

April 16, 2009

The Forrester Wave™: Email Filtering, Q2 2009

by Chenxi Wang, Ph.D.
for Security & Risk Professionals



April 16, 2009

The Forrester Wave™: Email Filtering, Q2 2009

Symantec, Cisco Systems, And Secure Computing Lead, With Google, MessageLabs, And Microsoft Close Behind

by **Chenxi Wang, Ph.D.**

with Robert Whiteley and Allison Herald

EXECUTIVE SUMMARY

In late 2008, Forrester conducted an in-depth evaluation of email security filtering, based on 57 criteria. Despite the flurry of recent market acquisitions, we found that this market is still characterized by strong appliance vendors with upstart cloud providers poised to win market shares in the long run. More specifically, we found that Symantec, Cisco Systems, and Secure Computing lead the field because of their strong functionality and focused strategy. Google, MessageLabs, Microsoft, and Websense are close behind with innovative cloud-based offerings. Trend Micro, Marshal8e6, and McAfee trail the field for the lack of data security and the breadth in functionality.

TABLE OF CONTENTS

2 **Email Filtering Is A Significant IT Initiative**

Cloud Computing Erodes The Strong Foothold Of Appliance-Based Email Filtering Solutions

3 **Email Filtering Evaluation Overview**

Evaluation Criteria Focused On Breadth Of Capabilities, Content Analysis, And Vision

Evaluated Vendors Offer Multi-Faceted Solutions Against Email-Borne Threats

6 **Email Security Filtering Is Mature, And The Market Is Consolidating**

8 **Vendor Profiles**

Leaders Offer Strong On-Premise And In-The-Cloud Solutions

Strong Performers Are Close Behind But Lack Data Security And Peripheral Functionality

13 **Supplemental Material**

NOTES & RESOURCES

Forrester conducted lab-based evaluations in June and July of 2008 with 10 vendor companies: Cisco Systems/IronPort, Google, Marshal8e6, McAfee, MessageLabs, Microsoft, Secure Computing, Symantec, Trend Micro, and Websense. We conducted interviews with more than 30 user companies.

Related Research Documents

["The Forrester Wave™: Content Security Suites, Q2 2009"](#)

April 16, 2009

["The Forrester Wave™: Web Filtering, Q2 2009"](#)

April 16, 2009

["Market Overview: Content Security Suites"](#)

October 29, 2008

["Content Security Is Becoming A Competition Among Suites"](#)

December 3, 2007

EMAIL FILTERING IS A SIGNIFICANT IT INITIATIVE

Email is an essential business tool, and many organizations now consider it a mission-critical application. To ensure the proper operation of business email, organizations have turned to antispam and antivirus as necessary protection tools. But rising compliance requirements and the need for data protection mean email security filtering is also an important protection function. So it's no surprise that in Forrester's 2008 security survey of 2,148 enterprise and SMB organizations, 83% of the companies we surveyed reported deploying some form of email monitoring or filtering technologies.¹

Email filtering may have been born out of the necessity for antispam, but today the nature of email-borne threat is changing, which in turn necessitates changes to the filtering technology. First, fewer spam emails now carry viruses and malware as malicious attachments. Rather, they help proliferate phishing or malware distribution URLs. This trend suggests more integrally linked email and Web threats and calls for integrated protection that goes beyond pure email. Second, compliance requirements continue to drive and shape this market. Instead of straightforward antispam and antivirus, email filtering must now incorporate sophisticated content filtering technologies to protect unauthorized leaks of private and confidential data. Compliance also drives integration with archiving and eDiscovery technologies, making email filtering a much broader IT initiative than what it was originally designed for.

More specifically, security and risk management (SRM) professionals find that with email filtering:

- **Antispam and antivirus are commoditized technologies, but performance is still critical.** The email filtering market has evolved a long way from point products that focus exclusively on antispam and antivirus. It's difficult to find much differentiation among the antispam and antivirus technologies. But one thing that makes or breaks a product is its performance and throughput while processing large volumes of email. As one leading financial institution told us, it routinely sees that at least 14 out of every 15 incoming emails are pure spam. The performance of the filtering solution determines whether the company's employees will have timely email access or whether everyone's emails will be delayed and even dropped by the filtering process.
- **Advanced content filtering features like full-blown DLP deployment are still rare.** Today's email filtering solutions need to provide sophisticated content-based operations that cater to business' complex policies. That includes content identification, policy enforcement, management, and business analytics reporting. Many organizations look to content security vendors to provide these technologies, but they don't necessarily require a full set of data leak prevention (DLP) features that would add content fingerprinting, fuzzy matching, and contextual policies. The result is the need for what we call "light DLP" functionality, which limits features to built-in compliance dictionaries, specific lexicons, and regular-expression-based specification.
- **Support for encryption, archiving, and eDiscovery is increasingly important.** Data security requirements necessitate that email filtering act as a prelude to a number of enforcement actions, including encryption, archiving, and quarantine. Traditional email filtering solutions

provide little support for integration with these related technologies. But today's business requirements necessitate a turnkey solution. A number of vendors, including Google, Microsoft, and Symantec, offer their own archiving products and provide built-in integration with email filtering. Additionally, some vendors provide an encryption module with email security or strong integration with third-party encryption products.

Cloud Computing Erodes The Strong Foothold Of Appliance-Based Email Filtering Solutions

Buyers of email filtering technologies today want a turnkey solution. Yet IT doesn't want to spend significant time managing the technology; they want user self-service and easy management, but at the same time, they want a full set of functionalities. Consider the evolution of email filtering:

- **First, server-based deployments gave way to a gateway approach . . .** Gateways can filter out unwanted content without burdening internal infrastructure. This leads to a direct cost saving and operational efficiency. As a result, we see that the market is led by appliance-based vendors.
- **. . . which in turn is giving way to cloud-based approaches.** Email filtering in the cloud promises an even lower total cost of operations (TCO), rapid user provisioning, and even less hassle to internal IT operations. In a recent Forrester survey of 36 US and European IT organizations, more than half indicated that they are willing to outsource email filtering to the cloud.²

In the email software-as-a-service (SaaS) market, MessageLabs and Google are the two biggest players. Before and after the Google acquisition, Postini saw its business user base grow from 10 million in spring 2007 to 15 million in October 2008. MessageLabs experienced a more than 20% growth rate for the past two years. Microsoft's Exchange Hosted Services (to be named "Forefront Online Security for Exchange" after April 16, 2009) is starting to garner enterprise attention. Websense has a presence due to the former BlackSpider Technologies. Other SaaS vendors include AppRiver, MX Logic, Proofpoint, Trend Micro, Trustware, and Webroot Software.

Forrester predicts that email, as an IT function, will increasingly be outsourced. The current economic turmoil may expedite some of the sourcing decisions.³ Email filtering can be outsourced as a standalone function or as part of email outsourcing. Either way, we see an increasing industry uptake on SaaS email filtering in the foreseeable future.

EMAIL FILTERING EVALUATION OVERVIEW

To assess the state of the email filtering market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of top email filtering vendors.

Evaluation Criteria Focused On Breadth Of Capabilities, Content Analysis, And Vision

After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of evaluation criteria. We evaluated vendors against 57 criteria, which we grouped into three high-level buckets:

- **Current offering.** We selected five key areas of email filtering: core capabilities, outbound DLP, reporting and management, performance and operations, and customer references. The criteria we chose have a decided focus on content analysis, which is one of the areas where there is still some level of differentiation among the different vendors.
- **Strategy.** To assess each vendor's overall strategy, we chose two sets of criteria: product road map, which includes strategy and vision, and partnership strategies.
- **Market presence.** In this category, we examined each vendor's customer install base, revenue, and revenue growth.

Evaluated Vendors Offer Multi-Faceted Solutions Against Email-Borne Threats

Forrester included 10 vendors in the assessment: Cisco Systems, Google, Marshal, McAfee, MessageLabs, Microsoft, Secure Computing, Symantec, Trend Micro, and Websense (see Figure 1). We carried out the Forrester Wave evaluation between June and October 2008. Each vendor included in this Forrester Wave has:

- **Antispam, antivirus, and content filtering for both inbound and outbound email traffic.** Email security filtering is not about pure antispam anymore. The solutions we evaluated all have a multitude of capabilities spanning antispam, antivirus, and content filtering.
- **Support for compliance.** Email security filtering must support a corporation's compliance needs regarding email content. While specific compliance requirements vary from organization to organization, we chose to evaluate solutions that have good support for common compliance policies, such as the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), the Sarbanes-Oxley Act (SOX), and the Gramm-Leach-Bliley Act (GLBA).
- **Brand recognition and sizable market presence.** Our clients demand, especially in the current economy, vendors that have a certain amount of brand recognition and market presence in the industry. We selected such vendors, ones that are frequently mentioned by clients in hundreds of Forrester's email inquiries.
- **Filtering capabilities beyond email either in Web or instant messaging.** Because this Forrester Wave evaluation is part of an integrated evaluation with two other Forrester Waves — The Forrester Wave™: Web Filtering, Q2 2009 and The Forrester Wave™: Content Security Suites, Q2 2009 — and because we believe the content security market is moving in the direction of consolidated content security suites, each of the vendors we chose has security filtering products in at least two out of the three primary content channels.⁴ These channels are email, Web, and instant messaging.⁵ Some of the pure-play vendors that do just email filtering like Proofpoint are not included in this Forrester Wave.

During the course of our evaluation, two acquisitions and one merger occurred: Symantec acquired MessageLabs, McAfee acquired Secure Computing, and Marshal merged with 8e6 (8e6 was not included in our assessment). To acknowledge this, in the remainder of the document, we will refer to MessageLabs as Symantec/MessageLabs, Secure Computing as McAfee/Secure Computing, and Marshal as Marshal8e6. However, the product evaluations remain separate.

Figure 1 Evaluated Vendors: Product Information And Selection Criteria

Vendor	Product evaluated	Product version evaluated
Cisco Systems	IronPort C-Series, Email Security Appliance	6.1
Google	Message Security	—
Marshal8e6	MailMarshal SMTP	6.4.5
McAfee	Email and Web Security Appliance 3200	5.0
McAfee/Secure	Secure Mail	6.5.4
Microsoft	Exchange Hosted Services	8.1
Symantec	Brightmail Gateway	7.7
Symantec/MLabs	Email Protect Services	—
Symantec/MLabs	Control Services	—
Trend Micro	InterScan Web Security Suite (IWSS)	7.0
Trend Micro	InterScan Messaging Security Suite (IMSS)	7.0
Trend Micro	InterScan Messaging Security Virtual Appliance (IMVA)	7.0
Trend Micro	InterScan Messaging Hosted Service (IMHS)	—
Websense	Email Security	6.1
Websense	Hosted Email Security	5.0

Vendor selection criteria

Does the solution have antispam, antivirus, and content filtering capabilities for both inbound and outbound email traffic?

Does the solution support compliance needs?

Does the vendor demonstrate strong brand recognition and market presence, with frequent mentions in Forrester's customer inquiries?

Does the vendor have filtering capabilities for either Web or instant messaging?

Source: Forrester Research, Inc.

EMAIL SECURITY FILTERING IS MATURE, AND THE MARKET IS CONSOLIDATING

Forrester found a mature email filtering market, with everyone qualified squarely for the Strong Performer category or better (see Figure 2). This is indicative of a market in which the differentiation among vendors is not substantial. Specifically, we uncovered that:

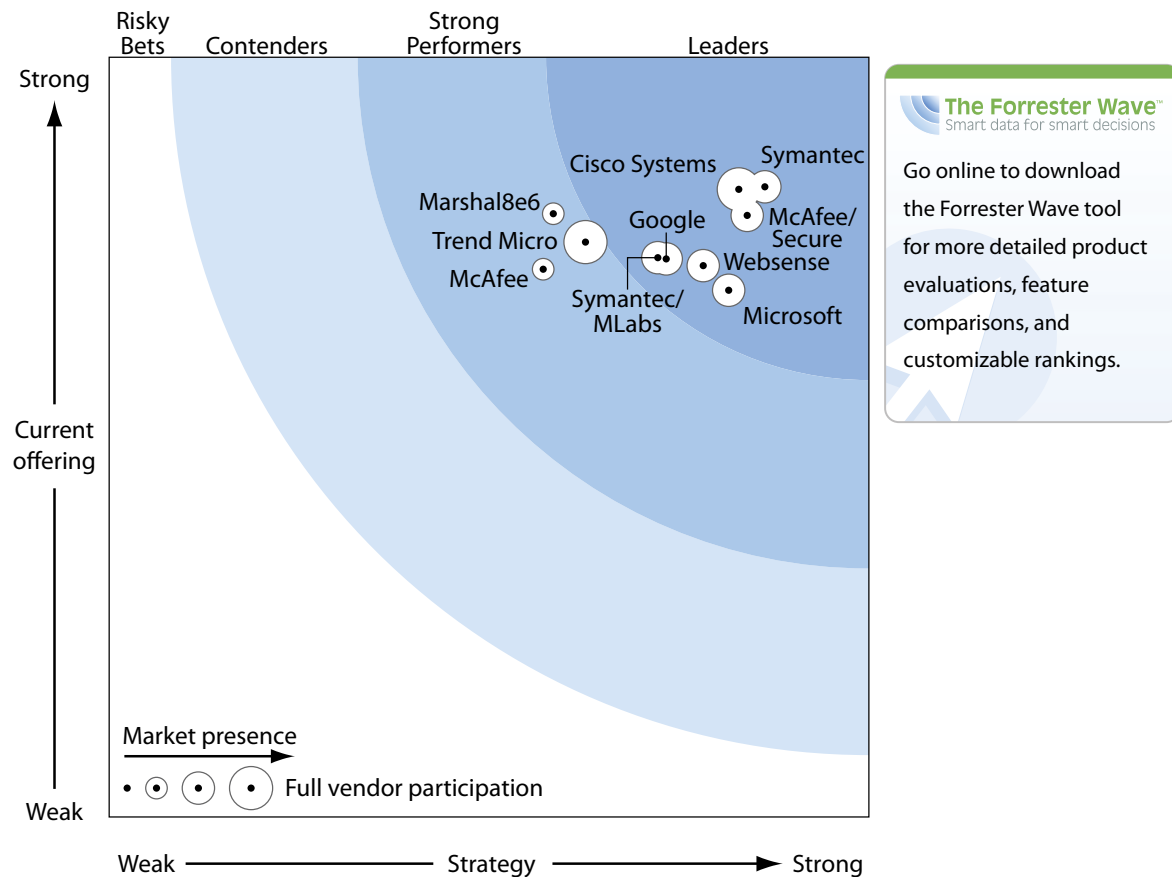
- **Cisco Systems, Symantec, and McAfee/Secure Computing lead the pack.** These three vendors distinguish themselves as the highest scoring Leaders in this evaluation. All three are appliance vendors. Cisco's IronPort C-Series tops the charts by being one of the most high performing, reliable appliances on the market today. Symantec's Brightmail Gateway appliance wins on its performance and deep content analysis capability, which is integrated from its data security product line (formerly Vontu). McAfee/Secure Computing's Secure Mail appliance series excels at offering a well-rounded appliance option, with solid functionality in almost every category.
- **Google, Microsoft, Symantec/MessageLabs, and Websense are close behind.** Google, Microsoft, and Symantec/MessageLabs are service vendors that offer email filtering in the cloud. Websense has both service and on-premise offerings. Although email-in-the-cloud — and thus filtering-in-the-cloud — is gaining momentum in the industry, the feature-by-feature comparison shows that the service offerings today don't quite match up with the high-end appliance offerings, but they are closing the gap. MessageLabs' ease of deployment, excellent scalability, and reliability combine with strong antimalware and content analysis scores, while Google and Microsoft offer good support for archiving and discovery. Websense's products provide strong support for outbound content filtering and have outstanding threat analysis support.
- **Marshal8e6, McAfee, and Trend Micro offer competitive options.** Marshal8e6's MailMarshal product, Trend Micro's InterScan Messaging Security Suite (IMS) product line, and McAfee's email/Web appliance turned in solid scores, which qualified them as Strong Performers. The MailMarshal product is one of the most flexible products we evaluated in the Forrester Wave, providing excellent support for customized policies and role-based management. Trend's IMS, working with its smart protection network, offers first-rate threat detection and analysis capabilities. McAfee's combined email and Web appliance is the only consolidated platform in this evaluation, providing customers a flexible deployment option.

There are many other email security filtering vendors that Forrester did not include in this evaluation, including Abaca Technology, Aladdin, AppRiver, Barracuda Networks, BorderWare Technologies, CA, Clearswift, Cloudmark, Fortinet, MX Logic, OPNET Technologies, Proofpoint, Sendmail, Sendio, St. Bernard Software, Tumbleweed, and Webroot.

Among the omitted vendors, St. Bernard Software declined to participate in our prequalifying survey exercise. Other vendors either failed to meet the full qualifying criteria or were omitted in favor of vendors that had a larger market presence or that Forrester clients inquired about more frequently. Their absence from this Forrester Wave evaluation doesn't constitute any judgment as to these vendors' capabilities or viability.

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

Figure 2 Forrester Wave™: Email Filtering, Q2 '09



Source: Forrester Research, Inc.

Figure 2 Forrester Wave™: Email Filtering, Q2 '09 (Cont.)

	Forrester's Weighting	Cisco Systems	Google	Marshall86	McAfee	McAfee/Secure	Microsoft	Symantec	Symantec/MLabs	Trend Micro	WebSense
CURRENT OFFERING	50%	4.18	3.72	4.01	3.66	4.00	3.51	4.19	3.73	3.82	3.67
Email filtering	35%	4.21	3.43	3.50	3.79	4.16	3.33	4.11	3.79	3.68	3.40
Data leak prevention	10%	3.87	2.55	3.90	3.62	4.15	2.37	4.80	2.29	3.66	3.80
Reporting and management	20%	3.45	3.11	4.44	4.27	4.06	2.67	4.43	3.04	3.73	3.45
Performance & operations	20%	4.56	5.00	4.32	2.78	3.20	5.00	3.94	5.00	3.87	3.88
Client reference scores and feedback	15%	4.80	4.30	4.30	3.75	4.50	3.80	4.00	3.75	4.30	4.25
STRATEGY	50%	4.12	3.66	2.90	2.84	4.18	4.06	4.30	3.59	3.11	3.89
Product strategy	70%	4.25	3.25	2.00	2.25	4.00	4.00	4.00	3.50	3.50	3.50
Partners	30%	3.80	4.60	5.00	4.20	4.60	4.20	5.00	3.80	2.20	4.80
MARKET PRESENCE	0%	4.60	3.70	2.65	2.58	3.70	3.54	3.95	3.54	4.12	3.70
Installed base	60%	5.00	4.44	3.08	4.04	4.04	4.04	4.32	4.04	5.00	3.64
Revenue	40%	4.00	2.60	2.00	0.40	3.20	2.80	3.40	2.80	2.80	3.80

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

Source: Forrester Research, Inc.

VENDOR PROFILES

Leaders Offer Strong On-Premise And In-The-Cloud Solutions

The fact that many cloud providers are in the Leaders' sector further solidifies the maturity of the market. Customers now have strong in-the-cloud alternatives as well as on-premise solutions.

Rounding out the Leaders are:

- **Symantec.** One of the largest security providers in the industry, Symantec very narrowly beat its closest competitor, Cisco Systems, for the honor of the top-ranked vendor in this evaluation, thanks to its balance of first-rate product capabilities and solid strategy. Symantec's Brightmail Gateway appliance leverages the DLP capabilities it acquired from Vontu to offer an email security appliance with one of the best built-in DLP capabilities on the market. In addition, the appliance received strong scores for scalability and throughput, making it one of the favorite products among ISP customers that leverage Symantec's appliances to offer antispam and email filtering to end users. But one of the more interesting aspects is Symantec's product strategy; whether it's through M&A and internal innovation, Symantec continues to amass a leading set of technology capabilities. Today, the Brightmail Gateway continues to benefit from the strong reputation of Brightmail, still one of the most widely OEMed solutions in the industry. Given consolidation trends in the industry, Symantec needs to continue the pace of innovation in content security or risk losing its tenuous hold of the top-ranked position.

- **Cisco Systems.** Cisco's IronPort C-Series Email Security Appliances are a perennial favorite among enterprise customers. The C-Series is second to none when it comes to connection management, reputation-based filtering, detection precision, and device performance. As a result, our evaluation determined that C-Series has the top score for core email filtering tasks. In addition, the C-Series really impressed us with its clustering architecture and excellent scalability. The C-Series is an enterprise-grade appliance, complete with comprehensive support for enterprise management and reporting tasks. Among few weaknesses, the C-Series lacks full DLP capabilities — it has built-in compliance dictionaries and lexicons but lacks extensive built-in policies and a sophisticated DLP analysis engine. Cisco's internal push of cloud computing points to a strategic, inevitable move toward cloud-based offerings. Although Cisco may be a bit late to the game, it will be a formidable contender in the service market as well.
- **McAfee/Secure Computing.** The former Secure Computing's Secure Mail product, also an appliance offering, received strong scores in many categories, making it one of the most well-rounded product offerings. Secure Mail comes with one of the best email reputation systems, TrustedSource. Although its content analysis capabilities are not quite on par with those of Symantec and Websense, Secure Mail has one of the best built-in light DLP solutions, complete with a sophisticated statistical analysis engine to detect and analyze similar documents. In addition, Secure Mail has great connection management capabilities and is easy to deploy, and customers cite excellent appliance reliability numbers. The product also provides an easy-to-use dashboard and has full support for delegated administration. Secure Mail comes with a reasonable per-user price tag, making it an attractive choice for enterprises and SMBs alike. In November 2008, Secure Computing was acquired by McAfee. Being part of the McAfee product family has many advantages for Secure Mail, such as integration with McAfee's ePo framework and access to McAfee's vast partner and reseller network. We trust Secure Computing's technologies will give McAfee a much-needed boost in winning business from outside its core of desktop-oriented buyers.
- **Google.** Although a notch below the top three vendors, Google's Message Security service (formerly Postini) does a great deal to boost the cloud-based email filtering industry. As a service vendor, Google offers outstanding throughput numbers and excellent support for scalability and reliability. In addition, Google's secure messaging services are integrated with Google's cloud archiving services. What Google lacks is sophisticated content filtering capabilities, tight integration with user directories, and good support for customized policy management. In addition, Google needs to reduce its false positive rates and enhance its centralized threat analysis capabilities. Instead of being heavily focused on email threats, Google must endeavor to bridge real-time intelligence to and from Web traffic.⁶ We expect enterprise buyers will increasingly look to Google if it strengthens its support for enterprise management, including policy customization, granular reporting, and compliance-driven policies.

- **Symantec/MessageLabs.** Similar to Google, Symantec/MessageLabs offers email filtering services in the cloud. MessageLabs' services have a solid foothold in midmarket companies, especially in EMEA. In our evaluation, MessageLabs' technology received the highest scores among the service vendors. Its offerings have roots in antimalware technology, and its Sceptic analysis engine offers sophisticated real-time malware detection capability and threat analysis. In November 2008, Symantec acquired MessageLabs to strengthen its position in the service market. At the close of our evaluation, MessageLabs had few DLP capabilities, but it will benefit from integration with Symantec's DLP products going forward. Today, MessageLabs' services are well-received in the midmarket; we anticipate that Symantec's strong brand name can take them into the enterprise market. As part of the Symantec family, MessageLabs will get a boost in both technology and market reach.
- **Microsoft.** Microsoft's Exchange Hosted Services (EHS) is a darling among enterprise customers looking to outsource both email operations and email security. In our interviews, customers gave EHS favorable scores for its enterprise readiness. Like other service vendors, EHS provides excellent performance, scalability, and reliability. In addition, it offers good support for email archiving and eDiscovery. Today, EHS does not offer much in the way of DLP and customized policy control and management. In addition, its support for intellectual property (IP) reputation, threat analysis, and real-time malware detection leave room for improvement. But Microsoft's forward-looking strategy, particularly its vision of the Stirling project — which will integrate many of its security products under one management platform — is attractive and will further propel EHS as a premier choice for enterprises. EHS will be renamed as "Forefront Online Security for Exchange" after April 16, 2009.
- **Websense.** Websense Email Security (WES) and Websense Hosted Email Security (HES) both came from Websense's acquisition of SurfControl. Websense also acquired a leading DLP vendor, PortAuthority, in 2007. As a result, Websense's email products have solid built-in support for outbound DLP, including extensive compliance dictionaries, lexicons, and regular expressions. For the on-premise WES, it also offers a separate add-on DLP module for more sophisticated DLP analysis, also built on PortAuthority's technology. Websense uses a link service that offers tight integration of content filtering and DLP.⁷ Today, the HES and WES come with disparate administrative interfaces and policy templates. Websense must work toward a more consolidated framework, which will put it on a path to integrated hybrid offerings. To compete with some of the top-of-the-line offerings, Websense must improve its performance for its on-premise offering and step up support for encryption, archiving, and eDiscovery — today it only natively supports Transport Layer Security (TLS) encryption. Its ThreatSeeker Network still focuses more heavily on the Web than on email, which Websense must improve going forward. Websense's strategy includes a big push for its service offering, but to compete with more well-known service vendors it needs to provide stronger policy management and play to its strength of being an on-premise software vendor with more flexible deployment options.

Strong Performers Are Close Behind But Lack Data Security And Peripheral Functionality

- **Trend Micro.** Trend Micro's IMS products are widely used in the industry. The product can be deployed as software, virtual appliance, and software appliance. Trend also offers a hosted email filtering service. The IMS products are easy-to-install and administer; customers praised their easy-to-use nature. The products also boast good support for high availability computing. Additionally, Trend's management interface provides excellent customization capability, and with the use of Trend Micro Control Manager (TMCM) software, customers get centralized reporting. Trend's acquisition of Provilla disappointed in that it made no impact on their content security products — their built-in DLP functionality never went beyond basic lexicons and regular expressions. In addition, Trend Micro needs to improve on its detection precision, particularly in the area of false positives. Today, the detection engine does not take into account user actions of releasing an email from the quarantine, which is a good indication for false positives. In addition, IMS's reporting and management functionality is not as flexible and granular as some of its peers in the Leaders' section. IMS has an integrated, identity-based encryption, but its support for other encryption standards (e.g., S/MIME, OpenPGP) is lacking. A traditionally endpoint-oriented company, Trend Micro's vision for gateway content security is somewhat uninspired compared with others in the same space. To distinguish itself, Trend must leverage more on the capabilities of its Smart Protection Network and endeavor to integrate network-based content filtering, endpoint antivirus, and in-the-cloud threat analysis capabilities under one unified management framework. Additionally, it needs to step up support for encryption and DLP as well as lower the cost of its offerings.
- **Marshal8e6.** Marshal8e6 is the smallest vendor included in this evaluation, but its email security product, MailMarshal, received favorable scores in its filtering capabilities and policy management. Primarily a software product, MailMarshal impresses with its flexible policy management capabilities, coming from one of the most expressive policy engines that we've seen in this evaluation. MailMarshal also offers a solid light DLP engine, despite the fact that the company itself does not own any DLP technologies. MailMarshal supports TLS encryption natively but sells an additional encryption server for other standards such as S/MIME. As a software product, MailMarshal turned in respectable performance and scalability scores, owing to its innovative array management architecture. In late 2008, Marshal merged with a Web security vendor, 8e6. This merger will provide Marshal8e6 more market visibility in Web security and deeper intelligence in Web threats, which is important for email security. However, it's unclear how this merger will affect their technology road map actions — such as implementing integrated solutions across email and Web. To remain competitive, Marshal8e6 must expand its platform support beyond its current Windows-only offering, improve on its false positive scores, and seek ways to simplify the policy-building process for mass market customers. MailMarshal today is a good fit for customers looking for a broad email security solution that has complex policy management requirements.

- **McAfee.** McAfee's combined email and Web gateway appliance is the only consolidated content security product in the Forrester Wave evaluation. This appliance offers customers a flexible deployment model — buy one appliance and selectively turn on different filtering modules. McAfee provides a number of different appliance options, from the low-end model 3000, which supports 200 users, to a high-end blade server for large enterprises. The appliances we evaluated have decent throughput numbers, but the lack of central policy management and clustering support puts the product line behind its peers. The appliance supports kernel-level Realtime Blackhole List (RBL), but McAfee's own IP reputation system lacks the extent of coverage and deep analysis compared with SenderBase or TrustedSource. In addition, McAfee's support for encryption and archiving is limited today; it only supports TLS natively, and little integration with archiving products is included. Overall, McAfee's strategy for its gateway content security product seems to be somewhat disjointed from the rest of its product lines. The gateway appliances do get threat information from McAfee's central threat analysis system (conducted by Avert Labs), but they don't contribute intelligence into Avert and the newly announced Artemis Technology. Similarly, McAfee's acquisition of Reconnex has not had an impact on its content security products. The email appliance has separate light DLP functionality with HIPAA and PCI dictionaries, but it lacks comprehensive policy support and sophisticated DLP analysis capabilities. At the close of this evaluation, integration with McAfee's ePo framework was nonexistent.⁸ Further, McAfee's acquisition of Secure Computing at the end of 2008 spells an uncertain future for McAfee's own content security products; it's not clear whether McAfee has long-term commitment for this product line.

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 four data sources to assess the strengths and weaknesses of each solution:

- **Hands-on lab evaluations.** 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. We evaluated each product using the same scenarios, creating a level playing field by evaluating every product on the same criteria.
- **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.
- **Customer reference calls.** To validate product and vendor qualifications, Forrester also conducted reference calls with two of each vendor's current customers.
- **Forrester inquiries.** Forrester's end user inquiries are another source of information for this evaluation. Whenever possible, the analyst discussed specific vendor capabilities with customers who have firsthand experiences with these vendors' offerings. We used no fewer than 10 end user inquiries as part of this evaluation.

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 Source: Enterprise And SMB Security Survey, North America And Europe, Q3 2008.
- ² Forrester conducted a survey of 36 IT professionals from US and European companies for the 2009 report, “Should Your Email Live In The Cloud? A Comparative Cost Analysis.” In this survey, seven respondents said that they plan to outsource email in its entirety to a cloud-based provider, and 20 said they plan to use a hybrid model, keeping their mailbox servers on-premise but running email filtering as a cloud-based service. See the January 5, 2009, “[Should Your Email Live In The Cloud? A Comparative Cost Analysis](#)” report.
- ³ In Forrester’s Enterprise And SMB Security Survey, North America And Europe, Q3 2008, we asked 2,014 IT professionals, “How interested is your organization in procuring email/Web content filtering as a managed or outsourced service?” Thirty-seven percent said they were already using a managed or outsourced service, and 15% said they would procure one in 2009. The results slightly predate the worst of the financial crisis that hit the world economy in late fall 2008.
- ⁴ Forrester evaluated leading Web filtering technology vendors across 53 criteria and found that Websense and McAfee/Secure Computing lead the pack because of their broad functionality and focused strategy vision. Trend Micro, Cisco Systems, Symantec/MessageLabs, and McAfee are Strong Performers but fall short in certain areas of technology. Google, Marshall8e6, Microsoft, and Symantec lack either strong capability or cohesive vision, and trail the field. See the April 16, 2009, “[The Forrester Wave™: Web Filtering, Q2 2009](#)” report. Forrester evaluated content security suite vendors, using a 41-criteria evaluation, partially based on the results of The Forrester Wave™: Email Filtering, Q2 2009 and The Forrester Wave™: Web Filtering, Q2 2009. We found that Websense alone leads the content security suite market because of its current functionality and suite-oriented product strategy. Symantec, McAfee/Secure Computing, and Trend Micro are close behind; these vendors have a clear strategy for content security suites. Cisco, MessageLabs, and Microsoft are Strong Performers but fall short in offering broad suite functionality. Google, McAfee, and Marshall8e6 sit on the border of Strong Performer and Contender; each shines in specific areas but lacks either suite focus or comprehensive capabilities. See the April 16, 2009, “[The Forrester Wave™: Content Security Suites, Q2 2009](#)” report.
- ⁵ The content security market shows no sign of slowing down, as users continue to invest in content security solutions. Growing regulatory pressure demands an increasingly sophisticated level of data protection and management integration. The technology landscape is far from static, and vendor consolidation is expected to continue as users demand easy-to-manage, comprehensive, content security suites. The impact of new technologies, including cloud computing, becomes more and more disruptive. This market overview report describes the market trends and recent directions. Security and risk professionals should be aware of these market shifts to make educated buying decisions. See the October 29, 2009, “[Market Overview: Content Security Suites](#)” report.

Websense recently completed its acquisition of SurfControl, not only taking out the No. 2 competitor in Web filtering, but also gaining a solid foothold in the email filtering space. Along with the information leak prevention (ILP) capabilities gained through its acquisition of PortAuthority Technologies, Websense now has one of the most comprehensive content security portfolios on the market. Its continued market dominance, however, is anything but certain, as many others are making strategic moves toward content security suites or platform offerings. Throughout 2008, we will continue to see the buildup of such multichannel content security suites and the incorporation of ILP functionality into these portfolios. Organizations should make strategic provisions to adopt a suite approach to content security, including the longer-term integration of capabilities for information leak prevention, encryption, content management, and archiving. See the December 3, 2007, "[Content Security Is Becoming A Competition Among Suites](#)" report.

- ⁶ Forrester uses Google secure messaging services, and the author continues to observe a certain number of false positives occurring with Google's services.
- ⁷ For more information about ICAP, visit <http://www.icap.com/>.
- ⁸ For the enterprise versions of its appliances, McAfee's integration with ePo came out in beta release in December 2008.

FORRESTER®

Making Leaders Successful Every Day

Headquarters

Forrester Research, Inc.
400 Technology Square
Cambridge, MA 02139 USA
Tel: +1 617.613.6000
Fax: +1 617.613.5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices

Australia	Israel
Brazil	Japan
Canada	Korea
Denmark	The Netherlands
France	Switzerland
Germany	United Kingdom
Hong Kong	United States
India	

For a complete list of worldwide locations, visit www.forrester.com/about.

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 Research, Inc. (Nasdaq: FORR) is an independent research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. Forrester works with professionals in 19 key roles at major companies providing proprietary research, consumer insight, consulting, events, and peer-to-peer executive programs. For more than 25 years, Forrester has been making IT, marketing, and technology industry leaders successful every day. For more information, visit www.forrester.com.