



VIRCOM
freedom of e-expression

Email Filtering Buyer's Guide

Shedding Light on Email Filtering Technologies

Table of Contents

Forward	1
Introduction	2
How To Use This Guide	2
Selection Criteria	2
Deployment	3
Software solutions	3
Appliances	3
Desktop solutions	3
Managed solutions	3
Email Filter Efficiency	4
Catch-rate	4
False-positive Rate	4
Key Features	4
Quarantine Management	6
System Quarantine	6
User Quarantine	7
Authority Delegation	7
IT Management	7
Spam Updates	7
Infrastructure Protection	8
User Account Management	8
Customer Service	8
Performance & Availability	9
Performance	9
High Availability	9
Evaluation Grid	10
About Vircom	11

©2007 Vircom, inc. This whitepaper is the exclusive property of Vircom, Inc. Distribution, reproduction or modification, in whole or in part, of this document is strictly prohibited without prior written consent from Vircom.

Modus and ModusGate are trademarks of Vircom, Inc. The trademarks or service marks of their respective companies or organizations identify all other products or services mentioned in this document.

Vircom Inc., 460 St. Catherine St. West, Suite 600, Montreal, QC, Canada, H3B 1A7
Vircom Europe S.A., 16 Place de l'Université, B-1348 Louvain-la-Neuve, Belgium

For more information, visit our Website at <http://www.vircom.com> or contact us at:
Vircom Inc. : +1 (514) 845-1666 (EST)
Vircom Europe : +32 (10) 48.35.04 (CET)



Forward

This white paper provides guidelines for selecting an email filtering solution. The paper aims to improve the reader's ability to make informed and accurate purchasing decisions by analyzing the various email filtering features and properties that shaping the overall quality of a product or service.

Introduction

When considering the purchase of an email filtering solution, it is easy to be overwhelmed by the selection of available products. The market is becoming saturated and the choices are as varied as they are confusing, ranging from basic freeware to state-of-the-art solutions. How can one make sense of the email filtering market hype? How does one choose the product that's right for their mail system?

This buyer's guide was developed by Vircom to help you understand the challenges faced by your organization when selecting an email filtering solution. We believe that solution's vendor should be open and honest with its clients and this guide should help you make an informed decision.

If you have further questions about the email filtering market or any of Vircom's solutions, please contact one of our sales partners or Vircom directly at sales@vircom.com.

How To Use This Guide

Read the guide to develop a better understanding of the terms used in the email filtering market and how they apply to you. Then use the evaluation sheet, included in this buyer's guide, to help you compare vendors and their solutions.

Selection Criteria

There are several quality criteria to look for when selecting an email filtering solution. Vircom has categorized these into five categories:

- Deployment: how is the solution deployed
- Spam filter efficiency: how effective the solution is at blocking spam
- Quarantine handling: how easily users and administrators manage quarantined messages
- IT management: how much effort and resources are required to manage the solution
- Performance and redundancy: how the system handles your performance and availability requirements

Deployment

The deployment model of a solution is as critical a choice as the technology itself, so understanding them is important.

There are four types of deployment models:

Software solutions

...are software products (such as Vircom's modus™ solutions) that are deployed on one of your servers. They are cost-effective and ensure that your data is stored on your premises. However, they require a systems administrator to manage them. Vircom addresses this issue by offering professional installation and monitoring services to organizations with greater corporate needs or limited IT resources.

Appliances

...are software and hardware bundles (such as Vircom's modusGate™ Appliance) that are deployed in front of your network infrastructure. They provide good value if you are looking for a total solution that is quick and easy to install.

Desktop solutions

...are deployed on individual computers on your network. While this method is satisfactory for home use, it is not recommended for organizations because spam has already entered your network by the time it is filtered by your users. Also, this type of solution does not protect you against DoS or open relay attacks.

Managed solutions

...are solutions that are installed on the vendor's network. They are 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 do not allow you full control over your solution. As the name implies, you pay a third-party to manage the solution for you.

Email Filter Efficiency

The effectiveness of an email filtering solution determines its success when protecting your mail system. The following features should be considered when purchasing a solution.

Catch-rate

The catch-rate measures the efficiency (identifying and blocking spam) of the spam filtering solution.

Some vendors make outrageous catch-rate claims so we recommend testing their claims. If the vendor provides a demo version, install it and calculate the catch-rate. The calculation used is:

$$\frac{\text{\# spam messages blocked}}{\text{Total \# spam messages}} \times 100$$



A good catch-rate is 90% or more.

False-positive Rate

A false-positive is defined as legitimate mail that is incorrectly identified and not delivered to a recipient's inbox. A low rate is the essence of any good spam filtering solution. However, the real challenge is creating a solution with a very **low false-positive rate** and a very **high catch-rate**.

Again, some vendors make some outrageous claims, so test this for yourself. The calculation used is:

$$\frac{\text{\# legitimate messages blocked}}{\text{Total \# messages blocked}} \times 100$$



A good false-positive rate is 0.1% or less.

Key Features

Combatting spam has proven to be technologically challenging. It does not merely involve compiling a keyword filter because, as with viruses, cunning individuals, intent on spamming, quickly react to the solutions that are put forth and find new ways to circumvent solutions.

There are many technological approaches to solutions on the market today. Unfortunately for the buyer of an email filtering solution, some are antiquated while others have major design flaws that would render them useless in merely a year. It is important to understand a vendor's approach when developing an email filtering solution.

Email filtering technologies can be broken down into three major categories:

Protocol-level Filtering

Protocol-level filters can block more than 75% of spam. These filters offer great performance because they work at the protocol level. It is crucial for a spam filtering solution to offer all or a combination of the following:

- **Greylisting:** Greylisting temporarily rejects mail from a sender it does not recognize. The originating mail server will resend the legitimate message and, this time, the destination server will accept it. This technique assumes that spammers are unlikely to resend failed messages at a later time.
- **Static and Real-time Blacklists:** *Blacklisting* is used to identify IP and email addresses from which mail will be rejected. This ensures that mail servers are not repeatedly hit by a spammer using a blocked IP or email address. Blacklists can either be maintained locally (static blacklists) or centrally by external organizations (real-time blacklists).
- **Whitelisting:** *Whitelisting* is used to identify IP and email addresses (trusted sources) from which mail will always be accepted. This important feature helps to reduce the false-positive rate. Even if the spam filtering solution you are testing has a low false-positive rate, make sure it also offers *whitelisting*.
- **Reputation Filters:** Reputation filters determine the probability that a message is spam based on the reputation of the sender. Reputation is determined using a number of factors, including the volume of spam previously received from a particular IP address.
- **Challenge / Response:** This system requires that first-time senders, trying to communicate with your mail server, must identify themselves before communication can begin. This is useful for people with little need to communicate outside of their own network, such as home users. This feature is not recommended for corporate environments.

Content Filtering

Because protocol-level filtering cannot block all spam, a second category of spam filters is required. Content filtering accepts or rejects mail based on content of the mail headers or message body (e.g. key phrases, the percentage of HTML, images, etc.). This is achieved with two sets of methods:

Statistical Methods

Using computer-driven methods, these systems attempt to detect patterns in a message to determine the likelihood of an email message to be spam or legitimate. They can be very efficient at fighting spam but are slower to adapt and can sometimes make questionable decisions when used alone.

These methods (which include Bayesian filters) are associated with self-learning engines that extract information from data in the context of spam filtering. Also known as machine learning, this mechanism helps the system adapt to new spam variations.

Deterministic Methods

Using information gathered from spam messages and by analyzing the Internet, these reactive methods effectively avoid false-positives and are more efficient in countering new spam techniques (not just variations). The following are two examples of deterministic methods:

Keyword filtering:

- An antiquated technology that filters incoming email by using keywords

- Catches large amounts of false-positives
- Is fooled by basic content manipulations such as intentional misspellings and is, therefore, not recommended as a primary email filtering technology

Checksum databases:

- Assign a unique identifier to each spam message they find
- A database of these identifiers is compiled so that incoming email can be compared to the contents of the database
- Unfortunately, there are many spam tactics employed to circumvent this and it also requires a huge network to function optimally

Today, deterministic methods use a wide variety of message arguments (IP addresses, URLs, keywords, common expressions, etc.) to filter spam. It is important that your email filtering solution combines the efficiency of predictive analysis and the accuracy of deterministic methods to deliver the best catch-rate possible and avoid the occurrence of false-positives.

Image spam

Image spam is the latest development in spam whereby the content of the message is presented in the form of an image. This makes it more difficult for the solution to catch spam because email filters cannot “read” messages embedded in an image. Spammers can easily bypass filters by sending the same image with slight variations (known as image serializing) for each spam campaign. Spammers combine this technique with the use of millions of spam zombies (*bots*) to relay their spam messages.

A recent variation is PDF-based spam which works on the same principle but attaches a PDF document to the message instead of incorporating an image. Blocking these new threats requires new technologies and new engines. Readers should verify how well their email filtering solution counters today’s image-based spam and how well prepared it is to counter tomorrow’s threats.

Quarantine Management

If your email filtering solution does not have a system quarantine, you run the risk of losing legitimate email. Forwarding to a mailbox is not efficient because there is no way to release email to a legitimate user in the event of a false-positive. Reliable solutions should offer an integrated quarantine system.

The following is a list of important quarantine-related product features that should be considered when purchasing an email filtering solution. These features add power and versatility to the solution and can considerably reduce the time users spend handling their blocked messages.

System Quarantine

System or centralized quarantines require network administrators to regularly review the quarantined mail to ensure that there are no false-positives. Unless your enterprise is fairly small, this implementation can quickly prove to be inefficient.

User Quarantine

User quarantines allow users to review their blocked messages themselves. Without it, the network administrator will have to regularly review the quarantine system to ensure that there are no false-positives. Unless your enterprise is fairly small, make sure that your users have access to their own quarantine.

- **Quarantine Reports:** Users receive a report listing the spam messages that are in their quarantine. The report displays messages since the previous update and allows users to quickly scan messages for false-positives.
- **Web Access:** Many solutions provide a Web interface for users to review their quarantine. There are key differences with quarantine reports:
 - The Web interface is more reactive – users decide when they access their quarantine
 - The Web interface is longer to access – users must provide login credentials

Authority Delegation

Your users will, likely, have varying requirements regarding spam so ensure that the email filtering solution you are considering allows for user delegation. At the minimum, the solution should allow users to:

- **Review blocked messages:** Does the interface (Report or Web) allow users to safely review their blocked messages?
- **Release false-positives:** Does the interface allow your users to release false-positives or does it require intervention from the system administrator?
- **Trusted Senders List:** Does the interface allow your users to *whitelist* trusted senders?

Because they can significantly increase users' productivity, the email filtering solution should also provide the following user options:

- **Change report schedule:** Quarantine reports can be distracting. Changing the quarantine report schedules allows user to find a balance between the distraction of receiving reports to frequently and worrying about false-positives.
- **Change spam settings:** Every user responds differently to spam. Allowing users to configure their own email filter enables them to fine-tune their environment to suit their needs.
- **Blocked senders list:** Users may want to block messages from particular senders, even if their messages are not considered spam.
- **Language filtering settings:** Language filtering allows users to block messages written in a foreign language.

IT Management

Spam Updates

First-generation solutions require administrators to modify existing filtering rules or write new ones as spammers change tactics and methods. If you run such a solution, be prepared to designate someone to update and maintain your solution and to handle employee complaints.

The majority of email filtering solutions (e.g. Bayesian filters) offer auto-updates but still require additional tweaking. Administrators will need to regularly feed a self-learning system with spam and non-spam email to maintain their catch and false-positive rates.

This level of user intervention is not required with fully auto-updated solutions where the tuning is handled by the vendor (such as with Vircom's modus™ solutions). These automatic solutions save time, internally improve corporate image and provide your enterprise with a uncluttered and professional mail environment.

Infrastructure Protection

A risk to corporate mail servers is coming under attack by spammers. Ensure that your email filtering solution includes sufficient protection mechanisms against:

- **Dictionary Attacks:** Also known as a Directory Harvest Attack (DHA), these attacks are used by spammers to harvest valid email addresses. Spammers send messages to millions of random email addresses. Any address for which the message is not bounced is added to the spammer's list of known-valid addresses.
- **Denial of Service Attacks:** Also known as DoS, this attack attempts to overwhelm your email server with so many messages that it becomes inoperable.
- **Open Relay Attacks:** With this attack, spammers hijack unprotected mail servers and use them to send spam. This can cause mail (and even network) down-time, loss of reputation and the possibility that your IP address is added to a real-time blacklist
- **Spoofing Protection:** To protect your email infrastructure from the use of forged senders' addresses, make sure your email filtering solution provides a way to validate senders. There are various technologies that may be used, including SPF, SenderID or DKIM (Domain Key Identified Mail).

User Account Management

Email filtering solutions provide different methods for creating the list of authenticated users. The most efficient method is to connect to an existing directory service such as LDAP (or Active Directory for MS Exchange) to automate the creation of the user list. Also taken into account are user aliases which eliminates multiple quarantines and administration hassles.

Another method is to use basic SMTP lookups to create a user list. This method does not take aliases into account.

Finally, some solutions create their user list by importing a .CSV file or entering each user mailbox manually. This method can be time consuming, particularly for ever-changing environments (e.g. companies with high turn-overs).

Customer Service

The types and quality of service offered by your email filtering solution vendor is very important. This can be difficult to gauge but interacting with the support staff during a trial period of the solution may be helpful. Quality support staff should be efficient, professional, friendly and quick to return your calls. Most important, you should feel comfortable when interacting with them.

Performance & Availability

Performance

The system's performance is a critical factor. Your email filtering solution should be able to sustain the load of messages being processed by your mail system. Performance is typically described as KB/sec. To determine how much performance is required, calculate, using 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 an email count, multiply the total number of messages by 10 KB.

The solution you choose should have a performance that is superior to your actual performance requirements. If you have particularly high performance requirements, ask prospective vendors if they offer high performance solutions.

High Availability

For most organizations, email is often a critical application so its availability is paramount. Even if not required today, make sure the solution you select offers high-availability either through a fail-over implementation or through full redundancy.

Vircom offers a Blockade version of its modus™ products.

Evaluation Grid

	Vircom	Vendor 1	Vendor 2	Vendor 3
Deployment				
Product				
Software	X			
Appliance	X			
Desktop	-			
Services	-			
Email Filtering Efficiency				
Catch-rate	>98%			
False-positive Rate	<0.1%			
Key Features				
Protocol Filtering				
Greylisting	X			
Static Blacklists, RBLs & SURBLs	X			
Reputation Filters	X			
Challenge / Response	-			
Content Filtering				
Statistical Filtering	X			
Deterministic Filtering	X			
Image Spam	X			
Quarantine Handling				
System Quarantine	X			
User Quarantine				
Quarantine Report	X			
Web Quarantine	X			
User Delegation				
Review	Report & Web			
Release	Report & Web			
Trusted Senders List (Whitelist)	Report & Web			
Report Scheduling	Report & Web			
Email Filter Settings	Web			
Blocked Senders List (Blacklist)	Web			
Language Filter Settings	Web			
IT Management				
Infrastructure Protection				
Dictionary Harvest Attacks	X			
Denial of Service (DoS) Attacks	X			
Open Relay Attacks	X			
Spoofing Protection (SPF, etc.)	X			
Spam Updates	Automatic			
User Account Management	LDAP/AD, SMTP			
Performance & Redundancy				
Performance	HW dependant			
High Availability				
Fail-over	X			
Redundancy	X			

About Vircom

Montreal-based Vircom is a leading developer of cutting-edge Internet infrastructure and secure messaging solutions for the demanding needs of Internet Service Providers (ISPs) and corporate clients. Vircom's mature modus™ secure email management technology incorporates over 10 years of industry expertise, making it a powerful driving force in the defense against spam and email-borne fraud.

Its award-winning products include email gateway software, a standalone email-gateway appliance and a complete email assurance mail server – all based on its core competence: delivering email assurance technology that protects email assets.

Vircom's state-of-the-art technology manages inbound and outbound email traffic and offers protection from spam, fraud, phishing, viruses, spyware, out-of-policy communications and other email threats. Its flexible design provides the email assurance capabilities necessary to meet today's threats and the essential flexibility and scalability to meet tomorrow's.

Labeled the Best Microsoft® Windows®-based email filtering solution by Network Computing Magazine, modus™ has gained important recognition, among which are a *CATAAlliance* Innovation & Leadership Award and a record-breaking five-award distinction including "Best Software Product" and "Most Innovative Product" from Windows® IT Pro magazine.