



## **Magic Quadrant for E-Mail Security Boundary, 2006**

25 September 2006

**Peter Firstbrook Arabella Hallawell**

**Source:** Research

**Note Number:** G00142431

The e-mail security boundary market continues to be a crowded one. Spam and virus filtering are becoming commodities, and buyers must look at high-end features to find significant differentiation.

## What You Need to Know

The market is poised for significant consolidation.

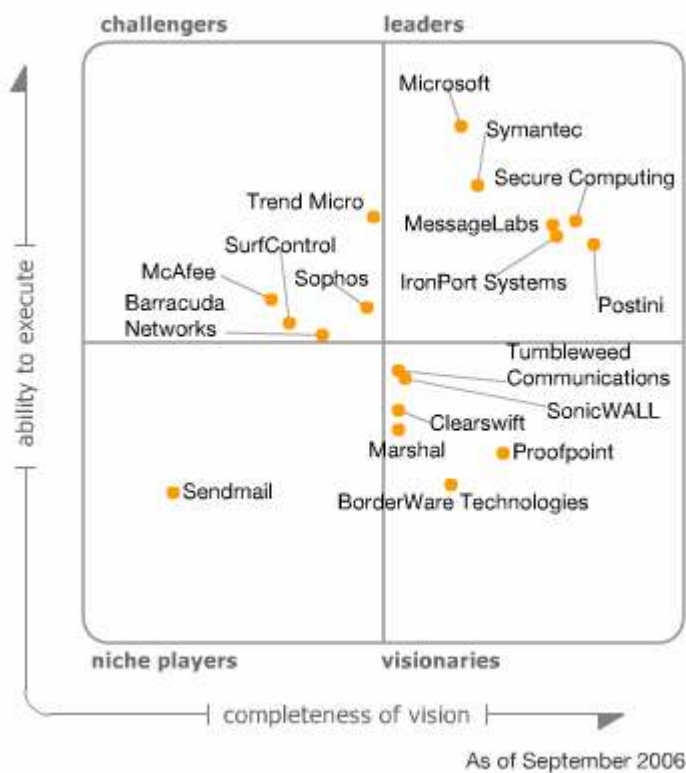
Efficient and accurate spam and virus filtering are common among leaders; to differentiate vendors, buyers need to look at manageability, message transfer agent (MTA) capabilities, outbound content filtering, encryption, instant messaging (IM) and Web integration, and archiving integration.

Appliances and service providers are the predominant form factor.

## Magic Quadrant

Figure 1.

Magic Quadrant for E-Mail Security Boundary, 2006



Source: Gartner (September 2006)

## Market Overview

Long-anticipated consolidation in the e-mail border security market is only gradually occurring. SonicWALL recently acquired MailFrontier, and Secure Computing bought CipherTrust; however, these are ownership changes and didn't really affect the number of players in the market. Meanwhile, SurfControl recently bought BlackSpider Technologies, and Microsoft bought Frontbridge Technologies, both consolidating moves given that the acquirers were already players in the market. A number of other vendors are making themselves available for sale, and Gartner projects that mergers and acquisitions will reach a peak during the next 12 months as such activity begins to resemble a game of musical chairs. Clearly, Microsoft's significant investment in boundary services — which will reach fruition in the forthcoming Exchange 2007 release — will have a significant impact on competitive dynamics over time. High growth in this market (40% year over year) has convinced venture capitalists to double their bets to keep their investments alive long enough to be bought, and market leaders have been unable to monopolize buyers' attention. Indeed, only one of the 20 vendors in our related MarketScope research has more than a 10% market share. Still, we continue to assert that market consolidation is inevitable, and buyers should beware of companies with weak financials and/or low market share, and we evaluated these factors carefully in the Ability to Execute dimension. Potential acquirers of e-mail security companies include firewall and network equipment vendors and competitors looking to rapidly acquire market share and/or eliminate competition.

Efficient and accurate spam and virus filtering with low administration overhead remain essential to buyers; however, it is generally the secondary features that win deals. Management features that lower administration overhead, policy-based outbound content inspection, encryption and appliance MTA capabilities have increased in importance as buyers look to consolidate e-mail infrastructure. Compliance and leak prevention concerns drive interest in outbound inspection and encryption, although most companies are only beginning to experiment with this capability.

Prescient organizations should be looking for integration of IM and other Web-based communications modalities on the front end and intelligent archiving integration on the back end. Indeed, the pending converged communications market represents a huge opportunity for e-mail vendors to elevate their status in the organization by providing policy and protection services across multiple communications media. Achieving this goal will require vendors to have deep packet inspection capabilities to identify communications traffic and a policy management architecture that is neutral to the message medium (e-mail, IM, chat, Web mail, blog postings, voice over IP [VoIP]).

While software products dominate the installed base, we see a rapid decline in interest in software products in favor of appliances and service provider offerings. Appliances were the form factor of choice for midsize to large organizations in 2005 and 2006. We continue to see broad interest in service provider offerings by all our clients; however, small businesses (fewer than 500 seats) compose the biggest segment of service provider customers. We anticipate an explosion of service provider resellers in 2007 as telcos re-

brand existing service provider offerings or buy their own infrastructure. Concurrently, Microsoft's Exchange 2007 offering will include an add-on service provider component (formerly Frontbridge). The combined marketing "noise" from these sources will lead to more market awareness and acceptability of service provider offerings, accelerating market share of this delivery model from 20% in 2005 to 40% by 2009. In response, many of the appliance and software vendors will launch their own hosted models or aggressively target the telcos to capitalize on this market opportunity. Buyers must carefully evaluate the source of the underlying technology in re-branded or hosted solutions and be wary of inexperienced vendors. We recommend buying service provider offerings directly from the source (such as MessageLabs, Postini, Microsoft or MX Logic) to avoid problems caused by multiple layers of support. New service provider solutions that cobble together enterprise equipment will experience scalability limitations and likely have a more expensive cost structure. Hosted solutions (those that do not share infrastructure across multiple customers) will be the most expensive, and most organizations should avoid them.

### **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. Initial capabilities and the primary buying motivation are spam and virus filtering, but as this capability matures, organizations are looking to consolidate e-mail infrastructure, and vendors are responding by integrating MTAs, outbound content inspection and encryption.

Market penetration is very high in Global 2000 companies, and most sales activity is related to the replacement of first-generation anti-spam software that is less effective at filtering unwanted e-mail and/or requires too much administration. Current buyers are looking to consolidate existing infrastructure and replace software with appliances or buy services to simplify administration. The SMB market is less-penetrated and more likely to have open-source solutions with high administration overhead. This market is very sensitive to price, and ease of use is a high priority.

Globally, the market is growing at approximately 40%. Most market growth has been in North America and Europe, the Middle East and Africa; however, the Asian market, which is underpenetrated, is beginning to heat up, and we expect this market to be a significant source of growth during the next two years.

The market in 2006 remains very fractured, with the top six vendors accounting for only 40% of total market revenue. Market consolidation of primary providers is under way, and we expect the top six vendors will garner a 65% share of the market by 2007.

### **Inclusion and Exclusion Criteria**

To be included in this Magic Quadrant, solution providers must directly offer enterprise customers a comprehensive e-mail security boundary solution that can filter and block

unwanted e-mail and viruses and provide basic intrusion prevention, such as denial of service, directory harvest and anti-relay technologies. The product must have generated at least \$10 million in revenue and maintenance fees in 2005. Products must also have a significant installed base (more than 1,000) of enterprise customers and/or be shortlisted or implemented by a Gartner client in the past 12 months.

### **Added**

In the 2005 Magic Quadrant, we evaluated 21 vendors; this year, we evaluated 18 vendors.

During the year, Microsoft bought Frontbridge, and SonicWALL acquired MailFrontier. Finally NetIQ, after acquiring Mail Marshal in 2001, sold that division back to management in December 2005, re-branded as Marshal Ltd., so these companies were added, but their predecessors' names were dropped. CipherTrust was acquired by Secure Computing in August 2006.

### **Dropped**

Cloudmark was dropped from this year's Magic Quadrant because it does not sell directly to the enterprise, preferring to sell to ISPs and telcos for reselling to enterprise buyers. Also, Cloudmark is focused solely on anti-spam and virus techniques and does not participate in the broader e-mail boundary security market. MX Logic was also dropped because it does not meet the inclusion criterion of having more than 1,000 enterprise customers, because it made a strategic decision in 2005 to target only the small and midsize business (SMB) market. Mirapoint also was dropped because it does not have more than 1,000 enterprise customers.

### **Evaluation Criteria**

#### **Ability to Execute**

The three most-significant factors contributing to a vendor's horizontal positioning were vendor viability, market responsiveness and sales execution. We also gave significant weight to customer experience.

- **Product or Service** — We rated vendors on the quality of their products on initial release, adherence to scheduled release dates and road maps.
- **Overall Viability** — This category ranked vendors on business fundamentals such as revenue, profitability, capital, growth rate, quality of investors, and the strength and tenure of the management team. However, it is important to note that large multiproduct companies were ranked on the strength of the e-mail division rather than the total company.
- **Sales Execution** — We considered the number of customers a vendor has as a good proxy for its ability to execute in the past, and we considered the quality of the vendor's sales channel (such as its direct sales force, channel partners, systems

integrators or OEM partners) as a good indicator of a future ability to execute. We also considered the rate of growth of a vendor versus the overall market as an indicator of momentum.

- **Market Responsiveness and Track Record** — Although most of the evaluation in this Magic Quadrant was retrospective, market responsiveness and track record was a component in the overall score that allowed us to look at the companies' past performance as an indicator of how they will likely perform in the next 12 to 18 months. While we gave some credit to companies that have recently changed direction, much more credit was given to companies that have demonstrated a consistent market direction. Companies that have been recently acquired were downgraded slightly because of transitional issues that are inevitable in these transactions.
- **Marketing Execution** — Successful marketing campaigns should lead to a heightened awareness of the product in the market, so we gave extra credit to companies that are consistently recognizable to Gartner clients and often appear on their preliminary shortlists.
- **Customer Experience** — We ranked vendors in this category based on the satisfaction level of Gartner clients and reference customers. While some customers are slow to upgrade to the latest version and may be dissatisfied by legacy product limitations or management problems, our view is that vendors' ability to grow and execute will depend significantly on the peer recommendations of satisfied customers.
- **Operations** — Finally, we ranked vendors based on the resources they dedicated to the issue of e-mail security and the efficient use of these resources.

<b>Table 1.</b>	
<b>Ability to Execute Evaluation Criteria</b>	
<b>Evaluation Criteria</b>	<b>Weighting</b>
Product/Service	low
Overall Viability (Business Unit, Financial, Strategy, Organization)	high
Sales Execution/Pricing	high
Market Responsiveness and Track Record	high
Marketing Execution	standard
Customer Experience	high
Operations	no rating

Source: Gartner (September 2006)

### **Completeness of Vision**

The completeness of vision score was heavily weighted by two major categories: market understanding and product offering (quality and functional completeness as of May 2006). Although the factors listed below were scored, they had a nominal impact on the horizontal positioning of the vendor.

- Market Understanding — We evaluated how closely the companies' current and past vision of the market aligns with Gartner clients' "pain points" and needs and our analysis of the market's future. Vendors that have recently shifted strategies to align with the market are given less credit than vendors that have had an unwavering market understanding.
- Marketing Strategy — A company's marketing strategy refers to its ability to effortlessly explain its product or company differentiation succinctly as well as the resources to get its message out.
- Sales Strategy — We gave credit to vendors that had reasonable list prices relative to the market and those that take a less aggressive “partnership” approach to negotiation (particularly renewals).
- Offering (Product) — We put the most weight on this category and scored vendors in the following seven functional categories. Top-listed functions that customers consistently mentioned as pain points are weighted more heavily than lower-listed functions, which are not yet essential to all customers.
  - Manageability — This category refers to a company's ability to lower administration overhead exploiting such features as intuitive management interface, end-user quarantine areas and controls, delegated administration of solution components, customizable reporting, real-time dashboards, and troubleshooting tools (such as tracking lost messages, finding filters responsible for false positives and so on).
  - Spam and Antivirus Effectiveness — Clearly effective spam/virus/phishing filtering with low false positives is a primary consideration for all buyers. More credit was given to vendors that had their own evolving filtering "cocktail" approach than vendors that OEM code and to those that demonstrated past ability to adapt quickly to changing spammer tactics. We also considered reputation services and connections management ability and sender authentication, value-added antivirus and specific phishing detection capabilities.
  - MTA Capabilities — Given that most clients are interested in e-mail infrastructure consolidation, we considered the product's capability to replace incumbent MTAs' products and to scale out and provide multiple 9s of reliability. Our consideration included native clustering/load-balancing capability, features that enhance scalability, a flexible routing policy and intrusion prevention capabilities (denial of service, directory harvest, open-relay protection, error message handling including spoofed message bounces and so on).
  - Outbound Content Filtering — Increasingly, companies are interested in inspecting outbound e-mail for regulatory or corporate policy compliance. We considered the product's capability to do efficient outbound filtering and content inspection with pre-configured dictionaries and rules that allow administrators to effortlessly set policy based on broad parameters (for example, Health Insurance Portability and Accountability Act [HIPAA]) without having to design these rules from scratch. We also considered the workflow to ease flagged message handling and alerting/notification.

- Encryption — Driven by information security and privacy concerns and regulation, e-mail encryption capabilities that are simple for end users to invoke, or that are automatic based on policy and content inspection, are rising in importance. We gave credit to vendors that have integrated e-mail encryption into their product such that it is transparent to end users and easy for administrators to set up and troubleshoot.
- IM and Web Channels — As interest in content inspection for e-mail increases, enterprises will want policy and inspection capabilities that can cover additional communications channels, such as IM, chat sessions, Web mail, blog postings and VoIP. Concurrently, inspecting for inbound malicious content requires a more complete understanding of the threats posed by malicious URLs and other Web dangers, such as phishing. We gave extra credit to vendors that have created policy architectures that are independent of the message type and that have invested in Web-based threat detection and filtering.
- Archiving Integration — Vendors that were able to provide some level of intelligent integration with e-mail archiving solutions or provide stand-alone archiving solutions were given extra credit.
- Innovation — Credit was given to companies that have demonstrated a good track record of innovation in the e-mail boundary security market as represented by innovative features and/or patents that are relevant to e-mail security.
- Geographic Strategy — Companies that have broader global coverage, as illustrated by a breakdown of revenue by geography, were given more credit than vendors that have a regional focus.

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

Source: Gartner (September 2006)

## **Leaders**

Leaders are high-momentum vendors (based on sales and "mind share" growth) with proven track records in e-mail security, as well as vision and business investments that indicate they are well-positioned for the future. Leaders do not necessarily offer the best products for every customer project; however, they provide solutions that offer relatively

lower risk. Although smaller leaders can be acquisition targets, intellectual property assets, revenue momentum and customer list tend to limit buyers to large, established vendors with significant capital resources and a well-conceived strategy. Indeed, we suspect the likely acquisitions of those small vendors in the Leaders quadrant will be positive events.

### **Challengers**

Challengers are well-executing vendors that compete but that do not offer strongly differentiated products or a commitment to innovation in this market. Challengers' products perform well for a significant market segment but may not show general value or feature richness. Buyers of challenger products are typically motivated by existing relationships with these vendors.

### **Visionaries**

Visionaries are vendors that are differentiated by innovation but have not achieved the record of execution in the e-mail security market to give them the high visibility of the leaders. Expect state-of-the-art technology from the visionary vendors, but buyers should be wary of a strategic reliance on these vendors and should monitor the vendors' viability closely. Given the maturity of this market, visionaries represent good acquisition candidates. Challenger vendors that may have neglected technology innovation and/or vendors in related markets are likely buyers of visionary vendors. As such, these vendors represent a higher risk of business disruptions.

### **Niche Players**

Niche players' products typically can solve some e-mail security problems with varying degrees of success, but they lack comprehensive features and market presence. Customers that are aligned with the focus of a niche vendor often find such providers' offerings to be good enough for their needs.

### **Vendor Comments**

#### **Barracuda Networks**

Barracuda Networks is a California-based company that has garnered attention for its aggressive marketing campaign, intense channel focus (sales are 100% channel-driven) and low pricing. The company also has good international coverage, with only 60% of its sales coming from the United States. The company has been quick to capitalize on its growing brand and customer presence by introducing separate appliances for anti-spyware and IM filtering as well as outbound content filtering. All of this adds up to impressive rapid customer growth, which caused Barracuda's significant vertical growth and its slight horizontal movement on the Magic Quadrant this year.

Barracuda has shown good vision in meeting customer requirements for an e-mail security boundary capability at a moderate price, and it has also put pressure on the rest of the vendors to raise the bar on features and services to merit premium pricing. For example, Barracuda offers connection management and valued-added antivirus capabilities, features that some premium-priced products often lack. E-mail filtering technology is based on a number of proprietary techniques, including open-source Spam Assassin and Clam Antivirus. Spam effectiveness is adequate, given the low administration overhead of the solution. Customers complain that key enterprise management functionality, such as centralized reporting and advanced MTA functionality, is not provided for sophisticated environments. Encryption is limited to Transport Layer Security (TLS). Outbound filtering is comprehensive and includes dictionaries and pre-configured policies, but it requires an additional appliance. Given rapid growth, it is not surprising that customers report that help desk service can be patchy at times.

In short, we see Barracuda as most appropriate for companies that have relatively simple environments and that are looking to simplify and lower administration of existing open-source implementation and/or have limited budgets.

### **BorderWare Technologies**

BorderWare spent the better part of 2005 redesigning its flagship MXtreme products to good effect. The company improved its native anti-spam capability with connections management and their own reputation service in addition to existing Symantec/Brightmail capabilities. Scalability was improved with native clustering and integration with partners Sun/HP and F5 Networks. Outbound content inspection capabilities were much-improved, and the company is making investments in dictionaries and canned policies to ease administration. Policy-based encryption is delivered via native TLS or optional integration of on-box PostX functionality. The company is maximizing its extensive firewall and SIP firewall capabilities to create a policy platform that can be leveraged across multiple communications modalities, although IM support is still in the future. While these improvements were dramatic for BorderWare, the new features are early versions that were not fully fleshed out. BorderWare therefore failed to leapfrog the competition, keeping it on the edge of the Niche Players quadrant.

Despite recent notable wins, such as Telus, BorderWare's ability to execute is hampered by its small market share and small installed base of large-enterprise customers in a consolidating market. Geographic distribution is above average because of a strong European channel, but the company's very low mind share in North America lowered BorderWare's overall marketing and sales execution scores. The company recently raised additional capital; however, its viability remains below average for this market, partly because of its strategic investments in VoIP. Like all companies in this market, it is an acquisition candidate. Fortunately, its firewall business and VoIP experience are solid assets that could attract a favorable buyer.

### **Clearswift**

Clearswift was an early entrant and innovator in the e-mail security market. The customer base has shrunk from its historic peak because of inattention to changing spam trends in 2004, but it has grown during the last 18 months and represents a respectable market share, especially in the European Union (EU). The company has implemented significant management changes in the past 12 months (for example, the CEO, COO, and vice president of engineering, vice president of marketing and vice president of business development are all new).

MIMESweeper for SMTP software is the most common delivery method, but Clearswift is also offering a new appliance and a new managed service (hosted in the EU), although capabilities and features are slightly different across the product line. Clearswift has a legacy of very poor spam detection and high false positives, but customers report significant improvement during the past 12 months. Virus signatures are not included with the software product. The new appliance includes Kaspersky Lab's antivirus scan engine, and the managed service offers multiple engines. Virus detection is enhanced with an outbreak service called ThreatLab, which issues alerts to quarantine suspect e-mails. MIMESweeper for SMTP includes very granular policy implementation and enforcement, but its complexity is not always appreciated, and it continues to receive poor marks for manageability and a heavy administration load. The appliance product is more user friendly. Clearswift gets very high marks for content inspection and comes with 30 dictionaries, including Sarbanes-Oxley Act (SOX) and Gramm-Leach-Bliley Act (GLBA)-type phrases. For encryption, Clearswift partners with PGP, GlobalCerts and Sigaba. The company is beginning to make some Web investments. It co-sells FaceTime for IM hygiene. Clearswift also offers a software Web gateway product and is working on a Web-filtering appliance and Web-filtering managed service that is due in the fourth quarter of 2006.

Clearswift is a leading vendor for enterprise content inspection requirements and is improving its spam detection capabilities.

### **IronPort Systems**

IronPort is another California-based company, focused solely on messaging security. A leader in 2005, IronPort is again one of our Leaders in the Magic Quadrant this year and is a top pick, especially for large-enterprise clients. IronPort is one of the fastest-growing companies in this year's Magic Quadrant. It has also built up its channel for SMB customers, showing initial success outside its traditional enterprise installed base. The company has expanded its operations significantly, with one of the highest employee head counts dedicated to this market in the industry.

IronPort pioneered connection management using its SenderBase reputation service and a high-performance/scalable MTA. Since last year, the company has also improved its enterprise-class management and reporting capability, along with the introduction of a management appliance to consolidate multiple logs and reports. IronPort customers are typically very enthusiastic, although some concerns have emerged about the efficacy and performance of the Brightmail engine and the lack of attachment filtering. IronPort has

wisely invested in its own anti-spam engine, which compares favorably with Brightmail at a lower cost, and it provides the company an alternative option to the Symantec engine; this partnership will become increasingly uncomfortable as Symantec's appliance offerings mature. IronPort suffered in its "vision" score this year because it has been slow to build more-comprehensive e-mail security functionality. Rather, it relies on partners for e-mail encryption (for example, PostX and PGP) and partners for IM filtering and outbound content monitoring. These partnerships vary in levels of actual integration and management but generally involve more administration overhead and expense than integrated solutions from the competition. IronPort's strategy — providing what it does well and partnering for the rest — has served the company well to date in the large-enterprise market. Customers in this segment want rock-solid reliability and scalability and is willing to buy best-of-breed components and integrate these themselves. Unfortunately, satisfying the burgeoning SMB market requires greater integration to lower costs and administration effort.

The company gained points for its recent focus on HTTP malicious-code protection appliances. However, this is a separate market for the enterprise today. Although it is a bold and strategic move, given the future of converged content inspection across multiple communications channels, IronPort must ensure it doesn't lose focus on its messaging security foundation as it builds expertise in HTTP security.

## **Marshal**

After the anticipated synergy with NetIQ's core business failed to materialize, Marshal separated from NetIQ in a management buyout (MBO) in late 2005. Unfortunately, NetIQ failed to invest in Marshal's product development, brand awareness and new features, and it damaged Marshal's reputation by decreasing customer support levels. Marshal is rebuilding itself, and the original founders and development team are back on board. The new company is back on track with regular product updates. However, the company is still understaffed, given the size of its client base compared with competitors, and it will have to grow rapidly. Although the MBO clearly reinvigorated the company, its acquisition detour reduced our opinion about the company's ability to execute since last year.

Marshal still has a significant installed base of customers, and the product excels in outbound content inspection with numerous dictionaries and pre-configured policies. It is reported to be easy to manage with hierarchical management, automatic population of policy to multiple nodes and a very intuitive GUI for Windows users. Anti-spam effectiveness declined under NetIQ management but seems to be recovering of late. Still, the product lacks support for DomainKeys Identified Mail (DKIM) or Sender Policy Framework (SPF) and is missing reputation services. Given customers' appetite for appliances and services, Marshal's software-only offering gets the company low marks for market responsiveness and limits its appeal. Encryption capabilities include policy-driven TLS and S/MIME. Marshal's Web product includes a proxy-based Web gateway with URL filtering, content analysis, and antivirus and spyware signatures, but it does not

include IM hygiene yet. Marshal's policy-driven archiving solution is also a positive factor.

## **McAfee**

Given its potential, McAfee has been surprisingly slow to react to the rapidly growing anti-spam market and customer needs, as evidenced by its minimal market share. Fortunately, in 2005 and 2006, it made great strides and is beginning to reach functional parity with some of the market leaders.

Improvements in anti-spam filtering, including streaming anti-spam updates (as frequently as every two minutes) and the licensing of Postini's Postini Threat Identification Network (PTIN) reputation system, seem to have cured past inconsistent spam detection rates, although support for SPF or DKIM is lacking. Value-added antivirus support is limited and, like Symantec, McAfee suffers from its success in the desktop market as buyers seek diversity of virus detection methods. McAfee enhanced its quarantine management and end-user quarantine controls with mail digests and individual block-and-allow list management. For management, McAfee relies on its universal management console ePolicy Orchestrator (ePO) for reporting and configuration. It provides excellent centralized configuration and policy synchronization and reporting, but it is constrained by its Microsoft Management Console format, and it is not as attractive or easy to use as other Web-based administration consoles. The lack of role-based administration (due in the next release) is notable for a management console that would typically be used by different IT departments. McAfee has very limited MTA capabilities. McAfee's Secure Content Management appliances have had outbound antivirus and content scanning for several years, including inspection of message attachments and dictionaries. Outbound scanning was enhanced in June 2006 with new regulatory compliance lexicons for HIPAA and privacy. TLS encryption was recently added to the appliance products, which also support external routing to third-party encryption tools but not on box solutions. McAfee was one of the first vendors to offer customers all three deployment types with a managed service offering delivered through an OEM relationship with Postini. McAfee gets high marks for its integrated e-mail and Web filtering appliances, which includes virus/spyware and URL filtering, but it is notably missing IM hygiene capability outside of blocking.

McAfee has an excellent channel, solid financials, global presence and a large installed base, giving it a high ability to execute. To achieve a higher vision score, McAfee needs to demonstrate more market leadership.

## **MessageLabs**

MessageLabs is a very mature service provider. It boasts the best international data center presence and a broad geographic customer presence. MessageLabs' own "Skeptic" heuristics e-mail filtering technology analysis is augmented with Symantec (TurnTide and Brightmail) anti-spam filtering. The company offers image detection services for intercepting pornographic images, a useful service for detecting acceptable-usage

violations. MessageLabs is noted for its outstanding antivirus protection, which has been successful at catching viruses before signatures were available from traditional antivirus vendors. Consequently, MessageLabs is able to offer a 100% virus detection service-level agreement. Outbound content inspection capabilities are above average and include dictionaries in multiple languages and credit card and SIN detection, but a canned HIPAA and SOX compliance policy is lacking, and workflow is limited. Encryption capabilities include native TLS and PostX policy-based encryption. MessageLabs was early to understand the significance of Web filtering investments. The company bought Omnipod, a small enterprise IM infrastructure vendor, as a platform to launch IM hygiene services expected later this year (see "MessageLabs Acquisition Deal Reflects E-Mail/IM Convergence"). An original partnership with ScanSafe to provide a hosted HTTP filtering service (URL filtering and anti-malware) was recently replaced by a MessageLabs' homegrown service. MessageLabs gets high marks on management ease because of the service provider delivery model; however, some customers have reported MessageLabs is less flexible in offering complex routing for global customers, delegated administration and self-service end-user controls. MessageLabs has invested wisely in building its channel and its data center infrastructure, thereby enhancing its ability to execute, its sales momentum and its mind share.

## **Microsoft**

Given its installed base of Exchange e-mail infrastructure users and the acquisitions of Sybari (soon to be called Forefront for Exchange) and Frontbridge (now called Exchange Hosted Services) — in addition to original investments in native anti-spam filtering — Microsoft is poised to become the de facto leader in the e-mail security market. Although its current market share is middling, it will be difficult to compete with the addition of anti-spam and antivirus services as part of both standard and enterprise licenses for Exchange 2007. We anticipate Microsoft will eventually use the Exchange Hosted Services data centers to forge into the software-as-a-service market with complete hosted e-mail infrastructure services in addition to existing IM hygiene services. Considering Microsoft's global customer base, Exchange Hosted Services must rapidly build out global data centers (it currently has six data centers in the United States and three in Europe), notably in Asia, or risk alienating regional customers.

While Microsoft's channel will be hard for incumbent leaders to beat, the SMB market — where cost and convenience are critical — will be the early adopters. Larger Global 2000 customers will continue to rely on best-of-breed vendors and be wary of investing in Microsoft for such core security functions. Moreover, pre-Exchange 2007 implementations face a bewildering array of components (ISA, antigen, Exchange Hosted Services and Exchange) with overlapping but not equivalent functionality, quality and completeness. For example, although both Exchange Hosted Services and Exchange server with Forefront security have outbound content inspection, the range of dictionaries and canned policy is wide. Similarly, encryption depends on the product or services, and without Exchange, MTA capabilities are missing.

Consequently, Microsoft clearly has the ability to execute and is poised for growth, but its current solution is overly complex and/or lacks key functionality common in competitors' products. Exchange Hosted Filtering Service is available as a stand-alone service that supports any SMTP mail platform, including Notes. Exchange Hosted Services has a large number of existing Lotus Notes customers that remain satisfied with the service; however, it is clear that Microsoft wants to enhance the "better together" integration story from server to client, and IBM Notes shops will not get the same integration attention.

## **Postini**

Postini is a very technically astute service provider, preferring to build its own core anti-spam and data center technology. Its e-mail processing is differentiated by all-in-memory processing rather than the store-and-forward method of rivals. Investments in fundamental data center design have led to lower costs and better margins — as well as better adaptability — than rivals. Anti-spam capabilities are very good and include connection management via PTIN and value-added antivirus capabilities with a 100% virus-free guarantee. From a product perspective, Postini has also invested in a number of recent ancillary services (encryption, archiving, IM hygiene, HTTP filtering) via a combination of native capability and the integration of numerous partner solutions. Postini provides better delegated administration capability for global and federated companies than rivals, and it has one of the best end-user capabilities in the market, including the ability for end users to set their own quarantine thresholds. Reporting could be improved, especially for connection management and for administration reports, and its outbound content filtering needs to mature.

Postini suffered from a lack of international channel partners and data centers, although data centers are planned in the Asia/Pacific region and Canada in the next 12 months. Although Postini has a larger enterprise installed base than service provider rivals, the difference is represented by customers with fewer than 500 seats.

## **Proofpoint**

Proofpoint continues to be a visionary player in our analysis, with a very solid product; however, its ability to execute declined since our last survey. Despite an influx of capital, Proofpoint has failed to develop a solid channel or improve its mind or market share. Proofpoint would make an excellent acquisition candidate for one of the companies in the Challengers quadrant, but we fail to see how it can break out of the Visionaries quadrant in a consolidating market. Still, given that leaders in this market are not immune to acquisition themselves, companies looking for best-of-breed technology should add Proofpoint to their shortlists.

Proofpoint gets high marks for ease of use because of an intuitive interface, simple policy implementation, solid reporting, and excellent global administration and consolidated reporting capabilities for large, complex multinationals. A beta Ajax interface, which allows for a very customizable dashboard, is promising. The company added Web-based

end-user quarantine to e-mail digests. Anti-spam capability, based on machine learning, is reported to be very effective; however, it lacks a reputation service. SPF authentication is supported, but DKIM will not be available until 2007. Customers report high Asian language spam detection accuracy and image-based spam. MTA capabilities are based on open-source sendmail. Outbound content inspection is also excellent, but advanced regulatory compliance and leak prevention capability cost extra. Encryption is delivered by integrating Voltage Security's Secure Messaging on an additional appliance. Proofpoint Network Content Sentry is a separate appliance that extends Proofpoint's SMTP e-mail-based outbound content monitoring and filtering features to HTTP and FTP message streams. Web mail handling is accomplished by recompiling Web mail into standard e-mail format. However, there is no enforcement on non-e-mail content inspection, only logging/alerts.

## **Secure Computing**

CipherTrust, a leader in our last Magic Quadrant, was acquired by Secure Computing in August of 2006. CipherTrust's flagship product, IronMail, is one of the most-full-featured appliance solutions on the market. Based on increased credit for advanced features, this year, Secure Computing/CipherTrust moves to the right in terms of vision. For anti-spam and antivirus defenses, it exploits its TrustedSource global reputation system, combined with connections management and several behavioral and content analysis tools, for very high spam detection with few false positives. Although the spam rules are pre-configured out of the box, users can tweak rules to suit their particular business requirements — a benefit to some, but an administration burden if customization becomes too complex. IronMail was early to offer content inspection, complete with dictionaries and regulatory policies, and integrated encryption. CipherTrust was also the first e-mail security vendor to have an IM hygiene platform that shares management and policy with the e-mail gateway. Although CipherTrust has made significant strides in improving manageability (intuitive graphical user interface [GUI], setup wizards, less reliance on rules, better reporting and monitoring), it is still the most common complaint from customers of earlier versions, illustrating the need for users to stay current with new versions.

The acquisition by Secure Computing has several positive points. It improves CipherTrust's viability, reduces acquisition uncertainty and improves its sales channel. There is little overlap between product lines. However, on the negative side of the ledger, we have lingering concerns about Secure Computing's market leadership ability in both the firewall market and now the e-mail security boundary market. Moreover, all acquisitions of this type incur transition disruptions. Secure Computing must continue to invest in CipherTrust's R&D to stay current with spam trends; early signs are encouraging — Secure Computing is keeping the CipherTrust R&D and Level 2 support in place. Given these conflicting issues, we rated this acquisition as neutral to CipherTrust's ability to execute.

## **Sendmail**

Sendmail is the “Red Hat” of open-source sendmail implementations. Sendmail is the overwhelming MTA market leader, and about a quarter of these implementations are corporate Sendmail customers (versus open-source sendmail implementations). The company exclusively targets large, complex enterprises that require platform flexibility and professional services expertise. The company founders were clearly innovators in MTA capability but decided early to focus on the integration of best-of-breed capability rather than integrate native security features. New corporate leadership sees the increasing importance of anti-spam/virus capabilities, encryption and outbound content inspection, but the strategy of using partners to deliver much of this functionality does little to improve the perception of high administration overhead of sendmail or reduce the cost of professional services to the midmarket buyers. Since this Magic Quadrant focuses on the needs of the broader midmarket, Sendmail's focus on the high-end, best-of-breed market relegates it to the niche market, and the company is refreshingly unabashed by this ranking.

Sendmail lost ground to the competition this year because we gave more credit to companies that have native capability. Sendmail has no native anti-spam capability, although it has good denial of service and address harvesting defenses and recipient verification to terminate unwanted connections at the gateway. It relies on Commtouch, Cloudmark or Brightmail for reputation and spam content filtering. Sendmail provides out-of-the-box, pre-built, privacy lexicons for HIPAA, GLBA and SOX and supports a broad range of attachment scanning. Encryption is delivered via policy-driven native TLS, PGP, S/MIME as well as through partners PGP, PostX and Authentica. Sendmail has its own archiving appliances solutions, so it gets high marks in that category.

## **SonicWALL**

SonicWALL acquired visionary vendor MailFrontier in February of 2006, increasing MailFrontier's channel dramatically and significantly increasing its financial viability. SonicWALL's primary market is the rapidly growing unified threat management (UTM) devices aimed at the midtier organization and below. The acquisition of MailFrontier gives SonicWALL the trifecta in UTM: network firewall and HTTP and e-mail filtering technologies. Still, its midtier focus did not significantly move SonicWALL's ability to execute for the Gartner client base. SonicWALL retains visionary status based on MailFrontier's capabilities; however, it must continue investing in the platform to retain this status in the future.

SonicWALL's focus is on extreme ease of use for its target midsize organization, so it is not surprising that larger-enterprise requirements, such as LDAP integration across multiple directories and SNMP traps for system management tools, are generally missing. The product has good Web-based end-user quarantine with individual control and rules, and central quarantines for inbound and outbound e-mail that are searchable and sortable. Spam effectiveness is very good, but most buyers we talked to were more attracted by the price. SonicWALL recently released a beta outbound content inspection functionality that includes record ID matching for pre-defined terms, including credit card numbers, Social Security numbers (SSNs), dates, custom and pre-defined policies for HIPAA, SOX,

NASD, Visa CISP, FERPA and data privacy regulations, along with common corporate governance requirements. Encryption is delivered through partners PGP and Voltage Security. Given the UTM focus of the company, it is not surprising that it scores very well in Web features. It can enforce user authentication for Outlook Web Access. SonicWALL Content Security Manager filters IM/P2P/HTTP/POP/SMTP and other protocols.

## **Sophos**

Sophos is a challenger in the desktop/server antivirus market and remains a challenger in the e-mail security market this year, with very little movement from last year. The Sophos brand is better-known in the U.K. and EU, where it does most of its business, but it is starting to get some recognition in North America. The company is well-known for providing excellent client services, abetted by a focus on creating easy-to-use products. It has colocated its threat research for virus, spyware and spam to provide better coverage of converged threats. Because of its core antivirus business, the company has excellent vendor viability, although longer term, the threat of antivirus commoditization looms if the company fails to execute on its client protection convergence strategy (see "Magic Quadrant for Enterprise Antivirus, 2006").

Sophos offers e-mail security solutions in software (Unix and Exchange) and recently released an appliance product (ES4000). Sophos also has a managed service offering that takes care of all appliance alerts (version control, availability and reliability of the hardware/software) outside of e-mail management. Capabilities and features vary across the Sophos product line, so buyers must ensure that the desired feature set is available in the desired form factor. For example, the ES4000 appliance does not yet support clustered deployments (this is due in the fourth quarter of 2006), while the Unix software does. Ease of management is a key design goal for Sophos, and it is launching a low-cost appliance for the small business in late 2006. Effective anti-spam is a derivative of multiple techniques, including reputation filtering, URL filtering to block bad destinations, and genotype filtering to block active campaigns and their variants. The appliance and UNIX products include full Postfix or sendmail capabilities. Outbound filtering capabilities include content inspection dictionaries covering credit cards, SSNs and HIPAA-related codes but are limited to the Unix compliance module. Encryption can be policy-enforced but is derived through partners (PostX, PGP and GlobalCerts) with only native TLS. Web investments include an OEM partnership with Akonix Systems but it lacks a shared IM and e-mail policy. The company has its own URL database and is beginning to develop a Web security appliance that is due in the fourth quarter of 2006.

Sophos is a solid competitor but needs to flesh out its appliance line and broaden its mind share to get into the leaders' category.

## **SurfControl**

SurfControl is a leading vendor in the URL filtering market (see "MarketScope for URL Filtering"), which accounts for approximately two-thirds of its total revenue and provides

a large customer base to cross-sell e-mail security solutions into. The company has seen a management shift in the past year, with a renewed focus on growth with a simplified licensing scheme (including one price for both Web and e-mail perpetual licenses). The company made a bold move recently (July 2006) with its acquisition of a small European e-mail security service provider, BlackSpider, which will launch the company into the service provider market (see "SurfControl Shores Up Its Market Presence With BlackSpider Buy"). SurfControl is one of the few vendors to offer all three delivery models. In addition to e-mail security, we expect this acquisition to enable SurfControl to launch a Web filtering service. The company has a relatively strong channel and good resources and international coverage, giving it high marks for ability to execute.

On the product front, SurfControl has been challenged to keep up in the highly competitive e-mail security market, in which vendors battle it out with rapid-fire releases of new features and functionality, which is a stark contrast to the sluggish status quo of the URL filtering market. SurfControl's strength is in its outbound custom e-mail content filtering. The company has improved its inbound e-mail security functionality during the past year, with more connection management and e-mail intrusion prevention, although it is still rather basic and lacks a reputation service. Limited IM hygiene capabilities that enable group and user-level blocking of public IM networks is a plus, but we would like the company to provide additional IM hygiene capabilities. Management has also improved, with more central reporting in the latest release. SurfControl's best chance for greater market leadership is with the convergence of SMTP and HTTP filtering and policy management, two areas in which it has significant experience. The accelerated growth of managed services for both also puts the company in a good position. SurfControl has a big task ahead to improve and harmonize functionality across all product lines to stay among the market leaders while adapting to a new service provider role and rapidly building out its data center presence.

## **Symantec**

Evaluating Symantec is not an easy task. On the one hand, it has enormous presence in this market, and numerous pieces of its e-mail security solution show great future vision, but the company has yet to integrate them into an easily consumable package that rivals the market leaders, which lowers its overall vision score. Symantec is the revenue market leader, albeit a portion is due to Brightmail's use in other vendors' solutions rather than direct sales of Symantec solutions. Brightmail remains the reference leader in spam effectiveness, but customers and partners complained about declining effectiveness in 2005 because of merger and integration activity. Effectiveness is improving of late, and attachment filtering improved in the latest release. Symantec invested in TurnTide's e-mail router solution to provide connection management; however, enterprise consumers are looking for all-in-one solutions and not component parts. Symantec's 8200 appliances is the embodiment of its integration strategy, but its immaturity is evident when compared against market leaders. Also, several technologies in the Symantec portfolio were notably absent in the first versions. The management interface and reporting are not fully fleshed out yet, and scalability is lacking. Advanced features, such as outbound filtering and native encryption beyond TLS, are also lacking, although Symantec has a

partnership with Voltage. We expect to see significant improvement and integration in the next two releases (due in October 2006 and the first quarter of 2007).

Symantec's market share in the desktop antivirus area is a liability in the e-mail security market for enterprise customers seeking virus signature diversity, and Symantec only recently released a non-signature-based antivirus technique to compensate. Symantec gets high marks for its early substantial investment in IM hygiene, buying market leader IMlogic, and it plans to integrate that functionality (see "IMlogic Deal Signals Convergence in 'IM Hygiene' Market" and "MarketScope for Instant Messaging Hygiene, 2006"). HTTP/URL filtering, however, could use more development attention. Two areas of strength for Symantec are its archiving integration with Veritas products and its vision of an end-to-end e-mail security infrastructure. Symantec is "dipping its toe" into the service provider market via a partnership with another management service provider.

We are disappointed that the company has not yet delivered all key functionality in one solution and is taking baby steps in emerging areas, such as managed services. Despite this and current product weaknesses, we don't doubt Symantec's commitment to this market nor its massive resources, channel and installed base; thus, the ability to execute is still high. We expect Symantec's integration and remediation work in 2006 to lead to much-stronger products in 2007 and beyond.

### **Trend Micro**

Trend Micro continues to disappoint customers with its painfully slow reaction to the e-mail boundary security market. Meanwhile, its dominance in the narrower e-mail antivirus market, with ScanMail and IMSS, will be challenged by Microsoft when the option to purchase antivirus (Sybari Antigen) and anti-spam services (Frontbridge) as part of Exchange 2007 becomes available. As a result, Trend Micro gets very low marks for market responsiveness. However, it continues to enjoy a large customer base, good financials and an excellent channel, giving it challenger status in ability to execute.

On the product side, Trend Micro has begun to change direction after several missteps. The acquisition of Kelkea, the innovator of reputation service, and the introduction of a native spam filtering engine (versus OEM of Postini's) were a good start to improve core functionality. Trend Micro now has connection and reputation management and some non-signature-based antivirus functionality for e-mail threats. Trend Micro also offers multiple delivery models with the recent introduction of a service and an appliance, thereby resolving issues that lowered its score in 2005. However, the market has not waited for Trend Micro, so it is still behind in several key areas. Management functionality continues to be a major challenge for customers. Centralized management and quarantine reporting will be available only next year. Outbound content filtering lags market leaders because of the lack of pre-configured content inspection policies. Encryption is notably missing, with only native TLS supported. Trend Micro IM security offers some IM hygiene capabilities for Microsoft's Live Communications Server implementations, but policy and management are not shared with e-mail products. MTA capabilities are limited. Overall, the product line is confusing, and a flagship appliance

product that can compete with market leaders is conspicuously absent, especially for a company that pioneered the network antivirus appliance with Network Virus Wall. The company must demonstrate a commitment to this market by accelerating feature development or risk falling back into being a niche antivirus supplier in 2007.

### **Tumbleweed Communications**

Tumbleweed Communications has a long track record in the e-mail security market and a good-size enterprise installed base. The company offers a comprehensive range of e-mail security boundary functionality, and it is one of the few vendors to offer its own best-of-breed e-mail encryption and content filtering capabilities in addition to strong inbound protection. Tumbleweed has strengthened its connection management and anti-spam capabilities during the past two years and licenses Commtouch for value-added antivirus protection. Tumbleweed has a series of appliances; the MailGate line was initiated by its 2004 acquisition of Corvigo, a company focused on the SMB market. Tumbleweed released an enterprise appliance in 2005 but has made little headway in the managed services segment or with IM or HTTP. The company must also make investments in these areas as the market moves swiftly toward consolidation.

Despite these product improvements, the company is growing slightly more slowly than the general market, causing it to lose market share. This lack of growth and its narrow geographic focus (North America) pushed Tumbleweed into the Visionaries quadrant.

### **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, skills, etc., 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 of the individual business unit to continue investing in the product, to continue offering the product and to 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 in order 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, 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, etc.

**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 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 product 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 set 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 verticals.

**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.