



The Radicati Group, Inc.

595 Lytton Avenue

Palo Alto, CA 94301

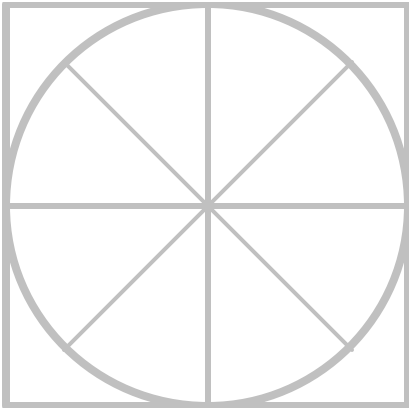
Phone 650-322-8059

Fax 650-322-8061

<http://www.radicati.com>

The Radicati Group, Inc.

Cloudmark: Spam Reduction Effectiveness Analysis



A White Paper

www.radicati.com

TABLE OF CONTENTS

1.0 Scope 4

2.0 Methodology..... 4

3.0 Executive Summary..... 5

4.0 Company Overview..... 6

 Cloudmark..... 6

5.0 Survey Sample 8

6.0 Radicati Group Models used in this Study..... 8

 6.1 Total Cost of Ownership Model..... 8

 6.2 Email Productivity Savings Model 9

 6.3 Spam Reduction Effectiveness Model..... 10

 6.4 General Assumptions..... 10

7.0 Total Cost of Ownership (TCO) Analysis 11

 7.1 Anti – Spam Environment 11

 7.2 Anti-Spam Filter Total Cost of Ownership 12

 7.2.1 Acquisition Costs 12

 7.2.2 Maintenance Costs..... 12

 7.2.3 Installation & Deployment Costs 12

 7.2.4 Operational Staff Costs..... 13

 7.2.5 Anti Spam Filter Total Cost of Ownership..... 13

8.0 Productivity Savings Analysis..... 14

 8.1 Email Productivity Savings..... 14

 8.2. User and Administrator Productivity Losses due to False Positives..... 14

 8.3 Total Productivity Savings after Deploying an Anti-Spam Filter 15

9.0 Spam Reduction Effectiveness (SRE) Analysis 16

 9.1 Inbox Spam Reduction Rate 16

 9.1.1 Rate of Spam before & after Deployment of Anti-Spam Solution16

 9.2 Rate of False Positives..... 17

 9.3 Spam Reduction Effectiveness 17

11.0 Appendix A: Spam Reduction Effectiveness Analysis Survey..... 19

Cloudmark: Spam Reduction Effectiveness Analysis

1.0 Scope

This Cloudmark: Spam Reduction Effectiveness (SRE) Analysis was conducted by The Radicati Group, Inc. in Q1 2004. The study shows the Total Cost of Ownership (TCO), Email Productivity Savings, and the Spam Reduction Effectiveness of Cloudmark's Cloudmark Authority. It provides extensive information on acquisition costs, maintenance costs, operational costs, spam filter effectiveness, rate of false positives and much more.

The Radicati Group conducted this study to report on a real-world scenario where an anti-spam solution is actually deployed and running overtime at an Enterprise gateway. Looking beyond non-standard editorial reviews and vendor claims, it was our intent to demonstrate customer(s) real-world experiences with Cloudmark Authority to more accurately depict the true value including TCO and effectiveness of a solution.

2.0 Methodology

The data and analysis in this report is based on primary research conducted by analysts of The Radicati Group, Inc. in the form of a specially designed questionnaire administered by phone or email. Respondents interviewed were largely senior managers, high-level administrators, telecommunications managers, and IT managers knowledgeable about the implementation of anti-spam filters within each of the organizations surveyed. A description of the survey population is provided in the Survey Profile section of this study. The full questionnaire used is included in Appendix A of this study.

All financial information presented in this study is in US\$.

3.0 Executive Summary

- It is clear from the results of this Spam Reduction Effectiveness (SRE) study that the deployment of an anti-spam filter provides organizations with a far more productive and cost-effective messaging environment.
- This study looks at the deployment of the following gateway anti-spam solution:
 - Cloudmark Authority.
- As part of the study, we surveyed 3 organizations that were provided as customer references by Cloudmark.
- Cloudmark has a low TCO of \$14.69 per user/year, and productivity savings at \$2.21 per user per day.
- To gauge the real-world effectiveness of anti-spam filters actually deployed in an enterprise, we surveyed organizations to determine the percentage change in incoming spam messages in their inboxes prior to and after the deployment of an anti-spam solution. It is worth noting that the companies surveyed are a sample size of Cloudmark’s customer-base. The average targeted Cloudmark customer is 10,000 desktops. Authority scales to service large enterprise businesses as well as deliver ISP and Carrier-grade solutions. As the number of seats increases, lower TCO is realized given lower pricing and the notable takeaway from this study that no new hardware is required to deploy Authority in an organization of any size.
- The percentage of spam in customer inboxes before and after the deployment of an anti-spam filter per user per day is as follows:

Inbox Spam Reduction Rate	Cloudmark
% of Spam Messages Before Filter Deployed	41.7%
% of Spam Messages After Filter Deployed	2.5%
Inbox Spam Reduction Rate	94%

- The Spam Reduction Effectiveness (SRE) of an anti-spam solution is the ratio of the rate of false positives to productive e-mails received. This rate shows the relative effectiveness of the individual spam filter in reducing the rate of spam while maintaining a low false positive rate.
- The SRE is calculated by dividing the False Positives Rate by the Spam Filter Effectiveness multiplied by 1,000, as follows:

$$\text{Spam Reduction Effectiveness (SRE)} = \frac{\text{False Positive Rate}}{\text{Spam Filter Effectiveness}} \times 1,000$$

- The SRE for Cloudmark is as follows:

Spam Reduction Effectiveness (SRE)	Cloudmark
% Spam Filter Effectiveness	94 %
% False Positives	0.20%
SRE (per 1000)*	2.13

- In the short time since this study was conducted, Cloudmark has released a newer version of its Authority software as well as delivered updates to its spamDNA™ cartridges which further improve its overall SRE with lower false positives and even higher accuracy.

4.0 Company Overview

Cloudmark

128 King Street

Second Floor

San Francisco, CA 94107

<http://www.cloudmark.com>

Cloudmark, Inc. takes a different approach to spam control both at the desktop with Cloudmark SpamNet for individuals and small-medium businesses, and with its gateway solution, Cloudmark Authority for large enterprises. Authority takes a non-traditional approach to email filtering that looks beyond text and basic message characteristics, to instead analyze the structure and techniques behind spam (what spammers can't easily change). This approach has garnered them enterprise customers such as American Century Investments, the Government Services Agency (GSA) and Documentum, along with strategic partners such as Sendmail, Openwave and Secure Computing.

On the desktop, processing more than 200 million messages every day, SpamNet has more than 900,000 users. First introduced in 1998, it's the first and largest real-time SpamFighting community in the world with the most up-to-date database of spam messages in a number of languages which are then used in Cloudmark's labs to automatically train the company's corporate solution to predict spam.

PRODUCT OVERVIEW

Introduced in November 2002, **Cloudmark Authority** is a gateway-based software solution that uses its first-ever automated spamDNA technology to evaluate messages by looking at patterns and mutations in the message structure called spamGenes. These 300 spamGenes, generated from input from SpamNet users and collectively called spamDNA, focus on the structure of spam messages (the techniques that spammers use to get around traditional filters) rather than words or characteristics in the messages.

Installed on the Gateway Message Transfer Agent (MTA), it has a very low impact on its performance, which ranges between 5% and 10%.

While Authority uses the input of SpamNet users in the labs at Cloudmark to automatically evolve and improve spamGenes via its genetic classifier, all corporate messages are filtered on corporate premises, and the solution doesn't require a connection to the Internet. Eliminating the need for hundreds of thousands of filtering rules requiring multiple daily updates, Authority customers only receive updates every 30 to 60 days, which are delivered in the form of spamDNA cartridges.

SpamNet is a service for individual users that encompasses more than 900,000 members. Offered as a free download, it works as an add-on to Outlook 2000/XP, Outlook Express and Lotus Notes installing Block and Unblock buttons on the toolbar.

Instead of using special filters and lexical analysis, SpamNet relies on users to identify spam messages. After a user receives a spam message, he or she hits the Block button that moves the message to the Spam folder, as well as automatically reports it to the Cloudmark servers in real-time, which tags similar messages for the rest of the community instantly.

Messages are never deleted or blocked, but rather automatically moved to the Spam folder where users can review them. In case a message has been mislabeled, a user can always use the Unblock button, to report it to the Cloudmark servers as a valid e-mail.

To reduce the rate of mistakes, Cloudmark implemented a rating system (a Truth Evaluation System) that ranks all participants based on the number of valid spam messages they have reported, as well as their validity. The higher a participant's score is, the more weight is given to his or her Block/Unblock submissions. All automatic submissions are treated anonymously in the form of a unique fingerprint, preventing members from knowing the type of spam reported by other users.

Cloudmark says that its SpamNet strategy captures over 97% of all spam messages. SpamNet is compatible with Windows 98/NT/2000/XP.

FINANCIALS

- 2003 Revenues: N/A
- 2003 Net Income: N/A
- Fiscal Year-End: N/A
- Ownership: Private

PRICING

- Authority is offered at \$8-\$15 per mailbox per year. It has a 30-day free trial period.
- SpamNet is currently offered for a free 30-day trial to individual users. The cost is \$3.99 a month or \$39.95 a year. Cloudmark also offers a free fraud prevention service for all users.

5.0 Survey Sample

- The survey sample consisted of 3 Global 1000 organizations which were provided as customer references by Cloudmark.

6.0 Radicati Group Models used in this Study

6.1 Total Cost of Ownership Model

The Radicati Group's Total Cost of Ownership Model (TCO) has been built to assist organizations in assessing the cost of their anti-spam solutions.

The TCO model looks at the following key cost components:

- **Acquisition Costs** - Acquisition costs refer to the costs of purchasing all hardware and software components that make up the Anti-spam Environment.
- **Maintenance Costs** - These comprise the cost of yearly support contracts for all hardware and software components. This also includes annual upgrade fees.
- **Installation and Deployment Costs** - This includes the amount of time that is required to install and deploy the anti-spam filter.
- **Operational Staff Costs** - These include salaries for full and part time administrators responsible for managing anti-spam filters.

The Total Cost of Ownership Model assumes a three-year, straight-line depreciation for acquisition, maintenance, installation and deployment costs and operational staff costs. Acquisition costs are included as a one-time initial payment in year 1 with no additional costs occurring in years 2 and 3. Maintenance costs are incurred in years 2 and 3 only. Installation and Deployment costs are only incurred in year 1 and not in years 2 and 3. Operational Staff costs are incurred in years 1, 2 and 3. The TCO is calculated as the sum total of each year's costs averaged over a 3-year period.

The TCO was averaged over a 3 year period as follows:

Total Cost of Ownership	Year 1	Year 2	Year 3
Total Acquisition Costs/User	X	n/a	n/a
Total Maintenance Costs/User	n/a	X	X
Total Installation & Deployment Costs/User	X	n/a	n/a
Total Operational Staff Costs/User	X	X	X
Total Costs/User	Year 1 TCO / User	Year 2 TCO/ User	Year 3 TCO /User
Total Cost of Ownership (TCO) / user/ year	(Year 1 TCO/User + Year 2 TCO/User + Year 3 TCO/User) / 3		

6.2 Email Productivity Savings Model

The Radicati Group's Email Productivity Savings Model has been built to assist organizations in assessing the productivity costs incurred before and after the deployment of an anti-spam filter.

- ***Email Productivity Costs before Deployment of Filter*** – This is the total time spent per user to delete spam messages before an anti-spam filter was deployed.
- ***Email Productivity Cost after Deployment of Filter*** - This is the total time spent by users and administrators to delete spam and deal with false positives after a filter was deployed. This includes three items:
 - ***Spam Productivity Costs after the Deployment of Filter*** - This is any lost productivity due to spam messages after anti-spam filters were deployed.
 - ***User Productivity Loss due to False Positives*** - This is the productivity time that is spent by users to recover messages that were erroneously labeled as spam.
 - ***Administrator Productivity Loss due to False Positives*** – This is the productivity time that is spent by administrators to recover messages that were erroneously labeled as spam.

- ***Email Productivity Savings after Deployment of Filter*** – This is the difference between email productivity costs before and after the deployment of an anti-spam filter.

6.3 Spam Reduction Effectiveness Model

The Radicati Group's Spam Reduction Effectiveness (SRE) Model has been built to assist organizations in assessing the effectiveness of their anti-spam solutions, reduce costs and make better decisions on how to reduce spam.

The SRE model is used to correlate the spam filter effectiveness with the reduction in the percentage of spam, and the rate of false positives.

The SRE model looks at the following components:

- ***Rate of Spam Messages before and after Deployment of Filter per user per month*** – This includes the percentage of spam messages received in customer inboxes before and after anti-spam filters were deployed.
- ***Rate of False Positives per user per month***

The SRE model calculates the SRE as the ratio of the percentage of false positives to the percentage of spam filter effectiveness.

6.4 General Assumptions

All financial information shown in this study is in US\$, unless explicitly noted.

The SRE model used in this study makes the following assumptions regarding salaries:

- \$60/hour for Full-Time Messaging Administrators fully loaded (i.e. includes overhead, benefits, taxes etc.), or \$124,800/year.
- \$60/hour for Part-Time Messaging Administrators fully loaded (i.e. includes overhead, benefits, taxes etc.), or \$124,800/year.
Note: Often, the salary of a Part-Time Messaging Administrator is lower than that of a Full-Time Messaging Administrator, but for simplicity's sake, our model assumes that they have the same salary.
- \$35/hour for Messaging users fully loaded (i.e. includes overhead, benefits, taxes etc.), or \$72,800/per year.

7.0 Total Cost of Ownership (TCO) Analysis

7.1 Anti – Spam Environment

Anti-Spam environments analyzed in this study utilize Cloudmark Authority. An average of 1,250 users was deployed on Cloudmark Authority, and the solution was deployed at the gateway server.

Anti-Spam Filters deployed	Cloudmark
Average Number of E-mail Users	1,250
At what level is the product/service deployed at?	Gateway

Table 1: Anti – Spam Filters Deployed

In terms of managing anti-spam filters, organizations deploying Cloudmark are relying predominately on messaging administrators rather than users.

The following table shows the messaging IT staffing level of companies deploying Cloudmark.

Messaging Staff	Cloudmark
Who Manages Anti-Spam Filters?	Administrators
Average # of E-Mail Users	1,250
Total Full - Time Messaging IT Administrators	2
Total # of Spam Administrators	1.7
Total % of time spent managing filters per week	5.7%
Total IT Admin Responsible for Managing Anti-spam filters	0.10

Table 2: Staffing Chart

Organizations surveyed considered an average of 1.7 anti-spam vendors and/or service providers before selecting Cloudmark.

Additional Information on Cloudmark	
How many Vendors/service providers did you consider?	1.7
Do you educate users about how to deal with Spam other than anti-spam filters?	Yes

Table 3: Additional Information on Cloudmark

All organizations surveyed indicated that they educate users on how to deal with spam, beyond just using an anti-spam filter.

7.2 Anti-Spam Filter Total Cost of Ownership

7.2.1 Acquisition Costs

The acquisition costs in this study look at the total purchase price of software licenses and hardware. All of these represent a one-time down payment.

Table 4 shows the acquisition costs of Cloudmark.

Acquisition Costs per User/Yr	Cloudmark
Average # of E-mail Users	1,250
Licensing Fees	\$10.00
Total Acquisition costs per User/Yr	\$10.00

Table 4: Acquisition Costs

7.2.2 Maintenance Costs

Organizations can expect to pay one or more of the following fees: annual licensing, subscription and maintenance fees. The majority of respondents indicated that annual upgrade fees were included in annual licensing fees.

Maintenance costs for Cloudmark per user per year are as follows:

Maintenance Costs per User/Yr	Cloudmark
Average # of E-mail Users	1,250
Annual Licensing Recurrent Fees	\$10.00
Annual Subscription Fees	\$0.00
Annual Maintenance Fees	\$0.00
Total Maintenance Costs per User/Yr	\$10.00

Table 6: Maintenance Costs

7.2.3 Installation & Deployment Costs

Installation and deployment fees represent the amount of time that is required to install and deploy anti-spam filters. Installation and Deployment of Cloudmark anti-spam filters cost an average of \$0.61 per user per organization.

Installation & Deployment Costs (per User/Yr – 1 time)	Cloudmark
Installation Fees	\$0.00
Costs to deploy and configure	\$0.38
Costs to train administrators	\$0.23
Costs to train users	\$0.00
Total Installation & Deployment Costs per User/Yr	\$0.61

Table 7: Installation & Deployment Costs

7.2.4 Operational Staff Costs

Operational staff costs include the time that administrators spend managing anti-spam filters per week.

Organizations with higher e-mail traffic will require more anti-spam administrators to manage higher volumes of e-mail messages.

Operational staff costs for Cloudmark per user per year are as follows:

Operational Staff Costs per User/Yr	Cloudmark
Average # of E-mail Users	1,250
Total Average Time spent managing anti-spam filters/week (hours)	1.8 hours
Salary per hour	\$60
Number of weeks per year	52
Total Operational staff costs per User/Yr	\$4.49

Table 8: Operational Staff Costs

7.2.5 Anti Spam Filter Total Cost of Ownership

The Anti-Spam Filter TCO for Cloudmark Authority for Years 1, 2 and 3 are as follows:

Anti-Spam Filter Costs	Cloudmark
YEAR ONE	
Acquisition Costs per user	\$10.00
Maintenance Costs per user	n/a
Installation and Deployment Costs per user	\$0.61
Operational Staff Costs per user	\$4.49
Anti-Spam Filter TCO per user for Year 1	\$15.10
YEAR TWO	
Acquisition Costs per user	n/a
Maintenance Costs per user	\$10.00
Installation and Deployment Costs per user	n/a
Operational Staff Costs per user	\$4.49
Anti-Spam Filter TCO per user for Year 2	\$14.49
YEAR THREE	
Acquisition Costs per user	n/a
Maintenance Costs per user	\$10.00
Installation and Deployment Costs per user	n/a
Operational Staff Costs per user	\$4.49
Anti-Spam Filter TCO per user for Year 3	\$14.49
Average Anti-Spam Filter TCO over a 3-Year Period per User/Yr	\$14.69

Table 9: Anti-Spam Filter TCO per User per Year

Cloudmark has an Anti-Spam Filter TCO over a 3-year period of \$14.69 per user/year.

8.0 Productivity Savings Analysis

8.1 Email Productivity Savings

To determine the email productivity savings per user per day as a result of anti-spam filters, we looked at the percentage of productive (legitimate) emails per user/day in organizations both before and after the deployment of the anti-spam filter.

Email Productivity Savings were calculated as follows:

$$\frac{(\text{Productivity Change} \times \text{Increase in \# of Productive Emails} \times 30 \text{ Seconds}) \times \$35}{60 \text{ Seconds}/60 \text{ Minutes}}$$

The email productivity savings for Cloudmark are as \$2.80, as follows:

Cloudmark Email Productivity Savings	
% of Productive Emails per user per day before deploying Anti-Spam Filter	58%
% of Productive Emails per user per day after deploying Anti-Spam Filter	95%
Email Productivity Savings per user per day (\$)	\$2.80

Table 10: Email Productivity Savings

8.2. User and Administrator Productivity Losses due to False Positives

Productivity loss due to false positives is based on the amount of productivity time spent by users and administrators recovering legitimate messages that have been erroneously labeled as spam.

The cost of false positives to users was derived using the following formula:

Users:

$$\text{Minutes Spent Recovering False Positives/User/Day} \times \$0.581 = \$\underline{\hspace{2cm}}$$

¹ Assuming \$35/Hour Rate = \$0.58/minute

The cost of false positives to administrators was derived using the following formula:

Administrators:

$$\begin{array}{l} \text{Minutes Spent Recovering} \\ \text{False Positives/Admin/Day} \end{array} \times \$1.002 = \$\underline{\hspace{2cm}}$$

To determine the total cost of productivity losses due to false positives, we combine the productivity costs per user due to recovering false positives with the cost per administrator due to false positives. Cloudmark products allow both administrators and users to determine their false positive messages. In the case of the companies surveyed, only administrators were allowed to recover false positives, not users. The total cost per user per day is as follows:

Cloudmark Total Cost per User per Day	
Cost/User/Day Due to User Productivity Loss	\$0.58
Cost/User/Day Due to Administrator Productivity Loss	\$0.01
Total Cost per User per Day	\$0.59

Table 11: Total Productivity Loss due to False Positives

Cloudmark had a cost per user per day of \$0.59 per user per day

8.3 Total Productivity Savings after Deploying an Anti-Spam Filter

To determine the total productivity savings per user per day after deploying an anti-spam filter we looked at the difference between the email productivity savings due to the reduction in spam messages per user per day and the productivity losses due to false positives per user per day. Total productivity savings per user per day are as follows:

Cloudmark Total Productivity Savings per User per Day	
Email productivity savings due to Reduction in Spam per User per Day	\$2.80
Productivity Loss Due to False Positives	\$0.59
Total Productivity Savings per User per Day	\$2.21

Table 12: Total Productivity Savings per User per Day

Cloudmark has productivity savings per user per day of \$2.21.

² Assuming \$60/Hour Rate = \$1.00/minute

9.0 Spam Reduction Effectiveness (SRE) Analysis

9.1 Inbox Spam Reduction Rate

9.1.1 Rate of Spam before and after Deployment of Anti-Spam Solution

To gauge the inbox spam reduction rate, we surveyed organizations to determine the percentage change in incoming spam messages in their inboxes prior to and after the deployment of an anti-spam solution.

The percentage of spam in customer inboxes before and after the deployment of an anti-spam filter per user per day are as follows:

Spam Filter Effectiveness	Cloudmark
% of Spam Messages in Customer Inboxes Before Filter Deployed	41.7%
% of Spam Messages in Customer Inboxes After Filter Deployed	2.5%
Spam Filter Effectiveness	94%

Table 13: Spam Filter Effectiveness

The following figure illustrates the percentage of spam messages in Cloudmark’s customer inboxes before and after the deployment of an anti-spam filter.

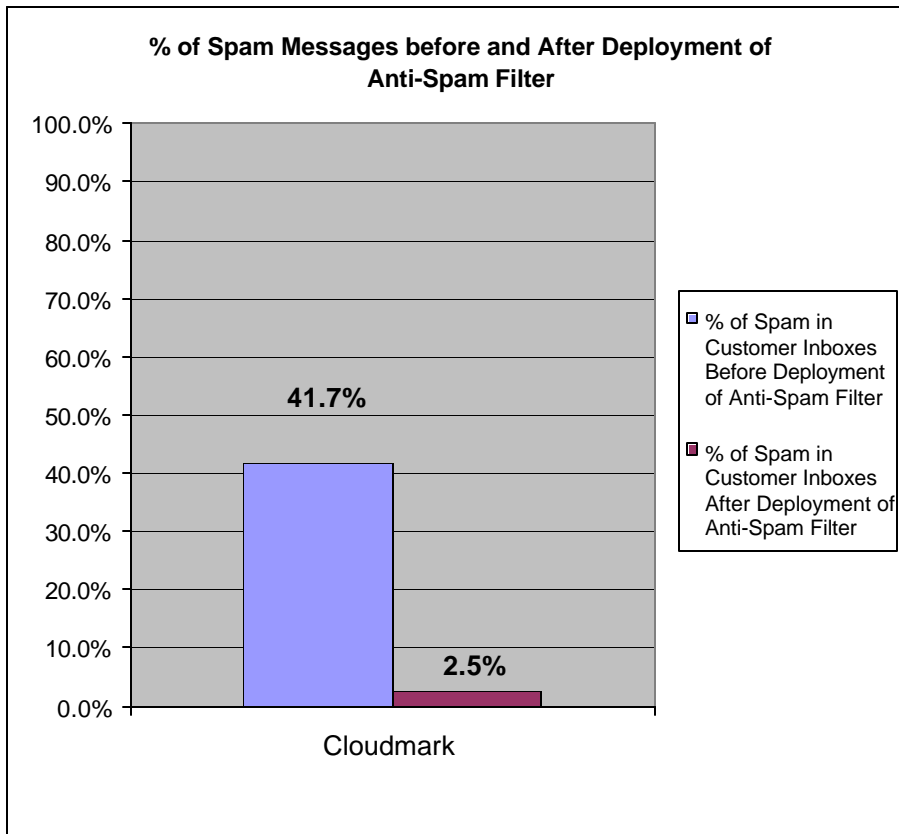


Figure 1: % of Spam Messages in Customer Inboxes before and after Deployment of Anti-Spam Filter

Cloudmark has a percentage change in spam messages received, or inbox spam reduction rate, of 94%.

9.2 Rate of False Positives

False positives are messages that are erroneously labeled as spam and are either deleted or quarantined, instead of being delivered to user's mailboxes. These messages may have some of the same characteristics as spam, such as common phrases used by spammers or HTML tags that make the spam filter believe that they are spam.

The majority of respondents indicated that they customize their anti-spam filters to control the rates of false positives, based on the specific needs of their organization. Anti-spam filters enable users and administrators to either increase or decrease spam scores (the system uses this score to label messages as spam) to control the rate of incoming spam messages, thus also affecting the rate of false positives.

False positive rates per user per month for each product are as follows:

* Please note that we assumed 1 month = 30 days.

Rate of False Positives	Cloudmark
Total False Positives Received per month per user	1.55
Total # of E-mails Received per Day per user	25.67
Total # of E-mails Received per Month	770.1
Rate of False Positives per Month	0.20%

Table 14: Rate of False Positives

The rate of false positives varied greatly among the organizations surveyed. Cloudmark had a rate of false positives of 0.20% false positives per user per month.

9.3 Spam Reduction Effectiveness

The Spam Reduction Effectiveness (SRE) of an anti-spam solution is the ratio of the rate of false positives to productive e-mails received. This rate shows the relative effectiveness of the individual spam filter in reducing the rate of spam while maintaining a low false positive rate.

The SRE is calculated by dividing the False Positives Rate by the Spam Filter Effectiveness multiplied by 1,000, as follows:

$$\text{Spam Reduction Effectiveness (SRE)} = \frac{\text{False Positive Rate}}{\text{Spam Filter Effectiveness}} \times 1,000$$

The SRE for Cloudmark is as follows:

Spam Reduction Effectiveness (SRE)	Cloudmark
% Spam Filter Effectiveness	94 %
% False Positives	0.20%
SRE (per 1000)*	2.13

Table 15: Total Savings with an Anti-Spam Filter

A low SRE indicates an effective anti-spam solution that is able to maintain a low false positive rate. Cloudmark is highly effective with a low SRE of 2.13 (i.e. for every 1000 messages there are only 0 false positives).

10.0 Conclusions

With the volume of junk messages escalating every day, spam is quickly turning from simply an annoyance issue for users, to a major productivity loss problem for corporations. Even though education of users is one of the important steps in fighting spam, it is clearly not enough to stop the deluge of messages from entering an organization. All of our survey participants have educated their users on how to avoid being spammed, which unfortunately, didn't result in any significant relief for their users.

The only reliable solution to curb the volume of spam, and trim down productivity losses for any type of company is to deploy a commercial anti-spam filter.

One of the arguments that are often voiced by users that haven't yet deployed a solution is the fear of false positives. Unless a company deploys a filter that instead of quarantining spam deletes all junk messages immediately, we've discovered that most solutions allow users (and/or administrators) to successfully recover such legitimate messages, erroneously labeled as spam, in a matter of minutes.

Cloudmark offers a viable and cost-effective anti-spam solution, with Cloudmark Authority's Total Cost of Ownership (TCO) being only \$14.69 per user per year, and providing productivity savings of \$2.21 per user per day.

The calculation of the Spam Reduction Effectiveness (SRE) ratio is based on the rate of false positives to productive e-mails received. This rate shows the relative effectiveness of the individual spam filter in reducing the rate of spam while maintaining a low false positive rate. This study shows that Cloudmark is highly effective at blocking spam while maintaining a low false positive rate, with an SRE of 2.13 (for every 1000 messages there are only 0.01 false positives).

11.0 Appendix A: Spam Reduction Effectiveness Analysis Survey

Spam Reduction Effectiveness Analysis Survey September 8th, 2003

Customer Profile:

Company Name _____
Respondent's Name and Title _____
Address _____
City _____ **State** _____ **ZIP** _____
Phone Number _____
Email _____
Number of Employees _____
Industry _____

Please note that even though we collect your personal information, it will be used only for our internal purposes, and only in relation to this study. Your name, title, your company's name or any other identifiable information about your company will not be revealed.

We will, however, publish the types of industries our survey participants represented to give our readers a better understanding of their background.

A. GENERAL

1). How many e-mail users do you have in your organization? _____

2). Do all of your e-mail users have anti-spam protection? _____ YES _____ NO

If you answered NO to this question, please specify the number of users who have the anti-spam filter _____

3). What anti-spam product or service do you use?
_____ (Product/Service Name)

4). Is it a product or a service? _____

If you answered PRODUCT to this question, please specify if it is deployed at the following level (check all that apply):

_____ Gateway
_____ E-Mail Server
_____ Desktop
_____ Other _____

5). Does your company use more than one anti-spam solution _____?

If YES, please name additional products/services used:

For the following questions in this section, please refer only to the main anti-spam filter you're using:

6). Who in your company is allowed to manage your anti-spam filter?

- Administrators
- Users
- Both

If you answered USERS or BOTH to this question, please specify the type of activities your users are allowed to perform (check all that apply):

- Adjust sensitivity of their personal filters
- Manage their quarantined messages
- Create White/Black lists
- Other _____

7). Does your solution allow you to perform other functions?

YES NO.

If YES, please specify:

- Content Filtering
- Anti-Virus
- Other (Please, specify) _____
- My filter came with (please circle all that apply) *content filtering*, *anti-virus*, *other feature* _____, but I don't use it

8). How many vendors/service providers did you look at before selecting your anti-spam solution? _____

9). Do you educate your users about how to deal with spam in other ways, besides using anti-spam filters? YES NO

10.) When did you deploy your anti-spam solution? _____

B. TOTAL COST OF OWNERHSIP

1). What were the initial costs associated with purchasing your anti-spam filter? Please, specify all that applies:

- \$ _____ Licensing fees (one-time payment)
- \$ _____ Hardware costs
- \$ _____ Appliance cost
- \$ _____ Installation fees
- \$ _____ Consulting fees
- \$ _____ Other (please specify) _____

2). What are the annual fees associating with maintenance and upkeep of your anti-spam filter?

- \$ _____ Annual licensing recurrent fees
- \$ _____ Annual subscription fees
- \$ _____ Annual maintenance fees
- \$ _____ Annual upgrade fees

3). What was your initial time investment to deploy the anti-spam filter?

_____ hours to deploy and configure
_____ hours to train administrators
_____ hours to train users (if any)
_____ hours other (please, specify)_____

4). What is the total number of full-time messaging administrators in your company? _____

a). How many of them are responsible for managing anti-spam filters? _____

b). What % of their time is spent on managing anti-spam filters (per week)? _____

5). Where are your messages quarantined?

_____ Gateway
_____ Mail Server
_____ Desktops
_____ Offsite
_____ Other _____

The following sections (C, D and E) will ask you to provide information on the effectiveness of your spam filters, as well as various metrics related to the e-mail volumes processed by your company.

For the purposes of this study we define SPAM as any message unwelcome by either the end user or the company that provides him or her with a corporate e-mail account. We appreciate your using the same definition while answering the following questions.

C). SPAM FILTER EFFECTIVENESS

1). Before you deployed your filter, approximately, how many messages (both legitimate and spam) was each corporate user receiving per DAY? _____

What % of these messages was spam? _____

2). After deploying your solution, on average, how many e-mail messages (both legitimate and spam) does each corporate user receive per DAY? _____

What % of these messages is spam? _____

3). On average, how many spam messages does your spam filter miss (i.e. delivers them to your users' mailboxes as legitimate mail) per WEEK per User? _____

4). What do you do with messages labeled as spam?

_____ Delete immediately
_____ Quarantine
_____ Tag and Deliver
_____ Other (please, explain) _____

5). Since you deployed your solution, and after the initial pilot program, has the effectiveness of your anti-spam filter changed?

- _____ It stayed the same
- _____ It increased
- _____ It decreased
- _____ I don't know

6). Can you customize the effectiveness of your filter for your corporate needs (i.e. to decrease the rate of false positives you can lower the spam score that the systems uses to label your messages as spam, or to increase the catch rate of spam you can increase the score?)

- _____ Yes, and we're doing it
- _____ Yes, but we're satisfied with the default settings, and are not using the customization features
- _____ No
- _____ No, but we'd like to have this option

7). How satisfied are you with you spam filter's effectiveness to stop spam messages from reaching users?

- _____ Very satisfied
- _____ Somewhat satisfied
- _____ Not satisfied at all

D). RATE OF FALSE POSITIVES

1). On average, how many false positives (*legitimate messages erroneously labeled as spam*) does each of your users receive per MONTH? _____

2). How do you know the rate of your false positives?

- _____ Conduct periodic tests
- _____ Ask users
- _____ Ask administrators
- _____ Other _____

3). How satisfied are you with you spam filter's capability to differentiate between spam and legitimate messages?

- _____ Very satisfied
- _____ Somewhat satisfied
- _____ Not satisfied at all

E). PRODUCTIVITY (TIME) LOST DUE TO FALSE POSITIVES

1) Approximately, how much time does a single user spend each WEEK recovering legitimate messages erroneously labeled as spam? (i.e. going through his/her quarantined email, etc.)_____

_____Not applicable.

2). Approximately, how much time do administrators spend each WEEK recovering legitimate messages erroneously labeled as spam?_____

_____Not applicable.

4). Approximately, how much time does a single user spend each WEEK dealing with spam messages (reading, deleting, etc.) that were erroneously delivered to his/her inbox (i.e. the messages that the filter missed)?_____

5). Do your users go through their spam folders on a regular basis to make sure that none of their legitimate messages were erroneously filed there?

- _____ Yes
- _____ No
- _____ Not applicable.

If you answered YES to the this question, how much time per WEEK does each user spend going through his/her spam folder?_____

How do your users access their quarantined messages:

- _____ Quarantined messages are delivered to users via email
- _____ Users are able to access them directly on the server
- _____ Other_____

6). When a legitimate message gets blocked, what steps do you have to undertake to retrieve it?

F). OVERALL

1). How pleased are you with your company's anti-spam approach?

- _____ Very pleased, it works great!
- _____ Somewhat pleased (please, explain)_____
- _____ Not happy at all (please, explain)_____

2). Are there any other features you wish your anti-spam filter had?

ADDITIONAL COMMENTS:_____