

## Magic Quadrant for E-Mail Security Boundaries

Arabella Hallawell, Peter Firstbrook

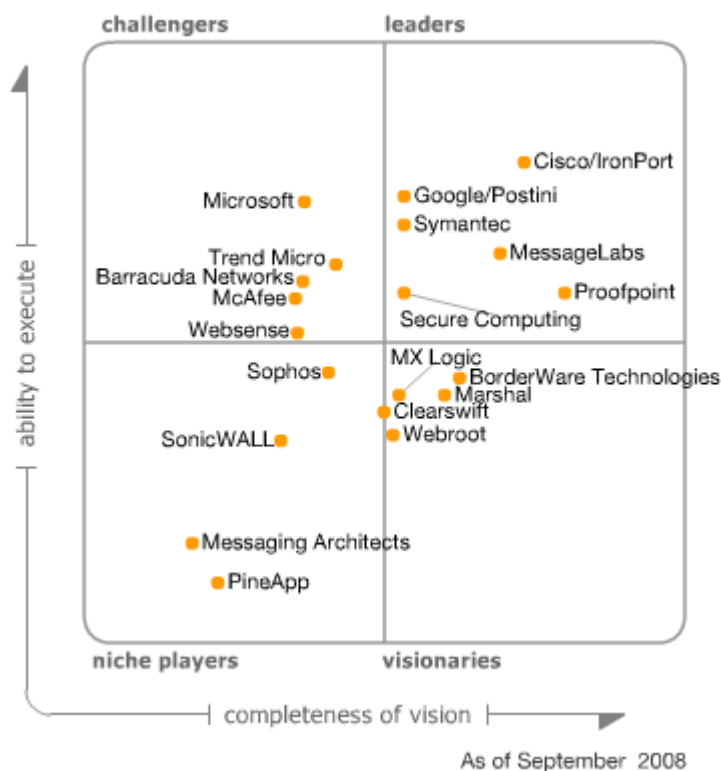
The e-mail security market is maturing, but speed and breadth of spam detection, and management and reporting capabilities, continue to differentiate vendors.

## WHAT YOU NEED TO KNOW

- Spam filtering effectiveness, the quality and flexibility of the management console, and reporting options should dominate buying criteria.
- Outbound content filtering, prebuilt dictionaries and custom capabilities, combined with policy-based encryption support, increasingly differentiate solutions.
- E-mail security solutions are available in various delivery models. Appliances and software as a service (SaaS) are seeing the fastest growth.
- E-mail threats are often part of a wider threat ecosystem. Expect leading solutions to use data sources from multiple sources (such as infected PCs and malware infections on Web sites and applications).

## MAGIC QUADRANT

Figure 1. Magic Quadrant for E-Mail Security Boundaries



Source: Gartner (September 2008)

## Market Overview

This document was revised on 16 September 2008. For more information, please see the [Corrections page](#) on gartner.com.

The e-mail security market is rapidly maturing, yet continues to show strong growth and remains a "must have" security purchase. Marked consolidation by infrastructure players has occurred during the past two years; Cisco acquired IronPort in January 2007, and Google acquired Postini in July 2007. This follows the acquisitions by Secure in 2006 (of CipherTrust) and Microsoft (FrontBridge Technologies) in 2005. Rumors abound that the remaining stand-alone players will be picked up by infrastructure and larger players because this market has become significant, with fast growth.

There are several indications that demand will continue. Spam volumes continue to grow (estimated at more than 90% of e-mail in North America), threats are escalating and outbound compliance initiatives drive further spending. Spam campaigns using new techniques to bypass filters (as evidenced by image, PDF and backscatter spam), cause upticks in spam rates as the vendors race to find a fix to the problem. Indeed, the industry has begun to resemble the antivirus (AV) industry, where effectiveness is measured by how quickly the vendor can keep pace with the ever-changing threats. A particularly profound change is the role that e-mail security threats are playing in the larger security threat ecosystem. Web-based malware has become a particularly potent vector for infection, and users unwittingly download malicious code onto their machines, which are then used to send out scam mail. Indeed, this trend has important consequences for buyers and sellers of e-mail security solutions. An e-mail solution will not be effective at tackling malware-bearing e-mail (that is, one that leads to a fraudulent Web site or was sent via a fraudulent machine), if they are investing in research and product capabilities to detect these sources. Further, interest in e-mail archiving and disaster recovery is accelerating in the small to midsize enterprise market. Archiving and disaster recovery SaaS services, while often a separate project and budget to e-mail security, are in particular demand.

Compliance has become a more important growth driver in e-mail security spending. Companies are investing in solutions to block and typically encrypt sensitive content in e-mail. Policies to protect sensitive data need to be replicated over HTTP, especially for Web e-mail utilities, such as Hotmail, Gmail and those within social networking tools. The messaging group will be increasingly involved in rolling out policies for Web-based e-mail and will drive the convergence of e-mail and Web security gateway solutions through 2010.

The e-mail security market is one of the few security markets where all three delivery models (software, appliance, and SaaS or managed services) are available. Appliances and SaaS models are seeing the fastest growth, with more than 30% annual growth for many companies selling e-mail security appliances or services. Some companies are exploring, by accident or design, hybrid options, whereby a SaaS service is used to clean unwanted inbound e-mail for spam and viruses, and an on-premises solution is used for outbound content filtering and custom requirements.

An emerging delivery model is the virtual appliance, which is especially attractive in the e-mail security world, because spam volumes and campaigns necessitate increased hardware investments. Increasingly, companies will expect a choice of delivery models, and leaders should expect to supply appliances and services by 2010.

## **Market Definition/Description**

The market is defined by vendors that provide enterprise protection against inbound e-mail threats, and fulfill outbound policy requirements at the SMTP gateway. The e-mail security market is estimated at \$1.2 billion in 2007, growing at 30%. The strongest demand is for the appliance and SaaS delivery models. Gartner expects SaaS to represent 30% of the e-mail security market by year-end 2008.

## Inclusion and Exclusion Criteria

- The solution must have its own proprietary capabilities to block or filter unwanted e-mail traffic. Supplementing with third-party technology is acceptable.
- The solution must provide e-mail virus scanning via its own or a third-party AV engine.
- The solution must provide basic intrusion prevention.
- The solution must offer e-mail encryption functionality beyond Transport Layer Security (TLS) (via its own or via a third-party relationship).
- The solution must offer the ability to scan outbound e-mail according to a set of basic vendor-supplied dictionaries and common identifiers (for example, U.S. Social Security number [SSN], credit card and bank account numbers, and routing numbers).
- Vendors must have at least 2,000 direct (not via OEM) enterprise customers in production for their e-mail security boundary products.
- We also expect a vendor to have appeared on a Gartner client shortlist or in production (presented to us via inquiry) in the preceding 12 months.

### Added

- Webroot
- PineApp
- Messaging Architects
- MX Logic

### Dropped

- Tumbleweed did not meet the minimum customer number threshold for inclusion in this year's Magic Quadrant. Tumbleweed has a long history in the e-mail security market, notably in providing outbound content filtering and e-mail encryption, and the company's installed base has been skewed toward larger enterprises. The company announced its acquisition by the Sopra/Axway group in June 2008. The road map for the e-mail security business will not be clarified until the deal is finalized.

## Evaluation Criteria

### Ability to Execute

Overall viability was given a heavy weighting. Overall viability was considered not only in terms of the overall revenue, channel reach, management team and resources of the vendor, but also the specifics of the e-mail security unit at each company. We also took into consideration our evaluation of the revenue and market share of each vendor. Although revenue, installed base, market size and growth rates relative to competitors are not absolute indicators of performance, they do signify success in the marketplace (be it from any combination of marketing, sales or engineering perspectives) and indicate the likelihood that the vendor will continue to invest resources in the product line. We also took into consideration the focus and transitions of the teams in charge of engineering, management, marketing and sales for the relevant product lines.

Market responsiveness measured the track record of the vendor in responding to features, functionality and service requirements of customers. This weighting takes into account a vendor's performance over time, but performance during the past 24 months was evaluated most significantly. Examples include the timely inclusion of key functionality, such as reporting functionality (Web-based GUI, intuitiveness of GUI, breadth of custom reports and central management of quarantines), and new, effective detection techniques for emerging threats, such as image and backscatter spam. Customer experience is a related, but distinct category. Here, we evaluated the customer experience when dealing with the vendor, be it for a product, service, or customer service and support. We incorporated research and reference call data on support responsiveness and timeliness, quality of releases and patches, and general experiences when installing and managing the product and service on a day-to-day basis.

**Table 1. Ability to Execute Evaluation Criteria**

<b>Evaluation Criteria</b>	<b>Weighting</b>
Product/Service	low
Overall Viability (Business Unit, Financial, Strategy, Organization)	high
Sales Execution/Pricing	no rating
Market Responsiveness and Track Record	high
Marketing Execution	standard
Customer Experience	high
Operations	no rating

Source: Gartner

## **Completeness of Vision**

We heavily weighted the offering strategy of the vendor in the completeness-of-vision criteria. We divided this product section into several subcriteria focused on specific functionality that Gartner deemed the most important. Management and reporting functionality, anti-spam effectiveness (which incorporated Gartner customer, reseller and other Gartner-conducted informal survey feedback on overall anti-spam effectiveness, investment in research and techniques). We also created a subcategory for connection/reputation functionality. Connection management is a vital component to any effective e-mail security solution. There is significant differentiation among vendor investment and capabilities whereby connection management capability justified its own category. Indeed, we believe connection management innovation and effectiveness is a leading indicator of e-mail security threat detection from this point on. Other subcriteria include outbound functionality, which includes attachment filtering and policies, and data leak prevention (DLP) capabilities. We also established separate criteria for encryption and investment in Web-based malware research and protection.

Other functionality or solutions relevant to the buyer in the target market of the supplier, such as archiving, disaster recovery and file transfer, were also taken into account. We also established delivery model capabilities as a subcriteria. Our clients overwhelmingly indicate that they are looking for choices and combinations of delivery models that include appliances, virtual appliances, SaaS and managed services. Vendors that are investing in multiple delivery mechanisms were given higher scores.

**Table 2. Completeness of Vision Evaluation Criteria**

<b>Evaluation Criteria</b>	<b>Weighting</b>
Market Understanding	no rating
Marketing Strategy	no rating
Sales Strategy	no rating
Offering (Product) Strategy	high
Business Model	no rating
Vertical/Industry Strategy	no rating
Innovation	low
Geographic Strategy	no rating

Source: Gartner

## Leaders

Leaders are performing well, have a clear vision of market direction and are actively building competencies to sustain their leadership positions in the market. Companies in this quadrant offer a comprehensive and proficient range of e-mail security functionality, and show evidence of superior vision and execution for current and anticipated customer requirements. Leaders typically have relatively high market share and/or strong revenue growth, own a good portion of their threat or content-filtering capabilities, and demonstrate positive customer feedback for anti-spam efficacy, and related service and support.

## Challengers

Challengers execute well, but they have a less-defined view of market direction, and, therefore, they may not be aggressive in preparing for the future. Companies in this quadrant typically have strong execution capabilities, evidenced by financial resources, a significant sales and brand presence garnered from the company as whole, or other factors. However, challengers have not demonstrated as rich a capability or track record for their e-mail security product portfolios as vendors in the Leaders quadrant.

## Visionaries

Visionaries have a clear vision of market direction and are focused on preparing for that, but may be challenged to execute against that vision because of undercapitalization, market presence or experience, size, scope and so forth.

## Niche Players

Niche players focus on a particular segment of the client base, as defined by characteristics such as a specific geographic delivery capability or dedication to a more-limited product set. Their ability to outperform or be innovative may be affected by this narrow focus. Vendors in this quadrant may have a small or declining installed base, or be limited, according to Gartner's criteria, by a number of factors. These factors may include limited investment or capability to provide e-mail security threat detection organically, a geographically limited footprint or other inhibitors to providing a broader set of capabilities to enterprises currently and during the 12-month planning horizon.

Inclusion in this quadrant does not reflect negatively on the vendor's value in the more narrowly focused service spectrum.

# Vendor Strengths and Cautions

## Barracuda Networks

### Strengths

- Barracuda is a California-based privately held company with more than four years of e-mail security experience. The company strategy is focused on growing a high-volume appliance business through the channel and caters largely to small or midsize businesses (SMBs).
- The company has demonstrated strong growth and relatively significant market share.
- The company has focused its investments on e-mail security and, more recently, has branched out into archiving, Web security, bandwidth management and Web application firewall appliance markets — all of which are relevant to its target market.
- Customers and resellers report that the products are easy to install and use.
- Anti-spam effectiveness is reasonable, although the company relies heavily on tweaking open-source tools.
- Reputation management is addressed by the use of open-source and third-party data, as well as its own resources — in particular, intent analysis (checks URLs against Domain Name System settings) and sender profiling.
- The management console and GUI are Web-based and intuitive for a non-security-focused administrator.
- The company has good international presence, particularly in Asia/Pacific.

### Cautions

- The e-mail security products use open-source technologies, such as ClamAV and SpamAssassin, although Barracuda augments spam and malware detection with its own rules.
- The company has come under patent fire with Trend Micro, and unsuccessfully tried to acquire Sourcefire, which owns ClamAV IP, in May 2008.
- Occasionally customers report that the appliances do not always scale in large environments or during peak performance periods, although that may be linked to an inappropriate choice of appliance capacity.
- There are sporadic reports of patchy customer support, although Barracuda has made customer service support a focus throughout the company.
- Relatively few resources are dedicated to research and development threat capabilities.
- There is a limited ability for custom policies, and it's burdensome to set up per-domain settings.

## BorderWare Technologies

### Strengths

- BorderWare Technologies is one of the few remaining vendors in this market that is primarily dedicated to e-mail security.
- Anti-spam effectiveness has been significantly improved with the introduction of the behavior-based BorderWare ReputationAuthority, which blocks more than 90% of spam at the connections layer.
- The product can also integrate reputation with Cisco and F5 to drop connections even earlier in the network.
- The management GUI includes the capability to fine-tune spam thresholds, if required.
- The Web-based management interface has strong reporting options and a policy development interface that comes with numerous dictionaries and formats for rapid policy development.
- The product can support multiple quarantine types and search options and can provide a decent summary of disposition actions, as well as a click-through, drill-down capability into actual logs.
- The appliance-based product leverages inbound and outbound policies for Web traffic and instant messaging (IM) traffic.
- For encryption, BorderWare natively supports TLS, Secure/Multipurpose Internet Mail Extensions (S/MIME) and PGP, and resells integrated Cisco/PostX for more-complex encryption needs.

### Cautions

- BorderWare's biggest challenge is growing its market and "mind share" in an environment that is increasingly dominated by bigger brands with best-of-breed or, at least, good-enough functionality.
- Some customers complained that the GUI was not intuitive and wanted a more-task-based orientation, although a new version of the interface is slated for release in the third quarter of 2008.
- Quarantine message tracking could be improved with better indicators of policy violations and improved workflow for compliance managers.
- Customers report mixed support quality.

## Cisco/IronPort

### Strengths

- Cisco/IronPort is the market share leader with strong growth rates.
- The company has one of the biggest development teams dedicated to anti-spam research.
- Spam detection rates for IronPort are excellent, with very low false-positive rates.

- SenderBase has expanded to include Web URL reputation. The local connection management policy is very granular.
- IronPort was early to develop a bounced-address-validation system to minimize backscatter spam.
- The company provides easy-to-change spam thresholds and disposition options by groups or users.
- The browser-based management interface has a nice, clean look with easy, intuitive navigation.
- Actions in the digests are limited, but a quick link takes users to the Web quarantine interface and personal safe/block senders lists.
- E-mail encryption (via the Cisco/PostX envelope functionality) is provided in the e-mail security appliance.
- Scalability and stability are prime differentiators. IronPort has a large percentage of very large enterprise customers.
- IronPort is continuing to build on its competitively priced small business line of appliances, sold through channels, such as Dell, with more options for midmarket companies.
- IronPort recently invested in the development of a secure Web gateway for HTTP.

## **Cautions**

- The biggest challenge for the company will be to manage growth and to ensure that service and support stay consistent. Although Cisco has been careful not to integrate IronPort too aggressively, the former IronPort CEO has taken the helm of the Cisco security business, which may steer that course differently.
- DLP capabilities, including workflow, detection mechanisms and precanned policy, are relatively weak.
- The central reporting functionality carries an additional licensing fee.
- Reporting could be improved with Web-based export file types (XML and HTML). There is no ability to change anti-spam rules or edit them. Some functions require users to switch from the GUI to the command-line interface.
- An additional license fee for the M-series appliance is necessary for centralized reporting and quarantine.
- Although it could be regarded as an indicator of value, IronPort pricing tends to be higher than average, especially in the midmarket.
- IronPort does not have a virtual appliance or managed service delivery options (except for a remotely managed appliance option).

## Clearswift

### Strengths

- Clearswift is a veteran U.K.-based e-mail security company with a significant installed base in Europe, the Middle East and Africa, and in large, complex organizations worldwide.
- Spam-detection rates for Clearswift are much improved since the introduction of a reputation service and edge appliance version of its product. Spam classification by reputation alone is typically 78% of inbound spam. Legacy customers should upgrade to the most recent versions or add the edge.
- The image manager (software-only) pornographic-image-detection engine is a bonus, and bounce address tag validation (BATV) is supported.
- The browser-based management interface provides a clean, logical interface for policy development that is easy to use, even for nontechnical users. Strong directory synchronization capabilities are included.
- Policy development for content inspection/DLP is very good, and numerous policy constructs (for example, the U.S. Sarbanes-Oxley Act, the Gramm-Leach-Bliley Act, Payment Card Industry and U.S. Securities and Exchange Commission, as well as accounting terms and stock-market terms) are included.
- IM, Skype and person-to-person traffic controlling is handled by MIMESweeper IM Enterprise Edition, which uses the FaceTime IM Auditor and RealTime Guardian appliance.
- Web DLP policy and policy constructs, such as dictionaries, can be shared across appliances.

### Cautions

- Clearswift's biggest challenge is, despite significant improvements, especially in the appliance, overcoming its legacy reputation for poor spam-detection performance and administrative overhead.
- As with other vendors with a legacy software installed base, it is a challenge to migrate customers to the appliance version. Some customers report that migration to new versions has been challenging in the past with Clearswift.
- Numerous customers use the product specifically for outbound policy compliance, a historic strength, rather than inbound protection.
- Some users report that the initial setup of the software product and day-to-day administration can be time-consuming.

## Google/Postini

### Strengths

- Google acquired Postini in mid 2007. As part of Google, Postini has significant resources on hand and a "cool" factor.

- The company introduced \$3 per user, per year pricing for anti-spam and AV scanning with Web-based support.
- Postini has its own anti-spam detection and connection management capabilities.
- The interface is easy to use and includes search capabilities.
- Sophisticated directory synchronization capabilities are available.
- Google has improved DLP dictionary capabilities.
- The company offers encryption and Web security SaaS via partnerships (ZixCorp for encryption and ScanSafe for secure Web gateway).
- It has an international presence and the ability to segregate traffic to different geographic locations.
- Its end-user capabilities include thresholds and can push settings.
- Its filters can adjust thresholds on certain categories.
- Postini can look at all parts of the message attachment (unlike Microsoft Exchange Hosted Filtering [EHF]).

### **Cautions**

- The focus on providing best-of-breed e-mail security threat detection, and enterprise-class functionality and support, may deteriorate as Postini becomes further integrated inside the Google organization.
- Customers report waning spam effectiveness with the Postini service.
- Google provides a relatively unsophisticated approach to detecting backscatter spam and does not have a date for BATV support specified.
- Google's dramatic pricing of a low-end, direct and Web-based support anti-spam service angered and alienated many Postini resellers. This could affect the end-user experience as resellers look to other solutions.
- Google does not own its own encryption or Web security, relying on reseller agreements with ZixCorp and ScanSafe.
- DLP is still limited, with only two predefined lexicons.
- There is no single place for message tracking or an easy way for users to report spam.

### **Marshal**

#### **Strengths**

- A New Zealand company in origin, with a deeply loyal customer and reseller base, this privately held company is headquartered in the U.K. and has major operations in the U.S.
- Marshal offers e-mail and Web security gateway products, although its e-mail product line constitutes most of its installed base.

- Marshal has comprehensive outbound functionality and dictionary support, with lots of flexibility for users who require it.
- The company has strong anti-spam effectiveness and increased investment in reputation and connection management functionality.
- Marshal has shown a commitment to new threat vectors and sources — the company has focused research on bots and Web-based threats.
- It has good e-mail encryption support. It supports S/MIME, TLS and pull via the Certified Mail service.

### **Cautions**

- Marshal's major challenge is to position the company effectively in a rapidly consolidating market where brand and channel presence are increasingly important, especially in the North American market.
- Some users report that the management interface can be complex and daunting for a nontechnical administrator, with limited ability to modify or customize views.
- Most Marshal customers use the software version, although a managed service is available internationally via partners, and an appliance was released in 2007.

## **McAfee**

### **Strengths**

- McAfee has a strong track record and focus on security. However, the majority of its enterprise revenue is still derived from endpoint solutions. McAfee has invested in the gateway business, rolling out appliances for e-mail and Web gateways during the past six years.
- McAfee e-mail security solutions can be purchased as part of a broader McAfee license.
- McAfee offers e-mail and secure Web solutions, and has launched a new portfolio of blade servers in the second and third quarters of 2008.
- The company has invested in URL reputation data and research (including SiteAdvisor).

### **Cautions**

- McAfee has yet to make a distinctive mark in the e-mail gateway space, relative to its brand and large enterprise installed base.
- The console is weak and Microsoft Management Console (MMC)-based, although significant improvements, including role-based support, were released in the second quarter of 2008.
- The appliances have generally only been suitable to small to midsize companies, although the recent blade servers may appeal to larger organizations.
- McAfee supports TLS, but does not provide on-box encryption.
- Aggregated reporting requires the installation of a separate Enterprise Policy Orchestrator server.

- The solution offers few canned reports.

## **MessageLabs**

### **Strengths**

- MessageLabs is a privately held, managed service provider with a long track record in e-mail security. The company has grown rapidly and is the largest stand-alone e-mail security SaaS player.
- Its operations cover the U.K., U.S. and Asia/Pacific, and the company has a significant international presence.
- Customers continue to report that MessageLabs delivers strong spam effectiveness. It maintains strong service-level agreements (SLAs) compared with the market, including 99% spam detection and 95% in Asia/Pacific. MessageLabs continues to offer among the strongest SLAs for anti-spam and AV today.
- Management and reporting are strong, with an intuitive Web interface, especially for a nonsecurity-focused administrator.
- MessageLabs launched a secure Web filtering service and has integrated e-mail and Web policies and reporting.
- The service can filter attachments based on file name.

### **Cautions**

- MessageLabs is likely an attractive acquisition target, especially to a large security, technology or services provider, although an acquisition event is neither inevitable nor will always be disruptive.
- There are few predefined dictionaries for DLP in the service, and consulting services are used to define them. There are no partial file-matching capabilities.
- The service does not yet support BATV to aid in backscatter spam detection, although the road map indicates it will be supported by April 2009.
- There is some use of third-party technologies; that is, Symantec Brightmail for spam filtering and connection management functionality.

## **Messaging Architects**

### **Strengths**

- Messaging Architects is a privately held, Canadian-headquartered e-mail and archiving vendor, with a predominantly education vertical-market focus, and a Lotus Notes and GroupWise installed base.
- It offers an easy-to-use policy interface.
- Its appliance is preconfigured on delivery.
- It has responsive customer service and support.
- There are good end-user controls with Outlook integration.

- Users can access the quarantine from IMAP, making it like a directory, with easy dragging and dropping of messages. It works on any client that uses IMAP.
- Reasonable spam-detection capabilities are provided.
- There are offensive-word dictionaries and the ability to find SSNs.
- Encryption capabilities are via a partner.

### **Cautions**

- Messaging Architects has a small market share and limited brand awareness.
- It does not have its own spam research or detection capabilities.
- It made a recent product transition from a Windows appliance to a Linux appliance.
- Dashboard reporting is weak.
- There are limited DLP capabilities beyond dictionaries.
- Occasionally, customers report having to manually block IP addresses that are top spam senders.
- There are no IM or secure Web gateway capabilities.

## **Microsoft**

### **Strengths**

- Microsoft has become a more-significant player in the e-mail security market since its acquisition of FrontBridge Technologies, a SaaS offering, in 2005. FrontBridge has been rebranded as EHF.
- The market share and revenue base are growing, yet revenue alone belies the sales and brand presence of the Exchange label. EHF is included as part of the Exchange Enterprise Client Access License and other Microsoft enterprise agreements.
- Microsoft has improved its spam effectiveness with updated reputation capabilities based on Hotmail and Windows Live data.
- EHF supports encrypted e-mail via an OEM of the Voltage Security technology.

### **Cautions**

- The integration of FrontBridge into the Microsoft Exchange business was lengthy and likely distracted from e-mail security threat and service improvements during 2006 and 2007.
- DLP capabilities are rudimentary. While there is one prebuilt policy for the Health Insurance Portability and Accountability Act (HIPAA), others require manual entry using regular expression queries.
- Microsoft EHF is not able to scan attachments for content.
- There are occasional reports of customer support challenges (unresponsiveness to customer requests for message tracking or legitimate IP block change requests). Microsoft now supports a Web-based portal to view connection management.

- Secure Web gateway functionality and threat research is largely maintained outside the Exchange business unit. Microsoft will launch a Threat Management Gateway in 2009.
- Microsoft only offers an e-mail security solution, which is suitable for enterprises in a service offering (EHF). They do not yet have a credible SMTP e-mail security solution — for example, Exchange Edge uses SmartScreen and must be purchased with an outside reputation service, although a road map to deliver Microsoft reputation is in place.
- Microsoft's e-mail security portfolio can be confusing to users. For example, there is confusion as to the spam capabilities with Forefront Security for Exchange, which is used on internal Exchange and only offers AV scanning.

## **MX Logic**

### **Strengths**

- MX Logic is a Colorado-based e-mail security service provider with a long track record in the e-mail services industry. The company has largely focused on the SMB customer segment.
- MX Logic has a strong reputation for spam effectiveness. The company maintains an active R&D and research capability.
- MX Logic offers an innovative product portfolio, despite its limited resources.
- The company has delivered multiple offerings since 2006, such as an archiving and Web security service, and rolled out a click-protect capability for Web links.
- The disaster recovery capability is particularly attractive, with a Web-based Outlook look and feel.
- MX Logic's e-mail security service has strong end-user controls and a Web interface.

### **Cautions**

- MX Logic does not have operations outside the U.S., which can be problematic for European Union customers or companies with an international presence.
- MX Logic's e-mail security service does not have dictionaries and cannot encrypt; thus, it cannot be used for outbound controls.
- The company uses multiple third-party technologies, such as Cloudmark and Brightmail, although it has its own message transfer agent (MTA), spam-detection technologies, and e-mail security research capabilities.
- Users report that the dashboard could be improved, and message tracking can be problematic, because the global blacklist cannot be accessed.

## **PineApp**

### **Strengths**

- PineApp is an Israel-based startup, with a small installed base of largely midsize organizations looking for a Barracuda alternative.
- PineApp offers granular end-user controls and a relatively strong connection management reporting capability.

- It has reasonable backscatter spam protection.
- The company has invested in secure Web gateway and Web threat research.
- It is competitively priced.

### **Cautions**

- PineApp is a small player with limited enterprise experience.
- Its outbound content filtering is extremely limited. No dictionary support or ability to filter keywords or attachments was evident during our assessment period.
- It has a limited ability to create custom reports.

## **Proofpoint**

### **Strengths**

- Proofpoint is a California-based, privately-held company that is focused solely on messaging security and compliance.
- It has received a recent influx of capital to invest in growth.
- Proofpoint acquired Fortiva, an archiving SaaS provider, in June 2008. Resellers of e-mail security solutions indicate a growing interest in archiving SaaS.
- It's one of the only vendors to offer all three delivery models: software appliance, virtual appliance and a hosted option.
- It offers rich DLP capabilities, including prebuilt dictionaries and the ability to set custom rules.
- On box encryption is provided through an OEM agreement with Voltage Security.
- Adjustable spam and connection/reputation management thresholds are available.
- Its strong end-user interface has an intuitive Outlook look and feel.
- Proofpoint is one of a small number of vendors to offer a separate file transfer capability.

### **Cautions**

- Proofpoint is one of a dwindling number of stand-alone e-mail security-focused players amid growing consolidation. Its installed base and market share are smaller than some of the other leaders, although the company is growing rapidly.
- It offers a limited secure Web gateway, aside from DLP capabilities.
- Proofpoint was late to invest in connection and reputation management; however, it was able to catch up quickly.
- The company lags behind some other vendors in its ability to detect backscatter spam, which will be better dealt with in an upcoming release.

## Secure Computing

### Strengths

- Since the acquisition of CipherTrust, Secure Computing has been busy integrating the company and the SecureMail appliance into its suite of network gateway products.
- SecureMail's market share is holding steady at approximately 8%. Support is improving as the acquisition integration effort stabilizes.
- Anti-spam performance is strong, and reputation capabilities deliver more than 90% detection rates at the connection layer.
- Secure is integrating TrustedSource across its firewall and Web gateway product lines and expanding reputation to Web URLs.
- A major recent improvement is in performance and scalability delivered via new software, hardware and operating system upgrades. Legacy hardware customers should take advantage of incentives to upgrade to the latest hardware version.
- The browser-based management interface is very granular and might be daunting at first for new users. The dashboard is one of the best in the market and provides a good balance of graphic and tabular information, and it can be customized for different administrative roles. "Virtual" management views also provide flexible role-based administration.
- Secure's capable inbound and outbound content inspection and mail-handling policy has always been a core strength of the SecureMail product. DLP capability is also strong, with lots of predeveloped policies, dictionaries and other identifiers, such as smart SSNs and credit card number validation. Secure offers a full range of encryption options.

### Cautions

- The biggest engineering challenge for Secure Computing is to rationalize the product line and get it on one code base and one management and reporting engine to deliver on the full promise of an integrated suite of related gateway appliances, while simultaneously improving code quality and feature details.
- Secure must improve its centralized management capability for consolidating policy, reporting, quarantines and cross-queue message tracing. Users report significant frustration with this element.
- End-user quarantine options are not as good as they could be, and there is no notion of a personal block-sender list. Allow-list names can only be added in the quarantine.
- Despite a powerful policy development focus, reading or auditing the established policy is difficult.
- The Secure Computing development team needs to improve the consistency of quality of new releases. Several customers commented on bugs in early versions and a lack of configuration preservation during the migration to new versions.

## SonicWALL

### Strengths

- SonicWALL offers a suite of security solutions (for example, firewalls, virtual private networks and backup), in addition to secure e-mail appliances and software.
- The company is endeavoring to grow from its traditional SMB focus to support midsize to large enterprises because its market share in the e-mail security gateway market is small and shrinking.
- The product supports real-time blacklists and has an automatic "allow" listing option tied to contacts to minimize false positives. Local connection-management options are rich.
- Spam thresholds for specific spam categories are adjustable, and administrators can delegate spam threshold setting to end users.
- The product is capable of creating custom, inbound e-mail filtering rules for company-specific policies, such as redirecting activist e-mail campaigns.
- The browser-based GUI is relatively simple and easy to use.
- The policy development has reusable policy constructs, including two predefined dictionaries and several common number formats (for example, Canada's Social Insurance Number). The interface is driven by drop-down menus and click boxes, which are simple to use, but somewhat limited for creating nuanced policy.
- End-user features and corporate quarantines are very complete. An Outlook client-side plug-in provides spam selection buttons and a local quarantine folder.
- SonicWALL Email Security has an e-mail archiving capability built in, although it is restricted by disk capacity.

### Cautions

- SonicWALL will find it difficult to attract large enterprise customers until it provides features that accommodate the complexity of the large enterprise, and the company invests more in support and channel partners that are capable of supporting large enterprises.
- Spam effectiveness and scalability are hampered by a lack of reputation data, which can drop more spam at the connection level.
- Enterprise management needs for elements such as roles-based administration, multiple LDAP directory synchronization — which we noted as a deficiency in "Magic Quadrant for E-Mail Security Boundary, 2006" — and more-robust policy development are lacking, although some of these elements are on the company's road map.
- Native encryption is limited to TLS.
- Improved scalability of appliances to support very large enterprises is needed.

## Sophos

### Strengths

- Sophos' primary focus is in the Endpoint Protection platform market, although the company derives reasonable market share from its Exchange, SMTP software and appliance businesses.
- Its spam-detection rate is good, and its reputation detection rates are good at around 90%, with low false positive, invalid recipient look-up done to the downstream mail servers, even if there is no directory interaction.
- Sophos is gradually improving the management GUI with a focus on ease of use, with a goal of three clicks to anywhere.
- It offers a good messaging-tracking facility with easy-to-understand disposition actions.
- Sophos offers managed appliances that monitor appliances for hardware or software issues, and provides proactive service and support. It also provides unassisted or one-click upgrades.

### Cautions

- Sophos' primary challenge is providing features and options for the more-demanding midsize and larger enterprise. For example, multiple directory server integration is missing on the appliance.
- The appliance is relatively new and caters to SMBs. Most of its business is derived from its Unix and Exchange software products.
- Although Sophos does a good job of simplifying management by hiding complexity, drill-down for more-technical users and advanced requirements are absent. Most spam options are binary with no ability to adjust thresholds.
- Reputation and connections management need to improve. Specifically, backscatter or bounced-message spoof detection and silent drop for reputation-blocked messages are necessary.
- End-user controls are weak, with no ability to extend spam thresholds to end users. There is no automated false-positive/negative reporting, and search options for end users are missing.
- Policy development is weak. Although it has the right reusable constructs, elements are stored as files and imported to specific policies, rather than simply referenced. Consequently, in complex environments, changes may need to be made in multiple locations' policies.
- Reporting is weak and only offers predefined reports, with no ability to create custom reports, save them and schedule them for distribution.

## Symantec

### Strengths

- Symantec has a significant enterprise and SMB installed base and a relatively large e-mail security market share. Since its acquisition of Brightmail in 2004, Symantec has

rolled out appliances, including a virtual appliance option, and offers a managed service (via a white-label partner).

- Symantec's enterprise licensing packages can make Symantec's e-mail security solutions attractive for purchase.
- The company offers good directory integration, flexible policy options, rich precanned dictionaries (including from Vontu) and some custom capabilities.
- Anti-spam effectiveness has improved significantly since 2006, when the company floundered on certain threats, such as image-based spam.
- Reputation capabilities have improved, with global and local reputation capabilities.
- Management and reporting, which were weaknesses in earlier versions, have been substantially improved with dashboards and threat indicators.
- Symantec offers breadth of delivery models, including a virtual appliance, and SaaS via a white-label partner.

### **Cautions**

- A large portion of Symantec customers uses the software version, which has much more limited reputation detection capabilities.
- Transitioning software customers to an appliance has been slow, because many of these customers do not want to invest in hardware or maintenance.
- As e-mail and Web security threats converge, and outbound policies need to be uniform for e-mail, Webmail and HTTP channels, Symantec's lack of a secure Web gateway will become more evident as a strategic hole.
- Symantec needs to ensure that it stays apace with spam-detection trends. It was supposed to offer effective image-spam detection in 2006, and does not currently support BATV to aid in detecting backscatter spam, unlike key competitor IronPort.
- Symantec also does not have any on-box encryption capability (that is, push/pull) beyond TLS. It relies on partners, such as PGP.
- Symantec had some stability issues and product functionality gaps with earlier versions of its appliances. Although the latest release has improved significantly, past misdeeds still linger in the minds of some resellers and customers.

### **Trend Micro**

#### **Strengths**

- Trend Micro ("Trend") is a leading AV vendor and is a major market leader of e-mail/exchange AV products.
- Spam detection rates are improving and are above average. Trend has a good reputation system that delivers as much as 80% detection rate at the connection.
- Trend is also extending its reputation data to a URL via a unique, in-the-cloud look-up. Spam thresholds can be set to low, medium or high sensitivity, or set to a specific threshold for groups and users. Trend has good international language spam-detection capabilities, particularly in Asia.

- The browser-based management GUI is average, and the real-time dashboard is good.
- The DLP policy development interface is good and has reusable policy objects, including numerous precanned dictionaries and a policy audit summary.
- Scalability was recently enhanced with a "parent/child" cluster design.
- Encryption includes native TLS and S/MIME, and off-box Sakai Kasahara Key Encapsulation Mechanism-based push client-to-client encryption (from its Identum acquisition).
- Trend offers a broad array of delivery options, including a hosted service, software and appliances. Virtual software versions are expected in late 2008.

### **Cautions**

- Trend's progression from just providing e-mail AV to offering a full-featured secure e-mail gateway has been uneven. It is hampered by inconsistent and often confusing features across product lines and multiple options.
- Customers commented on occasional quality issues with the new version.
- The service offering does not provide e-mail encryption, or advanced compliance/outbound content control, although these functions should be available by the fourth quarter and year-end 2008, respectively.

### **Webroot**

#### **Strengths**

- Webroot acquired Email Systems in 2007. Email Systems was a small U.K.-based e-mail security service provider.
- Webroot offers good message-tracking and end-user capabilities.
- The company offers strong outbound content filtering with a wide range of dictionaries, custom options and encryption support.
- It is one of the only solutions or services to support BATV to aid in detecting backscatter spam.
- Webroot offers an archiving capability and innovative disaster recovery capability.
- The company has invested in a secure Web gateway service.

#### **Cautions**

- The U.S. operations for the service are new, launched in April 2008.
- The service is owned by a U.S. company, Webroot, which has a limited e-mail security track record and service provider expertise, although it is investing significant resources and hiring expertise in these areas.
- Email Systems had limited e-mail security threat research detection capabilities — it used third parties (CommTouch, Cloudmark and Mailshell), although it owns its own MTA, reputation and connection management capabilities.
- The service offers limited ability to set filtering thresholds.

- White listing and releasing require separate interfaces.
- Webroot has a largely SMB installed base.

## **Websense**

### **Strengths**

- Websense is much better known for its Web URL-filtering solutions than secure e-mail gateways; however, the acquisition of SurfControl in 2007 provided e-mail security software and a service.
- Websense acquired DLP vendor PortAuthority Technologies, giving it DLP and compliance capabilities it can extend across e-mail and Web gateway solutions. Websense will leverage its Web threat intelligence for e-mail filtering and exploit spam samples to feed URL analysis engines.
- Websense has already integrated its threat-seeker URL risks into its e-mail filtering.
- The management interface is a combination of a browser-based dashboard and MMC-type consoles for policy development.
- Policy has good reusable objects (who, what, operation notification and actions) that can be dragged and dropped into policies.
- The product includes a comprehensive set of dictionaries in 12 languages, including weights, wildcards and templates, and is capable of creating multiple types of quarantines.
- End-user tools include a digest and a Web interface with personal allow/block lists.
- The Websense e-mail security service has a Web GUI that also includes Web security in the same management interface. Detailed reporting data is kept for 30 days, and summary information is retained for the duration of service contracts. The services have a wider spam threshold score for tuning and can do three different disposition options, depending on the spam score. Message-tracking options are good.
- The service includes a disaster recovery option that enables customers to view mail even if their mail servers are offline. The services offer TLS and pull-type encryption.

### **Cautions**

- Websense has made various acquisitions to create a common management and policy framework to deliver the strategic promise of a suite vendor, while simultaneously enhancing its e-mail product's manageability and spam-detection rates. Currently, there is limited integration from a policy and technology perspective between the e-mail and URL-filtering products.
- Users report that the software solutions require too many unique servers (SQL servers, personal e-mail manager and filtering servers) to scale and provide redundancy.
- Appliance products suitable for enterprises are absent.
- The software product has significant limitations for large enterprises compared with the leaders. The GUI, in particular, is a confusing mix of Web and MMC consoles, and has far too many windows and steps to complete tasks. Users report difficulty maintaining configurations across multiple servers.

- The Websense e-mail service is lacking advanced management functions, such as LDAP synchronization; the ability to customize, save, and schedule reports; alias; or handle distribution lists.

## RECOMMENDED READING

---

"Magic Quadrants and MarketScopes: How Gartner Evaluates Vendors Within a Market"

### Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

### Evaluation Criteria Definitions

#### Ability to Execute

**Product/Service:** Core goods and services offered by the vendor that compete in/serve the defined market. This includes current product/service capabilities, quality, feature sets and skills, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

**Overall Viability (Business Unit, Financial, Strategy, Organization):** Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

**Sales Execution/Pricing:** The vendor's capabilities in all pre-sales activities and the structure that supports them. This includes deal management, pricing and negotiation, pre-sales support and the overall effectiveness of the sales channel.

**Market Responsiveness and Track Record:** Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

**Marketing Execution:** The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word-of-mouth and sales activities.

**Customer Experience:** Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support

programs (and the quality thereof), availability of user groups, service-level agreements and so on.

**Operations:** The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

### **Completeness of Vision**

**Market Understanding:** Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

**Marketing Strategy:** A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the Web site, advertising, customer programs and positioning statements.

**Sales Strategy:** The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

**Offering (Product) Strategy:** The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

**Business Model:** The soundness and logic of the vendor's underlying business proposition.

**Vertical/Industry Strategy:** The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

**Innovation:** Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

**Geographic Strategy:** The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

This research is part of a set of related research pieces. See "Roundup of E-Mail Research Through 3Q09" for an overview.

## REGIONAL HEADQUARTERS

---

### **Corporate Headquarters**

56 Top Gallant Road  
Stamford, CT 06902-7700  
U.S.A.  
+1 203 964 0096

### **European Headquarters**

Tamesis  
The Glanty  
Egham  
Surrey, TW20 9AW  
UNITED KINGDOM  
+44 1784 431611

### **Asia/Pacific Headquarters**

Gartner Australasia Pty. Ltd.  
Level 9, 141 Walker Street  
North Sydney  
New South Wales 2060  
AUSTRALIA  
+61 2 9459 4600

### **Japan Headquarters**

Gartner Japan Ltd.  
Aobadai Hills, 6F  
7-7, Aobadai, 4-chome  
Meguro-ku, Tokyo 153-0042  
JAPAN  
+81 3 3481 3670

### **Latin America Headquarters**

Gartner do Brazil  
Av. das Nações Unidas, 12551  
9º andar—World Trade Center  
04578-903—São Paulo SP  
BRAZIL  
+55 11 3443 1509