Companies should evaluate broader inbound e-mail security threat protection capabilities, not just spam filtering, from vendors. The e-mail security market is volatile, both from a technology and a business operations perspective.

ANALYSIS

The “Magic Quadrant for E-Mail Security Boundary, 1H05” (see Figure 1) replaces the “Magic Quadrant for Enterprise Spam Filtering, 1Q04” and focuses on anti-spam, e-mail antivirus (AV), and intrusion prevention capabilities to prevent inbound e-mail security threats (see Notes 1, 2 and 3). The e-mail security boundary market is volatile, both from a technology and a business operations perspective. E-mail security will continue to require best-of-breed investments, and companies should consider that this market is poised for further consolidation. Only a handful of credible enterprise e-mail security boundary vendors will exist by the end of 2006. Many vendors do not appear on the Magic Quadrant (see Notes 1 and 4), including Microsoft, which acquired Sybari Software (see Note 5). Gartner clients should pay close attention to the evaluation criteria we used for this Magic Quadrant; they may not reflect your company’s requirements and circumstances.

1.0 Leaders

CipherTrust has a strong enterprise installed base with its IronMail appliance and has historically focused on inbound e-mail security threats. The company supports Transport Layer Security (TLS) and has a homegrown Web-based e-mail encryption product, along with partnerships with other e-mail encryption vendors.

Note 1

What Is the E-Mail Security Boundary?

E-Mail Connection Management
The volume of spam continues to increase for companies, and Gartner clients routinely report 80 percent to 90 percent of all incoming e-mail they believe is spam. Consequently, new architectures and technologies are necessary to slow or drop e-mail traffic instead of the prevailing practice of quarantining all incoming mail. IP and SMTP connection management that is based on better rules or data (reputation), which is more effective than traditional real-time spam black lists, will be critical here. Furthermore, management and reporting capabilities that indicate which e-mails have been dropped also will be important. We refer to these as e-mail connection management.

Value-Added AV Capabilities
E-mail security boundary vendors will play a critical role in virus management for your organization, particularly in the time period before an AV signature is available. E-mail security vendors are well-positioned to pick up anomalous e-mail traffic or content patterns and allow enterprises to quarantine or drop suspicious e-mails. Furthermore, granular attachment filtering or blocking based on policy or security vulnerability information are important too. We refer to this as value-added AV. Companies will find these capabilities will be more effective than investing in multiple signature-based AV signatures.

E-Mail Intrusion Prevention
E-mail intrusion prevention sometimes receives less attention than other solutions to e-mail security threats, but protection against denial of service attacks, directory harvesting attacks (DHAs) and invalid or malformed addresses is critical. All three of the above are essential capabilities to be provided by your e-mail security boundary vendor.

Note 1 Continued on page 2.
Note 1 continued from page 1.

Delivery Models
To complicate further selection criteria for these solutions, multiple delivery model options exist — software, appliance and managed services. We evaluated vendors spanning all of these delivery models, although capabilities for vision and ability to execute were different in some instances. For example, with managed services, it is important to look at latency and data center capabilities (including international coverage), customer service, response capabilities, service-level agreements (SLAs) and relevant audit feedback or certifications.

Note 2
Inclusion Criteria for This Magic Quadrant
Inclusion criteria included the following:

- The vendor must have its own capabilities to block or filter unwanted e-mail traffic; supplementing with third-party vendors is allowable.

- The vendor must provide e-mail virus scanning (via its own AV engine or via licensing a third-party engine).

- The vendor also must also offer basic e-mail intrusion prevention capabilities.

- We included vendors that have the capability to support companies that reflect the Gartner client base.

Note 3
Key Vision Criteria
We weighted most heavily the inbound e-mail security threat management capabilities for this Magic Quadrant. However, outbound capabilities also were taken into account. We considered production capabilities of the vendors as of May 2005.

Note 3 continued on page 3.
Inbound Capabilities

- **Spam management** – We looked at the architecture and technologies for better e-mail connection management. For spam filtering, we focused on sophistication of detection and clients’ feedback on the effectiveness, cost and effort of administration. We expect leading vendors to have enterprise functionality, which is critical for large enterprises.

- **Management** – The extent of end-user involvement is critical to any spam-filtering strategy. Also, international companies often need delegated administration and separate policies for different business units or geographies. Conversely, administrators in large companies should be able to manage multiple quarantines from a central point. Management and reporting capabilities should be critical to any e-mail security vendor’s purchasing decision. End-user functionality, such as end-user white lists that allow individuals to designate e-mail they do not want to be blocked as spam, and Web-based or Outlook integrated end-user quarantines, which allow users to easily check and release what messages have been blocked, are crucial.

- **Value-added AV capabilities** – Companies should also prioritize investments in value-added AV.

- **Research and content** – E-mail security threats are constantly changing. We expect companies to have strong research and content capabilities as well as be tracking and planning strategies for protection against emerging threats that may span protocols, for example, phishing, spyware, zombies/bots, and consumer IM and Webmail vectors. We tracked the quality of the vendor’s installed base and partnerships for receiving quality data for e-mail connection management and emerging threats.

- **Multiple delivery models** – Many Gartner clients are interested in multiple delivery models: software, appliance and managed services. We expect leading vendors to have some type of capability across all three of these models. "In the cloud services" will be more prevalent, and leading vendors should also investigate inclusion of their technologies or operations in this area. This does not mean we expect software or appliance companies to suddenly become service business specialists. Rather, leading vendors should recognize the opportunity and license their technology to, or otherwise partner with, relevant providers.

Outbound Capabilities

Increasing business requirements for outbound filtering are influencing buying decisions for e-mail security. Companies may want to consolidate the number of vendors of products they use for e-mail security. While we did not prioritize outbound e-mail filtering capabilities in our weightings, we did evaluate the vendor’s current functionality and partnerships in these areas.

- **Outbound content filtering** – The important capabilities for outbound content filtering are rules templates provided by the vendors for offensive content and industry regulations. Furthermore, the ability to create custom rules as well as appropriate workflow functionality for administration and reporting are essential.

- **E-mail encryption** – Companies are increasingly evaluating their e-mail encryption requirements. Desktop e-mail encryption deployments for large numbers of consumers or partner should be tackled by specialized vendors. However, TLS encrypts e-mail from gateway to gateway, and it is a comparatively simple way to secure sensitive mail with known partners. TLS functionality should be part of a standard e-mail security boundary solution. Leading vendors should provide TLS support. We expect vendors to also offer their own homegrown products or technology partnerships with best-of-breed vendors for desktop or staging server e-mail encryption deployments (see "No Vendor Can Fulfill All of Your Encrypted E-Mail Needs.") This is important because the filtering and policy functionalities from your e-mail security boundary vendor will often determine whether the e-mail should be encrypted as it leaves the gateway.

Key Ability to Execute Criteria

Our ability to execute criteria intersects with our vision criteria and examines whether the vendor has the finances, resources, channels and management record to make the technology and business investments necessary to be a longer-term player in this market. However, technology markets typically follow a distinct life cycle. This market is moving from an emerging one to the high-growth stage, poised for consolidation. At this stage, it is important that vendors invest in growth to push to the wider market. Many vendors in this
market are small, privately held and venture-backed companies with limited resources. In some instances, this means we may have weighted what we consider to be appropriate growth strategies over profitability.

We assessed channel and partnership arrangements, finances and access to capital to make acquisitions or developments in emerging areas. Customer service and organizational capabilities were based on Gartner client feedback. We also evaluated the strategy and road maps of the vendor, as well as the management vision and track record. Ability to execute factors, such as the strength of the channel, marketing and brand, are important indicators for success. Another criterion we weighted particularly highly was the extent and quality of the vendor’s enterprise installed base. As such, vendors with significant financial resources and a strong channel – even with a limited track record of strong vision or timely features and functionality for e-mail security - may have a relatively high ability to execute position.

Note 4
Vendors Not on the Magic Quadrant
The spam-filtering market is a crowded one, and many vendors that have enterprise solutions were not placed on the Magic Quadrant.

Examples of vendors in this category are: BlackSpider Technologies (which operates in Europe), Infocrossing (which acquired MailWatch in 2004), IntelliReach and MessageGate (which focuses on outbound filtering).

Note 5
Microsoft and the E-Mail Security Boundary
Microsoft acquired Sybari Software in February 2005. Sybari had a strong reputation with large companies because of its efficient AV scanning for the Exchange platform. Edge Services with Exchange 12 will be available in the first half of 2007 (0.8 probability). Spam filtering, AV and anti-spyware engines and update services will likely be available as separate add-on services. However, Gartner does not expect Edge Services to have a significant market impact before 2009. Some companies will want to delegate some responsibility to users to view quarantines or to set up rules within internal e-mail servers or e-mail clients. Microsoft’s initiatives should, however, spur best-of-breed anti-spam vendors to provide better integration and management of Microsoft’s and other vendors’ e-mail client/server platforms.

CipherTrust has improved its outbound filtering capabilities and has several prepopulated dictionaries. Unfortunately, as the volume of spam increases, the degree of granularity offered by IronMail for spam filtering has become an issue. However, the company has offered Connection Control for blocking e-mail connections from bad sources and filtering setting templates, to ameliorate the ascending administration requirements. The company should develop relationships with partners for broader e-mail “reputation” information.

FrontBridge Technologies has been adept at building its installed base and brand via channel partners, such as Sprint. FrontBridge was early to focus on outbound filtering and acquired MessageRite, an archiving service, in July 2004. FrontBridge also hosts management for the Voltage Security e-mail encryption products. FrontBridge has reasonable inbound e-mail security threat capabilities, such as connection management and intrusion prevention. However, the company must focus on value-added AV. Similar to MessageLabs, it does not support end-user white lists.

IronPort Systems continues to offer one of the stronger solutions for inbound e-mail security threats. IronPort’s architecture, in which a large percentage of e-mails can be blocked, based on its reputation database (SenderBase), is one that, according to some Gartner clients, appears to meet volume requirements quite well. The company’s competitors are beginning to offer similar architectures. IronPort has invested in AV protection beyond traditional signature detection. IronPort needs to strengthen its outbound functionality and provide prebuilt dictionaries, custom rules and better workflow management. Despite a contract with Symantec for Brightmail anti-spam through 2008, IronPort will likely have to provide alternative spam-filtering options, either homegrown or with another partner. IronPort’s struggles

Continued from page 1.
will be to fend off the might of Symantec in the channel and to significantly differentiate its offering from Symantec’s.

Postini continues to have an effective spam-filtering managed service and an extensive enterprise installed base. Postini has invested in significant end-user capabilities (including end-user white lists) and granular administration. Postini has connection-management capabilities, and the company has extended its AV engine support. However, Postini continues to lag behind on the outbound filtering functionality. Although TLS is available, the company has no e-mail encryption partnerships. Postini should extend its anti-phishing capabilities and evaluate Web-based threats. Limited international operations and the absence of heavyweight channel partners hinder the company’s ability to execute.

MessageLabs, a managed service provider, has improved its ability to execute over the past year. Its vision position has improved as a consequence of the wider lens of this Magic Quadrant, which goes beyond anti-spam capabilities. The company increasingly relies on content from other providers. In 2004, MessageLabs licensed the TurnTide “traffic shaping” technology (refer to Note 1) and Brightmail for anti-spam, from Symantec, to augment its own capabilities. MessageLabs has invested in value-added AV (quarantining and inspecting attachments and rules based on traffic patterns for detecting malicious code before a traditional signature is available) and has combined this with great marketing. “Reputation” and IP-based filtering must be given similar attention. MessageLabs has outbound capabilities (although the service needs better dictionaries and appropriate management and reporting). MessageLabs must focus on end-user capabilities and ensure its centralized approach to spam filtering is easy to administer. Channel partners in North America have increased MessageLabs’ brand clout and installed base. Fast growth must not lead to deteriorating customer service, as occasional reports suggest.

Symantec’s acquisition of Brightmail in May 2004 has turned the company around, elevating it to an industry leader in e-mail security products. Symantec has released traffic-shaping appliances, incorporating the technology from TurnTide, and it has a new appliance option. Brightmail’s reputation remains unsurpassed for ensuring that spam filters don’t block legitimate e-mail (false positives). However, Brightmail’s engines, combined with increasing spam volume, means more processing horsepower is required. Symantec will need to persuade customers to slow or drop more traffic, as well as provide better reporting to allow them to do so. Symantec needs to improve its outbound filtering and e-mail encryption capabilities, but the product line’s marriage to the Symantec AV engine will be a perceived drawback, because many companies like to diversify the number of AV engines they have and would like to have a different AV engine at the Simple Mail Transfer Protocol (SMTP) gateway than the one they have on the desktop. The company must focus on innovation in intrusion prevention and provide value-added AV. Symantec also launched a managed service that is being hosted by one of the best-of-breed e-mail security managed service providers. The company has licensed its anti-spam (and, in some cases, traffic shaping) to several competitors, such as IronPort, BorderWare Technologies, MessageLabs and MX Logic, which could lead to brand confusion in the short term.

2.0 Visionaries

Proofpoint continues to offer a strong enterprise-class e-mail security solution. Proofpoint is differentiated by its global administration and reporting capabilities, which are critical for large, complex multinational companies. Many competitors’ products are still playing catch-up to Proofpoint’s management functionality. Proofpoint also uses its engine for outbound compliance initiatives and has established relationships with best-of-breed e-mail encryption vendors. Proofpoint, however, has not made as great strides as we might expect in the e-mail connection management area, one we regard as important. Proofpoint must also fill out its value-added AV services.
MailFrontier continues to be an innovative player in the e-mail security boundary market. The company has invested in connection management and spam filtering. The company has shown vision with early partnerships for anti-phishing, for example with Cyveillance, and by rolling out a consumer desktop partnership with Zone Labs. We hear from clients that good customer service with an easy rollout is a typical experience. However, MailFrontier still has a small enterprise installed base and caters largely to midsize companies. Outbound filtering capabilities need to be improved. MailFrontier has released an appliance, but it is based on Windows, which may limit its appeal to large enterprises.

MX Logic has lagged behind the other e-mail security managed services vendors (FrontBridge, MessageLabs and Postini) on this Magic Quadrant, but it is strong from a technology and innovation perspective. The company supports end-user white lists, provides an Outlook end-user quarantine and has licensed Brightmail anti-spam from Symantec. MX Logic does not yet support TLS (or have any partnerships with vendors that provide e-mail encryption for large-scale deployments – refer to Note 3), and it has no prepopulated compliance dictionaries or specialized policy and reporting functionality for outbound filtering for compliance. MX Logic has increased its visibility with a recent “white label” agreement. However, MX Logic must expand its international operations.

3.0 Challengers

McAfee’s e-mail security boundary capabilities lag behind significantly, and the majority of enterprises will look to more-focused providers. McAfee provides limited-to-no-connection-management capabilities or intrusion prevention. It has extremely minimal outbound filtering and does not support or partner for e-mail encryption. McAfee does not have an end-user quarantine for the gateway product, and it has no central quarantine or delegated administration. Only extremely limited protection against newer threats, such as anti-phishing, is provided. McAfee must make an acquisition to garner enterprise credibility in the e-mail security market.

Sophos acquired its spam-filtering technology from ActiveState in 2003. However, despite the company’s global channel and operations, its presence among Gartner clients appears limited. As the volume problem with spam has increased, Sophos’ rules-based approach has meant heavier administration and server investments for customers. Sophos must invest in better connection management and offer multiple delivery models. Sophos offers strong policy management and reporting and provides reasonable outbound filtering capabilities, although e-mail encryption is lacking.

Trend Micro continues to lag behind in the e-mail security market. While the agreement with Postini was renewed, and Trend appears to be receiving more timely updates, questions remain over the long-term relationship. Trend has significant gaps in its e-mail security capabilities. Trend has no connection management and e-mail intrusion prevention. The company does not provide significant outbound filtering capabilities. TLS is not supported, and Trend does not have partnerships with e-mail encryption vendors. Instant messaging (IM) filtering also is not supported. Trend’s management functionality lags considerably. Trend does not provide a Web-based user quarantine, and Gartner clients note that reporting is highly burdensome. An enterprise appliance for e-mail security is not available, and the company does not offer managed service options. Trend’s lack of leadership in this area is perplexing, because the company has considerable resources and a significant enterprise installed base with its AV product for Simple Mail Transfer Protocol (SMTP).

Tumbleweed Communications has strengthened its e-mail security capabilities over the past year, and it has introduced appliances for e-mail connection management
and invested in anti-phishing. The company does not yet offer a combined enterprise-level anti-spam and connection management appliance. Gartner clients indicate Tumbleweed’s spam-filtering subscription service is improved but not always best of breed. Tumbleweed excels with its outbound filtering capabilities and is one of the only vendors to have a full range of homegrown best-of-breed e-mail encryption.

4.0 Niche Players

Barracuda Networks has significantly capitalized on open-source spam filtering and open-source AV products and is extremely reasonably priced. Yet Barracuda provides enterprise functionality at a level above many of the company’s higher-priced competitors. Barracuda has some connection management capabilities, basic e-mail intrusion prevention, and an end-user quarantine and scoring. Barracuda’s outbound filtering for compliance is fairly limited and so is the reporting. The company also released a uniform resource locator (URL) filtering appliance in April 2005. However, effective and extensive virus detection is critical at the SMTP layer, but Barracuda’s lack of a commercial AV partnership and value-added AV investments are a downside. The company has also provided quite significant international capabilities within its products. Barracuda has a large installed base among midsize companies, and the education and public sectors.

BorderWare Technologies has traditionally a strong presence in Europe and with the defense community. The company’s relationship with Brightmail increased recognition. The company has a partnership with 3Com for integrated small office/home office (SOHO) appliances. The company’s firewall experience may prove useful for innovation with emerging Web-based threats. BorderWare’s spam filtering is reasonable for midsize companies. To be an enterprise player, the company must invest in value-added AV capabilities and in outbound filtering for compliance, with prepopulated lexicons and broader e-mail encryption capabilities (the current product supports TLS).

Clearswift’s MIMEsweeper product line has been through a tumultuous period until the past year. We continue to hear complaints from Gartner clients about heavy administration load, and low spam detection and high false positives, especially with earlier product versions. Although the latest version supports spam URL real-time black lists (SURBLS), connection management and e-mail intrusion prevention are limited. MIMEsweeper has powerful outbound custom rules features, as well as good attachment scanning for inbound e-mail filtering. Clearswift has some prebuilt compliance-focused dictionaries, supports TLS and has IM filtering partnerships. The company still has a large enterprise installed base, and many organizations continue to use the product for outbound scanning, while augmenting for inbound e-mail security threats.

Cloudmark has been a pioneer in the consumer e-mail security arena. Cloudmark detects e-mail security threats based on real-time community feedback. Cloudmark has developed anti-phishing capabilities and offers a plug-in for consumers. We expect Cloudmark to continue to innovate in the consumer realm and to be widely used among Internet service providers and financial service providers. Cloudmark licenses its anti-spam engine to several vendors, such as Sunbelt Software and Sendmail. As enterprise e-mail security providers seek to augment their own content capabilities, and as reputation and behavior data becomes more important, the Cloudmark engines are expected to be widely licensed by vendors in this market. However, the company’s direct capabilities for providing enterprise products and support are limited.

Mirapoint has broad protection against a wide range of e-mail security threats. The RazorGate appliance has connection management and intrusion prevention and
augments its own spam filtering with signatures from Commtouch. Good end-user controls are provided. RazorGate provides some outbound filtering capabilities (although no pre-built dictionaries exist), but reporting and management is limited. Mirapoint has a limited enterprise installed base with RazorGate; Mirapoint’s messaging appliance drives the majority of its revenue.

**NetIQ** has not yet used its resources to capitalize on the MailMarshal brand and extend its installed base. However, the company appears to be refocusing some business and technology efforts on MailMarshal. The current version of MailMarshal has limited connection management and e-mail intrusion prevention. TLS is not yet supported within its product. The company has not capitalized on the URL filtering capabilities. For example, it does not support SURBLS. MailMarshal’s core strength in content filtering and enterprise management has not been extended to a strong outbound offering with prebuilt lexicons for compliance.

**Sendmail** sells several security and messaging product modules for the Sendmail message transfer agent (MTA), and the company caters to large, complex organizations. The product modules include e-mail connection blocking and e-mail intrusion prevention. Sendmail licenses spam filtering from Cloudmark. The company has outbound filtering functionality and offers directory integration and reporting capabilities for large-scale enterprises. However, the company offers a complicated software product portfolio for Sendmail infrastructures, which limits its appeal.

**SurfControl** is still predominantly a URL filtering vendor; however, some of the converging Web-based threats may play to its strengths by 2006. SurfControl has limited e-mail intrusion prevention and rudimentary e-mail connection management and reputation functionality. The company’s spam filtering can be heavy to administer. SurfControl has an appliance and has improved its end-user functionality and management. While outbound filtering for offensive content remains a differentiator, prepopulated dictionaries and compliance features are not well-supported.

### 5.0 Bottom Line

Companies should evaluate e-mail security boundary solutions through a broader lens. Companies should pay particular attention to the architecture and mechanisms for efficiently and accurately blocking or slowing e-mail from bad sources, low administrative overhead of the solution, e-mail intrusion prevention and value-added AV capabilities.

---

**Acronym Key**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AV</td>
<td>antivirus</td>
</tr>
<tr>
<td>DHA</td>
<td>directory harvesting attack</td>
</tr>
<tr>
<td>IM</td>
<td>instant messaging</td>
</tr>
<tr>
<td>MTA</td>
<td>message transfer agent</td>
</tr>
<tr>
<td>SLA</td>
<td>service-level agreement</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>SOHO</td>
<td>small office/home office</td>
</tr>
<tr>
<td>SURBLS</td>
<td>spam URL real-time black lists</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>URL</td>
<td>uniform resource locator</td>
</tr>
</tbody>
</table>