

The Anti-Spam Buyer's Guide

Shedding some light on anti-spam technologies

www.vircom.com



© 2003 Vircom, Inc. All rights reserved.

Foreword

At Vircom, we believe our anti-spam solution is the best on the market. That being said, rather than trying to convince you of that fact, we want to let you decide for yourself. This document is not a sales pitch, but a series of guidelines to evaluate your own requirements. We hope you will consider Vircom's solutions, but if another vendor suits your needs better, then this buyer's guide will have met our expectations regardless.

Introduction

When considering the purchase of an anti-spam solution, it is easy to be overwhelmed by choice. The anti-spam market is getting more and more crowded, and the offer is as varied as it is confusing, ranging from the state-of-the-art to the frivolous. How can one make sense of the noise and hype of the anti-spam market? How does one navigate the mess?

This Buyer's Guide was put together by Vircom to allow you to take a breath and understand the challenges and goals faced by your organization when selecting an anti-spam vendor. We believe that the best policy an anti-spam vendor can adopt is openness and honesty, and we hope to share with you some of the insights and wisdom we have gained by being on the anti-spam market since 1997.

If you have further questions on the anti-spam market or Vircom's solutions, we invite you to read *The Modus Manifesto*, available on Vircom's website, or to contact us directly at sales@vircom.com.

How to use this guide

We have provided you with an evaluation grid at the end of this document. Simply arm yourself of this grid when you select vendors, and see how they stand up. The rest of this document will help you make sense of the categories, and know exactly which questions to ask your potential vendors.

Quality criteria to look for

Catch rate

The catch rate of a solution describes the efficiency of the solution at identifying and stopping spam. It is expressed as a percentage, and is calculated by counting the total amount of spam that is actually blocked.

Some vendors make outrageous claims as for their catch rate, so it is strongly suggested to test this by yourself. If the vendor has a demo version, use it yourself. Count the number of spam messages that are stopped, and the number that comes through. The catch rate of the solution is thus:

$$\frac{\text{(Spam stopped)}}{\text{(Spam stopped + spam missed)}} \times 100\%$$

For instance, if your solution blocks 80 spam messages and lets 20 go through, its catch rate will be $80/(20 + 80) = 80\%$.

False-positive rate

The false-positive rate is the heart of any good anti-spam solution. Creating an anti-spam solution with a 100% catch rate is easy: just block all incoming email! Creating an anti-spam solution with a very high catch rate and a very low false-positive rate is the real challenge.

The false-positive rate is the number of messages blocked by your solution that are legitimate and falsely identified as spam. Again, some vendors can make some outrageous claims, so try to test this for yourself.

To calculate a false-positive rate, count the number of messages stopped, and the number of legitimate messages blocked. The false-positive rate is then:

$$\frac{\text{Legitimate messages blocked}}{\text{Total messages blocked}} \times 100\%$$

Performance

The system's performance is a critical factor. Your anti-spam system should be able to sustain the load of messages transiting through your system.

Performance is typically described as KB/sec. To find out how much performance you need, calculate, through your mail server's logs, the total size of files going through your system per day. Your performance is then:

$$\frac{\text{Total size of messages per day}}{86,400} \text{ KB/sec}$$

If you only have a count of email, multiply the number of emails you have by 10 KB.

Your anti-spam solution should have a performance that is at least superior to your performance requirements. If you have particularly high performance requirements, inquire with your prospective vendors, as they sometimes have high performance solutions. For instance, Vircom offers a clustered version of its Modus products.

A good
catch rate
is 90%
or more.

A good
false-positive rate
is 0.01% or less.

Anti-spam technologies

Solving the spam problem proves to be technologically challenging. It is not a mere matter of putting together a keyword filter: much like the virus problem, it is difficult to eliminate because cunning, stealthy individuals react to the solutions that are put forth.

There are almost as many technological approaches on the market today as there are vendors. Unfortunately for the buyer of an anti-spam solution, some are out-of-date and useless, and others have major flaws that will render them impractical in a mere year. It is important to understand the approach taken by vendors when putting together an anti-spam solution.

Anti-spam technologies can be broken down in 5 broad categories:

Heuristics describe anti-spam solutions that use computer-driven methods to fight spam. These systems try to detect patterns in the message that are typically associated with spam. They can be very efficient at fighting spam, but they are slower to adapt and can sometimes make disputable decisions when used alone. Also, spammers are aware of heuristic methods and often invent ways of bypassing them.

Checksum databases assign a unique identifier to each spam message they find. Then, they build a database of these identifiers, so that incoming email can be compared with the contents of the database. Unfortunately, there are many spam tactics employed to circumvent this, and it requires a huge network to function at an optimal level.

Keyword filtering is an archaic technology that filters incoming email using keywords. This catches a lot of false-positives, is fooled by basic content manipulations such as intentional misspellings and is not recommended as the primary anti-spam technology.

Filter scripting includes technologies such as Vircom's Sieve2 that uses advanced filtering logic methods. This can include scripting languages that can be used to build sophisticated anti-spam. Scripting is very efficient at blocking many or all spam tactics, but unless it is used with other technologies, it represents a lot of maintenance work and hardly copes with today's spam proportions.

Real-time blacklists, also called RBLs or DNSBLs, connect to an outside server that determines who spammers are based on their IP address. Unfortunately, this method is outdated, as it blocks legitimate senders who have been abused by spammers. As a result, RBLs have up to 60% false-positive rate.

Deployment

The deployment model of a solution is as critical a choice as the technology itself, so take the time to learn what they imply.

There are four types of deployment models:

Managed solutions are solutions that are installed on the vendor's network. They are very easy to deploy as you only need to change your MX record to point to the vendor's network. However, they represent a corporate privacy risk, and they do not allow you full control over your solution: you are paying somebody else to do it for you.

Software solutions are software products that you deploy on one of your servers, like Vircom's Modus solutions. They are very cost-effective and ensure that your data is stored on your premises, but they require a knowledgeable systems administrator to supervise. Vircom addresses this issue by offering professional install and monitoring services to organizations with higher corporate needs or with limited IT resources.

Appliances are software and hardware bundles that you deploy in front of your existing network infrastructure. They provide a good value if you are looking for a total solution, but they leave you little choice as to what hardware and OS configuration you want to use. As a result, you might prefer to purchase your own server and OS license.

Desktop solutions are deployed on each individual machine of your network. This is not recommended for enterprises, as the spam has already entered your network when it is filtered by your users. Also, this type of solution does not protect you against DoS or open relay attacks.

Service

The type and quality of service offered by your anti-spam vendor is very important. This can be difficult to gauge, but take the time to discover the quality of the service offered. Try to interact with the support staff during a trial period of the software. Good support should be efficient, professional, friendly, and quick to call you back. More importantly, you should feel comfortable with interacting with them on a regular basis.

Key features

Following is a list of important product features that should be considered when buying an anti-spam solution. Most of these features will add power and versatility to an anti-spam solution. These become particularly handy when buying a solution for a service provider (xSP) or corporate environment where multiple users with different needs are involved.

Auto-updates

Many anti-spam solutions today offer you auto-updates to your anti-spam signatures. Make sure your anti-spam solution is auto-updated, or else you will have to assign a member of your staff to updating and maintaining your anti-spam solution and dealing with employee complaints. Auto-updated solutions save time, improve corporate image internally, and provide your enterprise with a clean, professional environment.

User delegation

It is very likely that your users have varying needs when faced with spam. Programmers, for instance, will want aggressive spam filtering, while vendors will be much more open as to the type of emails they receive.

Unless your enterprise's needs are very uniform, make sure the anti-spam solution you are considering allows for user delegation.

Quarantine

If your anti-spam solution does not have a system quarantine, you run the risk of losing legitimate email. Forwarding to a mailbox does not prove quite efficient enough, as there are no mechanisms to forward email to the legitimate user in case of a false-positive.

User quarantine

Unless your anti-spam solution has an anti-spam quarantine, you will need a network administrator to review the quarantine system continuously and make sure there are no false-positives.

Unless your enterprise is fairly small, make sure your users will have access to their own user quarantine.

User reporting

One good tool to better user productivity is user reporting. This is not present in all anti-spam solutions, but is a very nice benefit. With user reporting, your users will receive a report - whether through email or on the web - showing them what spam messages were caught since the last update. This is a good productivity tool and will reduce lost time even more.

Open relay protection

One big risk to corporate mail servers is the possibility of "open relay attack" by spammers. Spammers will hijack a defenseless mail server and use them to send email to the rest of the world. This can mean downtime, loss of reputation, and impossibility to communicate with the outside world as your IP ends up on a real-time blacklist.

Make sure your anti-spam solution includes open relay protection mechanisms.

Custom filters

Your anti-spam solution should give you the possibility to react in the event that the system does not block a certain type of spam per default. Perhaps you are receiving harassing email from a fraudulent enterprise, or a hacker is trying to do a Denial of Service attack on your mail server.

The ability to write custom filters is important even if the solution is auto-updates, as it gives you the ability to react quickly to new threats.

Spam categories

Some anti-spam solutions allow you to decide which categories of spam you want to block, and which to allow through. This can be particularly useful if you are in a specialized industry, such as mortgage or the health sector, as these sectors tend to consider legitimate some e-mails considered by others as spam.

If you are in a specialized industry, consider a solution that includes spam categories.

Blacklisting

Blacklisting refers to the ability for your users to determine which email addresses they want to block. This ensures that they are not repeatedly hit by a spammer that the system does not block.

Whitelisting

Whitelisting refers to the ability to allow messages to go through when they come from a known, trusted source. This is an important feature that will help to reduce the false-positive rate. Even if the false-positive rate of the solution you are testing is very low, make sure it has whitelisting.

Challenge / response

A challenge / response system means that new senders trying to communicate with your users are required to identify themselves before they can initiate communication. This is useful for home users and for corporate users with little need to contact the outside world (e.g. programmers, engineers, upper management.) For sales, PR, marketing or HR, this is not a desired solution.

If you are looking for a challenge / response system, make sure it also includes user delegation.

Evaluation grid

| Vendor |  | | | |
|-----------------------|---|--|--|--|
| Solution | ModusGate ModusMail | | | |
| Catch rate | 98.2% | | | |
| False positives | 0.001% | | | |
| Performance | Hardware- dependant | | | |
| Technology | SCA™ + Custom Sieve scripts | | | |
| Deployment | Software | | | |
| Service | 8x6 eastern | | | |
| Auto-updates | Yes | | | |
| User delegation | Yes | | | |
| Quarantine | Yes | | | |
| User quarantine | Yes | | | |
| User reporting | Yes | | | |
| Open relay protection | Yes | | | |
| Custom filters | Yes | | | |
| Spam categories | Yes | | | |
| Blacklisting | Yes | | | |
| Whitelisting | Yes | | | |
| Challenge/response | No | | | |