How to Select Spam-Filtering Products and Services

Choose a spam-filtering solution by evaluating anti-spam providers' management, research and service capabilities, as well as your architecture, business and user requirements for spam-filtering technologies.

Where should I position anti-spam technology in my architecture?

Anti-spam technology usually is set up at one of four locations: an outsourcer, an internal SMTP mail relay, a native e-mail server (for example, Microsoft Exchange or IBM/Lotus Domino) or the desktop (see Figure 1). Choosing the most-appropriate location partly depends on the size and culture of your enterprise.

### Figure 1
Anti-spam Architecture Choices

- **Evaluation Criteria**
  - Ease and speed of implementation
  - Licensing model
  - Vendor relationships
  - Reporting flexibility

Source: Gartner Research (August 2003)
Outsourcer or internal SMTP mail relay: Usually, you should position spam filtering at the outermost edge of the e-mail boundary using an outsourcer or licensed software, or an appliance at the internal SMTP relay. This "catches" the spam before it travels the internal network and consumes bandwidth and, potentially, storage, once it reaches the native e-mail servers (for example, IBM/Lotus Domino, Microsoft Exchange and Novell GroupWise).

Native e-mail server: There is limited need to put additional anti-spam filtering at the native e-mail server (for example, Domino or Exchange) if you already block spam at the SMTP level or use an outsourced spam service. However, spam filtering should be considered where the native e-mail server also acts as the enterprise Internet SMTP mail relay. There may be a need for outbound or internal e-mail content filtering for regulatory compliance or IP protection purposes on internal e-mail servers.

Desktop spam filtering: There is widespread popular sentiment that spam filtering can and should be done only at the end-user level because spam is subject to personal choice. However, there are significant business and security risks from spam. Implementing centralized policies typically is the best way to reduce enterprise risk. Moreover, enterprise anti-spam products and services have limited capabilities for incorporating end-user-specific rules or "learning" into a boundary policy. Most enterprise vendors can support end-user "whitelists" (e-mail addresses and domains that should not be blocked). Established and new vendors will improve end-user-specific rule management in 2004. However, in the short term, this is the least appropriate location for enterprise use because of problems such as a lack of centralized management of enterprise-level filtering policies and deployment of desktop software.

In some situations, desktop spam filtering may be effective:

- As a "stopgap" measure for a select group of users (while enterprisewide spam filtering is being evaluated)
- For small businesses that can't afford an enterprisewide application
- In academia, where personal choice and freedom of speech issues may be imperative

The top priority for most enterprises is to stem the volume of spam and mitigate risks from offensive or malicious content. These goals can be met most efficiently by central controls, including workgroup- or geography-specific policies (see "Spam Filtering Works With a Management Policy").
Should I choose anti-spam licensed software, appliances or outsourced services?

This decision is based on your requirements and capabilities, while considering the trade-offs. Look at the number and capabilities of your IT or e-mail staff who will manage and operate the solution, as well as user and business requirements. Appliances are attractive if you don't want to lock down and administer your servers. Software solutions allow you to pick your hardware and setup. Outsourced services do not require upfront hardware and implementation investments. They will reduce administrative costs and possibly offer better quality of service to users. However, these services can be expensive for large enterprises. Also, they require administrators to deal with user issues and coordinate with service providers for policy changes or queries.

Advantages of using outsourced services include (see "Outsourcing Spam Filtering and E-Mail Boundary Services"):  

- They are pass-through services; the outsourcer does not hold messages. Your mail exchange record, which identifies which e-mail server handles your Internet e-mail, will need to point to the outsourcer. The outsourcer applies the "signed-up for" services to each message, then passes inbound messages to your internal mail relay and outbound, external messages to the Internet.

- They require no upfront infrastructure costs and can be implemented quickly. This is particularly attractive if you want a problem, such as spam, fixed immediately.

- Subscription pricing often can be negotiated on a per-mailbox or per-message volume basis.

- Subscription periods are negotiable. Thus, you can use an outsourcer on a temporary basis while you evaluate in-house solutions.

Advantages of in-house licensed software or appliances include:

- You own the hardware (can apply depreciation) and software.

- Infrastructure dependencies are managed in-house. Enterprises often cite "lack of control" as a reason that they don't outsource.

- Your enterprise may be culturally averse to outsourcing.

Anti-spam technology is an emerging area, with more than 100 products and services. However, fewer than 40 of these are "enterprise-class." By 3Q04, 50 percent of enterprise-class anti-
spam applications will cease to exist (0.8 probability). Examples of enterprise anti-spam providers with spam detection and research capabilities — that is, they don't license anti-spam technology from other vendors — include:

- **Software** — ActiveState, Brightmail, Cloudmark, GROUP Technologies, MailFrontier and Tumbleweed Communications
- **Appliance** — CipherTrust
- **Outsourcer** — FrontBridge Technologies, MessageLabs and Postini

**How should I evaluate anti-spam vendors?**

The IS organization is under tremendous pressure to "fix" the spam problem now because of exploding storage and bandwidth costs, as well as user complaints. Security and legal risks often involve the security, legal and human resources departments in the decision.

Decide which anti-spam architecture, product or service to use by answering these questions:

- How well do my current anti-spam methods work?
- What is my risk profile?
- How much do I want to spend?
- What are my personnel resources for managing and administering anti-spam technologies and policies, and responding to user issues?

Some enterprises may choose to develop an anti-spam solution with open-source products, such as SpamAssassin, or commercial "blacklists" (e-mail addresses and domains that should be blocked), such as the Mail Abuse Prevention System.

You can build your own blacklists and whitelists. However, you will pay in terms of time spent administering and updating your "home-grown" anti-spam solution. This solution likely will have a lower spam-detection rate and a higher false-positive rate than commercial products or services.

When evaluating open-source or commercial offerings, consider:

- **Breadth of detection techniques** — Most applications will include techniques such as heursitics-based anti-spam rules, adaptive "learning" engines (for example, based on Bayesian analysis), signatures (similar in concept to antivirus signatures and often based on fingerprints of current spam patterns), contextual filtering, whitelists and blacklists. Some
anti-spam vendors use a multilayered approach (messages are scanned through each filtering layer sequentially) or cocktail approach (messages are scanned through one layer that comprises multiple filters) for ranking the probability that a message is spam, rather than a signature approach. Strong spam-filtering vendors also can perform intrusion prevention for mail servers, for example, which prevents denial-of-service attacks.

- **Research and service abilities** — Anti-spam products, such as antivirus and URL filtering, and good detection (with a low false-positive rate) are based on continual research, updated detection technology, and "tweaking" and content updating. Consider the number of research staff, affiliations with industry standards group, university or industry connections, and intellectual property rights and research expertise.

- **Management and administration** — Key management and administration criteria include template and ad hoc reporting, central console, automated signature and heuristics updating, and a graphical user interface for creating policies.

- **User support and customization** — This area includes whitelists at the enterprise, business unit and user levels, as well as user access to quarantined messages, such as through a digest.

- **Integration with or additional antivirus and e-mail content-filtering capabilities** — Many IS organizations don't want three e-mail-filtering products or services. Antivirus vendors are starting to provide some spam-filtering offerings, although we estimate that they are six to nine months behind the best-of-breed providers. Other spam-filtering vendors can hook into an antivirus engine, in which case the spam vendor will handle antivirus support.

- **Service-level agreements** — Service-level agreements with outsourcers should include metrics such as percentage of spam caught, percentage of false positives and system availability.

**How will the anti-spam landscape shake out? Which vendors will survive?**

Use caution when choosing enterprise anti-spam providers because this market is at the Peak of Inflated Expectations in Gartner's Hype Cycle. Rapid consolidation will occur in the next 12 months. The anti-spam market also is confused by the presence of vendors that offer partial spam-detection capabilities or obtain these from original equipment manufacturers. Antivirus vendors and URL filtering providers recently have launched more-advanced spam-filtering capabilities, or have licensed these from others.
Some firewall vendors that currently focus on application and content inspection approaches will enter the market. For example, Fortinet is including rudimentary anti-spam capabilities in its firewall appliance. In addition, network and systems management vendors that focus on e-mail and business activity monitoring, managed service providers, independent service providers and Microsoft may move into the enterprise anti-spam area. Security-oriented vendors that can interpret and transform malicious or unwanted e-mail patterns into rules or "signatures" will be best-positioned.

Some best-of-breed anti-spam providers will successfully broaden their portfolios to offer related e-mail security services/functionality. Many have done this by providing granular/policy-focused e-mail content filtering and hooks to antivirus engines. These vendors will innovate and compete with larger enterprise security vendors. Others will be acquired or will leave the business. The result will be vendors that offer a framework or suite approach, comprising antivirus, anti-spam, content filtering and other e-mail security boundary services, and vendors that sell their anti-spam technologies to the first group.

What should I do now?

If you have urgent spam-filtering requirements, evaluate if a short-term vs. long-term strategy is needed. For example, use a managed service provider under a short-term (less than one year) contract or a desktop product for a limited number of users until the market shakes out. However, evaluate potential vendors critically. Similar to the antivirus market, spam detection is a content-driven business. Look at your methodologies and expertise in the anti-spam and related e-mail areas. Examine and negotiate contractual provisions carefully to incorporate provisions if your vendor is acquired, or because of deteriorating vendor performance because of greater competition or too rapid growth. Also, understand that anti-spam pricing will soften considerably during the next year. Negotiate short-term contracts and clauses, such as price increase caps for renewals (if licensed under a subscription model), or maintenance and custom support (if licensed under a perpetual model).