

April 16, 2009

The Forrester Wave™: Web Filtering, Q2 2009

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



April 16, 2009

The Forrester Wave™: Web Filtering, Q2 2009

Websense And Secure Computing Lead, With Trend Micro, Cisco Systems, MessageLabs, And McAfee Trailing As Strong Performers

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

with Robert Whiteley and Allison Herald

EXECUTIVE SUMMARY

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.

TABLE OF CONTENTS

2 **Web Filtering Is Essential To IT Security And Business Operations**

Hybrid Premise And Cloud Web Filtering Approaches Emerge To Meet Business Needs

3 **Web Filtering Evaluation Overview**

Evaluation Criteria Focused On Performance, Antimalware, And Product Vision

Evaluated Vendors Offer Varying Degrees Of Competency In Web Filtering

6 **Maturing Web Filtering Market Results In Large Gaps Among Vendors**

8 **Vendor Profiles**

Leaders Offer Broad Functionality And Best-Of-Breed Technologies

Strong Performers Need To Improve On Data Security And Enterprise Management

Contenders Lack Cohesive Vision Or Solid Capability

13 **Supplemental Material**

NOTES & RESOURCES

Forrester conducted lab-based evaluations in June and July 2008 with 10 vendor companies: Cisco Systems/IronPort, Google, Marshall8e6, 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™: Email 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

WEB FILTERING IS ESSENTIAL TO IT SECURITY AND BUSINESS OPERATIONS

In the past few years, the Web has become a critical social and business medium. Usage in and out of enterprises is increasingly common, and many workers require it for daily business operations. But with the rise in popularity comes a similar rise in Internet threats, which have also evolved to leverage the Web as its primary attack vector. Malware, which traditionally spreads via spam, now primarily reaches its victims through HTTP activity. Phishing, another prominent threat, is also a Web-centric threat.¹ Security and risk management (SRM) professionals are consequently turning to Web filtering — including URL filtering, antimalware, and content filtering — to protect their organizations from these Web-borne threats, allow visibility into employees' Web browsing activity, and prevent outbound leaks of sensitive content.

But it's not just about combating the next generation of threats. Companies that have an acceptable usage policy regarding Internet browsing also find Web filtering highly useful for gaining visibility into employee Internet activity, gauging business versus non-business bandwidth consumption, and enforcing usage policies. In fact, in Forrester's 2008 security survey of 2,148 enterprises and small and medium-size businesses (SMBs), 74% of the companies we surveyed reported deploying either passive monitoring or policy-based filtering for their Web communications.²

More specifically, security managers tell us that:

- **URL filtering is no longer sufficient.** Web filtering originally started out as URL filtering, and many organizations today still use nothing beyond simple URL filtering. URL filtering treats the Web and Web-borne threats in a static way. But many applications today, especially Web 2.0 applications, are virtually indistinguishable from each other when tunneled over HTTP. Deep content inspection is often the only means of telling them apart. For instance, RealMedia uses its own proprietary protocol over HTTP, and Apple QuickTime is only detectable when using real-time streaming protocol (RTSP) over HTTP.
- **Data-centric control is becoming essential to companies.** Applications such as Web mail, blogs, wikis, and social networking provide an easy vehicle for content to escape the organization. Without proper monitoring and control, Web communication can become a hotbed for information leakage. Deep content analysis and data-centric control is on many users' wish lists, yet Web filtering products that offer good data leak prevention (DLP) functionality are few and far between.
- **Mobile and remote filtering are increasingly important.** "Road warrior" workers today increasingly spend time outside of the corporate boundary. Distributed organizations with satellite offices are seeking a Web filtering approach without requiring expensive traffic backhauling. A gateway-centric architecture is ill-equipped for a dynamic or distributed environment since not all employees are guaranteed to funnel through any particular site. Alternative solutions, such as cloud-based filtering or a hybrid premise- and cloud-based deployment, allow branch office and mobile workers to access the Internet directly but at the same time permit the corporation to retain centralized policy management.

Hybrid Premise And Cloud Web Filtering Approaches Emerge To Meet Business Needs

Organizations want control over Web traffic for both security and management reasons. Often these requirements come from the business, not the security side of the house. This means that Web filtering is increasingly fulfilling a business role rather than a security-centric role. Vendors of Web filtering technologies are struggling to keep up with these changing business requirements and enhance offerings with deep content inspection and Web 2.0 application decoding.

Because of these requirements, we're seeing interest in Web filtering software-as-a-service (SaaS) offerings. The accelerated momentum of cloud-based email filtering has many asking the same question for Web filtering. Indeed, many vendors are entering or eyeing the Web filtering SaaS market. However, the real-time nature of Web traffic means filtering in the cloud is a challenging proposition for vendors. As a result, we see two distinct camps:

- **The SaaS-only or cloud approach.** Distributed organizations are the first to realize the benefit of cloud-based filtering: Utilizing cloud infrastructure allows each branch location to go directly to the Internet but under centralized policy control and management. But there's a catch — to fully realize cloud benefits for a global organization, the cloud vendor must install data centers in far corners of the world. It's hardly a cost-saving measure if an office in Africa has to redirect all its traffic through a cloud data center in Europe. As a result, security and business executives are responding with tepid enthusiasm, and Google, MessageLabs, and Webroot Software see many more email filtering customers than Web filtering customers. Purewire and Zscaler are still too new for one to properly gauge their growth.
- **The emerging hybrid approach.** So-called hybrid architectures allow remote offices (or mobile workers) to utilize cloud filtering to go directly to the Internet, while the large headquarter offices use some form of on-premise filtering mechanism. The cloud and the on-premise deployments are tightly integrated in management control, reporting, and threat intelligence but not in traffic redirection. Such an architecture delivers centralized policy management, allows traffic to be served where it originates, and leverages the cloud for what it does best: community intelligence. A good example is Trend Micro's Smart Protection Network, which integrates with the firm's gateway and endpoint technologies.

In the longer term, when email SaaS becomes more universally deployed, Web filtering SaaS will become more attractive because you will be able to retrieve your email and Web reports from one place — the cloud. In the meantime, however, we think the hybrid approach holds much promise and may even eclipse the growth of pure SaaS for Web filtering.

WEB FILTERING EVALUATION OVERVIEW

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

Evaluation Criteria Focused On Performance, Antimalware, And Product 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 53 criteria, which we grouped into three high-level buckets:

- **Current offering.** To assess product strength, we evaluated each vendor offering against four groups of criteria: Web filtering, outbound content filtering, Web reporting and management, and performance and operations. We complemented this analysis with feedback from customer references.
- **Strategy.** We reviewed each vendor's Web filtering strategy by evaluating each vendor against criteria based on two areas: product strategy and partners. This evaluation took into consideration elements such as advanced research and development efforts, planned enhancements, and integration partners.
- **Market presence.** To establish a vendor's market presence, we examined its Web filtering install base, including international presence and market segment diversity, as well as the company's yearly revenue and growth.

Evaluated Vendors Offer Varying Degrees Of Competency In Web Filtering

Forrester included 10 vendors in the assessment: Cisco Systems/IronPort, 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:

- **Basic Web filtering functionality, including URL filtering and antimalware.** With the exception of Microsoft, URL filtering and antimalware occupy the core of the vendors' Web filtering products. Almost all the solutions we evaluated utilize an extensive URL filtering database and some form of antimalware technology with varying maturity.
- **Deep content processing for Web communication.** Capabilities to process downloaded and uploaded content is important for malware detection, content leak protection, and compliance policies. We look for vendors that have at least deep content processing capabilities for download content. Outbound content leak protection was preferred but not required.
- **Brand recognition and sizable market presence.** Given the current economic environment, 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 email inquiries.

- **Filtering capabilities beyond Web — either in email or instant messaging.** Because this Forrester Wave evaluation is part of an integrated evaluation with two other evaluations — The Forrester Wave™: Email Filtering, Q2 2009, and The Forrester Wave™: Content Security Suites, Q2 2009 — and because we believe the content security market is moving toward consolidated content security suites, each of the vendors we chose has security filtering products in at least two of the three primary content channels.³ These channels are email, Web, and instant messaging.⁴ Some pure-play vendors that do just Web filtering, such as Blue Coat Systems, are not included in this Forrester Wave evaluation.

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 S-Series, Web Security Appliance	6.1
Google	Web Security for Enterprise	—
Marshal8e6	WebMarshal	6.1
McAfee	Email and Web Security Appliance 3200	5.0
McAfee/Secure	Secure Web Webwasher Web Gateway Security Appliance	6.7
McAfee/Secure	Secure Web Protection Service	6.7
Microsoft	Internet Security & Acceleration (ISA) Server 2006	5.1
Symantec	Scan Engine	5.2
Symantec/MLabs	Web Security Services	2.0
Trend Micro	InterScan Web Security Suite (IWSS)	3.1
Websense	Web Security Gateway	7.0

Vendor selection criteria

Does the solution have some form of URL filtering, antimalware, and content filtering for Web communications? How well does the solution support data cleansing?

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

Does the vendor have filtering capabilities beyond Web (e.g., for either email or instant messaging)?

Source: Forrester Research, Inc.

MATURING WEB FILTERING MARKET RESULTS IN LARGE GAPS AMONG VENDORS

The evaluation uncovered a market that is still maturing, with only two vendors qualified as Leaders (see Figure 2). We see large differences among vendor offerings, primarily in the areas of deep content analysis, mobile filtering, and product strategies. Our evaluation found that:

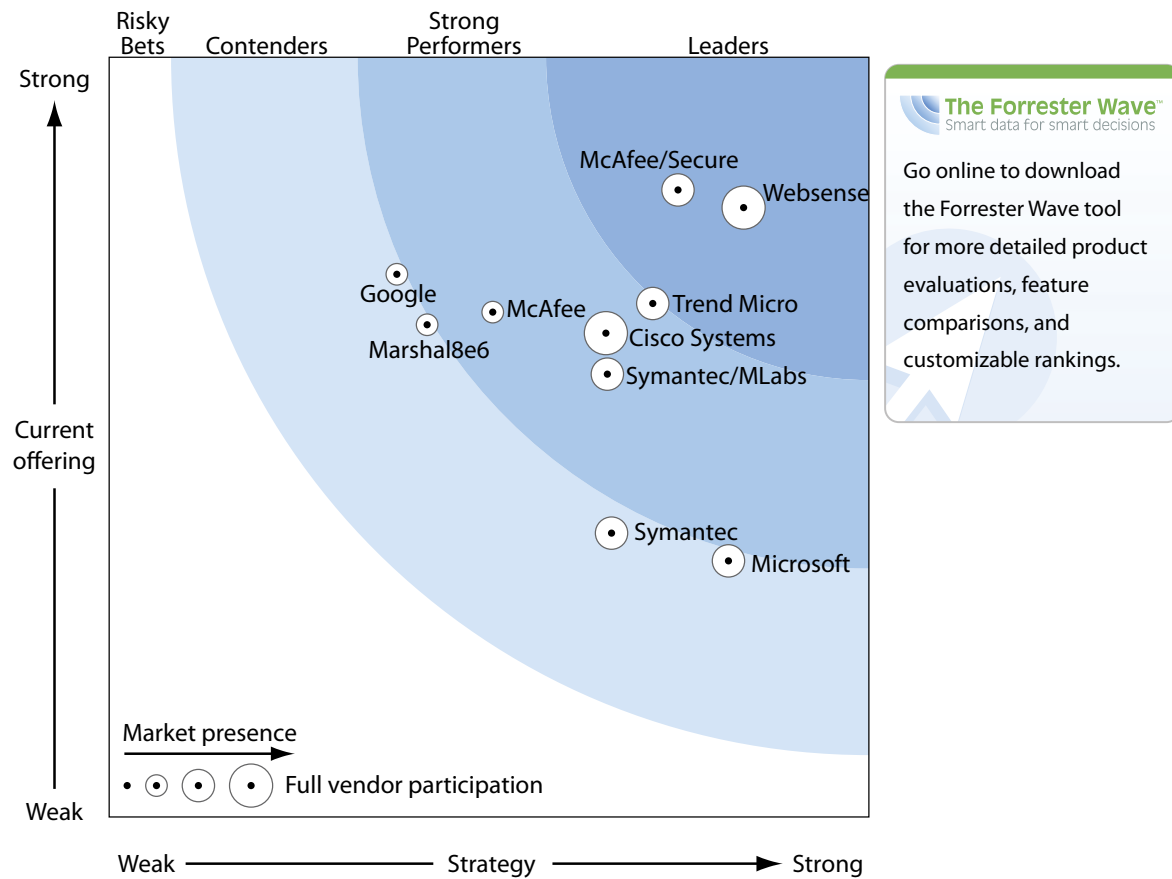
- **Websense and McAfee/Secure Computing lead the pack.** Websense and McAfee/Secure Computing distinguish themselves as Leaders in this evaluation. Websense is a software vendor, while Secure Computing sells a Web filtering appliance. Websense leadership comes from having the broadest solution on the market today, encompassing URL filtering, antimalware, DLP, and mobile filtering. Websense also owns many best-of-breed technologies, including its URL list and DLP technologies. Secure Computing's Secure Web appliance scored well in many aspects, especially its TrustedSource reputation system, data analysis capability, and enterprise management.
- **Trend Micro, Cisco, Symantec/MessageLabs, and McAfee are a few notches below.** Cisco and McAfee deliver Web filtering in an appliance form factor. Trend Micro's Interscan Web Security Suite (IWSS) product spans software and virtual appliance, while MessageLabs offers Web filtering in the cloud. These vendors lack good outbound content control.⁵ Many of them also lack support for remote/mobile filtering and essential enterprise management features like delegated management. As such, these vendors received evaluations that are a few notches below the top-ranked Websense and Secure Computing.
- **Google, Marshal8e6, Microsoft, and Symantec lag behind.** Google's Web filtering services (licensed from ScanSafe) and Marshal8e6's WebMarshal software turned in solid scores for their core Web filtering capabilities but fell short on strategy. Symantec's Scan Engine and Microsoft's Internet Security & Acceleration (ISA) Server can only be described as partial Web filtering products, as they do not perform the entire range of functionality required for Web filtering. However, the latter two scored well in their forward-looking strategy and product road map. Symantec's acquisition of MessageLabs should strengthen its position in the Web filtering market. Microsoft has been working on its Stirling project and on its version of a full Web filtering product, the Microsoft Threat Management Gateway.

There are many other Web filtering vendors that Forrester did not include in this evaluation, such as Aladdin, Barracuda Networks, Blue Coat Systems, BorderWare Technologies, CA, Clearswift, ContentWatch, Finjan, Fortinet, Mi5, Optnet, Purewire, St. Bernard Software, Webroot Software, and Zscaler.

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 Web 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™: Web Filtering, Q2 '09



Source: Forrester Research, Inc.

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

	Forrester's Weighting	Cisco Systems	Google	Marshall86	McAfee	McAfee/Secure	Microsoft	Symantec	Symantec/MLabs	Trend Micro	Websense
CURRENT OFFERING	50%	3.23	3.62	3.29	3.36	4.17	1.75	1.90	2.96	3.44	4.05
Web filtering	37%	3.14	3.36	2.96	3.05	4.55	1.79	1.60	2.36	3.45	4.10
Outbound content filtering	8%	0.00	1.79	2.80	2.82	1.54	0.90	1.38	0.00	1.28	1.73
Web reporting and management	20%	3.25	3.11	3.67	4.14	3.96	0.92	1.20	3.15	3.29	4.70
Performance & operations	20%	3.70	5.00	3.14	3.28	4.28	2.48	2.72	4.68	3.78	3.70
Client reference scores and feedback	15%	4.55	4.05	4.05	3.45	4.75	2.25	2.75	3.50	4.30	4.75
STRATEGY	50%	3.25	1.87	2.08	2.51	3.73	4.05	3.30	3.26	3.58	4.15
Product strategy	85%	3.25	1.75	1.75	2.25	3.50	4.00	3.00	3.50	3.50	4.00
Partners	15%	3.25	2.55	3.95	4.00	5.00	4.30	5.00	1.90	4.00	5.00
MARKET PRESENCE	0%	4.12	2.36	2.42	2.32	3.68	3.88	3.28	3.04	3.88	4.16
Installed base	60%	4.20	2.20	2.70	3.60	4.00	4.60	3.60	3.20	4.60	4.40
Revenue	40%	4.00	2.60	2.00	0.40	3.20	2.80	2.80	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 Broad Functionality And Best-Of-Breed Technologies

This evaluation uncovered only two Leaders. This is a market that is still maturing, so it's not surprising to see only a few players clearly leading the rest of the market. These two Leaders are:

- Websense.** The largest market share holder in the Web filtering market, Websense also has the most mature technology. Websense is the top-ranked vendor in this evaluation because of its broad functionality and innovative strategy. Websense now sells an appliance version of its offering in addition to its original software. Of all the vendors we evaluated, Websense has the best business accessibility in that it offers granular reporting and easy access to business analytics. The product also comes with excellent support for enterprise management, such as directory integration, multi-level reporting, and expressive policies. Websense offers good functionality for off-network Web filtering, a feature that many vendors currently lack. On the threat analysis side, Websense's ThreatSeeker lab is one of the best in analyzing Web threats. Websense's strategy includes investing heavily in Web 2.0 application processing technologies. Its recent acquisition of Defensio gives it a new cloud-based capability to process outbound blog content. We expect that this cloud infrastructure will no doubt take on more content filtering

capabilities going forward. Forrester sees Websense as an ideal solution for large enterprises that are diverse. To continue to stay ahead of the industry, Websense needs to expand its footprint outside of enterprise software and augment its URL-category-centric mentality with more fine-grained data security controls.

- **McAfee/Secure Computing.** Secure Computing's Secure Web appliance edged out Websense to receive the highest score on the technology portion of the evaluation, thanks to its innovative Web reputation technology, high-performing appliance, and reasonable per-user pricing. Secure Web is available primarily as a gateway appliance, but also as SaaS and server software. Secure's TrustedSource reputation technology is one of the best in the industry, comprising innovative distributed processing and data correlation technologies. Secure Web also offers excellent enterprise management support, including user directory integration, comprehensive reporting, and highly customizable policy management. Secure's antimalware technology includes licensed engines from McAfee and Sophos, as well as its own behavioral and heuristics detection engine geared specifically for Web malware. Secure Web uses a master-slave architecture to provide scalability and central management in a distributed setting. Its throughput and scalability performance are among the best in this evaluation. Secure also provides an endpoint software module that tunnels Web traffic through the nearest corporate Secure Web appliance, hence providing mobile filtering capability. To retain its Leader position, Secure Web needs to enhance outbound content protection, strengthen its Web 2.0 application control capability, and continue to expand its market presence. We are waiting to see how McAfee will assimilate Secure's product lines into the company, especially given that McAfee has its own gateway Web filtering product (see McAfee in the Strong Performers section below).

Strong Performers Need To Improve On Data Security And Enterprise Management

- **Trend Micro.** Trend Micro's InterScan Web Security Suite (IWSS) is offered as software for Windows, Linux, and Solaris, as well as in a software virtual appliance version. IWSS is the only hybrid Web filtering product in this Forrester Wave evaluation. This comes from integration with Trend's Smart Protection Network (SPN) in the cloud. Trend's URL database, malware signatures, and Web reputation all live in the SPN, while the on-premise software performs policy-based filtering, contributes intelligence into the cloud, and houses a small cache of URL and reputation information. We especially like this approach, which allows security teams to leverage many benefits of cloud computing without requiring the redirection of Web traffic. In addition, the SPN houses information across email, Web, gateway, and endpoints, giving the product near real-time threat intelligence and correlated knowledge across the different vectors. As a result, IWSS scored fairly well in the Current Offering section of the evaluation. What IWSS lacks is https scanning, outbound content protection, and other enterprise support features like customized reporting and delegated management. Trend offers a separate endpoint software module for off-network filtering but doesn't support integrated policies between the gateway and remote endpoints. We think Trend's IWSS product is a good alternative for both enterprise

and SMB customers. Forrester anticipates IWSS will continue to capitalize on the advantages of the Smart Protection Network, incorporating the same strategy to support mobile endpoints. In addition, Trend Micro should enhance support for enterprise management support and break out of its security-centric mentality to offer a broader set of functionality such as Web 2.0 application control for enterprises.

- **Cisco Systems.** The engineers at Cisco know how to build a network security box, and the IronPort S-Series is no exception. The appliance reports excellent throughput numbers and comes with good support for scalability and high availability. It also has decent URL filtering and real-time reporting, and it's very easy to install and start up. But beyond malware signature scanning, the S-Series doesn't provide deep content analysis and filtering for inbound and outbound Web traffic. It also has limited control capabilities for protocols that do not tunnel over HTTP. In addition, the S-series lacks support for remote and mobile filtering. The biggest complaint from customers about the S-Series has been its weak support for enterprise reporting, delegated management, and customized policies. IronPort's SenderBase reputation network, though hugely successful on the email side, has also seen challenging times when migrating to incorporate Web reputation. To stay competitive, Cisco needs to enhance the S-Series' enterprise management support and incorporate content analysis for Web traffic. Most importantly, Cisco needs to sharpen its focus on innovating Web filtering technology. Cisco recently announced its cloud email filtering offering. We are waiting to see whether and when Cisco will expand its cloud infrastructure to cover Web filtering.
- **Symantec/MessageLabs.** MessageLabs' Web filtering service offering is still somewhat new; the service was introduced in 2007. At the close of this evaluation (end of October 2008), it had amassed 1,800 clients, a far cry from its email filtering customer base of more than 19,000. As a service provider, MessageLabs reported excellent throughput, scalability, and reliability numbers. Customers of its Web filtering services also benefit from its Skeptic engine running in the cloud, conducting behavior, heuristics, and polymorphic malware analysis. However, the service has a very limited form of reputation-based filtering, no capability for outbound content leak protection, and no support for mobile filtering. More work is needed to supply a full set of enterprise management tasks, including policy violation reporting, customized policies, and delegated management. We see MessageLabs' services as being attractive to midmarket customers who are security-minded. The acquisition of MessageLabs by Symantec offers many exciting opportunities. In the near term, we expect MessageLabs' Web filtering service to benefit from integration with Symantec's Global Intelligence Network (GIN) and data security products (Vontu). Also, MessageLabs will be able to take advantage of Symantec's vast partner and reseller network.
- **McAfee.** Although a strong performer itself, McAfee's email/Web appliance is a notch below the others in the same category. The appliance uses Secure Computing's SmartFilter URL database and augments it with McAfee's own SiteAdvisor reputation system. McAfee has solid data-filtering capabilities in the appliance, providing some level of outbound content protection

for Web communications. This appliance also offers good enterprise management support, where its reporting and administration interface received solid scores, with good support for customization and role-based administration. Additionally, Forrester likes that the appliance has a range of architectural options. These options include explicit proxy, transparent bridge, router, and Internet Content Adaptation Protocol (ICAP) mode. However, the 1U appliances lack support for clustering configuration and centralized policy management (the blade version is an exception), which makes it difficult to be deployed in a large distributed environment. The appliances also have limited support for user productivity management and mobile filtering. With the acquisition of Secure Computing and previously of Reconnex, McAfee now has a set of strong content security technologies in-house. Utilizing these technologies going forward means strong synergy, like the one between TrustedSource and SiteAdvisor. Similarly, we see how Secure's products can benefit from integration with other McAfee initiatives like Reconnex and Artemis. In the long run, however, we expect McAfee's own gateway content security product will lose out to Secure's similar products.

Contenders Lack Cohesive Vision Or Solid Capability

- **Google.** Google resells its Web filtering service from ScanSafe. This kind of OEM relationship is tricky because it doesn't let you have direct control over technology innovation and product direction. The ScanSafe service received decent scores for its technology, but Google loses points for not having its own in-house Web filtering service. Among the categories that the service is lacking, Web reputation and content analysis are the two big ones. Google also has very little support for outbound content protection for Web communication. Additionally, Google's support for enterprise management is primitive — the interface allows very little customization and flexible management. The filtering service does provide a tamper-proof endpoint agent, which routes Web traffic to the nearest cloud scanning point. We estimate that Google's total Web filtering user seat today is slightly more than 10,000, which is a mere fraction of the size of its secure messaging install base. One of Google's channel partners told us that for every seven or eight inquiries they get on email filtering, they get one inquiry on Web filtering. Perhaps that's why Google recently stopped selling this service through its channels. As an ardent cloud computing advocate, Google must one day own this technology in-house. In the meantime, Google must enhance its enterprise support and build a strong in-the-cloud threat analysis center across real-time email and Web threats.
- **Marshal8e6.** Marshal8e6's WebMarshal is delivered as a software product. Like its email product, WebMarshal also has excellent support for flexible policy definition and comprehensive reporting. As a result, WebMarshal is one of the few products we evaluated that has a good approach for user productivity control, beyond being a security product. But unlike its email product, Marshal8e6 is not as successful in marketing its Web filtering product. WebMarshal's security-centric technology, including Web reputation, deep threat analysis, and performance of the product, is not quite on par with some of the leading products. In addition,

WebMarshal has no support for outbound content protection beyond limited lexical analysis and mobile filtering capabilities. In our evaluation, we found that the company's vision and strategy for its Web filtering product doesn't meet most enterprise requirements. We were therefore not surprised to learn soon after that Marshal was to merge with 8e6, a company with a much larger market share in Web filtering. It's not certain how long the combined company will continue to innovate and support both Web filtering products. In our opinion, a more likely outcome is that 8e6 will incorporate some of Marshal's strong suits, such as its policy engine, antimalware, and productivity management, but will eventually stop supporting WebMarshal.

- **Microsoft.** In terms of pure Web filtering functionality, Microsoft submitted its ISA server. We found this to be the weakest current offering, yet it provides one of the best strategies moving forward. This is because ISA, although widely deployed and able to perform some Web filtering tasks, is not meant to be a Web filtering product per se and doesn't support the whole range of Web filtering functionality. For instance, one can manually instruct ISA to block communication to and from a certain URL (or a list of URLs), but ISA doesn't come with a native URL filtering list. ISA can do state-based filtering on HTTP and HTTPS connections but has very few application layer inspection capabilities. There is no quota management, mobile filtering, or data leak protection. Microsoft knows its weakness in this area and is working to remedy it. The next generation of ISA is Microsoft's Threat Management Gateway, which promises to deliver not only the whole range of Web filtering functionality but also integration with AD, Stirling (Microsoft's next-generation enterprise security suite and security management system), and Microsoft's endpoint locking functionality. Although its content security strategies have been less than focused in the past, Microsoft is a market mover and is capable of shaping the industry with new products and technologies.
- **Symantec.** Symantec submitted its Scan Engine product for this evaluation. Scan Engine is out-of-band software that provides a URL list and antimalware functionality through an ICAP interface but has no traffic manipulation capability of its own. You can integrate Scan Engine with an ICAP-compliant Web proxy to complete the filtering action. As such, Scan Engine is not a self-contained Web filtering product. Because it doesn't perform direct traffic manipulation, Scan Engine doesn't integrate with user directories and can't support user/group-specific policies. Scan Engine doesn't maintain URL reputation information, nor does it provide integration with external reputation databases. The product also doesn't provide deep content analysis beyond dynamic URL categorization and malware scanning. Scan Engine is best used by organizations that already have a Web proxy and want to add URL filtering and antimalware to the proxy architecture. As aforementioned, this Forrester Wave evaluation began and closed before Symantec officially acquired MessageLabs, which does have a full Web filtering offering. In addition, we recently learned that Symantec is to announce the acquisition of Mi5, a Web filtering gateway company. This latest development should further propel Symantec forward in the Web filtering market.

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 one 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 scenario(s), 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 inquiries.** Forrester's end user inquiries is 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 The past year saw significant proliferation and continued evolution of cybercrime on the Internet. Security and risk professionals are increasingly challenged to respond to the dynamic and ever-changing cyberthreats, yet many feel ill-equipped to do so. Vendor solutions help, but before you consider yet another defense technology, you need to understand what likely threats you will be facing in the near future, how that impacts your organization's security posture, and where you should focus your limited resources to reduce risk. Forrester's 2008 look at the threat landscape presents an investigation across vendor data, public reports, and survey statistics. Our analysis into malware, spam, phishing, and emerging threats reveals an extremely dynamic threat landscape, fueled by an organized underground economy. Trust on the Internet is increasingly elusive as more and more trusted sites become unwitting participants in proliferating attacks. Web 2.0 emerges as a major threat factor. See the June 25, 2008, "[Threat Report: The Trends And Changing Landscape Of Malware And Internet Threats](#)" report.
- ² In Forrester's Enterprise And SMB Security Survey, North America And Europe, Q3 2008, we asked 2,014 security decision-makers in North America and Europe, "How does your organization control your users' Web browser activity?" Forty-five percent reported that they deploy policy-based filtering, 29% said they use passive-monitoring without filtering, and another 11% indicated that as a company policy, they block the entire Web communication protocol.
- ³ 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. 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. See the April 16, 2009, "[The Forrester Wave™: Content Security Suites, Q2 2009](#)" report.

⁴ 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, 2008, "[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.

⁵ MessageLabs will soon integrate Symantec's Vontu technology with its Web filtering services, which will amend its outbound data control deficiency.

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.