FOR: Security &
Risk Professionals

The Forrester Wave™: Endpoint Security, Q1 2013

by Chenxi Wang, Ph.D. and Chris Sherman, January 4, 2013

KEY TAKEAWAYS

Endpoint Security Competency Is Crucial To Your IT Security Posture

Today's enterprises are a dynamic and distributed environment, made up of diverse endpoints, data centers, and cloud services. IT security pros realize that endpoints are where the "perimeter" is, and traditional network-centric defenses may not work within a transient endpoint environment. Therefore, an IT security spotlight should focus on a better security posture for the endpoints.

Endpoint Security Suites Dominate The Enterprise Market

The endpoint security market is evolving from AV-only to one that favors multiple functions in an integrated suite. IT security pros see the benefits of consolidated management and reporting from a single console. Other related functions, such as endpoint encryption, web security, and endpoint DLP, are also being pulled into this suite for simplified management and integrated visibility.

Application Control, Real-Time Visibility, And Patch Management Are Key Differentiators

As the AV-only approach becomes less effective, organizations begin to realize the impact of managing their application portfolio and minimizing the attack surface. Application control and patch management are two functions that serve these purposes. Another crucial function is real-time endpoint visibility, which is a differentiator of a security suite rather than a collection of disparate functions.

The Forrester Wave™: Endpoint Security, Q1 2013

Endpoint Security Suites Take Center Stage In The Enterprise

by Chenxi Wang, Ph.D. and Chris Sherman
with Stephanie Balaouras and Eric Chi

WHY READ THIS REPORT

In Forrester's 50 criteria evaluation of endpoint security vendors, we identified nine top providers in the category — F-Secure, IBM, Kaspersky, LANDesk, Lumension, McAfee, Sophos, Symantec, and Trend Micro — and researched, analyzed, and scored them. To help security and risk professionals select the right partner to tackle endpoint security challenges, this report details our findings about how well each vendor fulfills our criteria and where they stand in relation to each other.

Table Of Contents

Notes & Resources

Forrester conducted product evaluations in May 2012 and interviewed 18 vendor and user companies: IBM, Kaspersky Lab, LANDesk Software, Lumension Security, McAfee, Sophos, Symantec, Trend Micro, and many other end user organizations.

Related Research Documents

Application Control: An Essential Endpoint Security Component
September 7, 2012

Prepare For Anywhere, Anytime, Any-Device Engagement, With A Stateless Mobile Architecture
June 29, 2012

Endpoint Security Adoption Trends, Q2 2011 to Q4 2012
December 5, 2011

ENDPOINT SECURITY: THE ACHILLES' HEEL OF IT SECURITY

Computing endpoints, clients, and servers make up the bulk of enterprise computing resources. Protecting these endpoints and the information resident on them is an important aspect of IT security. In the 2012 ForrSights security survey, security professionals ranked "managing vulnerabilities and threats" as one of the top IT priorities, ranked only behind "data security." Since user endpoints are often the first place where attacks and exploits happen, IT invests in endpoint security technologies to:

- **Defend against threats targeting user endpoints.** User endpoints are effectively the enterprise perimeter where attackers seek to break into the company infrastructure. The RSA breach and the Google Aurora attack each started from a single compromised user endpoint. Endpoint-based security technologies help protect the endpoint wherever it might be without relying on infrastructure-based security capabilities such as firewalls and intrusion prevention systems (IPS).

- **Manage vulnerabilities and reduce the attack surface.** With diversity increasing due to both corporate-owned and personally owned endpoints, and the number of unique variants of malware reaching the millions, addressing endpoint security can be daunting. Endpoint measures such as application control and patch management help eradicate vulnerabilities and reduce the endpoint attack surface, an especially important means in the ever-increasing threat landscape.

- **Monitor and gain visibility of user endpoints for compliance.** Organizations with compliance and continuous monitoring requirements demand the visibility that endpoint security technologies provide. Some of the products we reviewed are capable of reporting real-time compliance status of endpoints, which gives corporate IT a powerful tool to remediate noncompliance and ascertain security posture.

Endpoint Security Encompasses More Than Just Antivirus

Traditional endpoint security is synonymous with antimalware. It's no secret that signature-based antimalware technologies have not fared that well with today's modern malware. As a result, enterprise IT is moving away from point antimalware technologies and moving to deploy layered defense with a portfolio of measures that include not just antimalware but also host-based firewall/IPS, application control, device and media control, and endpoint encryption.[1]

In addition, management functions such as patch management and system management were separate from security functions in the past, with separate buyers and budgets, but in recent years, we've seen a growing inclination from enterprise IT to integrate management with security. Patch management, in particular, has the biggest security impact and is often considered as part of an endpoint security suite. In the customer interviews we conducted for this Forrester Wave, almost everyone reported that it's important to perform endpoint security tasks from the same console where patch management tasks are performed.

To help IT security achieve these goals, endpoint security suites now routinely include threat protection, patch and vulnerability management, and even system management functions. This Wave takes these trends into consideration. In particular, we placed an emphasis on the broad functionality of "endpoint security," which includes a plethora of endpoint security and management measures beyond antimalware. We give credit to those vendors that offer a truly integrated endpoint security "suite" rather than a laundry list of patched-together, disparate functions. True integration, in our definition, means an integrated client architecture, integrated management, and reporting.

We also look for vendor solutions that have a strong underlying strategy for cloud service delivery. Forrester believes strongly that cloud infrastructure will replace today's on-premises software and hardware for system and security management tasks. This is not just an SMB requirement — it's the future of how an enterprise will manage its endpoints.

In this Wave, we loosely define an "endpoint" as an end user computing unit, which is synonymous with "client." Although we did include a few criteria for server protection, security professionals should not view this report as a study for server security, as we have not specifically focused on that.

ENDPOINT SECURITY EVALUATION OVERVIEW

To assess the state of the endpoint security market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of nine endpoint security vendors.

Evaluation Criteria Focus On Enterprise Requirements

After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of evaluation criteria. We evaluated vendors against 50 criteria, which we grouped into three high-level buckets:

- **Current offering.** We evaluated core capabilities for protecting user endpoints against threats such as malware and exploits, as well as functions such as patch management, software distribution, and central management. We also spoke with customer references to validate vendor strategies and capabilities. Throughout this study, we leveraged Forrester client inquiries as a major source of information-gathering.

  In this Wave we conducted actual patch management tests. We built a Windows 7 laptop with various out-of-date applications, including Chrome, Firefox, Internet Explorer, RealPlayer, MS Office, Java, Adobe Reader, Flash, as well as missing OS patches. We loaded each vendor's patch management client (if it was available) on the machine, placed the machine in Forrester's DMZ, and asked the vendor to report patch assessment results from their management server. To the extent possible, we asked the vendor to administer patch remediation. We rebuilt the test machine to the exact specifications after each test, ensuring that every vendor could work with the same environment.

- **Strategy.** We looked at each vendor's vision for its endpoint security suite and its short-term road map for the next 12 months, and we evaluated this information against the broad IT climate as we know it. We also evaluated the cost of each product, the financial health of the company, and its partner and channel strategies.

- **Market presence.** We evaluated each vendor's enterprise install base for its endpoint security products, as well as the number of companies that license the vendor's technologies. We also took into account any presence in the consumer market and whether that presence contributed to the competency of the enterprise products.

Evaluated Vendors Have A Strategy To Deliver Integrated Security And Management

Forrester invited nine vendors in this evaluation: F-Secure, IBM, Kaspersky, LANDesk, Lumension, McAfee, Sophos, Symantec, and Trend Micro. We evaluated their endpoint security product portfolios (see Figure 1). Each of these vendors has:

- **A sizable enterprise customer base.** We selected companies that have 1,500 or more enterprise customers for their endpoint security products. We define an "enterprise" as a company with 1,000 or more endpoints.

- **A broad endpoint security portfolio.** Each vendor has multiple endpoint security functions, including, but not limited to, antimalware, host-based firewall/IPS, application control, device control, and patch management. We also look for solutions that have integrated management spanning these functions. Because of this, we did not include any pure-play AV or antimalware providers.

- **A strategy to converge endpoint security and management.** All of the evaluated firms have the ability to do endpoint threat protection as well as management. Some of the vendors offer substantial management capabilities, with security as new additions. Others have extensive security functions and are strengthening their management support. We did not include any security or management pure-plays.

There are many endpoint security vendors that we did not include in this evaluation. Some other interesting players in the space include:

- **Microsoft.** Microsoft has built increasingly more security functions into its Windows operating system. Because of Windows popularity, many IT organizations are now evaluating Windows native security as a viable option for endpoint security and management. We wanted to include Microsoft in this study, but Microsoft declined to participate. Ultimately, because of its inherent Windows focus, this might not have been the right study for Microsoft to demonstrate its endpoint security capabilities. Forrester plans to conduct a separate study of Microsoft's endpoint security functions and will publish that study following this Wave report.

- **Consumer- or SMB-facing endpoint security providers.** This category includes AVG, Avast Software, Bitdefender, ESET, eScan (MicroWorld Technologies), Malwarebytes, and many others. As we previously stated, we aimed this evaluation at the enterprise market, and therefore we did not include any consumer- or SMB-facing players.

- **Other business-facing solutions.** Other vendors that focus on supporting endpoint security and management for corporate IT include Check Point Software, Norman, Panda Security, and Webroot. These providers did not qualify based on our selection criteria.

THE ENDPOINT SECURITY MARKET HAS MANY MATURE TECHNOLOGIES

The evaluation uncovered an established market with many mature solutions (see Figure 2):

- **Symantec, Sophos, McAfee, and Kaspersky lead the pack.** Symantec, McAfee, and Sophos are established names in the enterprise security market, and they stood out for their extensive security capabilities as well as their approaches for integrated management. Kaspersky is a somewhat new entrant in the enterprise market, but its solid security technologies, combined with a vision for integrating endpoint security and management, make Kaspersky a solid competitor.

- **IBM, TrendMicro, LANDesk, Lumension, and F-Secure offer competitive options.** The vendors in the Strong Performer category come from two distinct lineages: enterprise management and endpoint security. IBM, LANDesk, and Lumension are in the former category, while TrendMicro and F-Secure come from the latter. Technologies in the two categories are converging, and as a result, each vendor is integrating security technologies with endpoint management capabilities, a trend that aims to simplify and streamline enterprise endpoint operations.

This evaluation of the endpoint security market is intended to be a starting point only. We encourage clients to view detailed product evaluations and adapt criteria weightings to fit their individual needs through the Forrester Wave Excel-based vendor comparison tool.

Figure 1 Evaluated Vendors: Product Information

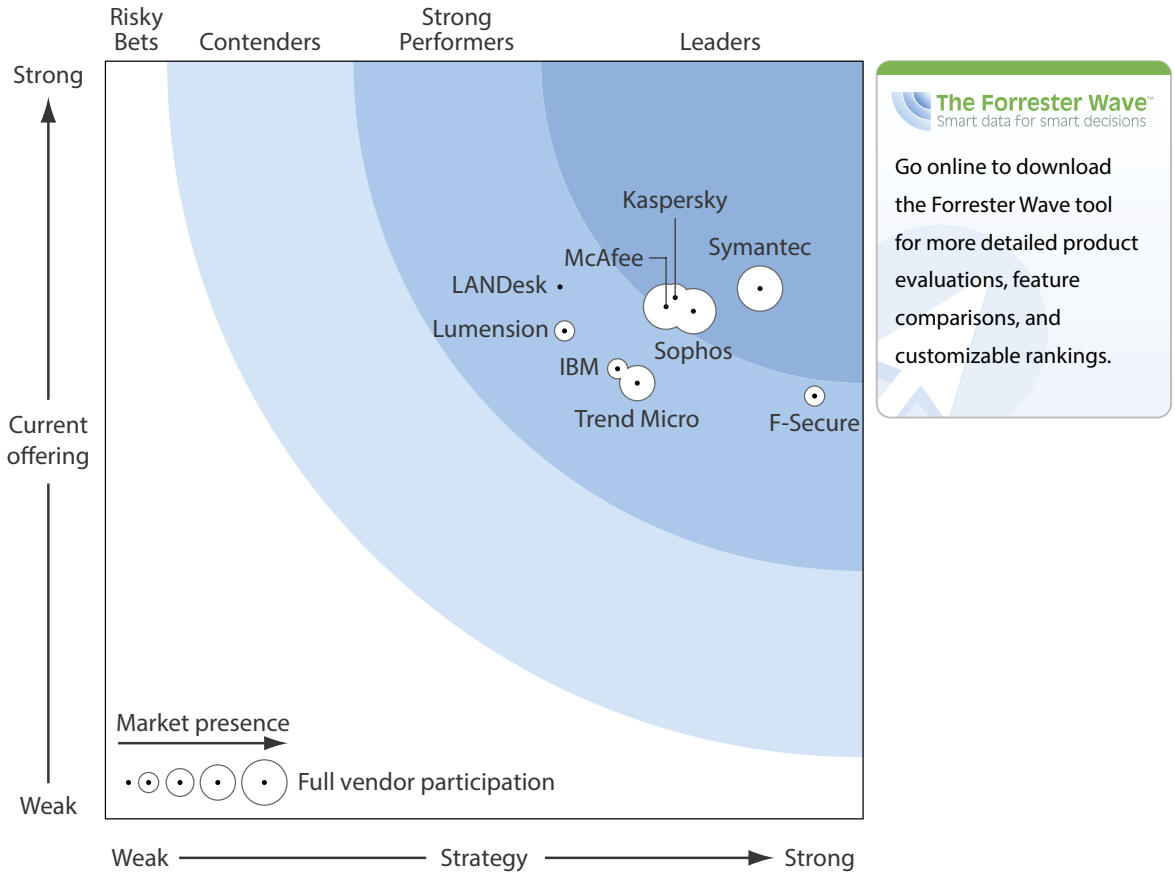
Vendor	Product evaluated	Product version evaluated
IBM	IBM Tivoli Endpoint Manager	8.2
Symantec	Symantec Endpoint Protection	12
McAfee	Total Protection Suite	8.8
Kaspersky	Endpoint Security	8.1
Lumension	Endpoint Management and Security Suite	7.2
LANDesk	LANDesk Security Suite	9.5
TrendMicro	OfficeScan	10.6
F-Secure	Business Suite — Client Security	9
Sophos	Endpoint Protection Advanced	10

Vendor selection criteria

A sizable enterprise customer base. We selected companies that have 1,500 or more enterprise customers for their endpoint security products. We define an "enterprise" as a company with 1,000 or more endpoints.
A broad endpoint security portfolio. Each vendor has multiple endpoint security functions, including, but not limited to, antimalware, host-based firewall/IPS, application control, device control, and patch management. We also look for solutions that have integrated management spanning these functions. Because of this, we did not include any pure-play AV or antimalware providers.
A strategy to converge endpoint security and management. All of the evaluated firms have the ability to do endpoint threat protection as well as management. Some of the vendors offer substantial management capabilities, with security as new additions. Others have extensive security functions and are strengthening their management support. We did not include any security or management pure-plays.

Source: Forrester Research, Inc.

Figure 2 Forrester Wave™: Endpoint Security, Q1 '13



Source: Forrester Research, Inc.

Figure 2 Forrester Wave™: Endpoint Security, Q1 '13 (Cont.)

	Forrester's Weighting	F-Secure	IBM	Kaspersky	LANDesk	Lumension	McAfee	Sophos	Symantec	Trend Micro
CURRENT OFFERING	50%	2.79	2.97	3.44	3.51	3.22	3.38	3.35	3.50	2.88
Core technologies	100%	2.79	2.97	3.44	3.51	3.22	3.38	3.35	3.50	2.88
STRATEGY	50%	4.68	3.38	3.76	3.00	3.03	3.70	3.88	4.32	3.51
Cost and licensing model	20%	4.65	3.67	4.32	3.00	4.65	4.02	4.67	4.35	3.65
Product road map	55%	5.00	3.00	3.00	3.00	2.00	3.00	4.00	4.00	3.00
Go-to-market strategies	25%	4.00	4.00	5.00	3.00	4.00	5.00	3.00	5.00	4.50
MARKET PRESENCE	0%	1.55	1.10	2.55	0.85	1.35	5.00	4.80	5.00	3.20
Enterprise presence	65%	1.00	1.00	2.00	1.00	1.00	5.00	5.00	5.00	3.00
Customer market presence	10%	4.00	2.00	5.00	2.00	2.00	5.00	3.00	5.00	5.00
License partners	25%	2.00	1.00	3.00	0.00	2.00	5.00	5.00	5.00	3.00

All scores are based on a scale of 0 (weak) to 5 (strong).

Source: Forrester Research, Inc.

VENDOR PROFILES

Leaders Provide A Breadth Of Mature Technologies

- **Symantec leads in breadth of product portfolio and in strategy.** Symantec excels in its broad functional coverage as well as its consistent strength across many different areas. Symantec continues to be a Leader in the endpoint security space and remains a good choice for enterprise customers.

  Strengths: Symantec is arguably the most recognized name in the enterprise security market. Symantec Endpoint Protection (SEP) v12 is one of the broadest product suites that we reviewed in this study. The suite includes antimalware, application control, device/media control, HIPS/firewall management, exploit protection, and network access control (NAC). Symantec's core AV product performs well in third-party tests. Customers we interviewed report good scalability and consistent performance with the SEP product. We also like the single-client architecture combined with the Symantec Protection Center management console — a good step toward true enterprise integration. Symantec also made significant investments in the mobile security space by acquiring Odyssey Software and Nukona to strengthen its mobile device management and mobile application management capabilities.

Weaknesses: SEP is not quite the one-stop shop you need. Although SEP provides many endpoint security functions, you would need Altiris, a separate product, for endpoint management. Endpoint encryption and DLP, two of Symantec's market-leading products, are sold separately. Although Symantec Protection Center (SPC) can manage these products together, customers that want true integration among endpoint encryption, DLP, and SEP still find the integration process not straightforward. Symantec also needs to move away from its threat-centric approach and demonstrate more thought leadership in managing attack surface and vulnerabilities.

- **McAfee shines in portfolio breadth and integrated policy management.** As an enterprise product, McAfee's Total Protection Suite delivers many bells and whistles for demanding enterprise customers. Its ePolicy Orchestrator provides extensive enterprise management functions, and McAfee is one of the few AV vendors that has made serious investments in application control and HIPS technologies.

  Strengths: McAfee's Total Protection Suite provides broad endpoint security functions, including antimalware, application control, device control, and HIPS/firewall control. McAfee stood out in its strong application control and device control functions. In addition, McAfee offers solid HIPS and firewall management functions. McAfee's e-Policy Orchestrator, its enterprise management console, remains a strong differentiator in the industry. With ePO, McAfee presents the most integrated management option in this evaluation. We were impressed with how expressive and powerful ePO is as a policy engine. It provides many configuration choices for even the most complex enterprise environments.

  Weaknesses: Customers have complained about performance and detection precision of McAfee's antimalware product. They reported CPU-hogging and a large memory footprint. In addition, McAfee falls short with its patch management function, which is entirely Windows-focused and which missed many third-party patches in the test we conducted. Even though the administration of the various security products are integrated, the architecture calls for separate client installs for each function, which adds operational complexity. Although McAfee moved early in the mobile security space, the company has not done a whole lot with the Trust Digital technology that it acquired.

- **Kaspersky is a rising star in the endpoint security space.** Kaspersky is a recent entrant in the enterprise market. Overall, the product has made significant improvements in its enterprise support features. Because of its extensive security strength and an attractive price point, we expect many organizations to short-list Kaspersky when considering an endpoint security product.

  Strengths: Kaspersky enjoys an impressive growth throughout the US and EMEA in both the consumer and SMB markets. The company is beginning to make a name for itself in the enterprise space as well. Kaspersky's antivirus technologies have received high marks

in many independent tests. The company continues to expand via an aggressive OEM and channel strategy, which has served it well. We like Kaspersky's forward-looking strategy, where significant architectural advances will make its endpoint security suite more integrated and more management friendly, as well as its focused R&D investments in endpoint encryption and mobile device management technologies. Aided by strong threat research and a broad portfolio of ancillary endpoint security technologies, Kaspersky's endpoint security products provide a good option for organizations with extensive security requirements.

Weaknesses: Version 8 of Kaspersky's endpoint security product does not support patch management. Some of its security products are not yet integrated with the endpoint security administration server. Kaspersky tells us that v10 will remediate this. Kaspersky also needs to augment its threat-centric strategies with more focus on endpoint data protection. Although Kaspersky provides mobile antimalware products, the company does not have much else in the way of mobile device management today. Kaspersky's virtualization and cloud computing support also have room for improvement. But above all, we think Kaspersky's strategy in cloud delivery is weak. Both system management and security functions for the endpoint are being moved into the cloud today; Kaspersky isn't quite there in terms of service delivery competency.

- **Sophos offers strong threat protection capabilities.** Organizations that have a strong endpoint management infrastructure but that need to strengthen their endpoint protection, as well as those that have a sizable consumer endpoint population (e.g., mobile devices, Macs), would do well to consider Sophos' products.

Strengths: Customers of Sophos agree that its endpoint security products deliver strong security capabilities. Sophos' antimalware product has one of the best malware detection rates on the market today and is well reviewed in third-party studies. Sophos is one of the small number of vendors that actually put R&D effort into its host intrusion prevention system (HIPS) product, as opposed to many others that simply pay lip service to HIPS. Sophos' HIPS function catches malware that its AV engine may have missed. In addition, SophosLabs is well known in the security industry and has built up a community around its threat and malware research. We also like Sophos' endpoint encryption capability, a recommended function to include in your endpoint security purchases. It's worth noting that Sophos has good support for mobility and Mac, which is becoming an increasingly important capability for enterprise environments.

Weaknesses: As an endpoint security suite, Sophos is heavy on threat protection but needs to strengthen its application control, device control, and patch management capabilities. The product's endpoint management functions also have room for improvement — customers of Sophos reported that large-scale deployments of Sophos endpoint security are best done via a third-party management system.

Strong Performers Excel In Either Security Or Management

- **F-Secure boasts strong antimalware functions.** Today, F-Secure's antimalware product is a solid competitor among the best in the industry. If the company executes its vision as it was laid out, F-Secure is on the path to becoming an innovation leader in this market.

  Strengths: F-Secure's AV product performs well in third-party comparison tests and received excellent marks from customers we interviewed. A distinct feature of F-Secure's antimalware product is its efficient use of resources. F-Secure's behavioral and heuristics analysis engines are among some of the best on the market. It's also one of the few vendors that offer browser plugins for automatic sandboxing. We were especially impressed with the road map and vision the company has laid out for the next two years. F-Secure is actively developing a service-enabling platform rather than continuing to sell software and appliances. This vision closely aligns with the biggest climate change happening in enterprise IT today, in which organizations are moving to procuring services rather than products. For a security-focused company, F-Secure also acknowledges and advocates that better patch management and better application control comprise a more effective way of protecting endpoints, and the company is actively working to strengthen those parts of its portfolio.

  Weaknesses: As a product suite, F-Secure offers rudimentary application control and device control functions. It also does not yet have any patch management capabilities. Auxiliary endpoint security functions such as encryption and host-based web security are also lacking.

- **IBM endpoint manager provides powerful endpoint visibility and management.** For environments that are large and have complex management requirements or for environments with continuous monitoring needs, Tivoli Endpoint Manager is your choice.

  Strengths: IBM's endpoint management products (AKA TEM) largely came from its acquisition of BigFix. Along with its antimalware technology, which IBM OEMs from Trend Micro, TEM offers unique endpoint management and security capabilities. Most notable is the product's fixlet architecture, which provides not only real-time visibility of the endpoint but also a powerful means of automating endpoint management workflows. Fixlets make it easy to ascertain in real time endpoint compliance and to effect changes to maintain compliance at scale. TEM is a truly integrated endpoint security and management platform, with a single client architecture. We also note that IBM recently made significant R&D improvements to its mobile device management product, also part of TEM.

  Weaknesses: TEM does not have application control functions. Endpoint encryption is also missing from the portfolio. The administration console is not particularly navigational friendly, which can be challenging to novice users.

- **LANDesk is an endpoint management platform that ventured into security.** Overall, we like LANDesk's strength in helping enterprises manage their attack surface and vulnerabilities, but we want to see more focus on endpoint security.

  Strengths: LANDesk Security Suite delivers strong application control, patch management, and HIPS/firewall functions. The suite also OEMs Kaspersky's endpoint AV. LANDesk's endpoint management functions are comprehensive and deep. Customers can use this suite to conduct complex asset management tasks. We were impressed with LANDesk's patch management capabilities, which received the highest score in this evaluation. Patch management with LANDesk can provide deep endpoint visibility, executing extremely complex workflows, but at the same time is easy to use. We also like LANDesk's vulnerability research capabilities, which feed its patch management product. The company also has a mobile device management product that is integrated with the same admin console as its PC platform.

  Weaknesses: Ultimately, LANDesk Security Suite is more management platform than security. LANDesk OEMs Kaspersky's endpoint AV, and in the past there would be a significant lag before LANDesk adopted the latest release from Kaspersky. The version of LANDesk's suite we reviewed included Kaspersky endpoint AV v6.0, even though v8.0 had been available for a while. LANDesk has recently moved away from using Kaspersky's SDK, which should allow for a timelier update. The company has since released Kaspersky v8.0, although we did not evaluate it as part of this study. Going forward, it remains to be seen how quickly LANDesk delivers on its promises to protect its customers from the latest cyberthreats. At times, some of the security capabilities feel bolted on rather than a natural extension of its core functionality. LANDesk also lacks native threat research, which can put it at a disadvantage in a dynamic threat environment.

- **Lumension expands from management to security.** Lumension's endpoint security suite is a good option for companies with a mature endpoint management strategy and a desire to consolidate endpoint security and management. In addition, even though we did not review them in this study, Lumension's compliance/risk intelligence module and the newly acquired CoreTrace product complement its endpoint security and management products nicely.

  Strengths: Lumension's roots are in patch management, and patch management is still one of its strongest offerings today. From a strategy standpoint, the Lumension Endpoint Management and Security Suite (LEMSS) offers a good balance between management and security functions. The product sports an impressive single-client architecture that ties many different functions into a unified infrastructure. This architecture simplifies deployment, management, and reporting, which sets it apart in a field rife with suites that are patched together from disparate products. The Lumension customers that we interviewed gave excellent marks for its patch and endpoint management functions, which are effective and easy-to-use. Many customers have since adopted application control and device/media control, two Lumension products that also stood out in our evaluation. Those who value single console management have further adopted Lumension's antimalware product, which it OEMs from Norman.

Weaknesses: Lumension does not offer mobile device management or mobile security products, and its virtualization support is still maturing. Customers may also find it confusing to navigate through the myriad product categories that Lumension has; the company very much needs to streamline and weave a more consistent theme among its various products.

- **Trend Micro provides good support for cloud and virtualization security.** Overall, Trend Micro's leadership in data center and virtualization security, road map to strengthen mobile support, and attractive price point make it a solid choice for many organizations.

  Strengths: Trend Micro continues to have a large presence in both enterprise and consumer markets. Its core business suite, OfficeScan endpoint protection, combines solid antimalware and HIPS/firewall functions and delivers them through a simple and streamlined interface. Trend Micro's Deep Security product is notable in the server security space. We especially like Deep Security's virtual patching capabilities, which can serve as an important defense layer for data center security. Trend's strategy supporting the burgeoning trends in mobile and virtualization also sets it apart: Organizations with basic mobile needs will find Trend's mobile device management technologies more than adequate. Additionally, Deep Security offers some of the best virtualization support on the market today.

  Weaknesses: Trend Micro's OfficeScan is not a comprehensive endpoint security suite. It falls short on application control and patch management capabilities. Additionally, Trend's endpoint encryption product is not integrated with OfficeScan, which means IT has to manage a completely separate endpoint security product if the company wants encryption along with endpoint threat protection.

SUPPLEMENTAL MATERIAL

Online Resource

The online version of Figure 2 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings.

Data Sources Used In This Forrester Wave

Forrester used a combination of five data sources to assess the strengths and weaknesses of each solution:

- **Hands-on lab evaluations.** Each vendors spent half a day with a team of analysts who performed a hands-on evaluation of the product using a scenario-based testing methodology. More specifically, Forrester used a machine to test the product's patch management functions. The test machine was built with an outdated Windows operating system as well as outdated

third-party applications. We loaded each vendor's patch management client on the machine and collected patch assessment results. Whenever possible, we asked the vendor to carry out patch remediation on the machine. We rebuilt the same test machine for each vendor, ensuring a level playing field by evaluating every product with the same environment.

- **Vendor surveys.** Forrester surveyed vendors on their capabilities as they relate to the evaluation criteria. Once we analyzed the completed vendor surveys, we conducted vendor calls where necessary to gather details of vendor qualifications.

- **Product demos.** We asked vendors to conduct demonstrations of their product's functionality. The demos were conducted alongside the lab evaluations. We used findings from these product demos to validate details of each vendor's product capabilities.

- **Customer reference calls.** To validate product and vendor qualifications, we asked each vendor to submit at least two enterprise customer references and we conducted reference calls with the customers.

- **Forrester client inquiries.** Each vendor included in this study appears frequently in Forrester end user inquiries. We leveraged heavily on the content of these inquiries to validate findings gathered from other sources.

The Forrester Wave Methodology

We conduct primary research to develop a list of vendors that meet our criteria to be evaluated in this market. From that initial pool of vendors, we then narrow our final list. We choose these vendors based on: 1) product fit; 2) customer success; and 3) Forrester client demand. We eliminate vendors that have limited customer references and products that don't fit the scope of our evaluation.

After examining past research, user need assessments, and vendor and expert interviews, we develop the initial evaluation criteria. To evaluate the vendors and their products against our set of criteria, we gather details of product qualifications through a combination of lab evaluations, questionnaires, demos, and/or discussions with client references. We send evaluations to the vendors for their review, and we adjust the evaluations to provide the most accurate view of vendor offerings and strategies.

We set default weightings to reflect our analysis of the needs of large user companies — and/or other scenarios as outlined in the Forrester Wave document — and then score the vendors based on a clearly defined scale. These default weightings are intended only as a starting point, and we encourage readers to adapt the weightings to fit their individual needs through the Excel-based tool. The final scores generate the graphical depiction of the market based on current offering, strategy, and market presence. Forrester intends to update vendor evaluations regularly as product capabilities and vendor strategies evolve.

ENDNOTES

[1] For more information on application control, see the September 7, 2012, "Application Control: An Essential Endpoint Security Component" report.

About Forrester

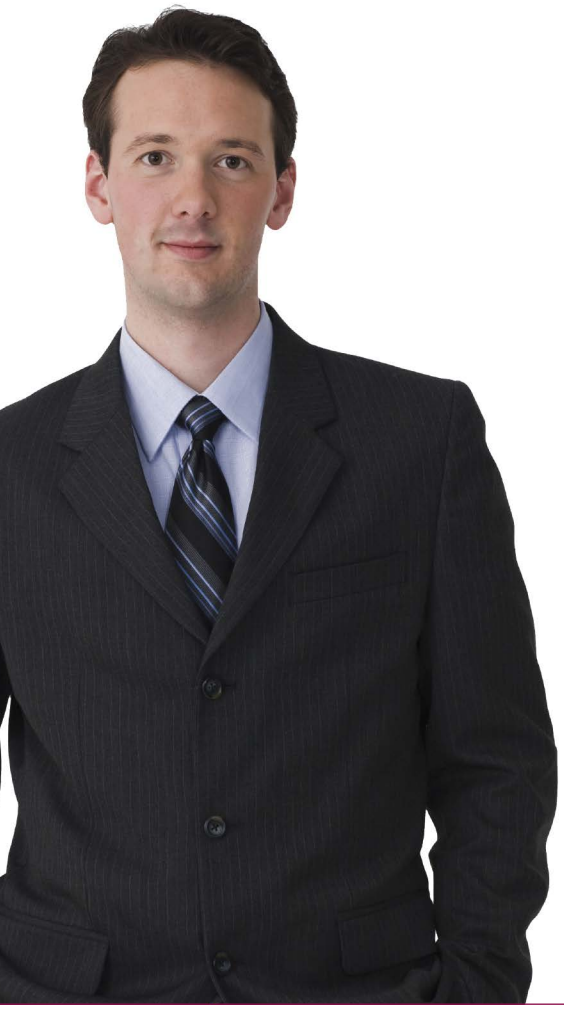
A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world's top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.



Forrester Focuses On
Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester's subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.

« **SEAN RHODES,** client persona representing Security & Risk Professionals