

Postini® White Paper

Debunking the Top 5 Myths of Outsourcing Email Security

Introduction

Spam and Viruses More Than Just a Nuisance

The flood of spam clogging the nation's email inboxes continues to rise despite legislation this year designed to curb spam practices and the huge losses in productivity caused by unsolicited email. META Group, for example, estimates that the volume of spam has increased from 50 percent of Internet traffic in 2003 to more than 70 percent in 2004.⁽¹⁾ ISP's and anti-spam vendors estimate that as much as 95 percent of inbound emails these days are spam.⁽²⁾

Enterprise IT managers don't necessarily need another report to confirm what most of them already know. Spam and email-borne viruses are no longer just a nuisance, but a threat to the productivity and stability of their mission critical email systems. They also represent a potential legal and reputation liability. At the same time, IT managers are taking a closer look at solutions that not only stop spam and viruses, but also help to enforce email policy compliance for their diverse group of users.

Some enterprises are naturally concerned whenever anyone brings up the topic of "outsourcing security" whether it relates to email communications or any other aspect of the IT infrastructure. Yet recent comments by leading industry analysts and corporate IT executives reflect changing attitudes towards outsourcing security—particularly when it comes to fighting spam and viruses.

This paper addresses the most common myths surrounding the concept of outsourcing email security to a managed service such as Postini, a leading provider of email security and management. Email security from a managed service like Postini is not the same as a hosted mailbox service. Postini's patented method for processing email messages does not store, screen and then forward email messages. Rather it processes messages in real time, blocking spam and viruses at the SMTP connection point while passing along legitimate messages without delay—a critical advantage over any other managed service provider.

MYTH # 1: We will lose control if we outsource email security

Many enterprises today, such as Merrill Lynch, are proving that loss of control in outsourcing email security is clearly a myth. An article published in *USA Today* described how CSO David Bauer and his staff chose Postini's managed service approach to protect their email system serving 48,000 employees at more than 600 offices in 36 nations.

Merrill considered 10 vendors before narrowing the choice to three. They looked at features. They considered costs. They worried some systems might be too complicated, slowing message delivery.

"Postini, started in 1999 in Redwood City, Calif., got Merrill's business because of its size and expertise in financial services," Bauer says. "Before using Postini, Merrill Lynch could only guess how much of its e-mail was spam. Now, it knows it's about 24% of messages."

The overall volume of Merrill's e-mail messages plummeted 30% as Postini blocked spam. Bauer has been happily surprised at how quickly Merrill squelched what had been a growing threat. "It's definitely not on my list of anything to worry about anymore—it's not even close." ⁽³⁾

Mathew Kovar, a vice president for analyst firm Yankee Group's security solutions group, recently predicted that large companies in particular would lead the move toward outsourcing security.

"Security outsourcing will prove attractive, said Kovar, for reasons other than the cost savings typically cited by companies that farm out business processes. Among the drivers toward managed services are the accelerated attacks of today's threats—giving enterprises virtually no time to put up defenses on their own before an attack infiltrates a network—legislative requirements such as HIPAA and Sarbanes-Oxley, and the trend toward pushing out the network perimeter to include partners and remote workers." ⁽⁴⁾

Kovar cites anti-spam services as a prime example of this trend. "'One of the easiest managed services to see success is E-mail anti-spam services,' Kovar said, 'People saw the pain and saw that they needed to outsource the solution.'" ⁽⁴⁾

Phebe Waterfield, another analyst at Yankee Group was more specific. Waterfield notes that many companies once tried to manage spam internally because they were concerned about entrusting their E-mail to an outside company. "'That's considered a little paranoid these days,' she says, 'now that the aggressive and ubiquitous nature of spam has led to a change in mindset.'" ⁽⁵⁾

MYTH # 2: We can't comply with our internal policies or regulatory standards if we outsource email security

This is where Postini's patented pass-through email protection technology has a clear advantage over hosted email or other outsourced anti-spam managed services. That's because the technology used by hosted email services as well as other managed service vendors must accept all messages and store them on disk. The messages are then analyzed, filtered and forwarded to the customer. Storing messages outside the company on a continual basis can create security and privacy risks that are a legitimate concern for enterprise IT managers.

Postini's exclusive pass-through technology, unlike any other vendor, conducts all analysis of SMTP connections and of messages in memory, in real time, so that no legitimate messages get stored but rather are instantly passed along to their respective recipients. This minimizes any concerns about privacy and security for the enterprise.

Messages do not get passed through directly if they are quarantined as spam or contain a virus, or in the event of a server outage inside the customer's network. If a customer's email system goes down for any reason, Postini has the ability to assure business continuity by spooling messages, rather than letting them bounce back to the senders. This guarantees that in the event of an email server outage inside a firm's network, Postini can retain messages until the customer's email server is again able to accept them.

Beyond its patented pass-through technology and business continuity advantages, Postini offers enterprises the added assurance in meeting internal policy and regulatory requirements.

Postini is the only managed service provider to be SAS-70 and WebTrust certified. Developed by the American Institute of Certified Public Accountants (AICPA) and based on the global ISO 17799 standards, Postini has earned both SAS-70 and WebTrust certifications. These certifications validate Postini's email security and management service by passing rigorous, third party testing and auditing of its data center processing and control methods. Both SAS-70 and WebTrust certifications provide enterprises with credible proof that Postini provides its service in a consistent, stable and secure environment. This means that you can be assured that Postini's business and security practices maintain the availability, integrity and confidentiality of its systems and your customer data.

Postini assures SEC-compliant Quarantine process—Postini's email protection service ensures that quarantined messages show only a subject line and cannot be read by users unless the user delivers the quarantined message from quarantine to his or her inbox. This assures that all email seen by the user can be archived in accordance with SEC regulations.

Postini helps reduce email storage as well as litigation discovery costs. Because Postini blocks up to 90 percent of messages before they reach a customer's email system, enterprises have substantially fewer archived messages to store or examine (and therefore lower fees) if a legal review becomes necessary.

**MYTH # 3:
It's more expensive to
outsource anti-spam and
email security**

The perception that outsourced services are more expensive than in-house solutions is clearly a myth when one considers the total cost of ownership involved in purchasing, updating and maintaining anti-spam software or appliances. When an enterprise chooses Postini's preemptive service for email protection, it gains immediate reduced costs and increased efficiency and effectiveness compared to typical in-house software and appliance products. These benefits include:

- **Lower infrastructure costs:** By keeping spam, viruses and attacks from ever reaching an enterprise's internal email servers, companies can eliminate or avoid purchasing additional servers since email traffic is significantly less. This preventive approach also reduces the firm's email archiving storage space requirements by as much as 90 percent since no spam messages are ever accepted or stored.
- **Reduced administrative burden on IT staff:** By eliminating the burden of maintaining additional in-house IT infrastructure, enterprise IT personnel are free to focus on supporting business objectives, and concentrating on revenue enhancing tasks.
- **Restored user productivity:** Beyond email infrastructure and IT staff-time savings, Postini's email security and management service more than pays for itself with improved productivity by all users.

- **Less complexity managing and maintaining email security:**

Postini can be activated in hours with only minimal IT time required, and is effective regardless of the mix of email platforms or operating systems in an enterprise environment.

- **Minimized risk of email system performance degradation or failure:**

Since intrusions cannot reach the enterprise's email gateway, its network cannot be overloaded or comprised from email threats, thus avoiding email slowdowns or system downtime.

At Circuit City, a leading specialty retailer of consumer electronics, personal computers and entertainment software, Chris Burroughs, Director of Desktop and Voice Services, helped select Postini's managed email security service to protect 3,000 users at more than 600 Superstores and five mall-based stores in the U.S.

"At first we were hesitant about pointing our MX records to Postini," Burroughs explained, "but we thought a 30 day trial would at least show us how big of a problem we had and what our ROI (return on investment) on an anti-spam solution should be." The trial process was easy to implement, and the trial was so successful at eliminating spam from employee inboxes that Burroughs was able to roll out the Postini service across the entire company.

"We barely know the Postini service is running," Burroughs said. "It's easy. It works. What else could we ask for? Postini was the quickest and least costly route to solve our spam problem

and it had the added benefit of stopping the directory harvest attack we experienced," she continued.

"Everyone in the company thinks our IT department is great for eliminating spam even though we really didn't have to spend much time and effort once we'd found Postini," she concluded. "All we had to do was point our MX records to Postini's service and figure out our email policy rules. People throughout the company are now much happier with our email service." ⁶

**MYTH # 4:
Outsourcing email security
can't accommodate my
diverse users**

While other managed service vendors may require a "one size fits all" approach, the opposite is true with Postini. In fact, Postini's email security and management service is known for its superior administrative flexibility that reduces the necessity of time-consuming IT staff oversight and empowers users to customize their email filtering within limits set by company policy. This distinction is particularly valuable to enterprises in regulated industries that must satisfy the needs of widely diverse users and user groups.

Postini, for example, provides the option of allowing individual users to control the severity of spam and blocking within limits set by the administrator, as well as the option to review quarantined (suspect) messages if they choose. This allows the administrator to satisfy the requests of individuals who may want to review all quarantined messages, and provides self-sufficiency in terms of enabling users to designate their own white lists.

Suspect emails are quarantined by Postini and can be viewed by users online through a web browser.

To comply with SEC Rule 17a-4, for example, Postini's email protection service ensures that quarantined messages show only the subject line and cannot be read by users prior to delivery. This assures that all email seen by the user can be archived in accordance with regulations.

**MYTH # 5:
Outsourcing email only lets me conduct content policy filtering for inbound mail**

Nothing could be further from the truth with Postini's email security and management service. Postini blocks viruses for both inbound and outbound emails, and enforces policy compliance for both in- and outbound messages. Postini's convenient web-based console allows the email administrator to set policy rules for individual users, user groups, as well as the entire organization.

Administrators can easily apply rules for in- and outbound emails for policies that can restrict a sender's or recipient's address, monitoring for key word or key phrase usage, or restricting attachment type and size. This flexibility is particularly useful for administrators in regulated industries with message

policies that vary according to employee roles and their contacts with customers and others.

Why Postini's Managed Service Approach is More Effective and Efficient

Today, Postini's patented email security and management service secures messages for more than 30,000 businesses throughout the world. That includes global enterprises such as Merrill Lynch, LSI Logic, and United Technologies, as well as hundreds of other companies of all sizes in all types of industries.

- **Stops new and evolving threats** such as directory harvest attacks and denial of service attacks at the SMTP (Port 25) connection point before they can impact your network.
- **Prevents spam and email borne viruses** from ever reaching your email gateway, including minimal- and no-content spam messages.
- **Provides a unified email security platform** through a common management interface, along with real time monitoring and reporting.
- **Assures the fastest, most up to date IP analysis and content filtering** rules to combat newly evolving threats.

Related Reading:

Visit Postini's Email Security Resource Center on the web at www.postini.com/resource where you will find additional articles, white papers, archived web casts and case studies

References:

- (1) *"Symantec and Brightmail: Consolidation Commences," Matt Cain, META Flash, May 21, 2004.*
- (2) *"Spam Avalanche Keeps Growing," Antone Gonsalves, TechWeb News/InformationWeek, Sept 1, 2004.*
- (3) *"Spam blaster does the job for Merrill," Jim Hopkins, USA Today, January 27, 2004.*
- (4) *"Report says Virtually All Big Companies Will Outsource Security by 2010," Gregg Keizer, TechWeb News/InformationWeek, August 23, 2004.*
- (5) *"Get Rich Quick Fighting Spam?," Esther Shein, CFO.com, April 27, 2004.*
- (6) *Telephone interview, Chris Burroughs, Director of Desktop and Voice Services, Circuit City, Richmond, Virginia, July, 2004.*

About Postini

Postini, Inc. is the industry's leading provider of email security and management solutions that protect email communications infrastructure by preventing spam and other SMTP attacks from reaching the enterprise gateway. Postini's patented managed services model utilizes exclusive preEMPT technology to eliminate spam and viruses, stop DoS and directory harvest attacks, safeguard content, and improve email performance. Founded in 1999, Postini processes more than one billion email messages per week for more than 30,000 businesses worldwide.



Corporate Headquarters

San Carlos, California

Toll-free 1-866-767-8461

Email info@postini.com

Web Site www.postini.com

Contact Postini for more information or to see if your organization qualifies for our free 30-day, no-risk trial of Postini Perimeter Manager.

© Copyright 2004 Postini, Inc. All rights reserved. WP16-01-0410

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.