

April 16, 2009

The Forrester Wave™: Content Security Suites, Q2 2009

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



April 16, 2009

The Forrester Wave™: Content Security Suites, Q2 2009

Websense Leads, With Symantec, McAfee/Secure Computing, And Trend Micro Close Behind

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

with Robert Whiteley and Allison Herald

EXECUTIVE SUMMARY

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 Marshal8e6 sit on the border of Strong Performer and Contender; each shines in specific areas but lacks either suite focus or comprehensive capabilities.

TABLE OF CONTENTS

2 Suites Are The Future Of The Content Security Market

The Market Is Rife With Consolidation Activities

3 Content Security Suites Evaluation Overview

Evaluation Criteria Focused On Breadth Of Capabilities, Integration, And Product Road Map

Evaluated Vendors Offer Uneven Suite Functionality

6 Suite Capabilities Are Immature Across The Board

8 Vendor Profiles

The Leader Has The Strongest Foundation For An Integrated Content Security Suite

Strong Performers Have Some Integration But Overall Leave Room For Improvement

Contenders Lack Suite Functionality

13 Supplemental Material

NOTES & RESOURCES

Forrester conducted lab-based evaluations in June 2008 and interviewed 10 vendor and user companies: Cisco Systems/IronPort, Google, Marshal8e6, McAfee, MessageLabs, Microsoft, Secure Computing, Symantec, Trend Micro, and Websense.

Related Research Documents

[“The Forrester Wave™: Email Filtering, Q2 2009”](#)
April 16, 2009

[“The Forrester Wave™: Web Filtering, Q2 2009”](#)
April 16, 2009

[“Market Overview: Content Security Suites”](#)
October 29, 2008

SUITES ARE THE FUTURE OF THE CONTENT SECURITY MARKET

As the content security market continues to evolve, Forrester sees a growing market demand for consolidated content security suites rather than point products. Forrester defines a consolidated security suite as one that provides integrated functionality among multiple communication protocols, such as consolidated platforms, integrated management, or integrated reporting. Today's security and risk management (SRM) professionals are looking to content security suites because:

- **Compliance and blended threats drive consolidated functionality.** Compliance needs, such as data protection, are often protocol-agnostic. Data leak prevention (DLP) policies, for instance, demand protection from unauthorized data leaks via outbound communication regardless of the source application. Therefore, companies must see across applications, and from a corporate standpoint, it's extremely useful if protocol-independent policies can be centrally defined and managed. Another factor that drives consolidation is blended threats that span multiple protocols, such as spam campaigns that help promote phishing on the Web. These factors help drive features like consolidated threat intelligence and integrated policy management.
- **SMBs seek integrated solutions.** For small and medium-size businesses (SMBs), especially for those with fewer than 500 employees, an integrated content security solution that handles email, Web, and other applications from a single device is attractive. These solutions come with integrated policy management and reporting, which has many benefits, including reduced cost, ease of deployment, and simple management.
- **Additional functionalities add to suite appeal.** Organizations that need encryption, archiving, DLP, and eDiscovery are frustrated dealing with disjointed point products. Content security solutions that integrate these functionalities are capable of delivering a highly desirable suite that spans both security and management.
- **Visibility and control are necessary across a broad set of communication applications.** Companies today have many content applications beyond SMTP and HTTP. Instant messaging (IM), voice over IP (VoIP), and other collaboration-oriented protocols are commonly used for business purposes. These protocols traditionally flew under the IT radar, but today they may carry business-critical information and impact an organization's compliance stance. Visibility of and control over these auxiliary applications is easier from content security suites where vendors can mitigate risks and threats from a broader set of applications.

Despite the rising interest in content security suites, Forrester cautions that SRM professionals should proceed with caution. Not all suites are mature yet. Organizations with distinct needs in the email versus Web filtering technologies may still want to look to standalone solutions for individual protocols, like those evaluated in other Forrester Waves.¹ However, Forrester expects that suites like those evaluated in this document will be the default choice by 2011.

The Market Is Rife With Consolidation Activities

We've seen extensive market consolidation activities in the past two years. In November 2007, Webroot acquired software-as-a-service (SaaS) vendor Email Systems and rolled out both email and Web filtering services. In November 2008, Symantec acquired MessageLabs and McAfee acquired Secure Computing. At the same time, Marshal and Web filtering vendor 8e6 announced their merger. Most content security vendors now have filtering capabilities for multiple protocols; pure-play email or Web filtering vendors are in the minority. But the consolidation frenzy is not done yet. We still expect that:

- **Content security vendors will continue acquisitions, especially for functionalities like DLP.** Content security vendors have been actively acquiring or building related functionality to round out their offerings. DLP, encryption, and archiving are but a few examples. In 2006, Websense acquired DLP vendor PortAuthority and as a result significantly strengthened the data security aspects of its content filtering products. Symantec acquired Vontu, and its email filtering appliance also benefited from integration with Vontu's DLP technology. Proofpoint is another vendor that has built-in DLP functionality in its email filtering products.
- **Cloud-based offerings are just gaining traction, starting with email filtering.** Led by Google, MessageLabs, and Microsoft, the content security industry is singing the tune of cloud computing. Websense is leveraging on its acquired BlackSpider Technologies to build a foundation for a broad set of offerings in the cloud. Cisco Systems will soon come to market with its own email security in the cloud. In the near future, we expect to see more vendors moving more functionality into the cloud. The cloud has the advantage of inherent integration — the concept of content security suite services will be reality soon enough.

CONTENT SECURITY SUITES EVALUATION OVERVIEW

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

Evaluation Criteria Focused On Breadth Of Capabilities, Integration, And Product Road Map

After examining past research, user needs assessments, and vendor and expert interviews, we developed a comprehensive set of evaluation criteria. We evaluated vendors against 41 criteria, which we grouped into three high-level buckets:

- **Current offering.** To evaluate the vendor's current offering, we looked at its product's capabilities across five areas: email filtering, Web filtering, other content protocols, integration, and client reference feedback. We placed particular weight on the evaluation of integration among filtering capabilities for different applications, as an essential element of delivering a content security suite.

- **Strategy.** To measure strategy and vision, Forrester considered criteria including the vendor's cost and pricing structure, product strategy, and business partners. We looked for cost-saving advantages for a suite purchase as opposed to separate point-product purchases. In addition, we gave high scores to companies that have a coherent and forward-looking suite/platform product road map.
- **Market presence.** We evaluated each vendor's presence in the content security suites market based on its product's install base, its market segment diversity, as well as its revenue and revenue growth.

Evaluated Vendors Offer Uneven Suite Functionality

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

- **Filtering capabilities for multiple content applications.** This Forrester Wave is specifically focused on content security suites, and the evaluation is part of an integrated evaluation with two other Forrester Waves: the Email Filtering Wave and the Web Filtering Wave.² Thus, each vendor had to demonstrate capabilities in security filtering products in at least two of the three primary content channels: email, Web, and instant messaging.³ This is why some of the pure-play vendors are not included in the Forrester Wave evaluations.
- **Strong support for IM security filtering.** One of the content filtering capabilities we evaluated in particular is support for IM security and IM filtering. Although not as widely used as email and Web, instant messaging is still an important business application. We evaluate vendors' technologies to perform deep content filtering for IM, not just detection and blocking of IM communication sessions.
- **A clear strategy toward a suite offering.** To deliver a content security suite, integration among the different content applications is a must. Integration can come in many forms, including an integrated platform, integrated policy management, or integrated reporting. We chose vendors that have either integration capabilities in place or a clear strategy toward integration.
- **Brand recognition and sizable market presence.** In the current economy, our clients demand 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 client security inquiries.

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
Cisco Systems	IronPort C-Series, Email Security Appliance	6.1
Cisco Systems	IronPort S-Series, Web Security Appliance	5.6
Google	Message Security	—
Google	Web Security for Enterprise	—
Marshal8e6	MailMarshal SMTP	6.4.5
Marshal8e6	WebMarshal	6.1
McAfee	Email and Web Security Appliance 3200	5.0
McAfee/Secure	Secure Mail	6.5.4
McAfee/Secure	Secure Web Webwasher Web Gateway Security Appliance	6.7
McAfee/Secure	Secure Web Protection Service	6.7
McAfee/Secure	IronIM	—
Microsoft	Exchange Hosted Services	8.1
Microsoft	Internet Security & Acceleration (ISA) Server 2006	5.1
Symantec	Brightmail Gateway	7.7
Symantec	Scan Engine	5.2
Symantec	IM Manager	8.4
Symantec/MLabs	Email Protect Services	—
Symantec/MLabs	Control Services	—
Symantec/MLabs	Web Security Services	2.0

Source: Forrester Research, Inc.

Figure 1 Evaluated Vendors: Product Information And Selection Criteria (Cont.)

Vendor	Product evaluated	Product version
Trend Micro	InterScan Messaging Security Suite (IMSS)	7.0
Trend Micro	InterScan Messaging Security Virtual Appliance (IMSVa)	7.0
Trend Micro	InterScan Messaging Hosted Service (IMHS)	—
Trend Micro	InterScan Web Security Suite (IWSS)	3.1
Websense	Email Security	6.1
Websense	Hosted Email Security	5.0
Websense	Web Security Gateway	7.0

Vendor selection criteria

Does the vendor have filtering capabilities for multiple content applications among email, Web, and instant messaging?
Does the vendor demonstrate strong brand recognition and market presence, with frequent mentions in Forrester’s customer inquiries?
Does the vendor offer any kind of suite functionality behind disjointed point products for each content protocol?

Source: Forrester Research, Inc.

SUITE CAPABILITIES ARE IMMATURE ACROSS THE BOARD

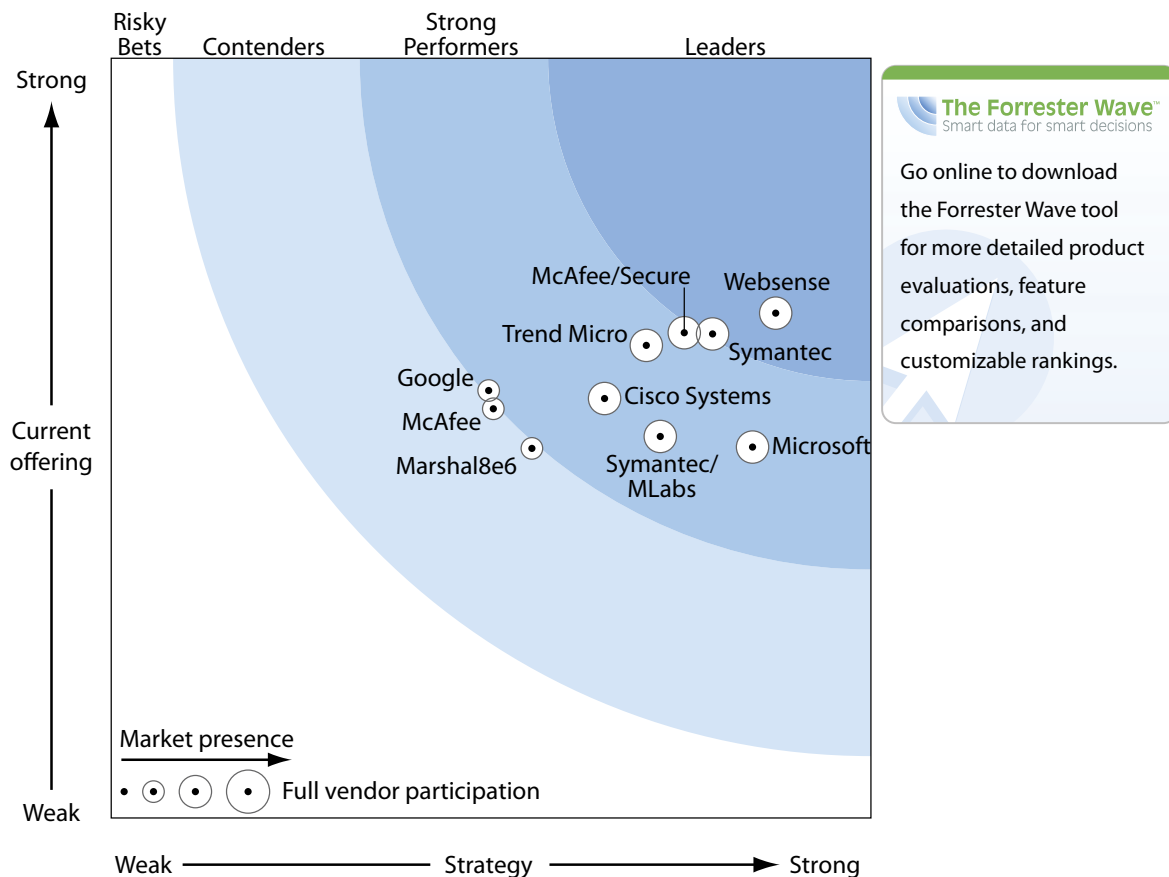
The evaluation uncovered a maturing market in which only a small number of vendors reported adequate suite functionality (see Figure 2). Today’s security and risk managers should note that:

- **Websense leads the market.** Websense is the only vendor that is clearly in the Leader category for content security suites. Compared with the rest of the field, Websense distinguishes itself by owning a broad set of key technologies across different content applications; by its ThreatSeeker technology that is integrated for the different product offerings; and by its vision toward a more consolidated content security suite. But even Websense did not turn up superior scores for its suite capability.
- **Symantec, McAfee/Secure Computing, and Trend Micro are close behind.** On the border of Leader and Strong Performer, Symantec, McAfee/Secure Computing, and Trend Micro scored well in the suite evaluation but have shortcomings in specific areas. These vendors need to either strengthen their capability for specific protocols or produce a more suite-oriented strategy.

- Cisco, Symantec/MessageLabs, and Microsoft excel at niche capabilities.** Cisco, Symantec/MessageLabs, and Microsoft each has its own strong point. Cisco excels at producing separate high-performance appliances for different protocols; Symantec/MessageLabs and Microsoft have solid email security in the cloud. But each falls short on comprehensiveness and pulling together an overall suite.
- Google, McAfee, and Marshal8e6 lack support for content security suites.** Google, McAfee, and Marsahal8e6 sit on the border of Strong Performer and Contender. Google has respectable scores for its technical functionality but fails to achieve a high strategy rating because of its weak focus in suite offerings. Marshal8e6 falls short on support for other content applications and undistinguished suite road map. McAfee has a consolidated email and Web filtering appliance but lacks concrete strategies to take it further to include other integrated functionality.

This evaluation of the content security suites 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™: Content Security Suites, Q2 '09



Source: Forrester Research, Inc.

Figure 2 Forrester Wave™: Content Security Suites, Q2 '09 (Cont.)

	Forrester's Weighting	Cisco Systems	Google	Marshal8e6	McAfee	McAfee/Secure	Microsoft	Symantec	Symantec/MLabs	Trend Micro	Websense
CURRENT OFFERING	50%	2.81	2.86	2.48	2.74	3.24	2.49	3.23	2.56	3.16	3.37
Email filtering	20%	4.18	3.72	4.01	3.66	4.00	3.51	4.19	3.73	3.82	3.67
Web filtering	20%	3.23	3.62	3.29	3.36	4.17	1.75	1.90	2.96	3.44	4.05
Other content protocols	15%	2.10	2.30	0.90	0.80	1.55	3.40	3.30	2.25	3.25	2.05
Integration	35%	1.69	2.00	1.60	2.48	2.72	1.72	3.40	1.65	2.30	3.16
Client reference scores and feedback	10%	4.25	3.50	3.25	3.50	4.25	3.30	3.30	3.05	4.20	4.15
STRATEGY	50%	3.26	2.50	2.79	2.53	3.79	4.24	3.97	3.63	3.54	4.39
Cost & pricing structure	12%	0.00	0.00	5.00	1.00	3.00	5.00	3.00	1.00	3.00	4.00
Product strategy	75%	3.65	2.50	2.05	2.50	3.70	4.00	3.95	4.10	3.65	4.35
Partners	13%	4.05	4.80	5.00	4.10	5.00	4.90	5.00	3.35	3.40	5.00
MARKET PRESENCE	0%	3.98	2.78	2.60	2.14	3.57	3.82	3.73	3.15	3.78	3.80
Installed base	60%	3.96	3.17	3.00	3.30	3.81	4.50	3.95	3.38	4.43	3.80
Revenue	40%	4.00	2.20	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

The Leader Has The Strongest Foundation For An Integrated Content Security Suite

The emerging nature of this market means there are few truly integrated content security suites. We found much strong leadership in individual evaluations of the email filtering and Web filtering markets. But this evaluation uncovered just one Leader:

- Websense.** Websense is the Leader in content security suites. Websense has mature products in both email and Web. Moreover, Websense's Secure Web Gateway has broad control over many different content protocols, for which they are either able to detect-and-block or regulate communicating parties, attachment policies, and specific content types. Websense also earned kudos for its integration with data security capabilities — the former PortAuthority technology — which provide protocol-agnostic policies and content classification functionality. More importantly, Websense delivers an excellent integrated threat analysis capability through its ThreatSeeker technology, which is behind all its content security products. Websense's individual products lack integrated features and deep content filtering for IM. However, we believe that Websense's product strategy, built on cloud-based intelligence and cloud delivery, laid the strongest foundation for an integrated content security suite. Websense is the best choice today for organizations looking for best-of-breed technologies that have a good suite focus.

Strong Performers Have Some Integration But Overall Leave Room For Improvement

- **Symantec.** Symantec is a Strong Performer in the content security suite evaluation. Symantec has the strongest IM security product in this evaluation due to its 2006 acquisition of IMlogic. The IMlogic product is now marketed as the standalone IM manager and as built-in functionality in Symantec's Brightmail Gateway email filtering appliance. As such, the Brightmail Gateway appliance is a consolidated content filtering device across email and IM, and the built-in data security functions benefit both applications. What Symantec lacks in the overall suite offering is strong Web filtering, as well as capabilities to detect and regulate other communication protocols like File Transfer Protocol (FTP) and peer-to-peer (P2P).⁴ Even with the addition of MessageLabs, Symantec is still not on par with others like Websense in the Web filtering market. Symantec's Global Intelligence Network has great potential but at present doesn't support the Scan Engine product. However, Symantec has a great track record of identifying and acquiring best-of-breed technologies. Its vision of integration across content security, data protection, archiving, backup, and disaster recovery is particularly compelling. Symantec's Brightmail Gateway appliance is a good choice today for organizations interested in consolidated email and IM security. In the long term, we believe that Symantec is one of those vendors that can credibly deliver a content security suite that combines both cloud and on-premise methods.
- **McAfee/Secure Computing.** McAfee/Secure Computing is a Strong Performer in the content security suite evaluation. Secure Computing offers the SME 250, which is a consolidated appliance across email and Web for smaller customers. Beyond that, its Secure Mail and Secure Web product lines are essentially separate. One integration point is its reputation service, TrustedSource, which conducts integrated analysis across email and Web. At the time of evaluation, Secure Computing had ceased support for its IM gateway product (formerly Iron IM) and was in the process of integrating IM gateway into the next release of Secure Web. McAfee/Secure Computing also lacks extensive support for other content protocols beyond the ones tunneled over HTTP. Its product road map, however, includes a number of concerted efforts toward suite functionality, including specific integrations with data security functionality across email, Web, and IM, and deeper correlation with TrustedSource. McAfee/Secure Computing needs to improve the product's support for an integrated platform and also auxiliary functionality like email archiving and discovery.
- **Trend Micro.** We consider Trend Micro a Strong Performer in the content security suite market. Trend's InterScan Web Security Suite (IWSS) product uses application signatures and URL filtering to detect and block IM communications. Separately, Trend offers an IM security product for Microsoft Office Communications Server (OCS) with deep content filtering capabilities. Trend's products today lack control capabilities for protocols beyond email and HTTP. Its Trend Micro Control Manager (TMCM) product integrates with both IWSS and InterScan Messaging Security (IMS) to offer integrated reporting across email and Web. Trend's

content security suite vision is centered on its Smart Protection Network (SPN) that will be extended to other product lines. Its current strategy is gradually moving more things off-premise and onto SPN in the cloud. A direct result of this strategy will be more consolidated functionality, such as integrated policies and reporting. Trend is not quite there yet, but we anticipate seeing SPN playing a larger role in its content security strategy, including data security in the cloud. Trend's offerings today are best suited for organizations that have a hybrid need — those who want to take advantage of cloud computing but want to keep certain controls on-premise. Trend allows one of the most flexible deployment models we've seen thus far.

- **Cisco Systems.** Cisco's IronPort C-Series (email filtering appliance) and the IronPort S-Series (Web filtering appliance) share a similar administrative interface, but the similarity stops there. The company does not offer shared policies, integrated management, or reporting. Its separate management appliance, M-series, which centralizes reporting, quarantine, and tracking for email, can also be used to perform centralized management for the S-series. However, there are still no integrated policies or reporting across Web and email. At the back end, Cisco's SenderBase Network is a shared reputation network across email and Web, which aggregates, correlates, and analyzes URL and Internet protocol (IP) reputation data across protocols. On the IM side, Cisco provides pre-built signatures to detect commonly used IM protocols but lacks content filtering for non-HTTP based IM communications. The S-Series is a proxy device and does not control communication protocols outside HTTP. Cisco's long-term content security suite strategy includes a two-pronged approach: 1) Enable local sharing of reputation and threat information across email and Web, and 2) offer an integrated appliance or cloud options providing both email and Web filtering. Today, Cisco's solid technology in email and Web renders it an attractive choice for enterprises that have distinct needs for email and Web filtering. Going forward, Cisco should strengthen data security, application control, and significantly enhance its enterprise support for Web filtering.
- **Symantec/MessageLabs.** Symantec/MessageLabs is a Strong Performer in our content security suite evaluation. As a cloud service provider, Symantec/MessageLabs has good support for integrated threat analysis and malware detection. The company also has a separate IM filtering product, MessageLabs Professional Online Desktop (POD), which runs as a replacement to normal IM clients. POD performs content filtering and security controls and can federate with public IM systems. MessageLabs' email and Web services share antimalware functionality and integrated controls for common administrative tasks, but actual policy management and reporting remain largely separate today. Additionally, user directory integration needs to be set up for each content application. Symantec/MessageLabs does not have content control capabilities for protocols beyond SMTP and HTTP. We see many integration opportunities for Symantec/MessageLabs, including spanning threat analysis, directory integration, data security policies, and reporting. Symantec/MessageLabs reports a sizable research and development budget specifically allocated for developing a unified set of services. It remains to be seen whether the acquisition by Symantec will ultimately expedite or adversely impact some of the integration

initiatives. SRM professionals looking to outsource both email and Web filtering should consider Symantec/MessageLabs, as it is one of the few companies today that can offer both functionalities in the cloud and is therefore in a good position to offer integrated cloud services.

- **Microsoft.** Microsoft is a Strong Performer in the content security suite evaluation because of its support for IM and its consolidated product strategy. Today, Microsoft has a list of content security products, including Forefront Online Security For Exchange, Internet Security & Acceleration (ISA) server, and its IM product, Antigen For IM. These products come with separate lineages and are largely disjointed point products. Microsoft's next-generation security project, Stirling, promises to integrate security functions across edge, client, and server, as well as cloud services, and unite the policy management and reporting aspects of these products. Microsoft's product is best suited today for enterprises that are looking for a cloud solution for email filtering and archiving but that have on-premise requirements for other functions, such as filtering for IM, SharePoint, and other applications.
- **Google.** Google very narrowly qualified for the Strong Performer category; its overall suite evaluation score is close to the border of Strong Performer and Contender. Google's message security service and Web security service are two separate service offerings today; the latter is licensed from ScanSafe. The two services run from two separate infrastructures and do not share even threat analysis information. Although you can access the top level portal for email and Web from a single URL, actual policy management and administration are separate. Google offers an IM security service as an add-on module to its message security service, although at the time of writing, information about Google IM security service is no longer available from Google's Web site. Google's infrastructure is capable of delivering strong suite functionality, but we don't see a clear focus on content security suite services other than continued support for archiving and eDiscovery. Google's priority is providing security support for Google Apps. Today, the demand for message security may be higher than Web or IM, but Google must strengthen its capabilities in data security and compliance support for common content applications and increase management visibility — or risk losing ground on enterprise readiness.

Contenders Lack Suite Functionality

The two Contenders, McAfee and Marshal8e6, are on the edge between Strong Performer and Contender.

- **McAfee.** McAfee's email and Web appliance offers some rare platform functionality, such as integrated user directories, AV, and encryption engine. Customers can deploy the device once and choose to run any subsets of the combined modules. But despite being a consolidated product, the appliance ultimately received disappointing scores as a suite offering. First, although housing both email filtering and Web filtering modules, the appliance offers no integrated policy management and reporting capabilities. Second, users of both email and Web filtering modules don't receive any price incentives; you pay the same for the consolidated

appliance as you would if you bought two appliances separately, one for email and one for Web. McAfee also has very limited support for IM and other content protocols. More importantly, the two sides — email and Web — don't share threat analysis and reputation information, either through McAfee Threat Center or locally on the appliance. McAfee can improve its standing by taking these immediate actions: 1) integrating Secure Computing's TrustedSource with McAfee's own gateway products; 2) integrating the gateway product with McAfee's ePolicy Orchestrator to produce aggregated reports and dashboards; and 3) enhancing the data security side of the content security products, more specifically integrating capabilities like Reconnex.⁵

- **Marshal8e6.** Marshal8e6's two products — MailMarshal and WebMarshal — come from the same code base and share similarities, including interfaces and the ability to process text censor scripts. But MailMarshal and WebMarshal are fundamentally separate products today with few integration points between them. WebMarshal can detect and block common public IM protocols but has no IM filtering capability and cannot control content protocols beyond those tunneled over HTTP. Marshal8e6's threat analysis center is a common entity behind both MailMarshal and WebMarshal and performs blended threat analysis in the cloud. Marshal had plans for a unified management console between the Web and email products, which will allow automated sharing of scripts between the two sides and potentially support integrated policies. However, the recent merger with 8e6 throws a wrench in some of the integration plans, as the first order of business must be integration between the two companies. Companies should wait to see how the merger will affect Marshal's (and 8e6's) short-term product road map.

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 three of each vendor's current customers.
- **Forrester customer 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 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, Marshal8e6, 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. 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. See the April 16, 2009, "[The Forrester Wave™: Email Filtering, Q2 2009](#)" report.
- ² See the April 16, 2009, "[The Forrester Wave™: Web Filtering, Q2 2009](#)" report. Also see the April 16, 2009, "[The Forrester Wave™: Email Filtering, Q2 2009](#)" report.
- ³ 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.

- ⁴ Symantec's acquisition of MessageLabs will strengthen its Web filtering offerings. However, because the acquisition closed after our evaluation, we did not take it into account in the Wave evaluation.
- ⁵ Integration with ePo became available as a beta release download in December 2008 for the enterprise version of McAfee's email and Web security appliance.

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.