

## **Magic Quadrant for Enterprise Spam Filtering, 1Q04**

**Many enterprise spam-filtering vendors will be gone by 2005 because of market volatility, and most vendor positions will radically change within six months. Choose vendors according to their detection and management capabilities.**

---

### **Core Topic**

Security and Privacy: Security Infrastructure

### **Key Issue**

How can enterprises secure e-mail, stop malicious code and reduce spam?

### **Strategic Planning Assumptions**

By year-end 2004, fewer than 10 enterprise spam-filtering vendors will remain (0.8 probability).

By 2005, the stand-alone spam-filtering market will evolve into a boundary e-mail security market (0.8 probability).

Enterprises must tread carefully in the enterprise spam-filtering market. Although there is pressure to implement a solution quickly to address massive spam volumes, confusing vernacular abounds (for example, machine learning, Bayesian logic and heuristics), and many solutions are offered by unknown startups. Dozens of vendors claim to have the best products, highest detection and lowest false-positive rates. Also, the enterprise spam-filtering market is poised for rapid consolidation and acquisition. This is an inevitable evolution for most nascent technology markets, and illustrates that the spam problem will not disappear for at least three years.

Larger vendors see significant opportunities in this emerging market, and enterprises will prefer more-consolidated e-mail security solutions over time. Instead of having several e-mail-security-related point products at the boundary, many enterprises will want only one or two. Antivirus software, basic e-mail server security protection, and inbound and outbound content filtering will form the core of boundary e-mail security solutions.

During this functionality consolidation, many vendors that offer spam filtering will fail, others will be acquired and several will succeed. Although firewall, Web-filtering and antivirus vendors will invest in spam-filtering technology, best-of-breed functionality will continue to be the primary criterion for enterprises choosing a spam-filtering vendor through 1Q05. Successful vendors will develop better detection and management capabilities for spam-filtering solutions, and build out their broader e-mail security offerings.

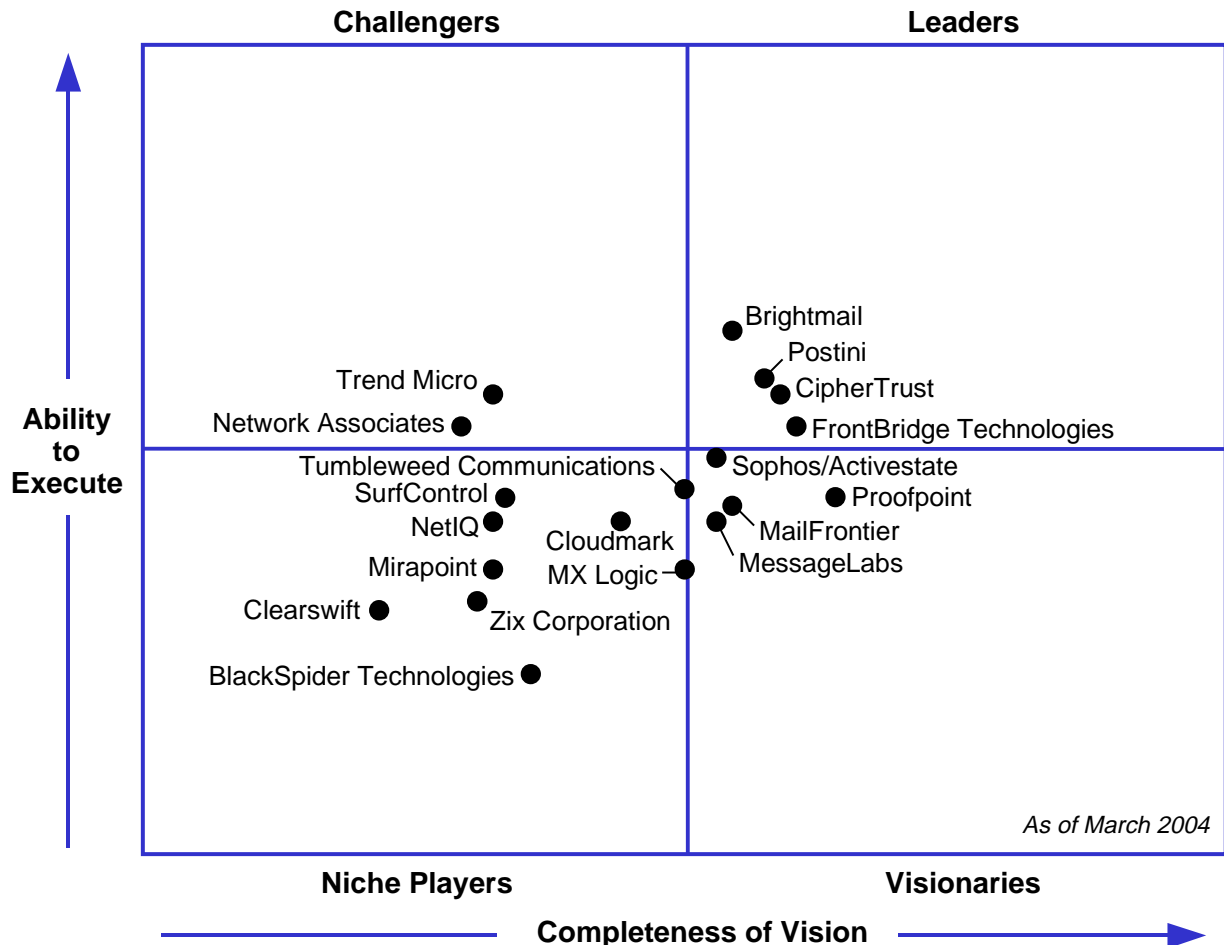
For the Magic Quadrant for Enterprise Spam Filtering, 1Q04 (see Figure 1), vendors were evaluated according to their ability to provide enterprise spam-filtering capabilities. Because many enterprises don't know if they will choose spam-filtering software,

### **Gartner**

© 2004 Gartner, Inc. and/or its Affiliates. All Rights Reserved. Reproduction of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

appliances or managed services, we included all three, although the evaluation criteria varied (see "Magic Quadrant Evaluation Criteria for Spam Filtering, 1Q04"). The North American market was emphasized in this evaluation — for example, when evaluating factors such as brand and business clout, and installed base — because the majority of Gartner clients that have implemented spam-filtering solutions have been based in North America (although they often deploy spam-filtering technology for their international operations).

**Figure 1**  
**Magic Quadrant for Enterprise Spam Filtering, 1Q04**



Source: Gartner Research (March 2004)

### Leaders

Leaders have most or all of the best-of-breed features and functionality that enterprises require for effective spam filtering. They demonstrate capabilities to move to the next level of customer needs, and support large enterprises effectively. In this Magic Quadrant iteration, the leaders are small, privately held companies. Ability-to-execute positions indicate *relative* business operations that are relevant to enterprise spam-filtering needs through 1Q05.

**Brightmail** has significant brand recognition, although its transition from managed service provider (MSP) to software provider has been bumpy. It has started to catch up in the features area, and it's a good option for enterprises with deletion and low-false-positive spam-management strategies. Brightmail must provide functionality beyond spam filtering to better cater to enterprise needs.

**CipherTrust** is an e-mail security appliance vendor that leads with features and provides large enterprises with a range of related e-mail security functionality. It faces greater competition as firewall vendors aggressively market appliances in this area. CipherTrust must incorporate best-of-breed functionality for content filtering and encryption to stay ahead.

**Postini** and **FrontBridge Technologies** are MSPs. Postini, along with Brightmail, has significant brand recognition and was one of the earliest vendors to offer end-user spam tuning and quarantines. However, it has not entered Europe, and must focus on extending its infrastructure and strategy to wider e-mail security needs. FrontBridge, despite lacking Postini's brand recognition, also has shown strong vision. It can effectively support larger enterprises looking for managed spam-filtering services.

## **Visionaries**

Visionaries have demonstrated strong vision and offer a full range of the functionalities that enterprises require for effective spam filtering: sophisticated detection, management and spam content expertise. Visionaries may not have as well-established an enterprise installed base or business operations as leaders.

**Activestate** was acquired by **Sophos**, a highly regarded U.K.-based antivirus vendor, in September 2003. Activestate is a strong software solution that has been attractive to midsize organizations. This is Sophos' first acquisition, and there will be a transition period, especially because Sophos has succeeded as an original equipment manufacturer partner to several spam-filtering vendors (including CipherTrust). Activestate customers likely will benefit in the long term from Sophos' reputation for product quality and excellent customer service.

**Proofpoint** is a new entrant to this market, but has garnered significant traction in large enterprises. Proofpoint provides a software solution, and has innovative detection methods and good management functionality.

**MailFrontier** gained recognition with its consumer-focused desktop product. It has developed a software gateway product

with strong detection and management. Although partnerships with Cyveillance and Sygate are interesting, MailFrontier must focus on antivirus and e-mail server security.

**MessageLabs** is a U.K.-based MSP with a stellar record for its antivirus service, which remains its core differentiator. MessageLabs must focus on improving spam management functionality and related e-mail security services.

## Challengers

Challengers have more-extensive business and financial resources, but they lag significantly in vision and comprehensive features and functionality.

**Trend Micro** licensed the Postini engine to supplement its spam-filtering functionality in early 2003. Although Postini's capabilities are available in Trend's core e-mail antivirus product, InterScan Messaging Security Suite, limitations remain in detection and, especially, management and reporting capabilities.

**Network Associates** acquired Deersoft in January 2003. Deersoft's spam-filtering technology was available with the e500 and e1000 appliances in late 2003 (Domino and Exchange also are supported). Similar to Trend, detection and management capabilities are lacking.

Despite their significant resources, these antivirus vendors lag considerably behind best-of-breed vendors. Therefore, antivirus and firewall vendors likely will quickly acquire better technology.

## Niche Players

Niche vendors have more-limited business resources or focus. They also have gaps in vision, features and functionality.

**Tumbleweed Communications** has the strongest software spam-filtering solution in detection and management capabilities of the traditional content-filtering vendors. It made significant improvements to its spam-filtering capability in 2003, although its detection and management features lag behind the leaders. Tumbleweed's core differentiator is that it also has best-of-breed outbound e-mail content filtering and e-mail encryption (which is a separate product). Tumbleweed likely will be well-positioned to meet broader enterprise e-mail security needs, particularly if it focuses on a non-Windows appliance.

**Cloudmark** has strong spam detection, but it also has a strong consumer/Internet service provider installed base. It is not

entirely focused on serving enterprise requirements, which will be a challenge through 1Q05.

**MX Logic**, an MSP, is another recent addition to the market. It has developed a strong set of detection and management capabilities, but must focus on building a wider installed base and business operations to serve enterprise customers effectively.

**SurfControl** is a leading Web-filtering vendor, but it has significantly penetrated the e-mail content-filtering market or spam-filtering area. SurfControl's spam-filtering capabilities are included in its e-mail filtering product. The optional spam agent (for the signature database) is bundled for free with the e-mail product in the first year. Enterprises appear to choose SurfControl when they have a relationship with it. Some desired features (for example, end-user quarantine) are not provided by SurfControl.

**NetIQ** acquired MailMarshal in 2002, but the business integration between the two vendors doesn't appear to be complete. MailMarshal is lagging considerably in detection sophistication and management (for example, it only provides a Microsoft-Management-Console-based console).

**Mirapoint** is a small messaging vendor that offers a messaging server appliance and an e-mail security appliance. It must focus on enhancing its spam detection and management capabilities, because competition from firewall vendors will intensify in the e-mail security appliance space.

**Zix Corporation (ZixCorp)** is an e-mail encryption service provider with a significant installed base in healthcare. It acquired Elron Software, a content-filtering vendor, in September 2003. Elron was developing spam technology prior to the acquisition; ZixCorp's spam capabilities are thus a work in progress.

**BlackSpider Technologies** is a U.K.-based spam-filtering MSP that also provides antivirus and content filtering. It focuses exclusively on Europe and is in the early stages of its operations.

**Clearswift**, despite its extensive installed base and its reputation for content filtering, has not delivered the level of detection, management and administration capabilities that many enterprises require.

### **Vendors Not on the Magic Quadrant**

BorderWare Technologies, IronPort Systems and Sendmail are secure e-mail gateway appliances that have spam-blocking

capabilities, but also license other vendors' spam-filtering software and updates. Many enterprises bought these appliances during the past 18 months to obtain better spam filtering. Some secure e-mail gateway appliance vendors, such as CipherTrust and Mirapoint, only have their own spam detection and filtering technology, and thus have been placed on the Magic Quadrant. BorderWare, IronPort and Sendmail offer mechanisms to detect and block spam, but they also supplement or replace their detection capabilities with spam filters that detect and classify spam e-mails.

**BorderWare** has a track record in firewalls and security (it was spun out from Secure Computing). BorderWare appeals mainly to the midtier market. It has its own spam-filtering detection and classification capabilities, which are not sufficient for enterprise use, that can be swapped out for Brightmail's detection capability.

**IronPort** sells a secure e-mail gateway and caters to larger, high-end enterprises. It has a particularly good quality appliance and message transfer agent, and it provides spam blocking via its reputation database, augmented with a spam filter that classifies spam. It works closely with Brightmail.

**Sendmail** sells a commercial version of an open-source secure e-mail gateway. It offers spam-blocking capabilities, and it can also supplement its detection capability, and classify spam, using the Cloudmark engine. Its update capabilities and reporting functionality are basic.

Other vendors that offer various levels of spam filtering include:

- **BT Syntegra** is a messaging service provider (spun out from British Telecommunications). Syntegra licenses Brightmail for spam-filtering technology, and other vendors for encryption and antivirus capabilities.
- **GROUP Technologies** is a Germany-based vendor with a good track record for its Lotus Notes and Exchange content-filtering and spam-filtering products. Its SMTP product is early to the market.
- **Symantec** provides spam filtering in its antivirus gateway product and via plug-in for Notes and Exchange products. Only rudimentary spam-filtering functionality is provided.
- **webwasher** is a German Web-filtering vendor with a strong reputation that has also developed e-mail content-filtering and spam-filtering software (in addition to licensing Mailshell).

### **Microsoft and Third-Party Products**

Outlook 2003 has enhanced user "white list" and junkmail capabilities, and Exchange 2003 will have basic inherent filtering and via application programming interfaces and third-party spam-filtering engines. However, enterprises will need to rely on third-party spam-filtering products for enterprise-level detection and management capabilities. Some enterprises will want to devolve some responsibility to users to view quarantines or to set up rules within internal e-mail servers or e-mail clients.

Third-party spam-filtering vendors must provide better support for e-mail rules from native e-mail clients and servers within their gateway solutions. Management, reporting and boundary strength will become more important for vendors as Microsoft becomes involved in the market.

**Bottom Line:** The enterprise spam-filtering market is highly immature and volatile. Evaluating vendors that offer the best-of-breed functionality that fits your spam-filtering strategies is critical. Carefully consider the vendor's core business fundamentals and if it has a quality installed base to mitigate short-term vendor risks. Understand that your vendor may be acquired or exit the spam-filtering space during 2004.