MailFrontier
Email is good again.™

WHITEPAPER

Putting Anti-Spam Solutions to the Test ...Before You Buy

The best argument yet for testing anti-spam solutions
… three things growing organizations
should consider in selecting products to test...
and a five-step plan for getting results you can trust!

MailFrontier
Email is good again.™

Table of Contents

1. Test Before You Buy

With spam volumes increasing daily, organizations are under great pressure to implement anti-spam solutions quickly. In their haste to fix the problem, some have chosen products that seem easy to implement on the surface, yet offer limited effectiveness or incomplete protection from known spam types, or lack the ability to extend their protection to new or blended types as they emerge. A recent survey of 563 members of the CNET Networks TechRepublic Community [1] revealed that while *nearly 70 percent say they have an anti-spam solution in place, just 12 percent consider their spam problem solved.*

Selecting an anti-spam solution is an especially important decision for growing organizations. Spam can be just as devastating to you as it is to large enterprises, but with more limited financial and technical resources, the impact of choosing the wrong anti-spam solution can be worse. *To avoid the buyer's remorse that is epidemic in the industry right now, you must test solutions thoroughly and effectively before you buy*. Key to successful testing is to design a test for your unique needs and your unique environment.

In this whitepaper, MailFrontier–an innovator in email security that protects growing organizations from spam, virus and fraud and other email threats–takes the anxiety out of testing anti-spam solutions. By following our five-step plan, you can test anti-spam solutions quickly and easily. Most important, you will get results you can trust–enabling you to make the right decision the first time around.

But first, a few words about how to select which anti-spam products to test.

[1]For full survey results, visit www.mailfrontier.com and download the whitepaper: *"TechRepublic IT Survey Results: Best Practices for Overcoming Spam."*

2. How to Decide Which Products to Test

Despite numerous and conflicting vendor claims about what's important in an anti-spam solution, just three things matter:

Is it effective?

While most anti-spam solutions will have at least a 90 percent spam-blocking effectiveness rate, you need to decide the minimum effectiveness that is acceptable to your organization. And while an effectiveness rate of 90 percent might sound good, think about the actual impact of it on your employees and on your corporate email system. For every 10,000 emails that pass through a spam filter with a 90 percent effectiveness rate, 1,000 of them are spam; for every 50,000, 5,000 are spam; and so on. Before long, these numbers add up to an unacceptable volume. Another aspect of effectiveness is whether the solution allows good email to get through. After all, it's easy to achieve a spam-blocking effectiveness rate of 100 percent if you block all email.

What you really want is a solution that blocks as much spam as possible while ensuring that good email reaches its destination. A good email that gets classified as spam is called a false positive and if it is deleted without the recipient being given the opportunity to review it first, it is lost forever.

Industry standards suggest that the good anti-spam solutions miss 5 percent or less; don't even test–let alone purchase–a product whose maker won't stand behind a claim that it is at least 95 percent effective.

Is it easy?

As an IT professional, you carry the burden of any problems an anti-spam solution creates for your organization. If a solution is more difficult to install than you expected, that is time that takes you away from other critical tasks. Once installed, if a solution requires more management time than you anticipated, you will have to devote those extra hours on an ongoing basis. And if a clumsy or complex user interface makes the solution more difficult for your employees to use than you thought, all those emails from unhappy users will come flooding into you.

The best anti-spam solution offers organizations easy deployment, user ease of use and effortless administration without sacrificing control. These attributes preserve your flexibility while keeping total cost of ownership low and user satisfaction high.

Will it keep you a step ahead?

New types of spam can appear at anytime, limited only by the imaginations of their perpetrators. When fighting an enemy who changes every day, agility is critical. The best anti-spam solution will evolve to stop new spam types as they emerge, offering you protection now and for the future.

In addition, spam is not the only email threat facing your organization. Other threats include viruses, fraudulent email–including phishing scams - directory harvest attacks and dictionary and denial-of-service attacks.

Fraudulent emails pose an especially serious threat to businesses as fraudsters are now discovering that techniques that work well with consumers work equally well with unsuspecting employees. Fraudulent emails aimed at employees often appear to come from trusted sources such as company management or partners; use legitimate company graphics, layout, content and links; and ask employees to take actions that seem reasonable in a business context, such as verifying company information. Simply by following directions, employees unwittingly provide the fraudster with sensitive financial data or network access information.

And increasingly, perpetrators are combining several of these methods into a single attack, creating a blended threat. An example of a blended threat is a hybrid worm/virus sent via email that self-replicates and infects servers to spread the contagion. A blended threat can also include a Trojan horse–malicious code contained a seemingly harmless program–that will be activated at a later date.

When facing blended threats, even an outstanding anti-spam solution that stands alone will fail to protect your organization. Your anti-spam solution should be part of an integrated email security solution that offers you comprehensive and all-in-one protection.

3. A Five-Step Plan for Success

Step #1: Define your Test Criteria

After you decide which products to test, the first step in getting test results you can trust is to define your criteria. Your criteria will emerge from answering these important questions:

How does your organization define spam?

Spam is most often defined as unsolicited commercial email. But, spam also can be non-commercial, for example, chain letters or political solicitations. And spam can be legitimate business email that is unwanted by the user, such as inquiries from potential partners or job seekers. Bottom line, spam is any unwanted email that comes into your organization in volumes high enough to affect employee productivity or system and network performance.

How will you measure effectiveness?

You want a solution that blocks as much spam as possible while ensuring that all good email is delivered. A good anti-spam solution misses less than 5 percent of spam and lets through all good email through a feature that blocks suspect emails yet allows recipients to review them before they are permanently deleted.

How will you measure ease of installation and management?

As part of evaluating an anti-spam solution, you want to assess how much overhead the solution will create for your IT staff. A good anti-spam solution is easy to install and requires just a few minutes a week to manage. Once up and running, it should provide summary and detailed reports that enable you to fine tune your spam strategy, respond quickly and easily to unique threats and implement changes with a minimum of day-to-day management. You make the decisions and the solution implements them and tracks their effectiveness, ensuring a high degree of flexibility and a low total cost of ownership. And if you have other email security solutions, your anti-spam solution should integrate easily to provide you comprehensive and all-in-one protection from the full spectrum of email threats, including viruses, fraudulent email–including phishing scams–directory harvest attacks, dictionary and denial-of-service attacks and blended threats.

How will you measure ease of use?

The biggest single contributor to the failure of anti-spam solutions is user dissatisfaction. Key to user satisfaction are easy to use interfaces and features such a summary reports of blocked email that allow users to retrieve emails that have been blocked mistakenly without IT intervention. The day you turn on an anti-spam solution you should expect a flurry of unsolicited emails from delighted users. After that, you should hear complete quiet.

Step #2: Develop Your Test Methodology

Every organization is unique with its own set of needs. This is true even when fighting spam. The second step to successful testing is to understand your requirements and develop a test methodology to meet them.

Test with real email

Every company has a unique vocabulary and email patterns. To understand how a solution is going to work in your environment, you need to test it in your own environment with your actual email. If your company is in an industry that has a "spam-like" vocabulary such as insurance, financial services or pharmaceuticals, testing with real email becomes even more important.

Test with live email

For accurate results that reflect how the solution is really going to perform in your live environment, you test with live company email in real time.

Test in-line

The simplest and surest way to test an anti-spam solution is to insert it into the production mail flow–at the perimeter of your email flow or the corporate mail hub - so that it can filter email traffic for all users at it arrives.

Test across all users

The only way to make sure you become one of the select few organizations that is satisfied with your anti-spam solution is to test the proposed solution in production across your entire user base.

Test for two weeks

We recommend running each test for about two weeks. This will give you enough time to experiment with different settings, monitor the effectiveness of each and to evaluate the product's ability to adapt and fit your environment.

Test one solution at a time

In the past, some vendors have recommended evaluating multiple anti-spam solutions by running them in-line simultaneously, with each solution filtering the same email stream one right after the other. This will not give you good results. The first product in the chain will invariably let some spam through that the second one will pick up. You might think this has proven the second solution better, since it picked up spam missed by the first. But you have no way to measure how many spam messages the first trapped that would have been missed by the second if the positions were reversed. Rotating their position periodically doesn't make up for this weakness.

Step #3: Prepare Your Employees

Given that the biggest single contributor to the failure of anti-spam solutions is user dissatisfaction, it's critical to involve your employees in your tests and actively solicit their feedback.

Start by instructing employees to use their own definition of good and bad email and to use it consistently across all products being tested. Show your users the steps to review quarantined spam and to correct a false positive for each solution being tested.

Next, instruct your employees to take the following two actions each day. It is important that they do these things every day, as many anti-spam solutions "learn" from a user's behavior.

- Move any missed spam from their inbox into a new folder called "Missed Spam in Inbox". This is critical to evaluating the spam-blocking effectiveness of the solutions you are testing.

- Review the messages quarantined as spam. The good solutions provide your employees with an email in their inboxes that summarizes their spam for the day, with the ability to unjunk a false positive from within that email. Have them look for false positives and retrieve any they see. This is critical to evaluating how effective solutions are at allowing good email to reach its destination.

Step #4: Run Your Test

You now are ready to run your test. Be sure to let your employees know you have started the test.

Check results daily

Check in with your employees daily to make sure they are completing their tasks, and to hear their feedback while it is fresh. This feedback may lead you to make adjustments to improve the effectiveness of each solution as it is being tested.

Track IT management

We recommend that you start a log for each product you test. As you administer each product, keep a record of how long each task takes. Also record each time a user calls with a question or complaint.

Step #5: Evaluate Results

After running the test for two weeks, you now can evaluate results.

Calculate missed spam

Throughout the test, your employees moved any missed spam into a separate folder. Count and record the total number of missed spam messages. Next, go to the spam quarantine and count the spam captured during the test period. Divide the total number of missed spam messages by the total number of spam messages.

Calculate false positives

Throughout the trial, track the number of false positives (if any) from a cross-section of users.

Measure IT management

Walk through any administrative tasks that will be required of the product on an ongoing basis, regardless of whether they were required during the trial. Calculate how long each takes, and multiply by the estimated frequency. We also recommend you survey any other IT members who were involved in supporting the trial. Following is a recommended survey.

IT Survey

IT Participant: _____ Anti-Spam Product: _____

Circle the number that most closely represents your experience
1=completely agree 10=completely disagree

The installation went as smoothly as I could have hoped.	1 2 3 4 5 6 7 8 9 10
The solution was virtually self-running after installation, yet gave me flexibility and control.	1 2 3 4 5 6 7 8 9 10
The solution significantly decreased the overall time required to manage spam.	1 2 3 4 5 6 7 8 9 10
Overall I am very satisfied with this solution.	1 2 3 4 5 6 7 8 9 10

Measure user satisfaction

You have collected live feedback from each user on a regular basis and by this time have an idea of overall satisfaction with each solution. As a final step, you should survey each of them. Following is a recommended survey.

Participant Survey

Name: _____ Anti-Spam Product: _____

Circle the number that most closely represents your experience
1=completely agree 10=completely disagree

The process for ensuring none of my good email ever got lost was fast and easy to remember.	1 2 3 4 5 6 7 8 9 10
The anti-spam solution helped me be more productive.	1 2 3 4 5 6 7 8 9 10
The anti-spam solution was easy to use and non-intrusive.	1 2 3 4 5 6 7 8 9 10
Overall I am very satisfied with this solution.	1 2 3 4 5 6 7 8 9 10

4. Conclusion

While vendor claims are a valuable starting point in evaluating anti-spam solutions, the true measure of an anti-spam solution is how well it performs in your organization and how well it meets your unique requirements. The only way to determine the best anti-spam solution for *you* is to test several solutions that appear to meet your needs and make a definitive judgment based on objective criteria.

Take the time to carefully set up your criteria, test on live email in a production environment and monitor results carefully during and after the test. This will ensure that the anti-spam solution you choose will solve your spam problem and that you avoid the buyer's remorse that is epidemic among customers of anti-spam solutions today.

5. About MailFrontier

MailFrontier is an email security company that protects your organization from spam, virus, fraud and the growing number of other costly email threats. Fighting an enemy that changes daily, MailFrontier is an agile innovator, offering best-in-class protection from all known threats, blended attacks and new threats as they emerge. Only MailFrontier is effective and easy, and ensures that you stay a step ahead of email threats that can cripple your productivity, increase your liability and cause your IT costs to skyrocket.

MailFrontier is dedicated to serving growing organizations by delivering product, service and partner experiences that meet your unique requirements. The industries we serve include media & entertainment, insurance, financial services, utilities, healthcare, manufacturing, high technology and other sectors. We have more than 800 customers, including Pier 1 Imports, the San Francisco Giants, Wyndham Hotels & Resorts and Peet's Coffee & Tea.

For more information about MailFrontier, contact us at:

MailFrontier, Inc.
1841 Page Mill Rd.
Palo Alto, CA 94304
Phone: 650.461.7500
Fax: 650.461.7501
www.mailfrontier.com

1841 Page Mill Road
Palo Alto, CA 94304
886-3NO-SPAM
www.mailfrontier.com