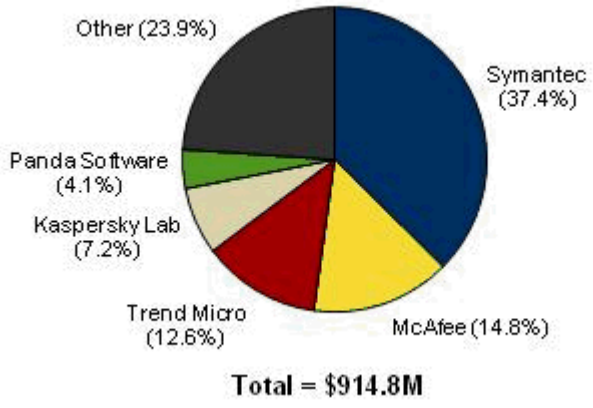
Source: IDC, 2010

The corporate endpoint security is broken into four subcategories. Figures 1–4 display 2009 market shares for leading antimalware, server security, security suite, and access and information protection vendors, respectively.

Table 3 displays 2009 worldwide revenue and market shares for consumer endpoint security vendors.

FIGURE 1

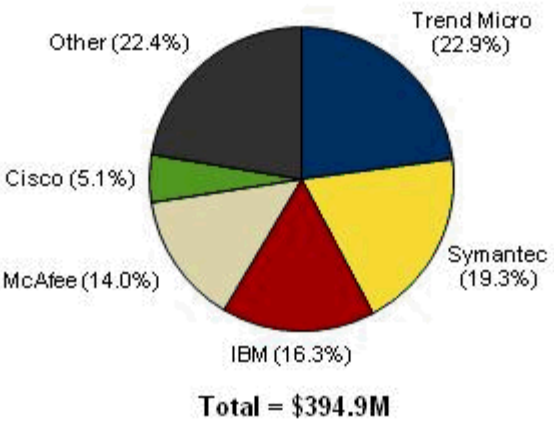
Worldwide Corporate Antimalware Revenue Share by Vendor, 2009



Source: IDC, 2010

FIGURE 2

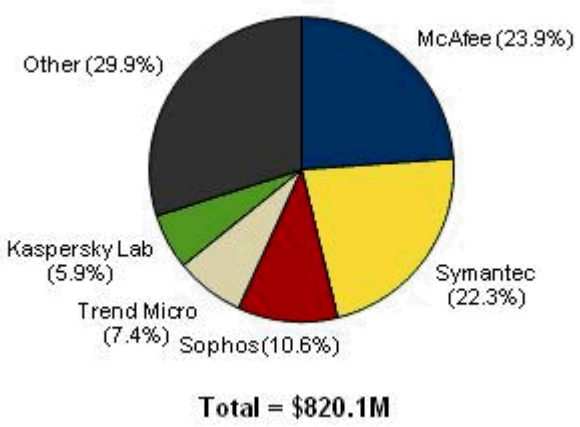
Worldwide Corporate Endpoint Server Security Revenue Share by Vendor, 2009



Source: IDC, 2010

FIGURE 3

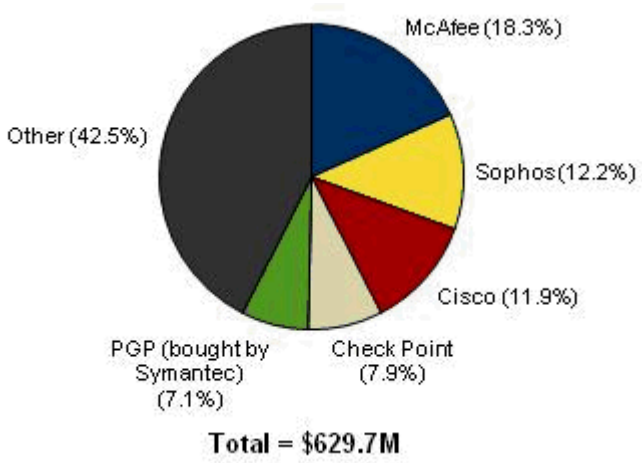
Worldwide Corporate Endpoint Security Suite Revenue Share by Vendor, 2009



Source: IDC, 2010

FIGURE 4

Worldwide Corporate Endpoint Access and Information Protection Revenue Share by Vendor, 2009



Source: IDC, 2010

TABLE 3

Worldwide Consumer Endpoint Security Revenue by Vendor, 2008 and 2009

	Revenue ($M)			
	2008	2009	2009 Share (%)	2008–2009 Growth (%)
Symantec	1,667.2	1,749.0	45.6	4.9
McAfee	621.5	689.6	18.0	11.0
Trend Micro	294.3	321.6	8.4	9.3
Kaspersky Lab	165.7	258.9	6.7	56.3
AVG	112.4	139.4	3.6	24.0
BitDefender	110.7	119.6	3.1	8.0
ESET	59.9	95.5	2.5	59.5
F-Secure	85.5	92.2	2.4	7.8
Webroot	85.5	89.7	2.3	4.9
Panda Software	62.9	64.7	1.7	2.9
Check Point	50.3	43.7	1.1	-13.2
CA	20.1	25.0	0.7	24.4
Avast	4.0	22.9	0.6	472.5
Norman ASA	9.1	17.7	0.5	95.2
Agnitum	5.3	8.0	0.2	51.5
Subtotal	3,354.4	3,737.5	97.4	11.4
Other	156.6	100.7	2.6	-35.7
Total	3,511.0	3,838.2	100.0	9.3

Source: IDC, 2010

FUTURE OUTLOOK

Forecast and Assumptions

Worldwide revenue for the endpoint security software market reached $6.6 billion in 2009. IDC currently forecasts that the endpoint security market will increase at an 8.3% CAGR and reach $9.9 billion in 2014. The forecast is initially segmented by consumer and corporate endpoint security software products, as shown in Table 4. The consumer market is larger than the corporate market, and IDC forecasts that the consumer market will continue to outpace the corporate market throughout the forecast period. This is the result of efforts by vendors to greatly increase the rate at which people convert free trials to paid subscriptions and additional services offered with consumer security products, and it is also due to the fact that there are still a large number of consumers who do not yet purchase security software. The corporate market will continue to grow by expanding features, such as browser security, encryption, and centralized management. The customer base for corporate endpoint security will increase slightly as a result of more devices, but revenue growth will also be impacted by lower per-seat prices, which result in lower prices for suites as opposed to selling multiple individual applications.

Between the corporate and consumer submarkets, the most dynamic is the corporate market, with its shift from standalone security to suites and the growing need for other endpoint security, which primarily covers data protection (endpoint encryption and data leak prevention). Table 5 provides the forecast for those submarkets.

TABLE 4

Worldwide Corporate and Consumer Endpoint Security Revenue, 2006–2014 ($M)

	2006	2007	2008	2009	2010	2011	2012	2013	2014	2009–2014 CAGR (%)
Corporate	2,399.0	2,647.8	2,874.2	2,759.6	2,867.4	3,030.9	3,327.7	3,691.7	4,078.9	8.1
Consumer	2,551.0	2,991.5	3,511.0	3,838.2	4,247.7	4,603.6	4,991.6	5,401.2	5,773.5	8.5
Total	4,950.0	5,639.3	6,385.2	6,597.8	7,115.1	7,634.5	8,319.3	9,093.0	9,852.4	8.3

Note: See Table 7 for key forecast assumptions.

Source: IDC, 2010

TABLE 5

Worldwide Corporate Endpoint Security Revenue by Submarket, 2006–2014 ($M)

	2006	2007	2008	2009	2010	2011	2012	2013	2014	2009–2014 CAGR (%)
Antimalware	1,271.8	1,146.8	1,017.3	914.8	804.9	709.4	665.8	661.0	638.5	-6.9
Server security	444.7	387.5	395.3	394.9	400.1	410.3	440.3	482.1	544.0	6.6
Security suites	363.5	637.8	847.4	820.1	952.7	1,124.8	1,348.6	1,605.6	1,907.1	18.4
Access and information protection	319.0	475.8	614.2	629.7	709.8	786.3	873.0	943.0	989.3	9.5
Total	2,399.0	2,647.8	2,874.2	2,759.6	2,867.4	3,030.9	3,327.7	3,691.7	4,078.9	8.1

Note: See Table 7 for key forecast assumptions.

Source: IDC, 2010

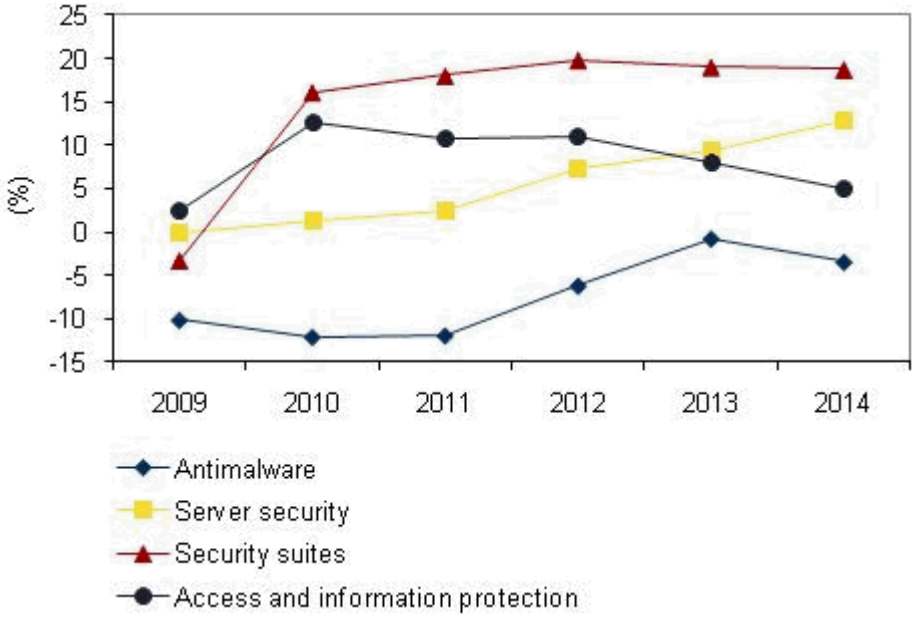
Figure 5 provides an illustration of the growth rates associated with the corporate endpoint security submarkets.

Figure 6 illustrates the revenue attributed to three regions: the Americas; Europe, the Middle East, and Africa (EMEA); and Asia.

IDC's security research team is now providing forecasts of how products will be delivered to the customer. The delivery platforms are software, hardware, virtualized, and software as a service (SaaS). Hardware for endpoint solutions generally represents security products that will be included on a USB token (encryption tokens and virtual environments) so it can be used on different devices. For virtualization, this is a delivery mechanism so the product itself resides on a hypervisor to protect the hypervisor or to centrally protect the virtual machines on the hypervisor. For SaaS, the management of the endpoint resides in the cloud and there are some features that are also performed in the cloud, but given this is endpoint security, there will be a client component that resides on an endpoint. However, all of the activities associated with deploying and managing the endpoint will be performed in a cloud architecture. Table 6 presents this forecast. Table 7 provides the key forecast assumptions for the worldwide endpoint security market.

FIGURE 5

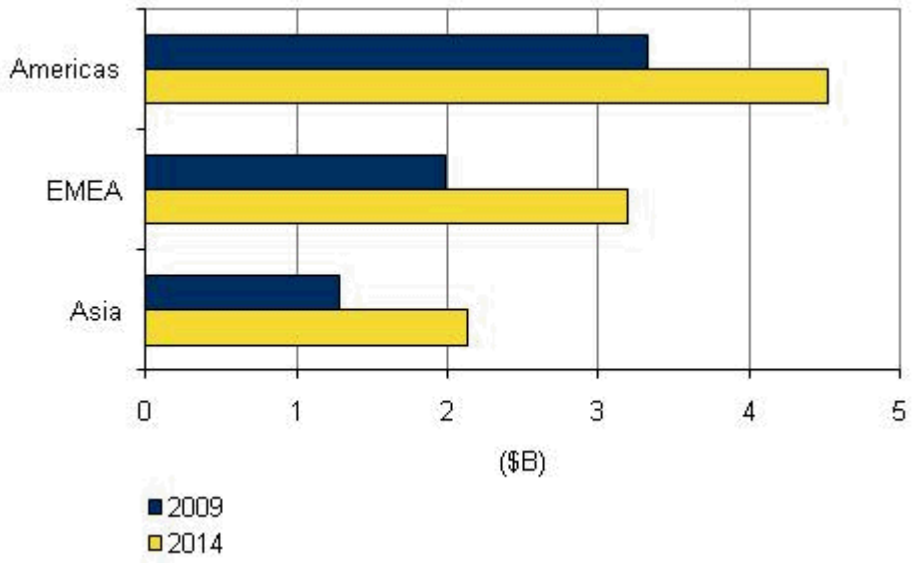
Worldwide Corporate Endpoint Security Revenue Growth by Submarket, 2009–2014



Source: IDC, 2010

FIGURE 6

Worldwide Endpoint Security Revenue by Region, 2009 and 2014



Source: IDC, 2010

TABLE 6

Worldwide Endpoint Security Revenue by Platform, 2008–2014 ($M)

	2008	2009	2010	2011	2012	2013	2014	2009–2014 CAGR (%)
Software	6,196.8	6,383.1	6,842.6	7,284.1	7,800.6	8,330.1	8,874.0	6.8
Hardware	6.4	7.3	9.2	12.1	15.4	20.0	25.6	28.7
Virtualized	3.2	9.5	21.3	36.6	91.5	172.8	305.4	100.2
SaaS	178.8	197.9	241.9	301.6	411.8	570.1	647.3	26.7
Total	6,385.2	6,597.8	7,115.1	7,634.5	8,319.3	9,093.0	9,852.4	8.3

Note: See Table 7 for key forecast assumptions.

Source: IDC, 2010

TABLE 7

Key Forecast Assumptions for the Worldwide Endpoint Security Market, 2010–2014

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Macroeconomics				
Economy	IDC assumes that worldwide economic growth will rebound to 3.2% in both 2010 and 2011. During the first half of 2010, the forecast trended slightly up.	**High.** The economy has been an inhibitor on IT spending. However, the impact on endpoint security is less than on other sectors as companies still see the value of these products, and consumers are willing to pay to mitigate their worries about cybercrime.	↓	★★★☆☆
Policy, IT governance, and regulatory compliance	Increased attention to sound IT governance policies and compliance with regulatory requirements drive an increased focus on content, storage, and data protection.	**Moderate.** Compliance and governance will have a positive impact on security spending. Compliance spending seems to be funding itself through better-run business operations.	↑	★★★☆☆

TABLE 7

Key Forecast Assumptions for the Worldwide Endpoint Security Market, 2010–2014

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Technology/ service developments				
Enterprise 2.0	Enterprise 2.0 tools, aka Web 2.0 tools used for business, will be selected because information workers find them helpful. These tools also will continue to be either free as a shadow IT self-initiative or lower priced than traditional tools as an IT-supported initiative. Reductions in IT budgets to many areas will mean that information workers will need to be self-sufficient to find the tools they need.	**Moderate.** The combination of a global recession, the need to do even more with even less, and the growing availability of Enterprise 2.0 tools means that adoption of enterprise social networking, blogs, wikis, and other tools will skyrocket. Security for these efforts will fuel innovation and product growth.	↑	★★★☆☆
Innovation	Vendors will continue security software, hardware, and services innovation at the same rate as in the past.	**Low.** The security market will not face bottlenecks from lack of new product development.	↔	★★★★☆
Modular IT/ risk aversion	Many firms remain cautious with regard to major IT investment/project implementation and have shifted to a more modular approach with longer periods of testing and slower rates of decision making and implementation.	**Moderate.** Overall demand will still fluctuate in the face of macroeconomic drivers/inhibitors, but the market should be less volatile. Large firms are taking a more long-term approach to IT than in previous years.	↔	★★★☆☆
Security threat environment	Hackers and organized crime continue to find ways to misuse other people's software. Attack vectors will move to focus on the application layer including Web applications. Endpoints and browsers are a key target.	**High.** The ability to bury malware within other software remains a dangerous trend that will lead to improved spyware software and increase the need for software and application security tools. It will increase the need for security to enforce application execution.	↑	★★★☆☆

TABLE 7

Key Forecast Assumptions for the Worldwide Endpoint Security Market, 2010–2014

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Market ecosystem				
Buyer sentiment	Buyers will remain pessimistic until they see solid changes in the economic environment.	**Moderate.** Buyer sentiment has long-term consequences for the approval of IT projects.	↓	★★★★☆
Labor supply				
Distribution of talent	IT security personnel are in short supply.	**Moderate.** The limited supply of trained security personnel requires solutions that are easy to use, reduces the need for trained security personnel, and adds value to other IT solutions.	↑	★★★★☆
Capitalization				
Venture capital and M&A	Venture funding of security start-ups has been reduced as investors have looked toward taking public companies private or encouraged mergers and acquisitions. However, promising security technologies are still being funded.	**Moderate.** There doesn't seem to be a funding limitation to IT innovation that would alter IT forecasts.	↔	★★★★☆
Market characteristics				
Vertical specialization by large vendors	Many large applications vendors that play in the "horizontal" markets have begun to add industry-specific offerings, through organic development and/or acquisition, to their product lines.	**Moderate.** Security-specific best-of-breed vendors will move to differentiate themselves. In addition, larger vendors can put pricing pressure on small vendors by offering deals involving horizontal applications, industry-specific applications, and infrastructure. This should shift revenue to larger vendors, albeit at lower prices, and augment overall large vendor market share but slow overall market growth.	↓	★★★☆☆

TABLE 7

Key Forecast Assumptions for the Worldwide Endpoint Security Market, 2010–2014

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
The Internet	Internet adoption is still going strong, especially in emerging economies. In the next four years, 700 million new users will come online and commerce will double. As people spend more time online, actively participating in Web 2.0 technologies, information workers will start expecting Enterprise 2.0 applications in the workplace.	**Moderate.** As more people get online, threats will increase and security solutions will be in greater demand.	↑	★★★★☆

Legend: ★☆☆☆☆ very low, ★★☆☆☆ low, ★★★☆☆ moderate, ★★★★☆ high, ★★★★★ very high

Source: IDC, 2010

Market Context

Table 8 and Figure 7 show a comparison of IDC's current forecast with the forecast published in *Worldwide Endpoint Security 2009–2013 Forecast and 2008 Vendor Shares* (IDC #220273, October 2009). IDC has slightly increased the growth of the endpoint security market in 2010 due to continued strong consumer sales. In the following years though IDC has reduced the forecast growth rate, primarily because that growth was anticipated as a bump from poor sales in 2009 and 2010, but the dip isn't as great, so the rebound won't be as high either. The overall CAGR of 8.3% is similar to the previous forecast CAGR of 8.5%. The Market Trends section provides some insight on how IDC believes this market will develop.

TABLE 8

Worldwide Endpoint Security Revenue, 2006–2014: Comparison of October 2009 and November 2010 Forecasts ($M)

	2006	2007	2008	2009	2010	2011	2012	2013	2014
November 2010 forecast	4,950.0	5,639.3	6,385.2	6,597.8	7,115.1	7,634.5	8,319.3	9,093.0	9,852.4
Growth (%)	NA	13.9	13.2	3.3	7.8	7.3	9.0	9.3	8.4
October 2009 forecast	4,950.0	5,639.3	6,385.2	6,650.0	7,085.9	7,713.3	8,582.3	9,583.9	NA
Growth (%)	NA	13.9	13.2	4.1	6.6	8.9	11.3	11.7	NA

Notes:

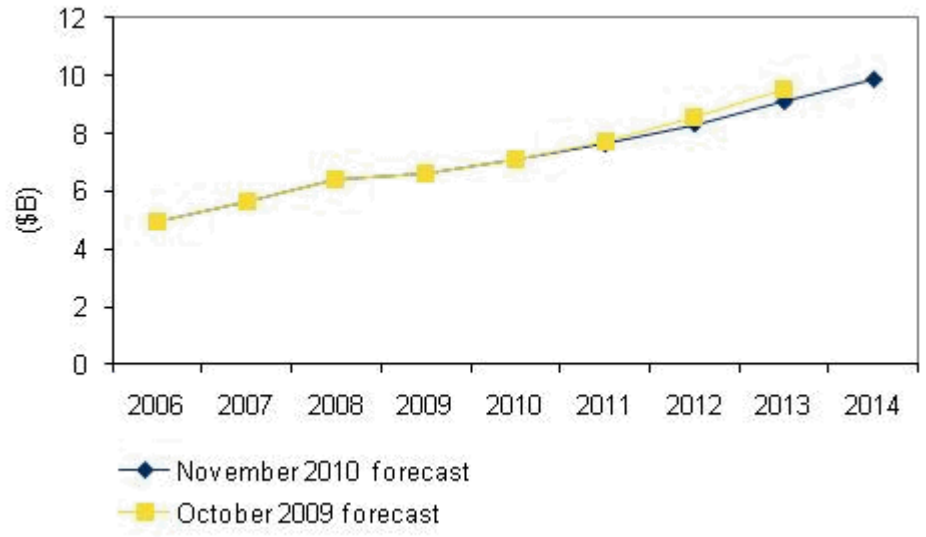
See *Worldwide Endpoint Security 2009–2013 Forecast and 2008 Vendor Shares* (IDC #220273, October 2009) for prior forecast.

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, 2010

FIGURE 7

Worldwide Endpoint Security Revenue, 2006–2014: Comparison of October 2009 and November 2010 Forecasts



Source: IDC, 2010

Market Trends

The developments that will shape this market in the future include the following:

- **Global market.** The endpoint security software market is global. This doesn't represent that these security features are used globally, which they are, but that the leading vendors in this space span the globe. Of the 12 leading vendors, two-thirds of them are headquartered around the world. The vendors have headquarters in Japan (Trend Micro), Russian Federation (Kaspersky Lab), the United Kingdom (Sophos), the Czech Republic (AVG Technologies), Finland (F-Secure), Romania (BitDefender), Spain (Panda Software), Israel (Check Point), and the Slovak Republic (ESET). This globalization illustrates how important endpoint security is, how it is important to catch threats as early as possible, and the value of regionalization. Because endpoints are used by end users, the products need to be in the language of the end user and have other cultural and social familiarization. IDC believes there will continue to be leading vendors located around the globe.

- **Growing threats changing protection landscape.** Threats targeting endpoints continue to grow. The speed with which threats are increasing (millions of malware variations) is making it increasingly difficult for signature-based antimalware to keep up. Signature databases are growing, thus impacting performance, and making antimalware less accurate. To ensure that endpoints can remain secure (clean of malware), antimalware products are changing to deal with these threats. Security products are moving to rely less on signatures and instead adopt other forms of detection. Many products have incorporated heuristics to uncover malicious activities. Other products are incorporating "white listing" that will only allow authorized applications to run. Other technologies such as browser security and virtualization are also being used to improve endpoint security. Additionally, to reduce the growth in signature files, many vendors are using reputation services that can identify threatening and malicious content available on the Internet and blocking access to that content before it ever gets to the endpoint. Reputation services are part of larger software-as-a-service offerings, which can provide standard scanning in the cloud. These services are especially important for consumers and small and medium-sized businesses.

- **Virtualization.** Endpoints, especially laptops and netbooks, are increasingly difficult to protect given the growing malware threat. One method that can strengthen trust in endpoints is through the use of endpoint virtualization. By using virtualization, the user's environment can be locked down to remove unnecessary functions and features. Virtualization can remove threats in that when the virtual machine is closed, any malware that was picked up will be eliminated. Endpoint virtualization can be delivered using standard virtual desktop technology but virtual endpoints can also be delivered on a USB thumb drive. In addition to desktop virtualization, server security will see resurgence with virtualization. As more enterprises utilized virtual servers, they will be searching for security solutions that will protect the server hosting the virtualized environment; the hypervisor; and protect the virtual servers from malware and hacker attacks. IDC expects enterprises to be very interested in virtualization security both as a means of protection and as a method of protection.

- **Web attack protection.** A new technology impacting endpoint security is Web attack protection. Many browsers have included pop-up protection and antiphishing features, but consumers and organizations are beginning asking for more. Reputation services, which are used to improve the performance of endpoint security (see "Growing threats" above), has the added benefit of improving Web attack protection by identifying Web sites that are suspected of providing malicious content, are phishing sites, or provide infected downloads. The tools, which in many cases provide basic capabilities using a free browser plug-in, can notify users about sites before they go to the site or while they are doing Web searches.

- **Free endpoint security.** Some of the fastest-growing products in the endpoint security market are free. Providing free security to consumers is nothing new. However, more and more people are turning to free antimalware products. Although free security is better than no security, in most cases the free products only provide a basic level of protection. In most cases, the free products are only providing basic antivirus but customers are looking for a complete suite of security capability. In many cases, free security software allows customers to "kick the tires" before purchasing a full service product. IDC believes that free endpoint security software is not a detriment to the market but is a viable channel for many vendors to reach customers. Paid products continue to incorporate advanced features that are worth the investment. IDC sees free consumer software would in the future be part of managed security services that can offer consumers professional remote IT expertise in such areas as software installation, printer setup, PC tune ups, backups, and virus removal.

ESSENTIAL GUIDANCE

As computers and networking continue to be critical to business success, endpoints become an engine for business success. People use computers and other devices to communicate, share information, and run applications. As endpoints proliferate, they gain in importance and become more valuable to attackers. With ever-increasing mobility, endpoint security becomes even more important. IDC believes that endpoint security will remain a critical component of a security in-depth strategy. IDC would expect that the separate desktop antivirus, desktop antispyware, desktop firewall, host intrusion prevention, and desktop data protection products will all be incorporated into an integrated endpoint security product. Many vendors have already introduced such products. This single agent is easier to install and manage while being able to match the capabilities of individual standalone products. Like all security technologies, endpoint security has to respond to an ever-changing and increasingly aggressive threat environment. Due to the need to respond to these threats, IDC believes that endpoint security solutions will not become a commodity that can be swapped in and out. Instead, customers will need to continuously assess which product(s) meet their existing and future security needs.

For consumers, endpoint security is generally the only line of defense. IDC believes that the consumer security market will continue its evolution from product to service. We believe the consumer security market will ultimately shift from a set of point products to a more comprehensive solution that encompasses security, backup and

storage, system management tools, and other consumer PC technologies. IDC believes the key to success in the consumer security market will be product differentiation through improved performance and features. With the proliferation of products, customer confusion can occur. For vendors to win in such a competitive environment, they need to stand out in the marketplace. This can be done in a number of ways: price, performance, the mix of security functions incorporated in the product, and a mix of nonsecurity features such as backup, storage, and system management tools.

LEARN MORE

Related Research

- *Worldwide Network Security 2010–2014 Forecast and 2009 Vendor Shares* (IDC #225381, November 2010)
- *Worldwide Messaging Security 2010–2014 Forecast and 2009 Vendor Shares: SaaS Is Here to Stay* (IDC #225194, October 2010)
- *Enterprise Security Survey: A Historical Review* (IDC #225151, October 2010)
- *Worldwide Web Security 2010–2014 Forecast and 2009 Vendor Shares: Web Security Takes to the Cloud* (IDC #224801, September 2010)
- *Worldwide Identity and Access Management 2010–2014 Forecast Update: Identity Moves to the Cloud* (IDC #224845, September 2010)
- *Intel's $7.7B McAfee Acquisition: Baking Security Versus Smearing It On* (IDC #IcUS22462910, August 2010)
- *Worldwide Endpoint Security 2009–2013 Forecast and 2008 Vendor Shares* (IDC #220273, October 2009)

Methodology

The IDC software market sizing and forecasts are presented in terms of packaged software revenue. IDC uses the term *packaged software* to distinguish commercially available software from custom software, not to imply that the software must be shrink-wrapped or otherwise provided via physical media. Packaged software is programs or codesets of any type commercially available through sale, lease, or rental, or as a service. Packaged software revenue typically includes fees for initial and continued right-to-use packaged software licenses. These fees may include, as part of the license contract, access to product support and/or other services that are inseparable from the right-to-use license fee structure, or this support may be priced separately. Upgrades may be included in the continuing right of use or may be priced separately. All of these items are counted by IDC as packaged software revenue.

Packaged software revenue *excludes* service revenue derived from training, consulting, and system integration that is separate (or unbundled) from the right-to-

use license but does include the implicit value of software included in a service that offers software functionality by a different pricing scheme. It is the total packaged software revenue that is further allocated to markets, geographic areas, and operating environments.

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

- **Reported and observed trends and financial activity.** This study incorporates reported and observed trends and financial activity in 2009 as of the end of March 2009, including reported revenue data for public companies trading on North American stock exchanges (CY 1Q09–4Q09 data in nearly all cases).
- **IDC's *Software Census* interviews.** IDC interviews all 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 models on more than 1,000 worldwide vendors.
- **IDC demand-side research.** This includes thousands of interviews with business users of software solutions annually and provides a powerful fifth perspective for assessing competitive performance and market dynamics. IDC's user strategy databases offer a compelling and consistent time-series view of industry trends and developments. Direct conversations with technology buyers provide an invaluable complement to the broader survey-based results.

Ultimately, the data presented in this study represents IDC's 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.

The data in this study is derived from all the sources mentioned previously and entered into the Software Market Forecaster (SMF) database, which is then updated on a continuous basis as new information regarding software vendor revenue becomes available. For this reason, the reader should note carefully the "as of" date in the Methodology discussion within the In This Study section, near the beginning of this study, whenever making comparisons between the data in this study and the data in any other software revenue study.

Historical Market Values and Exchange Rates

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 markets other than the United States, these as-published values are therefore based on a different exchange rate each year.

Because many individual countries contribute to regional totals, it is difficult to give precise differences between current and constant currency values in this document. However, the scale of the difference can be understood from the movement of the U.S. dollar against major regional currencies. Customers should consider multiplying regional historical market values for each year by the change in value of the U.S. dollar against representative currencies in the region as shown in Table 9. This will provide a better approximation of local market growth. For example, to restate 2008 EMEA values into 2009 dollars, one would adjust the 2008 value downward by 5% (because the dollar appreciated against the euro in 2009).

Please refer to IDC's regional research studies containing historical forecasts for multiple countries for more accurate regional growth in local currencies. Note that this discussion applies only to historical values prior to 2009. 2009 and all future years are forecast at a constant exchange rate.

TABLE 9

Exchange Rates, 2003–2009 (%)

	2003	2004	2005	2006	2007	2008	2009
Euro	123	112	112	111	102	95	100
Pound	96	85	86	85	78	85	100
Yen	124	116	118	124	126	111	100
Canadian dollar	123	114	106	99	94	93	100
Mexican peso	80	84	81	81	81	83	100
Brazilian real	155	146	121	109	97	92	100

Note: To restate prior-year U.S. dollars, multiply historical market values by the percentage indicated in the table.

Source: IDC, January 2010

Synopsis

This IDC study examines the endpoint security market for the period from 2009 to 2014, with vendor revenue and market growth forecasts. Worldwide market sizing is provided for 2009, and a five-year growth forecast for this market is shown for 2010–2014. Revenue and market share of the leading vendors is provided for 2009.

"Endpoint security has always been the final line of defense against malware and other threats," said Charles Kolodgy, research vice president of IDC's Security Products program. "These solutions are now a primary line of defense as employees become more mobile. Endpoint security allows these users to become an 'island onto themselves,' providing the key security and data protection needs of the end user."

Copyright Notice