



VIRCOM
freedom of e-expression

Assessing the Cost of Blocking Spam

The Total Cost of Ownership

Table of Contents

Introduction	2
The Cost of Blocking Spam	3
Solution Costs	3
Selection Cost	3
Acquisition Cost	3
Installation Cost	4
Installation	4
Initial Configuration	4
Cost Weight	4
IT Operation Costs	5
System and Software Maintenance	5
Email Protection	5
Quarantine Management	6
User Settings	6
Monitoring and Reporting	7
Cost Weight	7
Productivity Loss	7
Spam Delivered to Inbox	7
False-Positives	7
Quarantine Management	8
Quarantine Report	8
Web Interface	8
Number of Reported Messages	9
User Settings	9
Cost Weight	9
Conclusion	10
Vircom's Lowest Total Cost of Ownership	11
About Vircom	13

©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)

Assessing the Cost of Spam

This white paper explores the three main cost factors of email filtering solutions (solution costs, operation costs and productivity losses). Readers will learn about the various attributes influencing these costs. Ultimately, this paper aims to improve the reader's ability to make informed and accurate purchasing decisions by analyzing the various email filtering features and properties shaping the total cost of ownership of a product or a service. The white paper will also highlight how Vircom's experience and customer focus has enabled them to deliver email filtering technology with the lowest total cost of ownership.

Obviously, spam is only one aspect of email security. Additionally, anti-virus, policy enforcement and information control are important elements. We are not disputing this. However, each of these elements has its own, and often independent, cost attributes. For the sake of consistency and clarity, we have opted to focus the content of this white paper on the cost of blocking spam.

Introduction

When considering the purchase of an email filtering solution, the choices can be overwhelming. How do you make sense of the market's noise and hype? How do you measure the real value of the products and services?

Productivity Savings

Initially, to assess product value, companies compared the cost of spam with the price of the email filtering solution. Spam causes a loss of productivity (employees must search through their email to identify and delete spam), a rise in operation costs (network and storage costs), security breaches, downtime, sullied reputations, legal liability and a loss of employee confidence.

Numerous spam cost calculators provided an understanding of the savings companies could expect with good spam protection. These calculators identified that user productivity losses have the highest costs associated with spam, which, in turn, represented the biggest savings of a spam filtering solution.

Operation Costs Savings

Soon, however, the market realized that these cost saving calculations were misleading. Some vendors claimed outrageous catch-rates and list prices often omitted yearly subscription costs or hid required hardware or maintenance costs. Nevertheless, even with accurate information, these estimates had their limit: pricing stands for only a fraction of the total email security cost. Companies that selected freeware or open-source solutions often discovered this the hard way.

While all spam filtering vendors claim similar catch rates (which are far from being confirmed by industry benchmarks), companies started analyzing the value of product candidates based on their operating costs (i.e. the cost to install, run, or maintain the solution).

Today, software-based solutions, appliances and email scanning services distinguish their features based on how they reduce IT-related costs. For instance, appliance vendors put forward their reduced installation costs while Managed Security Service Providers (MSSP) present a fully out-sourced service reducing installation, maintenance and support costs.

The Total Cost of Ownership

Because spam remains an issue for employees, spam filtering vendors now focus on giving employees the discretion to manage spam themselves. Productivity loss is mainly determined by the rate by which spam gets through to a user's inbox, the false-positive rate (forcing users to search for blocked email), quarantine administration and the impact of user delegation.

Even if it is no longer the focus for spam filtering solution vendors, productivity loss remains consequential for organizations. It may not be for individual users but yearly calculations for all users demonstrate that it often represents more than 75% of the total cost of ownership. Therefore, organizations must re-evaluate their cost analyses. While pricing remains a key factor for decision making, product efficiency and user effectiveness must also become factors of any total cost of ownership assessment.

The Cost of Blocking Spam

When assessing the cost of blocking spam, the following three main cost areas should be considered:

- **Solution costs:** this represents the actual cost of selecting, acquiring and installing/subscribing to an email filtering solution (product or service)
- **IT operation costs:** these are the costs to implement and run the solution, which can be broken down into two categories:
 - *Administration costs:* the costs related to maintaining and running the system
 - *Help desk costs:* the costs related to maintaining help desk staff to assist users
- **Productivity losses:** these costs represent lost time while users review their quarantine, change personal settings or call for assistance

The amounts for each of these costs vary depending on the chosen solution. For instance, the IT operation costs will be lower for organizations that selected an email filtering service instead of a product but their solution costs will likely be higher. Similarly, productivity costs vary with the accuracy of the chosen solution and the quality of its user interface.

We will detail these costs in the following sections and highlight how specific spam filtering features can influence the different cost items.

Solution Costs

Selection Cost

This cost is inherent to any IT product or service purchase cost and does not vary regardless of the selected solution. It represents the time required by the IT staff (or by external consultants) to:

- Define the scope of the required solution and the list of mandatory and optional features
- Create a short list of solutions and vendors (reseller, manufacturer...)
- Evaluate and compare the short list of solutions
- Negotiate pricing and finalize selection

Acquisition Cost

The acquisition cost fundamentally depends on the type of solution (software, appliance or service). Service providers usually charge a per-domain setup fee and a monthly per-user subscription fee. Most contracts can be reviewed annually. For a cost assessment, it is important to note that most of these spam filtering services ensure high-availability. In addition to purchase and renewal prices, organizations must also review the cost of additionally required hardware and/or software and their related maintenance and service plans.

Appliance vendors have a more complex pricing structure. Apart from the yearly spam filtering subscription fee, hardware replacement and firmware upgrade services add to the cost of the appliance itself. High availability configurations often double the purchase price.

Software solutions have the most varied cost structure. For instance, small organizations can install the software solution directly on their mail server, thus avoiding the additional hardware cost. However, large or redundant configurations may require incorporating extra pieces of hardware and/or software to benefit from a full service.

Installation Cost

This represents the labor cost for the installing and configuring the email filtering solution.

Installation

Managed services require minimal labor to set up the service, needing only a change to the organization's MX-records to redirect incoming email traffic to the scanning services.

Appliances require more labor for them to be integrated within the existing infrastructure, including changing the mail-flow and firewall configurations.

Software solutions require the most effort. Organizations must install and configure the software and, once configured, it must be integrated into the existing infrastructure.

Another factor to consider, when assessing installation costs, is the user-related requirements such as user-list import, client plug-ins and the initial spam filtering tuning (as discussed in Initial Configuration).

Initial Configuration

While some solutions will function adequately with the out-of-the-box configuration, most will require additional labor (e.g. to integrate the user list, adapt the default settings to their organization specifics or to feed a self-learning system with messages deemed as spam or non-spam to optimize catch and false positive rates).

In addition, some solutions may require or suggest installing a plug-in on client desktops to allow users to review their quarantine, define personal settings or report false-positives. This, obviously, adds to the overall installation cost (and productivity loss).

Cost Weight

While the acquisition and installation costs can widely vary, Vircom's TCO Model¹ estimates that these costs only represent 5 to 25% of the total cost of a commercial email filtering solution.

1. Vircom: *Calculating the Cost of Spam*, July 2007

IT Operation Costs

These costs are associated with the five major administration tasks of an email filtering solution:

- System and software maintenance
- Email protection
- Quarantine management
- User settings
- Monitoring and reporting

The implementation and administration costs are tightly linked to specific features of the selected solutions. We will highlight these as we review the various operation cost items.

System and Software Maintenance

The maintenance costs essentially depend on the type of solution (software, appliance or service).

By removing the stresses of updates, upgrades and patch management from the organizations, Managed Security Services reduce maintenance costs. Remote filtering, however, raises a different issue: blatant blocking. Blatant blocking discards messages without placing them into quarantine, either because of a specific MSSP setting or because of a handling error. As a result, administrators may be required to spend time locating the cause of their employee complaints, which can occur frequently for larger installations.

Conversely, software solutions are confronted with maintaining the hardware, the OS, the MTA and the actual application. We explained the maintenance plans for these items in Solution Costs. What we cover here is the time spent by the IT staff to apply upgrades, updates and patches, report bugs, and replace defective hardware. To reduce these costs, several software vendors automate upgrades, updates and patches by self-installing them (once confirmed).

Appliance solutions fit somewhere in the middle. Administrators will spend some time updating firmware, applying patches and replacing defective hardware. However, since the updates cover the full appliance (OS, MTA & application), they are less frequent and subject to fewer incompatibilities.

Since these costs are not related to the amount of traffic or the number of mailboxes, they will affect smaller companies more than larger ones.

Email Protection

This covers the time spent by the IT staff to protect the email infrastructures from attacks (DHAs, DoS, Zombies, etc.) and the users from spam and false-positives.

Email protection is usually part of the delivered Managed Service, so its related cost will mainly affect corporations that select a software-based solution or an appliance.

Higher-end products offer built-in defenses against infrastructure attacks and automatically adapt their settings to keep impact to a minimum. Other products rely upon advanced reporting and alerting capabilities to identify problems, allowing administrators to react accordingly. Most products, however, offer poor network defense capabilities and administrators can spend hours (sometimes days) to combat these assaults.

Fighting spam can also require varying amounts of time, depending on the technology being used. Bayesian filters often require a constant feeding of spam and non-spam messages to maintain a high catch-rate with minimal false-positives. With heuristic filters, administrators adapt existing filters and write

new filters as spammers change their tactics and methods. Statistical filters will require that administrators adapt their range of probabilities for “definite spam” or “potential spam”. These technologies vary in efficiency and flexibility and most higher-end solutions use several of them in parallel. Advanced network-level defense and frequent fully automated updates are two key elements for reducing the daily protection efforts.

Quarantine Management

Because spammers disguise their messages to appear as legitimate emails, filters are constantly being fine-tuned. As a result, some legitimate email can be caught as spam. These scanning errors are called false-positives and must be retrieved when identified. This is why solutions collect blocked email into quarantine.

As will be discussed in Productivity Losses, most solutions delegate quarantine administration to the end-users. Some solutions, however, offer a centralized quarantine (either by design or as an option).

The copious amounts of spam that organizations receive make it counterproductive for one person to review messages for possible false-positives (end-users can manage their own spam faster and more efficiently). When administrators manage the quarantine, they only search and release messages upon request, with the following consequences:

- The more false-positives, the higher the administration cost (more help desk calls to release messages or to retrieve supposed messages that were never sent)
- Only a small portion of the false-positives is actually noticed by the users (adding to the hidden costs of lost reputation and lost business, even if these are difficult to evaluate)

Organizations soon discover that, in the end, only using a centralized quarantine is not a viable option. However, when limited to handling rare exceptions, it can be an effective tool.

User Settings

Because all users are different, most solutions offer the possibility to adapt settings to specific user needs, such as adding entries to their trusted list or changing the frequency of their quarantine report.

When these settings are configured centrally, the cost doubles since these changes impact not only the administrator but also the users who actually place the requests. When delegated to the end-user (through web access or via the quarantine report), user settings still add to the administration costs in the following ways:

- Account management: mainly consists of maintaining the user list (including managing aliases and passwords). This list is required to differentiate users and to grant management access. Most solutions offer the possibility to build this list automatically. Some require additional alias management and, for others, administrators must create these lists manually.
- Delegation management: used to control the delegated rights. For instance, administrators can allow advanced users to manage all or parts of their individual settings and force corporate-wide settings for less experienced users to avoid incorrect configurations.
- Exception management: consists of applying configuration changes required by less experienced users or correcting user configurations. When available, good delegation management should keep these exceptions to a minimal.

Centrally managing user settings can become very costly. Therefore, solutions should allow users to customize their own settings but allow administrators to distinguish between advanced and standard users when planning the levels of this authority delegation.

Monitoring and Reporting

Mainly serving Email Protection, monitoring and reporting can become very time-consuming for an administrator (especially as they are required). Dashboards and status reviews can effectively help to correct defense problems (attacks, zombies, etc.) and trend analyses can help to prevent problems or downtimes.

Another factor to consider is the management reports required by the executive staff to highlight the ROI of the implemented solution. These are required, at least, once per year (to justify the budget) but are often delivered on a quarterly basis.

Trend analyses and status reports are effective management tools but only when these reports are easy to create, customize and generate.

Cost Weight

IT administration costs can vary significantly depending on the level of automation (updates, user lists. etc.); the level of delegation (quarantine management, user settings, etc.) and the quality of reporting. Vircom's TCO Model² estimates that IT administration costs can vary from 5 to 20% of the total cost.

Productivity Loss

Productivity losses are mainly influenced by the rate by which spam gets through to a user's inbox, the false-positive rate, quarantine administration and the impact of user delegation.

Spam Delivered to Inbox

There are many tools available to calculate the cost of spam and these tools can also be used to calculate the cost of spam that gets through to the user's inbox.

Using our Spam Cost Calculator model³, for a company of 1,000 mail users, each receiving 25 spam messages per day, we estimate that a 5% difference in catch-rate would represent approximately \$18,000 in productivity loss! The catch-rate remains a significant element of the total cost.

False-Positives

False-positives *directly* affect user productivity because users have to release and potentially report them as non-spam. Most often, they will also add the senders in their trusted list. Some solutions require users to call the help-desk to release their messages; some require users to start a web-session and some offer the possibility to release the message directly from their quarantine report. Obviously, all have different cost implications.

False-positives also have an *indirect* impact. The higher the false-positive rate, the more often users will

2. Vircom: *Calculating the Cost of Spam*, July 2007

3. Vircom: http://www.vircomeurope.com/CostofSpam_Vircom.xls

review their quarantined messages. Benchmarks have shown that the best products' false-positive rates vary between 0.01% and 1%. For an average user, this would represent from 3.47 false-positives per year to 1 false-positives per day. Obviously, these numbers influence users' behaviors.

Companies, therefore, must examine the efficiency of the solution (false-positive rates) and the ease with which false-positives are retrieved.

Quarantine Management

Quarantine management is the biggest part of the total cost. In a recent report⁴, Ferris Research estimated that a typical medium-sized organization with good spam protection spends about \$61 per user per year for quarantine management or approximately 51% of the total cost. Since this cost is substantial, companies should take particular care to review the vendor's quarantine implementation and, more important, how users access their quarantine data.

Quarantine Report

Quarantine reports have the advantage of being pro-active. They regularly appear in users' inboxes and serve as a reminder for reviewing their blocked messages. Two key factors will influence the effectiveness of the quarantine report:

- Frequency of the quarantine report
- Ease in distinguishing between valid email and spam

Upon receipt, most users will peruse their quarantine report for legitimate email, which causes a disruption in their daily activities. Whenever possible, changing the quarantine report schedules will allow users to find a balance between reducing the disruption and assuaging worries about false-positives.

Quarantine reports must also contain sufficient information to help users quickly decide whether blocked email is spam or legitimate messages. Displaying relevant envelope details (sender's name, message title, etc.) and providing the possibility to preview the message content are key options that help reduce the review time (and increase decision accuracy).

Web Interface

Many solutions provide a web interface for users to review their quarantine. There are several key differences with the previously described quarantine report:

- The web interface is more reactive – users decide when to access their quarantine
- The web interface take more time to access – users must enter their login information to access their quarantined email
- The web interface usually displays all the blocked messages – users have a longer list to review

Obviously, the same efficiency considerations discussed in Quarantine Report should be taken into account to reduce review time.

The web interface should be used to complement the Quarantine report. When used alone, the web interface shows a far substantial cost impact.

4. Ferris Research: *Calculating Spam Cost in Your Organization*, Report #511, February 2005

Number of Reported Messages

Vendors also try to reduce the amount of spam to review in quarantine by offering the opportunity to delete Medium and High-probability spam instead of quarantining it. This, too, affects the time users spend reviewing their quarantine, looking for messages that may have been deleted.

Companies should use this option carefully to avoid blocking legitimate email and requiring administrators and users to look for false-positives that, in fact, were deleted. Instead, companies should look for solutions that limit the number of messages displayed in quarantine but still keep them for retrieval later.

User Settings

This cost is related to users changing their personal settings. These settings can range from adding an entry to trusted lists and changing the frequency of the quarantine report to changing scanning levels and blocking actions (e.g. quarantine, delete, tag and pass through).

This cost depends upon the number of available per-user settings and the rate at which these settings are changed. For instance, users will more often modify their trusted list than their quarantine report schedule.

Another key cost factor is the ease of changing these settings. The more easily users can apply changes, the more cost-effective the implementation will be. This being said, readers should keep in mind that:

- there are two available interfaces for users to change their settings (report and web)
- inexperienced users should be restricted in the settings they may access

Allowing users to manage their settings could lead to configuration errors. However, the cost of these errors must be compared to the time saved when users rely on the administrator to customize their settings.

Cost Weight

Vircom's TCO Model⁵ shows that productivity losses represent approximately **65 to 85%** of the total cost. When selecting an solution, special attention should be paid to the user interfaces and how each solution's implementation further reduces the spam impact on user productivity.

5. Vircom: *Calculating the Cost of Spam*, July 2007

Conclusion

The various Solution and Administration costs are used by most vendors to highlight their product's advantages. However, these only represent a small part of an solution's total cost. The biggest part is related to productivity loss.

Therefore, when selecting an solution, companies should assess the potential productivity losses that the solution could induce and review how the solution performs in relation to the four main productivity loss factors:

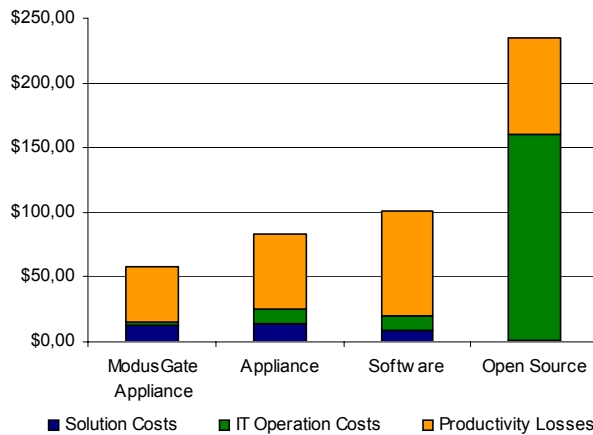
- The rate by which spam gets through to a user's inbox
- The false-positive rate
- The efficiency of the user interfaces
- The strength and pertinence of the authority delegation

Vircom's Lowest Total Cost of Ownership

More than 10 years of email security innovation and experience has guided Vircom in considering all cost aspects of email security.

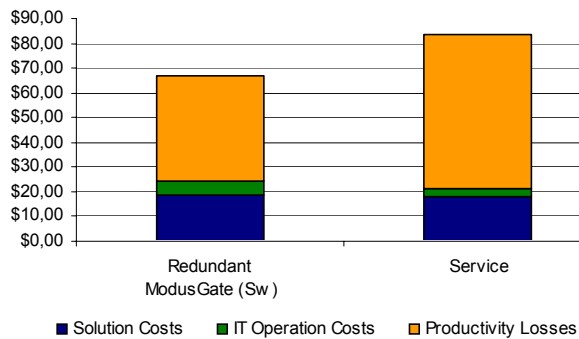
Using its TCO Model, Vircom evaluated various types of spam solutions, observing broad varieties in their total cost. As highlighted in the tables below, Vircom's modusGate™ offers the lowest Total Cost of Ownership.

This graph compares the TCO of Vircom's modusGate™ Appliance with the TCO of competitive spam filtering products (software and appliances).



TCO Comparison (modusGate™ vs. AS Products)

This graph compares the TCO of Vircom's redundant modusGate™ software implementation with the TCO of competitive spam filtering services.



TCO Comparison (modusGate™ vs. AS Services)

Vircom's lowest Total Cost of Ownership can be explained by two of the several cost reducing features:

- Vircom's SpamBuster team, not your staff, combines human analysis with an unparalleled self-learning mechanism to update your spam engine. The team gathers spammer and spam information through Internet monitoring, distributed honeypots and from users reporting spam and false-positives. The bottom line is that modusGate™ constantly delivers an out-performing, out-of-the-box accuracy of 98.2% with minimal false-positives, without your staff having to fine-tune the system.
- modusGate™ offers another major benefit: by constantly enhancing the efficiency of their Quarantine user interfaces, Vircom has considerably reduced the time users spend reviewing their blocked messages. Currently, no other spam solution vendors offer similar productivity gains!

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 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.