



SPECIAL REPORT

ENTERPRISE-CLASS

SPAM

SOLUTIONS

A Q&A SESSION
WITH GARTNER

Exclusive Gartner Analyst Interview with Arabella Hallawell

As e-mail volume continues to increase, enterprises are faced with the costly, time-consuming tasks of infrastructure maintenance, spam reduction, and virus attack protection. Because legislature alone cannot solve the spam problem and its' drain on productivity, enterprises must proactively develop policies and procedures, and then select and deploy anti-spam tools. Here, Arabella Hallawell, a research director at Gartner, Inc., provides an overview of the current state of e-mail security, then discusses the various techniques that enterprises can utilize to filter spam and the evaluation criteria for an enterprise-class spam solution.

*How will legislation affect the spam problem? What are the Best Practices for managing spam?
What are the most important factors to consider when choosing an enterprise-class spam solution?
What are the pros and cons of the different deployment models for anti-spam solutions?*

Q ■ *What is e-mail security?*

A ■ E-mail administrators have increasing responsibility to ensure that the message infrastructure is kept up and available. In addition to dealing with the reduction of spam and viruses, most often at the e-mail boundary, the e-mail administrators also have to protect the enterprise against denial of service or directory harvesting attacks. Increasingly, they need to look at overall e-mail security and e-mail intrusion prevention. Additional considerations may be to implement e-mail encryption and content filtering as part of the company's intellectual property protection program.

Q ■ *What impact does spam have on the bottom line?*

A ■ E-mail administrators are devoting more attention than ever to the problem of unwanted e-mail, or spam. They are under tremendous pressure from their businesses to reduce spam, which is estimated to comprise 50 percent to 60 percent of enterprise e-mail. The volume alone is a source of frustration for both users and executives. The costs include storage of the unwanted e-mail as well as the consumption of bandwidth. Other softer concerns are around hostile workplace lawsuits. To protect itself, the enterprise must block or attempt to block the obscene or offensive content in e-mails.

Implementing an anti-spam solution, however, does not necessarily reduce costs. The new anti-spam system is an expense, as is the system training for end-users and administrators. The time it takes to administer, manage and update the solution must be added to costs—as must failure to do so, i.e., continuing to quarantine many spam messages or flag them and send them to the end-user.

Q ■ *How will legislation affect the spam problem?*

A ■ In general, we do not think that the U.S. spam regulations — or any of the international regulations — are going to be effective at dealing with the spam problem. Rather, we believe that upcoming technology changes will be more useful. Legislative regulations will fail to reduce spam volume for a number of reasons. First, even though some spammers are located within the United States, most of the spamming activity takes place offshore, where U.S. legislation will not be particularly effective. Second, some of the new laws, especially the federal law, may be difficult to enforce in some places. Furthermore, while the new U.S. regulations will allow enterprises to block e-mails tagged as advertising, a lot of

end-user or business-required e-mail (e.g., newsletters) may be dropped if enterprises blanket-block advertising e-mails. Invariably, administrators will have to revisit and alter those types of blanket filters.

We think more useful spam solutions will come from the technology coordination at the ISP, carrier or enterprise level, which is being evaluated with trusted or better authenticated e-mail and other initiatives.

Q

■ *What are the various ways to filter spam, and which ones work?*

A

■ There are many different ways of filtering spam. Enterprises are often deluged with a potpourri of techniques with various terminology and hype. In general, there is not one "silver bullet" method of dealing effectively with spam. Much relies upon the sophisticated combination of the many different detection techniques. The myriad of spam detection methods incorporated by enterprises may include:

- Signature-based (e.g., proprietary or real-time black hole lists and honeypots)
- Content-based (e.g., content filtering, header analysis and lexicon scanning)
- Intelligent or automated (i.e., those that use heuristics)
- Bayesian analysis
- Statistical-based analysis

The most-effective spam filtering solutions combine the techniques and often deploy them in a particular sequence. Therefore, enterprises should be wary of companies that have just one detection method. Also, end-user administration is often increased when the enterprise's detection method relies purely on signature- or content-based approaches because the system requires frequent updating and/or customizing, particularly when employing white and/or black list content filtering. Enterprises should, therefore, supplement this singular method with some of the more automated and statistical-based analysis approaches.

Q ■ *What are the Best Practices for managing spam?*

A ■ Enterprises must define their strategy upfront and take a staged approach to implementing the chosen solution. They should begin by defining spam, and the roles and responsibilities for both end-users and administrators in controlling the problem. All policy decisions should align with the business culture. For example, an administrative policy to eliminate all personal e-mail or travel/auction type notifications would be problematic without end-user buy-in and consideration of the existing culture. Next, a decision must be made as regards to end-user or central control of the policy. For example, will end-users be involved in reviewing quarantines or selecting their white lists from e-mails that might otherwise be blocked?

Once a product or service is selected, it should be turned on in either audit mode or with the filters turned down low for the first month to six weeks. Though under pressure to control spam, enterprises must avoid the temptation — as soon as a solution is in place — to turn it on high. This may obliterate the opportunity to identify spam patterns and create appropriate policy. Allow administrators time to assess spam traffic patterns before fine-tuning the filters.

Finally, pay attention to business processes. Train end-users and administrators on their responsibilities. Also, make sure that helpdesk processes are up to speed, as, invariably, there will be administrative issues and costs associated with handling blocked e-mails.

An effective spam filtering solution will reduce costs to the enterprise by allowing the enterprise to start dropping spam comfortably (as pure spam, without false positives) — and not by continuing to quarantine, or flag, all messages.

Q

What are the most important factors to consider when choosing an enterprise-class spam solution?

A

There are three main factors to consider when choosing an enterprise spam solution:

- Detection and analysis methods
- Management administration
- Customer service and content expertise

Detection rates depend on the enterprise's definition of spam and how the solution is implemented. Enterprises must be wary of vendor marketing hype, or snake oil, surrounding detection and analysis techniques. Proclamations of 99.9 percent detection rates and zero false positives are not reliable. Look for a fairly sophisticated engine that incorporates many of the detection methods described earlier. Confirm the substance beyond industry buzzwords, like Bayesian filtering. Ensure that the solution includes a way to customize, or weight, those different methods.

Second is management administration of the solution. Enterprises should look closely at how easy the product or service is to update, and how the updates are received. Reporting, administration and quarantine capabilities should also be considered carefully. For example, ask how easy it is for the administrator to look through the quarantine. Verify that the type of end-user quarantine available is appropriate for the business need.

Customer service and content expertise is the third important consideration when choosing an enterprise-class spam solution. High-quality customer service and proven expertise are mandatory, as are vendor resources dedicated to ensuring that the vendor remains current on the various spam techniques. The vendor must be able to respond quickly and effectively to issues that arise. Ensure that the vendor has the vision to deal effectively with constantly changing spam techniques well into the future. Another consideration is the other functionality offered by the vendor or its vendor partners. This is important when an enterprise wants to go beyond a pure spam solution and, for example, install an anti-virus engine or add content filtering.

Q

What are the pros and cons of the different deployment models for anti-spam solutions?

A

Once the enterprise has determined the deployment location (desktop, internal e-mail server or boundary), the deployment model can be selected from among three choices: software, appliance or managed service.

The best place for spam filtering is at the boundary. The other options, desktop and internal e-mail server, have limited applications. Desktop deployment will require touching every desktop with software, as well as providing end-user training. It also gives control of spam filtering policies to the end-users, which is not necessarily of value to many enterprises. Only for very specific cultures does desktop filtering make sense. This may be a better option in the future as vendors develop better link spam controls in desktop e-mail programs to the gateway filters and rules. The other location option is on internal e-mail servers. Again, this has limited value as it is not a good idea to allow all of that unwanted e-mail onto internal systems before it is classified and dropped or quarantined. Enterprises and vendors have touted the tiered approach for spam filtering. We think the tiered approach to spam detection is a big fallacy. The reason it works for virus detection is because there are different vectors for infection at the different tiers. With spam, there are not different vectors for infection, it all flows through the gateway and subsequently the most effective blocking occurs as far from internal systems as possible. That way, enterprises can drop or quarantine spam before it hogs internal servers or reaches end-users.

We recommend deploying the anti-spam solution at the boundary. Basically, there are three different options:

1) Use a software product at the SMTP gateway.

The pro of software is that it can be customizable on lockdown to enterprise specifications. Software is appropriate for a specific type of box, or for security people that like to harden those boxes in a specific way. It could also, potentially, be more configurable to enterprise requirements, and to hooking in some other types of software. On the flip side, the cons of a software approach are that the

enterprise has to purchase hardware and then have the expertise and resources to properly configure and maintain the solution.

2) Use an appliance.

The pros of using an appliance are that it can offset a lack of in-house security expertise — eliminating the need to harden the operating system, and it may be easy to implement. The con is the lack of customization available compared to what the enterprise would have with a software deployment.

3) Use a managed service, where, typically, MX records will be pointed to a services provider.

The primary pro of a managed service is the delegation to a more efficient and expert resource and to an outside source of the every day responsibility of administration of the spam filters and keeping the solution up-to-date. Likewise, one con is the resulting lack of control. Some enterprises feel that critical enterprise applications like e-mail should not be outsourced and if a problem does arise with the spam filtering solution, at least the enterprise may have some control to physically walk over and deal with it. Some enterprises do not want a third party immersed in their “critical infrastructure”. Another con is the expense of outsourcing the anti-spam solution. Whereas appliances and some software typically require more of an upfront license cost investment and may take more admin to operate on an everyday basis, managed services are more expensive on an ongoing basis in terms of pure product license costs.

Q ■

Can you give us an idea of how the anti-spam industry is going to evolve, and how that will affect my organization's e-mail security strategy?

A ■

Right now, enterprise spam filtering is a very nascent market with an extreme amount of hype. The hype has encouraged a lot of companies to come out of the woodwork, all proclaiming that they have the best spam-filtering solution. Currently, the very small start-up companies and smaller vendors have the best-of-breed spam filtering technology. During the next year, we anticipate a large shift in this marketplace due to consolidation.

Consolidation will result not only from acquisitions, as more of the big vendors enter the market, but also from the collapse of some of the smaller vendors, whose narrow expertise and domain will fall short of enterprise requirements for broad e-mail security needs. Of the 30 to 40 enterprise-class anti-spam vendors right now, more than 50 percent will disappear by the end of 2004.

We have already seen a number of acquisitions. These will continue as the larger anti-virus and firewall vendors aggressively seek better technology. Some of the smaller organizations will fall by the wayside as those vendors exert their sales and marketing might.

When evaluating a solution, enterprises should, therefore, bear in mind vendor risk issues, and how those might be mitigated in contractual protections, and in the type of solution or architecture chosen. Also, enterprises should take a long-term view of their security needs beyond spam filtering — to more granular content filtering such as attachments, and anti-virus and other broad e-mail security requirements. Consideration must be given to the provider of such products and/or services, with an eye toward avoiding a pile-up of solutions at the gateway.

Arabella Hallawell is a research director in Gartner Research. She currently focuses on information security and privacy strategies. Ms. Hallawell also examines security-related international regulatory and public policy issues. Ms. Hallawell holds degrees in history and law from University College London and Exeter University, England.

Source: Gartner Research



Postini, Inc.
510 Veterans Boulevard
Redwood City, CA 94063
www.postini.com
1.888.584.3150