VIRCOM
email security matters

Understanding the
Costs of Email Security

Table of Contents

The three main cost factors associated with email filtering solutions are: solution costs, operating costs and productivity losses.
This paper aims to help the reader make an informed decision when purchasing an email filtering solution by analyzing the various features and properties that contribute to the total cost of ownership.

Introduction

Ferris Research estimates that in 2009 the cost of spam will reach $130 billion worldwide, $42 billion of which is spent in the US alone[1] How does this impact your organization?
There are many anti-spam technologies on the market and one can easily be overwhelmed by the industry jargon, such as "best spam catch rate," "zero false positives," and so on. When considering the purchase of an email filtering solution, the choices can be overwhelming. How do you measure the real value of products and services amid the market's noise and hype?

When assessing an email security solution, the main areas to consider are:
1. Solution Costs
2. Operating and Hidden Costs
3. Productivity Losses

Calculating Savings

Companies often compare the cost of spam with the price of an email filtering solution. Factors include the loss of employee productivity due to searching through email to identify and delete spam, rising operation costs resulting from increased demands on network and storage systems, security breaches, downtime, sullied reputations, legal liability and the loss of employee confidence.
Spam cost calculators[2] provide an understanding of the savings companies could expect with spam protection in place.

These calculations, however, have proven to be misleading. Some vendors claim difficult-to-prove catch-rates, and their pricelists often omit yearly subscription, hardware and maintenance costs. Even with accurate information, the calculations are limited: pricing only accounts for a fraction of the total email security cost. Companies that opted for open-source or free-ware solutions often discovered this the hard way.

Since most vendors claim similar catch rates, companies have started analyzing the value of candidate solutions based on their operating costs such as: installation, administration and upkeep.

As such, vendors have started to distinguish their features based on how they reduce IT related expenses. For example, a vendor with an appliance based solution may mention their reduced installation costs while a Managed Security Service Provider (MSSP) will present a cloud solution thatreduces installation, maintenance and support costs.

The Total Cost of Ownership

Because spam remains an issue for employees, vendors provide the option for end-users to manage spam themselves. Productivity loss is measured as the rate by which spam gets through to users' inboxes, the false-positive rate (forcing users to search for legitimate email), quarantine administration and the impact of user delegation.

Consequently, organizations make their assessment; they must re-evaluate their cost analyses and include product efficiency and user effectiveness in addition to the price.

The Cost of Blocking Spam

1. Solution Costs

These represent the actual cost of selecting, acquiring, installing and/or subscribing to an email filtering solution, whether a product or service.

Aquisition

The acquisition cost begins with the time spent by IT Staff or external consultants to evaluate what the organization needs and to conduct product evaluations to determine the best solution. The solution type is also factored into this price, e.g. software, appliance or service. The latter option includes the time Service Providers normally charge for a per-domain set-up fee and a monthly peruser subscription fee, in addition to contract renewal, which is usually annual. It is important to note that most Service Providers will ensure high availability for an extra fee.

Appliance vendors have a more complex pricing structure which includes the yearly spam filtering subscription fee, hardware replacement and firmware upgrade services, in addition to the cost of the appliance itself. Redundant, highly available configurations will often double the price.

Software solutions vary in cost depending on the size of your organization. Smaller companies often install the software directly onto the mail server, thereby eliminating additional hardware costs. Large organizations, on the other hand, will require additional hardware to prevent overloading the mail server, and may require a redundant configuration depending on the volume of traffic.

Installation

Represents the cost associated with installing and configuring the email filtering solution. Managed or Hosted solutions require the least amount of effort to set up, requiring only changes to the DNS records to redirect incoming traffic to the scanning service provider.

Appliances require more labor as they must be integrated with the existing network, including changing the mail-flow and firewall configurations.

Software installations will require the most effort, requiring installation and configuration of the software as well as integration into the existing network.
Initial Configuration: While the rare solution works out-of-the-box, most will require some tweaking,namely integrating the user list, adapting default settings to the organization's needs, or to train a self-learning system with spam and non-spam messages to optimize catch rates and false positives.

2. IT Operation Costs

These are associated with implementing and maintaining the solution, which can be broken down into the following:

• System and software maintenance
• Threat protection updates
• Quarantine administration and management
• User settings and administration
• Monitoring and Reporting

These costs are tightly linked to specific features of the selected solutions, which we will highlight and review.

System and Software Maintenance
The maintenance costs will depend on the type of solution implemented, i.e., service, software or appliance.

Managed services present lower maintenance costs as the Service Provider takes on the responsibility of updates, upgrades and patch management. However, because the solution operates remotely, it is harder to manage and control issues such as messages being blocked at the connection level.

Software solutions, on the other hand, require maintaining the hardware, Operating System, the mail server (MTA) and the filter application itself. There are costs associated with upgrades and patches, issues with bugs and replacing defective hardware. To help reduce costs, several software vendors automate the upgrade/update processes.

Appliance solutions fall somewhere between the other two: most updates cover the full appliance: OS, MTA and application. Updates tend to occur less frequently and are less vulnerable to compatibility issues.

Threat Protection Updates
Depending on the system set-up, IT administrators may have to intervene manually if there are DHAs (Dictionary Harvest Attacks), DoS (Denial of Service Attacks), Zombies, etc.

Threat and email protection are usually part of a Managed Service, thus these costs mainly affect software-based and appliance solutions.

Higher-end products offer built-in defenses against infrastructure attacks and automatically adapt their settings to keep the impact to a minimum. Other products rely on advanced reporting and alerting capabilities to identify problems, permitting administrators to react in a timely manner. Most solutions include automated updates of their anti-virus, anti-spam and anti-phishing engines. However, self-learning solutions require training with spam and non-spam messages, which represents a non-negligible cost. Advanced solutions will use several network defense technologies in parallel, thereby minimizing the cost and effort required by administrators to keep their networks "safe."

The combination of advanced-network defense and frequent fully-automated updates are key elements in reducing the cost associated with daily threat protection updates.

Quarantine Administration and Management

Filters constantly need fine-tuning as spammers find new ways to disguise their emails and circumvent filtering solutions. Consequently, legitimate email can still be caught as spam, known as false positives, and must be retrieved when identified. For this purpose, most solutions will "collect" blocked email into quarantine.

While some solutions offer centralized quarantine management, the copious amount of spam received by most organizations makes it counterproductive for one person to administer and review false positives. Most solutions enable end users to manage their own quarantine, which is faster, more efficient, and reduces the number of calls to the Help Desk.

User Settings and Administration

Most companies will want custom settings for their users, such as whitelists or blacklists. Creating mail accounts and their respective settings can be time consuming if not automated through LDAP/AD integration or other user-populating services. To reduce administration costs, companies should favor solutions that ease this process through user delegation and configuring exceptions only.

User settings will contribute to the administration costs in the following ways:
- Account Management: configuring and maintaining the user lists
- Delegation Management: Administrators can allow advanced users to manage all or parts of their individual settings and force corporate-wide settings for less experienced users to prevent incorrect configurations
- Exception Management: consists of applying specific configuration to a subset of users or correcting user configurations. When available, good delegation management should keep these exceptions to a minimum.

Centrally managing user settings can become very costly in terms of productivity; solutions should allow users to customize their own settings while allowing administrators to distinguish between advanced and standard users when planning levels of authority delegation.

Monitoring and Reporting

Dashboards and status reviews can monitor and aid the correction of defense problems such as DoS attacks, Zombies, etc., and provide trend analysis to highlight potential problems or downtimes.
Management reports that highlight the solution's ROI are often required on a regular basis to justify the expenditure.

Reports are effective management tools when they are easy to create, generate and customize.

3. Productivity Loss

Productivity losses represent lost time while users review their quarantine, modify configuration settings or require assistance from help desk staff. They are determined by the rate at which spam gets through to users' inboxes, the false-positive rate, quarantine administration and the impact of user delegation.

Spam Delivered to Inbox

According to Ferris Research, the percentage of email messages sent daily that are spam messages is greater than 75%. The amount of spam that actually reaches users' inboxes varies from solution to solution.

False Positives

False positives directly affect user productivity due to the time required to release and potentially report messages as legitimate email. Some solutions require help desk support for users to perform these actions; some require logging into a web session, yet others allow for the message to be released directly from the quarantine. Each option presents different cost implications.

False positives also have an indirect impact. The higher their rate, the more time is required by users to review their quarantine, and on a more frequent basis.
The purchaser must therefore examine the efficiency of the solution and the ease at which false positives can be identified and released.

Quarantine Management

Productivity losses due to quarantine management include inspecting and deleting spam that is overlooked by the filters (false negatives), searching for legitimate emails that are filtered in error (false positives), and the operational costs of administration and help desk personnel.

Because this cost can be substantial, companies should take particular care to review the vendor's quarantine implementation and how users access their quarantined emails.

Quarantine Report

Quarantine Reports have the advantage of keeping users up to date with the contents. They appear regularly in users' inboxes and serve as a reminder to review blocked messages. To be effective, the reports should contain sufficient information to help users quickly decide whether blocked email is spam or legitimate. Displaying relevant details such as the sender's name and message title, and allowing the message content to be previewed, are key components to helping reduce review time and increasing decision accuracy.

Web Interface

Many solutions offer users a web interface for viewing the quarantine. Unlike the Quarantine Report, which offers immediate access, the web interface approach requires the user to a) decide when to access the quarantine, and b) to log in. Furthermore, the web view usually displays all the blocked messages, thus presenting a longer list to review.

The web view should provide the same efficiency considerations discussed in the Quarantine Report section to reduce review time. The two options should be used in conjunction, as, when used alone, the web interface shows a substantial cost impact.

Number of Reported Messages

Some solutions can reduce the amount of quarantined messages with options to delete those with medium and high probability spam content, which can greatly reduce the time users spend reviewing their quarantine.

However, Administrators should use this option carefully to avoid the consequences of deleting legitimate email. A better solution is to limit the number of messages displayed in the quarantine but keep them for later retrieval, if necessary.
your network.

User Settings

Allowing users to manage their personal settings, from modifying trusted sender lists to setting the Quarantine Report schedule or even changing the scan levels, go a long way towards reducing administrative overhead.

This cost will vary depending on the number of available per-user settings and the frequency at which these settings are changed. For example, users will modify their trusted lists more often than their Quarantine Report schedule.

Although allowing users to manage their settings could lead to configuration errors, their resulting cost savings must be weighed against the time saved by not relying on the administrator to make the changes.

Conclusion

Solution and administration costs are used most often by vendors to highlight the advantages of their product. However, they only represent a small part of the total cost.

Companies should also assess the potential for productivity losses that could be introduced by the solution and review how it performs in relation to the four main productivity loss factors:
• The rate at which spam gets through to a user's inbox
• The false positive rate
• The efficiency of the user interface
• The strength and relevance of the authority delegation

The weight of all the factors outlined will determine the final solution price: IT operation costs will be lower for organizations that opt for an email filtering service while their solution costs will be higher. Productivity costs will also vary with the accuracy of the chosen solution and the quality of its user interface. Differing spam filter features will also influence the decision process.

Vircom's modus™ suite of products offer complete security, from spam and virus protection to perimeter defense and compliance. With its team of security experts and leading technology, Vircom emerges as a leader in safeguarding email infrastructures and ensuring peace of mind.

About Vircom

Vircom is a global leader in email security, specializing in software, appliance solutions and professional services. With over 15 years of experience, Vircom has been the first to market with several solutions, including technology to block image spam and predictive email content management.

Their award winning, proprietary modus™ software technology is built to provide peace of mind to the organizations that present the highest risk, both to their operations and their shareholders.

Vircom's products include modusMail™, modusGate™ software, modusGate™ Appliance and are made available to several major security providers and deployed through third-party vendors to more than 6.6 million inboxes worldwide. For more information, visit www.vircom.com.