

# Top Five Frustrations of Legacy Anti-Spam Products—and How to Resolve Them

## INTRODUCTION

Not that long ago spam was deluging your email systems, slowing your servers to a crawl and choking your email communications bandwidth. So you rapidly found a solution. It could have been a freeware software product, or one that promised the most effective filtering with the most immediate updates. It could have been an appliance that seemed reasonably priced. But a strange thing happened along the way to solving the spam problem. Other issues began to crop up—especially over the past several months.

For some organizations, that initial anti-spam software product or appliance has rapidly become a productivity killer. It's starting to cost far more in time and effort than its purchase price suggested. Its accuracy may be inconsistent, letting more spam than usual land in company email boxes. End users may be complaining more about false positives—legitimate messages that are being stopped by the spam filters.

This white paper describes many of the symptoms and issues you may be experiencing with your first-generation anti-spam solution. More important, it suggests an alternative solution in the form of a unique integrated message management service that overcomes these issues while delivering the comprehensive security and management control you need to meet today's messaging demands for security, encryption, archiving and more. If you find yourself identifying with one or more of the common frustrations described here, it could be time for you to switch to Postini Integrated Message Management.

## FRUSTRATION #1—SPEED, ACCURACY AND EFFECTIVENESS ARE RAPIDLY DECLINING

End users expect email communications to arrive in their inboxes without delay. In many cases, companies depend on immediate email delivery as the very lifeblood of their day-to-day operations, critical to the success of their business. Yet many first-generation anti-spam products and appliances are experiencing latency problems that range from five-second delays up to several minutes or even hours.

Part of the reason for these delays is found in the growing number of email viruses and threats plaguing email communications. The outbreak of a virus such as SoberP, which occurred in 2005, is one example. The spike in email traffic caused by SoberP simply overloaded many anti-spam software filters and appliances. Because these products operate inside your email gateway your email servers are forced to handle these sudden increases in email traffic. As a result, email servers slow to a crawl. In some cases, you may have to actually shut down email servers in order to wait for a filtering update from the software or appliance vendor. In other cases, a smaller or less sophisticated anti-

**Fast Facts from our Customer Survey:**

In a recent survey of customers switching to Postini Integrated Message Management services, email administrators responded with these reasons for switching:

- 92 percent switched to Postini from a software product to gain better anti-spam and anti-virus accuracy and effectiveness.
- 76 percent switched to Postini from another managed service because Postini offered better accuracy and effectiveness in blocking spam and viruses.
- 85 percent switched to Postini from another managed service citing better speed of email delivery.

spam managed service may not have the capacity to handle such spikes in service, therefore delaying your email delivery for extended time periods.

One of the most insidious causes of server slowdown or shut down is the Directory Harvest Attack (DHA). These attacks bombard your servers with thousands of bogus email messages addressed to speculative names hoping to harvest responses that signify legitimate email users. Known as the “silent killer,” DHA’s are impossible to detect with conventional anti-spam filtering technology, yet they can overload your email servers with endless cycles of non-delivery reports (NDR’s) in the outbound queue and bounce messages that clog your inbound queues with the potential to crash your servers.

Another symptom of aging legacy anti-spam filtering software and appliances is a growth in user complaints about false positives. This often manifests itself in a surge of help desk calls from end users missing legitimate messages. Administrative staff then has to search quarantined messages hoping to locate the missing email. Even when they can find the blocked legitimate message the damage from the delay has already occurred.

**HOW POSTINI RESOLVES THE PROBLEM:**

A test published by Network WorldFusion confirms Postini’s effectiveness when it was selected, two years in a row, as the managed service solution of choice for spam protection. Of all the products tested, Postini’s Perimeter Manager managed service offered the best balance between spam capture and false positives, with a 97 percent spam catch rate and only six false positives in more than 10,000 emails tested.

Postini’s proven effectiveness stems from several key differences from server software or gateway appliances. As a managed service, spam and newly evolving email threats are effectively dealt with before they have a chance to impact an email system. That’s because Postini sits between

the Internet and the customer’s email server —analyzing and filtering all messages before they can reach the email gateway. Postini’s Stateless Message Technology processes email in real-time, through a highly secure system architecture that operates with no detectable latency, no data loss, and no security compromises. Legitimate email is instantly forwarded to an email server and suspicious email is either blocked and discarded or quarantined to a web-accessible storage area for review by your email administrator and/or end users.

**FRUSTRATION #2—OVERHEAD AND STAFF ADMINISTRATIVE BURDEN GROWING**

In-house anti-spam software and appliances inevitably add to overhead costs and staff administration and maintenance tasks. In some cases, organizations have had to eventually devote a full time equivalent at a cost of \$50,000 to \$75,000 annually just to manage and maintain in-house anti-spam systems or appliances. This staff resource is thus diverted from other IT initiatives in order to create and tune spam filtering rules, maintain white/black lists, manage version control and troubleshoot errors after vendor updates have been downloaded. In larger more complex companies, managing email security for multiple email servers becomes an administrative nightmare. In house anti-spam software also places an additional burden on your gateway/email servers, forcing companies to add costly server capacity just to handle spikes in traffic from email attacks.

Few organizations can afford the additional in-house hardware/software and staff costs required by anti-spam software and appliances just to keep pace with growing email threats.

**Fast Facts from our Customer Survey:**

72 percent of appliance users, and 65 percent of software product users indicated they switched to Postini because their in house anti-spam products created too much administrative burden on IT staff resources.

**HOW POSTINI RESOLVES THE PROBLEM:**

As a managed service, Postini has the advantage of delivering reduced overhead and lower administrative costs compared to software or appliance products. Because Postini sits between the Internet and the customer's email gateway, email threats are preemptively stopped before they can impact the customer's network. Thus, customers save on bandwidth since spam, viruses, phishing and other email attacks are never allowed inside the network. In addition, there is no installation or distribution of software or appliances, and no worries about conducting frequent updates or version control issues.

**FRUSTRATION #3—ONE SIZE FITS ALL NO LONGER WORKS**

For many organizations, the initial goal was to stop spam. Period. However, a “one size fits all” approach to stopping spam no longer works for them. Different users or user groups often require different levels of message filtering. While one general filtering level may suffice for most employees, executive management or the legal department may, for example, have special requirements that require fine-tuning or direct access to quarantined or suspect emails. In many of these cases, legacy anti-spam software and/or appliances provide little or no visibility into email traffic or threats, are difficult to work with from an email administrator's perspective, and require an expert to manage.

The administrative interface of these products is not intuitive, nor do they provide real time email traffic statistics to administrators. Changes and updates to anti-spam filters are not immediate, and in some cases, must be distributed to email servers only during downtime periods. In other cases, configuring or adjusting spam filter sensitivity is an operation only the vendor can

perform. Most organizations today, however, need flexible administrative controls and more user self-sufficiency when it comes to managing their anti-spam and email security functions.

**HOW POSTINI RESOLVES THE PROBLEM:**

As a managed service, Postini provides maximum flexibility for email administrators and optimum self-sufficiency for end users. Using Postini's Active Policy Management, message administrators can quickly configure management options through a single, convenient web interface that lets them select pre-configured settings for email policies, or customize settings where desired.

- Convenient web console for easy configuration, management supervision and reporting
- Administrators can direct messages to more than one server
- Customers never have to pay for secondary email addresses
- Real time email traffic statistics are available on demand
- Email management and trend reports can be generated in minutes versus hours

**FRUSTRATION #4—END USERS CAN'T MANAGE THEIR EMAIL SELF-SUFFICIENTLY**

Frustration with managing end users is directly related to the “one size fits all ” problem exhibited by most legacy anti-spam products. Many conventional anti-spam software and appliance products simply have no way to set up individual quarantines for end users. This forces the IT staff to spend countless hours culling through spam, searching for blocked legitimate messages on behalf

**Fast Facts from our Customer Survey:**

- 72 percent of appliance users, 87 percent of software product users, and 45 percent of managed service users indicated they switched to Postini because their existing anti-spam solutions did not have the flexibility to accommodate diverse user needs.
- Nearly half of all customers switching to Postini cited the need for a solution that went beyond stopping spam to include enforcement of policies, disaster recovery, and in-and-outbound traffic control.

of end users. Just as frustrating and costly, is the increased volume of calls by end users to the help desk.

Even more frustrating for the IT staff is the search for legitimate emails blocked by the anti-spam software or appliance that may contain confidential information. By law the IT staff may not have permission to view the contents of a blocked message, yet the staff is tasked with finding and releasing this email to its legitimate recipient. It's a proverbial "Catch 22," with no easy resolution.

**HOW POSTINI RESOLVES THE PROBLEM:**

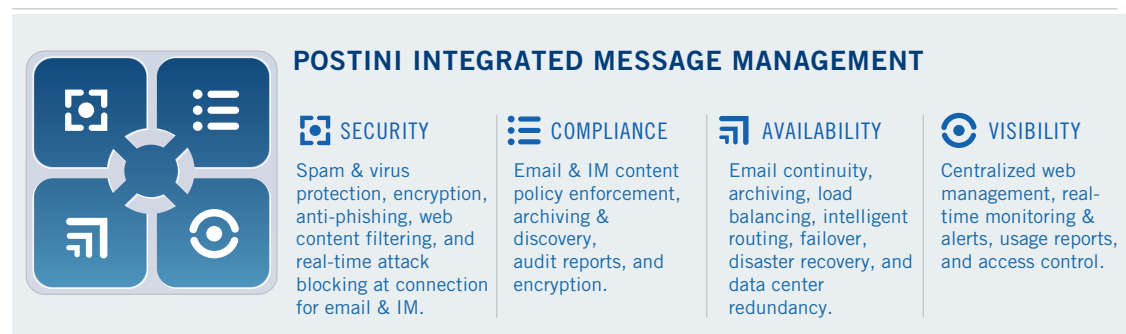
Postini offers a flexible policy framework that goes beyond the "one size fits all" restrictions of other services to allow inbound and outbound email filtering and policy enforcement that suits the needs of different domains, user groups and even individual users. End users have the flexibility to examine their own quarantined messages via online Message Center, and can maintain their own white/black lists, all within parameters set by email administrators. Daily notifications can be emailed automatically to end users alerting them to newly quarantined messages. These notifications can be delivered in twelve different languages.

**FRUSTRATION #5 —YOU NEED MORE THAN JUST ANTI-SPAM PROTECTION**

By now message administrators recognize that spam is not an isolated problem. They know that message security involves far more than simply blocking unwanted junk email. In the wake of well-publicized email virus attacks, the creation of zombie networks or "bot-nets," the growth of instant messaging (IM) and worm threats over public IM networks, the archiving requirements of message storage and retention for compliance and legal discovery, most organizations are looking for comprehensive message management solutions, not just an anti-spam product.

Message administrators are also looking for solutions that will assure reliable disaster recovery capabilities should email servers go down for any reason. Protecting users from unwanted Web content or links, as well as enforcing email policies for both inbound and outbound messages has also become a major issue in the wake of new regulations and high-publicized lawsuits and penalties for violations of privacy and confidentiality.

All of these issues add up to a need for broader email and IM security controls and insight that conventional anti-spam software and appliance products were never designed to address, let alone manage.



**Figure 1:** Postini Integrated Message Management (IMM) offers a comprehensive, flexible, trusted managed service that protects your messages without burdening your IT infrastructure. Postini delivers comprehensive security for IM and email, enables message archiving for compliance, assures availability and continuity, and provides the visibility to achieve more efficient message management.

**Is an anti-spam appliance really cheaper?**

A Frost &Sullivan research report shows that Postini's managed services proved to be much more cost effective than typical anti-spam software or appliance products. Frost &Sullivan analyzed the costs associated with other anti-spam and email security solutions based on total cost of ownership (TCO) models that compared the true costs of the various solutions over their lifetime of use.

The report shows that Postini cost 10 percent less than an appliance solution for a 300-user company and cost 40 percent less than a software solution for a large enterprise environment with 10,000 users. According to the report: "The results prove that by leveraging a services model, customers are not only able to save money on the total cost of ownership of an email security solution, but are able to increase security and scale their deployments more linearly than by purchasing software or appliance solutions that are installed at the customer location."

**HOW POSTINI RESOLVES THE PROBLEM: INTEGRATED MESSAGE MANAGEMENT**

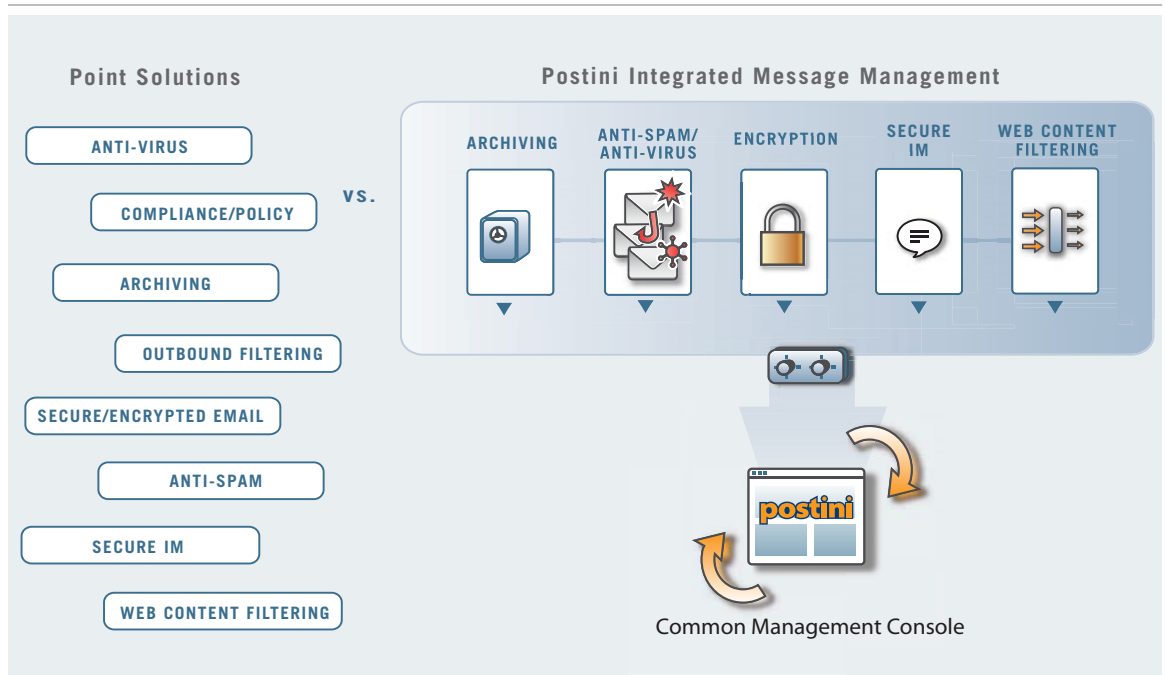
Offering far more than simply anti-spam protection, Postini provides a single integrated message management solution that combines email and instant messaging (IM) protection, archiving, encryption and message continuity---all managed through a single web-based administrative interface. Postini is unique in that its managed service model utilizes a single, common policy framework making it easier and much more efficient to manage multiple message functions and enforce policies. Thus, Postini provides a comprehensive suite of services that work together from a single managed service platform, enabling businesses to instantly add services in any combination and on any scale to fit their needs.

Given the rapid evolution and convergence of messaging threats combined with increasing legal requirements and regulatory mandates, Postini goes beyond simply eliminating spam to deliver a unique integrated message management solution that includes:

**Security**

Postini blocks spam, viruses, IM worms, directory harvest attacks, and other email and IM threats before they can reach your network or mobile users, with patented technology that delivers unmatched protection for email and instant messaging. In addition, Postini provides web content filtering to protect you from objectionable and offensive web content, reduce recreational surfing, conserve network bandwidth and enforce web access policies.

**POINT SOLUTIONS vs. POSTINI'S INTEGRATED SOLUTION**



**Figure 2:** While many organizations struggle to control the complexity of multiple security point products, Postini provides a single integrated solution that combines email and IM protection, archiving, encryption and continuity, all managed through a single console.

**Compliance**

Postini enables enterprises to enforce content policies, safeguard proprietary data, ensure legal readiness and compliance, and protect business relationships through policy-driven content filtering, email and IM archiving, and automatic encryption based on global, group or individual user requirements.

**Availability**

Postini ensures email continuity and prevents message loss via automatic disaster recovery, failover support, offsite message archiving, and data-center redundancy, delivering the uptime, responsiveness and message integrity you demand regardless of traffic volume or complexity of the enterprise environment.

**Visibility**

Postini provides unmatched, real-time command and control of the entire enterprise messaging environment by allowing you to manage and supervise all services and policies—for all users and locations—from a single Web-based administrative console that displays real-time dashboard views, detailed usage reports, and a corporate message archive.

**GAIN ALL THE BENEFITS OF INTEGRATED MESSAGE MANAGEMENT**

As a managed service, Integrated Message Management from Postini enables you to deliver the business benefits of email and IM as communications tools without the associated costs, risks and complexities of in-house software or appliance products.

**Mitigate Business Risks**

Postini protects your message systems from the latest threats, prevents policy violations and liabilities, as well as protecting intellectual property from theft or abuse.

**Enforce Policy Compliance**

Postini's single policy framework enables you to set, streamline and enforce policies for message usage, attachments, archiving and encryption, helping to achieve compliance.

**Eliminate Complexity**

Postini's managed service model provides single point of control and management that eliminates the cost and complexity of deploying multiple point solutions.

**Reduce Operating Costs**

Postini replaces escalating capital and capacity costs associated with appliance or software point products with a predictable monthly operation expense that scales to suit your needs.

**Assure Message Continuity**

Postini's certified, secure multiple datacenters throughout the world assure 99.999 percent uptime through a managed service that scales to your message needs.

**Improve Productivity**

Postini improves employee productivity and reduces help desk overhead by enabling user self service within policy limits. From one convenient Web-based Message Center, users can access their own spam quarantines, search personal archives, adjust personal filters, maintain white- and blacklists, and control other settings, without help from an administrator.

**Expand International Support**

Postini makes it easy for any business to offer protection to users around the globe. Our end-user Message Center is available in 14 European and Asian languages, while Postini customer service and support is available 24/7 at locations worldwide.

To learn more about Postini's Integrated Message Management services please visit our Solutions Overview online at [www.postini.com](http://www.postini.com).

**References:**

- (1) "Phishing on the Increase, Group Says," by Bob Francis, *InfoWorld*, Nov. 29, 2004.
- (2) Telephone interview, Richi Jennings, Lead Analyst for Spam and Boundary Services Practice, Ferris Research [www.ferris.com](http://www.ferris.com), Dec. 17, 2004.
- (3) Postini 2006 Message Management & Threat Report, published January 2006, [www.postini.com](http://www.postini.com).
- (4) IMlogic "2005 Real-Time Communications Security: The Year in Review," and "Understanding the IM Security Threat," IMlogic White Paper, [www.imlogic.com](http://www.imlogic.com)
- (5) "Spam in the Wild: The Sequel," by Joel Snyder, *NetworkWorldFusion*, Dec. 20, 2004.

**ABOUT POSTINI**

As the leader in Integrated Message Management, Postini protects businesses from a wide range of email, instant messaging (IM) and Web threats, provides message archiving and encryption, and enables the management and enforcement of enterprise policies to meet regulatory compliance requirements.

**Corporate Headquarters**

San Carlos, CA USA  
Toll-free: 1-866-767-8461  
Email: [info@postini.com](mailto:info@postini.com)  
[www.postini.com](http://www.postini.com)

**EMEA Headquarters**

London, UK  
Tel: +44 (0)20 7082 2000  
Email: [info\\_emea@postini.com](mailto:info_emea@postini.com)

**Asia Pacific Headquarters**

Tokyo, Japan  
Tel: +81 80 3089 7470  
Email: [info\\_apac@postini.com](mailto:info_apac@postini.com)

© Copyright 2006 Postini, Inc. All rights reserved. WP29-01-0508

Postini, the Postini logo and Postini Perimeter Manager are registered trademarks or service marks of Postini, Inc. PREEMPT is a trademark of Postini, Inc. All other trademarks listed in this document are the property of their respective owners.