Ferris Research

The Case for Managed Anti-Spam Services

A Ferris Research White Paper
August 2003. Report #386

Sponsored by

MessageLabs®

Ferris Research
408 Columbus Ave., Suite 1
San Francisco, Calif. 94133, USA
Phone: +1 (415) 986-1414
Fax: +1 (415) 986-5994
www.ferris.com

Recent Reports From Ferris Research

The Cost of Spam False Positives
Wireless Access to Messaging and Collaboration: Tutorial
Cross-Organizational Calendaring and Scheduling: Tutorial
Regulations and Email Archiving
Cross-Organizational Calendaring: Key Trends
Encrypted Email
Tech-Ed 2003: A Messaging Perspective
Integrating Presence into Business Applications: Key Trends
Anti-Spam for Businesses and ISPs: Market Size 2003-2008
Spam: Ferris User Panel Discussion
Instant Messaging and Presence: Market Analysis, 2002-2007
Lotusphere 2003
Corporate Email Issues: Part 2, Spam
Instant Messaging and Presence: Market Size, 2002-2007
Corporate Email Issues: Part 1, Systems & Usage
Spam Control: Problems and Opportunities
The Total Cost of Ownership of Lotus Notes/Domino
Corporate Email Issues: About the Survey
MEC 2002: Putting Microsoft's Messaging Plans in Context
Microsoft Exchange Titanium and Microsoft Outlook 11
Voice Telephony for the Enterprise: Business Implications
The Total Cost of Ownership of Microsoft Exchange
The Cost Savings of Upgrading to Notes/Domino 6
The Outlook for Human Business Communications
Instant Messaging and Presence: Vendor Success Criteria
The Cost of Notes, Exchange, and Samsung Contact
The Email Archiving Market: 2002-2007
Desktop Conferencing
Email Archiving and Records Management
Instant Messaging: Vendor and Service Provider Survey
The Future of SMS on Mobile Phones
Microsoft Exchange's Mobile Connectivity Strategy
Email Standards Update
Email Archiving Survey
Instant Messaging: Current Issues, Key Trends
MEC 2001: A Conference in Transition
Instant Messaging and Presence Standards
Email in Higher Education
Message Archiving: Leading Vendors, User Requirements, Pricing
Microsoft's .NET My Services: Strengths, Weaknesses, Opportunities

Table of Contents

Executive Summary

When organizations decide to deploy an anti-spam solution, many begin by evaluating products that would be installed on their own premises, on their own PCs and servers. However, there is an alternative—managed services. Managed services, also known as outsourced services, provide similar benefits to customer-premises-based solutions, along with some unique advantages of their own.

This paper looks at the benefits of adopting a managed anti-spam solution. The most obvious is that outsourcing eliminates the need for much of the internal staff needed to design and manage a traditional solution. In addition, the centralized nature of managed solutions allows their experts to update their systems more rapidly in order to react to new forms of spam, and thus provide more current protection to customers.

Organizations looking to adopt an anti-spam system can use this paper to help them decide whether they might be a candidate for a managed solution.

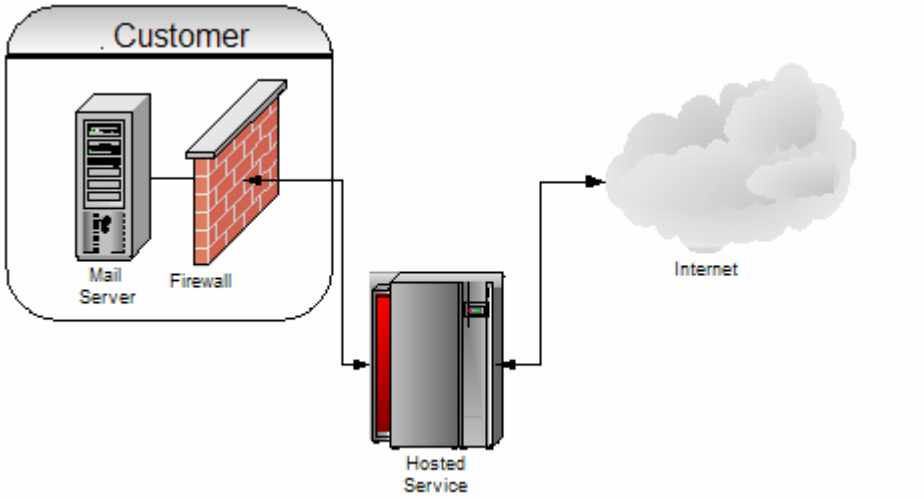
How Managed Anti-Spam Systems Work

Managed anti-spam systems operate as a gatekeeper between an organization and the Internet (Figure 1). Email destined for an organization is first received by the managed service. There it is examined for spam, viruses or other dangerous or unwanted content, and finally forwarded on to the intended organization.

It is relatively easy for an organization to re-route their email through a managed services provider. Every domain's DNS record holds an *MX* entry. "MX" stands for "Mail Exchanger". The MX entry identifies the server that receives mail for a particular domain. For example, the MX entry for the domain *globalcorp.com* might be the server named *mail.globalcorp.com*. For load balancing or redundancy, some organizations might have more than one MX entry. By changing the MX entry from mail.globalcorp.com to the server name of a hosted provider, a company can quickly reroute its email through this new location.

In addition to inbound email, customers can also have their outbound email routed through a managed service. By doing so, organizations ensure that they aren't sending virus-infected attachments to their customers and partners. Managed services also provide additional services, such as adding custom disclaimers to messages.

FIGURE 1 MANAGED SYSTEM DIAGRAM



Managed anti-spam systems route an organization's email through an off-site filtering service.

Managed providers generally have web-based management consoles that allow administrators to control their mail flow, receive reports about system activity, and access other common functions. Outsourced providers also make available technical support in order to help administrators configure the system or resolve problems.

The Advantages of a Managed Service

We now discuss the case for managed services. Note here we focus on the strengths; for a fully balanced assessment, you obviously need to consider the drawbacks as well.

Free Up Scarce IT Support Staff

IT staff are a scarce resource. A managed service greatly reduces the time they have to spend handling spam, and they are thus freed up for other work.

First, we present some general staffing considerations:

- IT staff always have more work on their hands than they can handle. There are always important projects that are pending, such as developing customer management or supply chain management systems.

- Messaging support staff are scarce. Time they put into developing an anti-spam solution will directly detract from other projects they must work on, such as an Active Directory upgrade.
- It's hard to hire someone that will quickly understand your email environment, and evaluate and deploy anti-spam technology in a timely way.

Using a managed service—as opposed to a traditional software solution installed and maintained by the customer—greatly reduces the burden on technical staff.

True, the evaluation and selection of an anti-spam solutions will take time, whichever approach is chosen. However, a managed approach is much simpler to implement. For example, servers don't have to be installed and configured, and staff don't have to manage the phase-in. We return to this point later in the document.

A managed solution is also far easier to maintain. For example, software doesn't have to be periodically upgraded, system capacity doesn't have to be tracked and projected, servers don't need to be upgraded, no alert systems have to be put in place in case the system goes down, patches and new filters don't have to be applied, and most of the user helpdesk services are provided.

Thus a managed service gives significant leverage to an organization's messaging support team. Their role becomes that of the manager of the managed service. They're not dragged into the gory implementation details, or the delights of responding to beepers in the middle of the night. They are freed up to work on other projects.

24x7x365 Technical Support

Most organizations, with the exception of large corporations, do not have technical support staff available 24 hours a day. In some cases, support staff carry pagers that alert them to system failures or other problems, but they are not available to perform ongoing maintenance and updates except during business hours.

In contrast, hosted providers have technical support 24 hours a day, seven days a week. This takes the form of technicians who monitor the message flow through the hosted provider's servers and gateways, and apply new spam filters.

In addition, they monitor the flow of email to customers' mail servers. They can detect slowdowns or delays routing mail to a customer site before the customer themselves. In addition, if there is an outage at a customer site, the mail will not be lost; instead it will be queued at the hosted facility until the customer's servers come online again and begin accepting mail.

Ease of Implementation

In most large organizations, rolling out an anti-spam solution is a three to five month project that has some or all of the following steps:

- Determine needs & requirements
- Develop RFP document. Or, request vendors to submit products for evaluation
- Evaluate products against requirements
- Negotiate pricing and purchase product
- Select & order hardware
- Deploy hardware with operating system updates
- Perform pilot test
- Make any changes required
- Perform rollout

In addition, there are ongoing activities required to maintain the system. These steps include updating whitelists and blacklists, applying updates to the spam rulesets, and updating the anti-spam software with new versions, service packs and other patches.

In contrast, implementing a managed solution is often a much shorter process that takes from one to three months. The steps involved in implementing a managed solution can include some or all of the following:

- Determine needs and requirements
- Develop RFP document
- Evaluate hosted solutions and products against RFP
- Purchase solution
- Perform pilot test
- Make any changes required
- Perform rollout

Once the solution is in place, there are fewer ongoing management requirements. There is no need to apply updates to the spam rulesets or to the anti-spam software, since that is done by the managed service provider. The primary ongoing management activity is to make any updates to a company's whitelists if required.

Some of the reasons why it is easier to adopt a managed solution are obvious. With managed solutions:

- There is no hardware or software to buy and maintain.
- You have an immediate implementation of a working, effective system. In essence, the system has the benefit of the accumulated knowledge and learning from seeing large amounts of spam destined for many organizations.
- The solution requires less up-front configuration and administration to become fully effective.

Immediate Implementation

One result of having an easier implementation is that they can also take significantly less time. In the analysis above, the managed solution requires only one to three months to fully deploy, although significant results can be seen immediately. Traditional server-based solutions require significantly more time.

Managed solutions can be implemented even more rapidly if necessary. To do so, you sign up with the service for an account or trial and then update your MX records in the DNS system. From that point, the messages begin flowing through the managed partner's site.

In this way, an implementation at a managed facility can begin in as little as 24 hours. It is difficult to imagine a company deploying a server-based solution as quickly.

Ability to Handle Traffic Spikes and Outages

When companies plan their messaging systems, they install servers and data connections in anticipation of an expected level of traffic. In most cases, the servers are able to handle the expected load as well as normal variations in traffic volume.

In some cases however, traffic generated by specific events might overwhelm a company's email server, causing the company to lose effective communication. These situations are not common, but the past few years have seen several such occurrences, mostly related to an email-based virus or other events that generated high amounts of traffic.

Managed solutions should be better at handling large spikes in message volume, because they are architected to handle larger overall amounts of message traffic. In addition, some outsourcers provide security services, such as detecting and preventing denial of service attacks.

In cases where a company's internal mail servers have failed or must go offline for maintenance, a managed provider can act as a backup receiver. Messages can be queued at the hosting facility until the company's mail servers come online and can again receive email.

Self-Management Capabilities

Because outsourced systems are not deployed at a customer's location, they have had to offer strong remote management and self-management services.

Remote management refers to tools that administrators use to manage and report on overall system operation. For managed systems, they are typically web-based interfaces. The tools allow administrators to view overall system activity and get reports on what messages are being blocked, the top email senders, top receivers and so on. Using remote management tools, administrators can change SMTP routing to the organization's location, or pause mail temporarily in order to perform server maintenance.

User-management tools are tools primarily aimed at end users. They are also typically web-based, and allow end-users to control their personal settings. In some cases, users can add entries to personal whitelists or blacklists, or view mail that is in their personal quarantine area.

Strong remote management tools allow administrators to be more self-sufficient, which ultimately reduces costs for the hosting partner. On the other hand, strong user self-management tools are critical to reduce the customer's own costs, by reducing the need for internal help desk support and assistance. Users can also be more effective than administrators at reviewing their own spam junk folders.

Simplified Messaging Management

By cutting off spam before it enters an organization's email system, email management is made simpler than it would otherwise be. Spam hinders many different aspects of managing an email system. For example:

- Spam is now a large proportion of email arriving from the Internet. Typically it represents about half of email incoming from the Internet. Throughout an organization's network, WAN links are having to be upgraded sooner than they would be without spam. Usually the rapid increase in spam has meant that these upgrades have not been planned or budgeted.
- Spam takes up server hard disk space. Servers are being expanded or replaced sooner than they would without spam. As with WAN links, these upgrades have usually not been planned or budgeted.
- Backups must cover many more messages, and take longer to run. This may require splitting users across multiple servers, or longer system downtimes. New techniques must be implemented to partition off spam messages.
- Restoring damaged message stores takes longer. New techniques must be implemented to screen out spam messages.
- Message delivery times are slowed.

Thus the overall effect of spam is to make it harder to run an email system. Stopping spam coming in makes messaging management simpler.

Potential Advantages

There are two areas in which managed services *may* have an advantage over customer-premises-based solutions. Due to the newness of the anti-spam marketplace, we weren't able to confirm these potential advantages during our research.

Perhaps, in a years' time, we'll be able to be more definitive about these potential advantages. But in the meantime, we want to describe them. They are worth considering when evaluating a managed solution.

Cost Savings

Managed solutions often end up being cheaper than internal systems, when you add up all the hidden costs. For many customers, this will probably turn out to be the case for managed anti-spam services.

Managed and server-based solutions have some costs in common. Moreover, these are roughly equal, assuming similar deployment options:

- Junk mail folder monitoring by end users
- Whitelist updating by end users
- Whitelist updating by administrators
- False positive retrieval by end users
- False positive retrieval by administrators

On the other hand, the following represent areas in which managed solutions offer intrinsic savings:

- Hardware acquisition
- Operating system license for hardware platforms
- Management of operating system (patches, updates)
- Software license or subscription to anti-spam server software
- Support contract for anti-spam server software
- Applying anti-spam server version updates and patches
- Applying/changing anti-spam server rulesets
- Required bandwidth
- Improved detection of spam

It's beyond the scope of this paper to assess whether in fact outsourced anti-spam solutions save money over customer-premises-based solutions. And in any case, whether an outsourced solution will save over an internal solution will depend on the particular services and fees of the outsourcer concerned.

When you figure the costs for organizations with more than about 1,000 users, an internal anti-spam solution is likely to cost around $15 to $25 per mailbox per year. This would cover anti-spam detection software, vendor support, anti-spam updates, hardware depreciation and management costs, and an allocation of bandwidth charges. Some outsourcers ought to be able to undercut this.

More Frequent Filter Updates

A managed solution has two built-in advantages that may help it catch more spam:

- Many vendors of server-based anti-spam products provide updates on a weekly basis; in extreme cases as frequently as every fifteen minutes. However, the chances are that a managed service will apply updates at the fastest rate. It's typical for a managed service to be updated several times per hour.
- Instead of having to update thousands of dispersed customer locations, managed services only have to update a handful of servers. The service can ensure that sufficiently fast data links ensure timely updates. With a managed service, you can be sure that filter updates deploy very rapidly.

Summary

Companies that lack internal IT resources or expertise are the best candidates for anti-spam outsourcing. Outsourcing allows them to maximize their internal IT resources and focus them on projects that are more aligned with a company's objectives.

Outsourcing also provides an easier and more rapid implementation than with server-based approaches. It may also have lower costs.

The types of organizations particularly likely to adopt an outsourced solution are those that:

- Have limited IT resources
- Need to maximize bandwidth and server resources
- Need to implement a solution quickly and easily
- Want to implement anti-spam without hardware or software capital costs

MessageLabs

MessageLabs' Email Security System provides a range of managed services that monitor email outside an organization's network to keep the email free of harmful content. The system consists of anti-virus, anti-spam, porn filtering and content control services. These are delivered on a 24x7x365 basis through a global infrastructure, which currently spans the United States, the United Kingdom, Germany, the Netherlands and Hong Kong. No extra hardware or software is required.

Anti-Virus

The anti-virus service uses multiple commercial scanners and proprietary algorithms, known as *Skeptic*, to detect and stop viruses, both known and unknown. The service comes with a 100% Service Level Agreement against emailed viruses.

Anti-Spam

This uses a combination of Skeptic technology and customer configurable blacklists/whitelists to identify and stop spam. Skeptic is a multi-tiered, predictive technology that uses techniques such as dynamic heuristics (1,200 pattern matching rules), Bayesian probability, smart signatures/fingerprints and insecure sender detection.

Porn Filtering

The porn filtering service uses image composition analysis to detect pornographic images and has different sensitivity settings and routing options.

Content Control

This allows the definition and application of organizational, group and user email policies, as well as the identification of confidential, malicious or inappropriate content in email. Features include managing the delivery of email based on keyword usage, email size, attachments and allowable file formats.

MessageLabs Contact Information

Telephone: +1 (866) 460-0000

Email: info@messagelabs.com

Web: www.messagelabs.com

Ferris Research White Paper. Report #386. August 2003.

MessageLabs Sponsorship

In May 2003, MessageLabs asked Ferris Research to comment on the strengths of managed services. The purpose was to provide credible third-party validation for MessageLabs' service, and to provide MessageLabs management with an independent view of its strengths. This document explains our findings. Clearly, it's not a complete product or service assessment, since all products and services have weaknesses in addition to their strengths. We do, however, think this document is an honest and straightforward analysis of the strong points of a managed anti-spam service.

Ferris Research

Ferris Research is an established market research firm headquartered in San Francisco. Our senior analysts are located throughout N. America, Europe, and Asia/Pacific. We study messaging and collaborative technologies, and provide business intelligence and market analysis to vendors and corporate IT managers.

Based on self-funded market surveys and primary research, Ferris Research publishes reports and newsletters that help our clients spot important new trends and developments, while escaping the problem of information overload. In business since 1991, Ferris Research enjoys an international reputation as the leading analyst firm in this important field.

The firm's international clientele encompasses a wide range of large organizations with extensive IT operations, in addition to vendors. Ferris Research is located at 408 Columbus Ave., Suite 1, San Francisco, Calif. 94133, USA. For more information, visit http://www.ferris.com or call +1 (415) 986-1414.