

# A Comparative Analysis of Leading Anti-Spam Solutions



an Osterman Research white paper

## Overview

---

Spam continues to be the most critical problem faced by IT departments in organizations large and small. Spam robs users of productivity, it consumes unnecessary bandwidth and storage, and it requires IT staff time to manage. Complicating the issue further is that even if 100% of spam is blocked by an organization, it does nothing for an organization's bottom line. In other words, even if spam is managed perfectly, it gets an organization back only to even – it provides no competitive value to the organization.

*Any spam-blocking technology in an enterprise setting should block as much spam as possible, process inbound email as accurately as possible, and require only very small investments in IT staff time to manage.*

Because of this, any spam-blocking technology in an enterprise setting should block as much spam as possible, process inbound email as accurately as possible, and require only very small investments in IT staff time to manage.

This white paper reviews several leading anti-spam solutions and compares their performance based on testing from a variety of sources.

## Staying Ahead of the Evolving Spam Problem

---

As any user of email or email administrator will confirm, the problem with spam for organizations large and small is a serious one. Spam negatively impacts employee productivity, increases messaging system storage requirements, clogs network bandwidth, slows email server performance and lengthens message delivery times. Osterman Research surveys consistently find that spam is the leading problem faced by IT organizations.

Although about 90% of organizations currently have anti-spam systems in place, the spam problem is by no means solved. In an Osterman Research survey conducted during July 2004, we found that one-third of organizations still view spam as a "huge" problem. Clearly, despite the widespread penetration of anti-spam technology, much of this technology falls short in solving the spam problem.

As evidence of the worsening spam problem is the fact that spam capture efficiency (the percentage of spam that an anti-spam solution can correctly place into quarantine) is improving for less than one-half of organizations.

### *False Positives are Even More Serious*

False positives are an even more critical problem than spam capture efficiency. Because four out of five enterprises use

email for conducting transactions, placing orders, finalizing negotiations and other business-critical activities, a valid email that is mistakenly identified as spam can have substantially more dire consequences than simply receiving too much spam. For example, a sales inquiry from a new prospect that is mistakenly identified as spam and remains in quarantine until it is discovered hours or days after it is sent can have serious ramifications for an enterprise.

Here, too, currently installed anti-spam systems are performing rather poorly: false positive efficiency is staying the same or getting worse for three out of five enterprises.

*A sales inquiry from a new prospect that is mistakenly identified as spam and remains in quarantine until it is discovered hours or days after it is sent can have serious ramifications for an enterprise.*

## Comparative Analysis and Methodology

---

In evaluating the best method of comparing leading anti-spam solutions, Osterman Research considered holding a “bake-off” of sorts, in which we would conduct real-world testing of various anti-spam solutions using a corpus of valid email and spam, much like many other organizations have done. However, the disadvantage of that approach is that Osterman Research is a market research and consulting firm and, quite frankly, we could not do a better job of evaluating various solutions than many of the testing labs that have already conducted these comparisons.

Instead we chose a somewhat different, but related, methodology while maintaining the bake-off concept: we chose to use the published test results from other organizations instead of generating our own test results. In order for these results to be considered for this analysis, they had to meet two criteria:

- They had to be conducted by an independent testing laboratory and not by vendors themselves.
- They had to have been conducted during 2004. While there are a number of useful testing results from 2003 and earlier, anti-spam solutions change frequently and we wanted to be sure to provide as fair a comparison as possible.

Other criteria used in selecting test data for this analysis included using data from as broad a range of independent sources as possible, comparing results over time where these results were available and selecting the best results for each

vendor so that we did not place undue emphasis on anomalous results.

## Results

In all, we evaluated published testing results from a total of 23 vendors of anti-spam solutions. Further, as noted above, where we had multiple results for a particular vendor, we selected the best result for that vendor that we found in terms of both spam capture efficiency and false positive percentage.

*Where we had multiple results for a particular vendor, we selected the best result for that vendor that we found in terms of both spam capture efficiency and false positive percentage.*

### Spam Capture Efficiency

The following table shows the spam capture efficiency of those solutions that provide a spam detection rate of at least 94%.

Comparison of Leading Anti-Spam Solutions  
Based on Spam Capture Efficiency

Vendor	Spam Capture Efficiency %	Source
Cloudmark	98.20%	PC World, June 2004
CommTouch	97.00%	Netopus, September 2004
Clearswift	96.32%	Network Computing, 13 May 2004
iHateSpam	96.20%	PC World, June 2004
MX Logic	96.06%	Network Computing, 13 May 2004
Barracuda	95.67%	Network Computing, 13 May 2004
Proofpoint	94.70%	Network Computing, 13 May 2004
IronPort	94.43%	Network Computing, 13 May 2004
Brightmail	94.38%	Network Computing, 13 May 2004
BorderWare	94.32%	Network Computing, 13 May 2004
Postini	94.00%	NW Fusion, 23 May 2004

### False Positive Efficiency

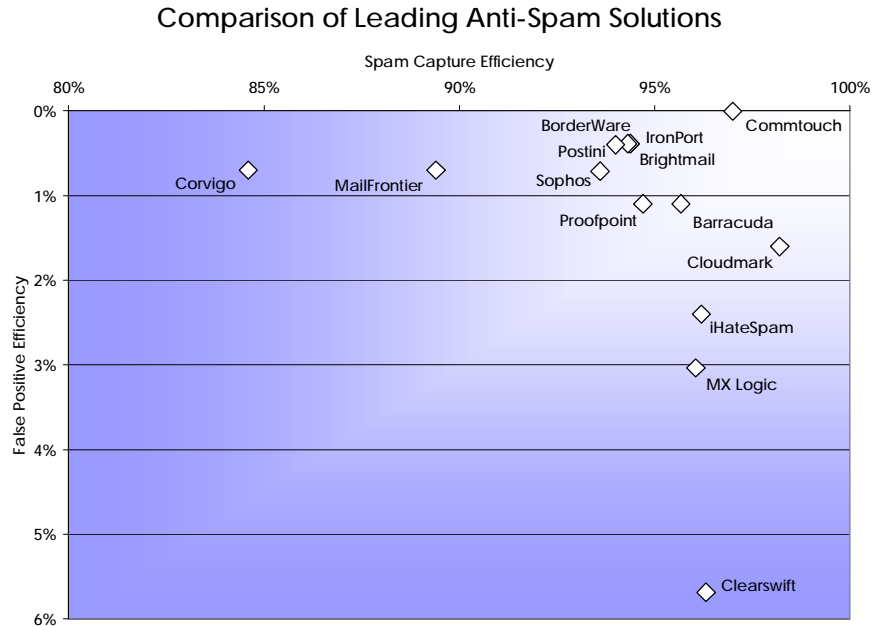
The following table shows the false positive efficiency of those solutions that generated a false positive ratio of no worse than 1:100.

Comparison of Leading Anti-Spam Solutions  
Based on False Positive Efficiency

Vendor	False Positive Ratio	Source
CommTouch	1:27,900	Netopus, September 2004
IronPort	1:258	Network Computing, 13 May 2004
Brightmail	1:258	Network Computing, 13 May 2004
BorderWare	1:258	Network Computing, 13 May 2004
Postini	1:250	NW Fusion, 23 May 2004
MailFrontier	1:143	NW Fusion, 23 May 2004
Corvigo	1:143	NW Fusion, 23 May 2004
Sophos	1:141	Network Computing, 13 May 2004

A scatter diagram showing spam capture efficiency vs. false positive percentage for the leading anti-spam solutions is shown below. Please note that any anti-spam solution will ideally be as close to the upper right corner of this chart as possible.

*Solutions that deliver both very high capture and extremely low false positive are indeed hard to come by, yet not impossible. It is recommended to aim for solutions that do not force a compromise between these two crucial factors.*



## Conclusion

---

The selection of which anti-spam solution to choose will depend on a variety of factors, including:

- **Spam capture / false positive trade-off**  
Many accept the conventional wisdom that in fighting spam, one must compromise spam capture efficiency in order to maintain an acceptable level of false positives. However, the conclusion drawn from our analysis is that solutions that deliver both very high rates of spam capture while generating low false positives are available today. Whenever possible, we recommend selecting a solution that does not force a compromise between these two crucial measures of spam-blocking performance.
- **Availability of internal IT resources**  
This document has not focused on the level of IT labor investment required to maintain various solutions, although the amount of time required to maintain anti-spam solutions can vary widely. Organizations that find it difficult to find talented IT staff should focus particularly on those solutions that require the least amount of IT labor to maintain, focusing on solutions that are automatically updated versus those that require the ongoing creation of rules by internal IT staff to address new spam threats. Our research has found that maintenance of anti-spam systems can consume significant amounts of IT staff time.
- **Outsourcing spam protection**  
Some of the solutions discussed in this white paper are provided by managed service providers that process all email at an external data center, while others are managed internally on in-house appliances or servers. There are advantages and disadvantages to both approaches that are not the subject of this white paper.
- **Internal testing results**  
Although the testing results we have chosen, as well as the sources that generated them, are reliable and provide a useful benchmark for evaluating the respective solutions, results can vary. Because what is spam to one organization may not be spam to another, results for both spam capture efficiency and false positive efficiency can be different from one

*There are a number of very good anti-spam solutions currently available, solutions that can capture the vast majority of spam entering a corporate messaging system while generating very few false positives.*

organization to another. It is important, therefore, to evaluate anti-spam solutions based on a representative corpus of email from a particular organization.

In summary, there are a number of very good anti-spam solutions currently available, solutions that can capture the vast majority of spam entering a corporate messaging system while generating very few false positives. This white paper focuses on the specific attributes of spam filtering and false positive efficiencies, and draws no conclusion as to the "best" solution that is currently available.

© 2004 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed outside of the client organization that has purchased it, nor may it be resold by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

THIS DOCUMENT IS PROVIDED "AS IS". ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.