



CLEARSWIFT™

Managing and securing
electronic communications

Effective Spam Management

January 2003

© January 2003 Clearswift Ltd.
All rights reserved
All trademarks acknowledged

Table of Contents

EXECUTIVE SUMMARY 1

INTRODUCTION 3

ELEMENT 1: POLICY 7

ELEMENT 2: PRODUCT 8

ELEMENT 3: PROACTIVE SERVICES 12

ABOUT CLEARSWIFT 14

Executive Summary

- Spam is growing at an alarming rate within organizations, with estimates suggesting that spam could encompass between 10% and 20% of all business email traffic within the next 5 years. Moreover, unlike viruses, which are universally unacceptable, one person's spam could be another's business email. In addition, we see the nature of spam varies significantly by geography and industry sector. This subtlety and global disparity creates an added complexity when it comes to managing spam effectively
- Spam is changing to outwit simplistic attempts to control it. We are battling intelligent and crafty marketers whose primary mission is to ensure that their marketing message gets delivered; a solution that is not configurable and extensible will soon be circumvented.
- Against such an intelligent, pervasive and growing threat, a single line of defense is effectively useless. Although spam may appear trivial, it requires a robust and well-conceived solution to deal with it effectively. Simple products may offer short-term relief but will become useless as spammers bypass them.
- Clearswift believes defense-in-depth is the only effective way to combat and manage spam, and therefore developed its solution based on the 3 Elements of Effective Spam Management.

Element 1: POLICY

Clearswift can help you develop, deploy and manage effective policies to help your staff minimize the spam they bring into the organization

Element 2: PRODUCT

BEST CONFIGURATION PRACTICES: Clearswift will help you configure your Clearswift perimeter defenses using field proven best practices

REAL TIME BLOCKING LISTS: There are more than 150 real-time blocking lists available on the market. Many are free, some require an annual subscription. We'll help you pick the best list for your organization

LOCAL BLOCKING LISTS: Clearswift products allow for the customization of a local block-list to include spam sources that are a particular nuisance to your organization

TEXTUAL ANALYSIS SPECIFIC SPAM - Much like an anti-virus signature, repetitive specific-spam is identified by specific titles and phrases and blocked using Clearswift products and services

TEXTUAL ANALYSIS- GENERIC SPAM -The generic-spam textual analysis looks for the characteristics and generic traits of spam messages to block spam

Element 3: PROACTIVE SERVICES

Clearswift's Threatlab™ Active will make sure your defenses remain current with daily updates that address the ever moving spam threat, as well as minimize your ongoing management burden by keeping you abreast of issues in the outside world that can effect your policies. Clearswift will then provide you with the tools and services to make the maintenance of policy simple.

- The Clearswift solution uses an integrated approach designed to detect spam based upon:
 - Where it comes from, and/or
 - What it contains

Depending on your individual spam problem, and the actions you want to take once an email is identified as spam, you may wish to choose selectively from our solution options.

The following document describes each of our approaches in detail. In consultation with our staff, you'll determine which parts of our spam solution are required for your situation.

- Clearswift distinguishes its solution from the competition based on the depth, flexibility and accuracy of its offering

Depth

Complex problems require robust, multi-variant solutions. Clearswift has more than 20 years experience helping its 12,500 plus customers solve complex issues surrounding messaging policy, management and security. Spam is just the latest in a series of threats that Clearswift manages for its clients. Rest assured, when you choose Clearswift, the solution you choose for spam will also form the basis of response to tomorrow's emerging threats.

Flexibility

Unlike anti-virus type solutions, one size does not fit all. Clearswift provides the ability for customers to select and implement the tools from the solutions that match their specific problem.

Accuracy

More customers have bought Clearswift for spam management than any other solution on the market. IDC notes Clearswift is the market share leader for email content filtering.

CONCLUSION: Spam is here to stay and a defense-in-depth solution based upon fine grained content analysis offers the only viable, proactive long term protection against the emerging methods of dedicated spammers.

Clearswift continues to focus considerable R&D effort on staying one step ahead of the spammers including the development of next generation software that is capable of learning your organizations specific definition of spam and auto-updating itself. For more information contact your Clearswift reseller or sales representative.

“about 2.1 million spam messages are received and circulated every year in a typical 1000 employee organization.”

IDC 2001

“According to an official European Commission study, junk mail inflicts an annual cost of 10 billion euros (US\$8.7 billion) on Internet users.”

e-Business Advisor- Reduce the Effects of Unwanted Email, 07/01/02

Introduction

Unwanted and unsolicited email (spam) is a serious issue that directly impacts the productivity of the organization as a whole. The solution to the spam problem is not one easily solved. Senders of spam routinely investigate new and innovative ways to avoid having their emails blocked. Blocking spam by using technology can be difficult because what is spam to one organization is a legitimate message to another. The best solution is one that presents a flexible approach that combines multiple techniques, giving the organization a series of options that allow them to customize a solution to best meet their needs. This paper outlines the scope of the problem presented by spam email and describes the techniques provided within the range of Clearswift services and product to reduce this problem.

What is spam?

A commonly accepted definition of Internet spam is “one or more unsolicited messages, sent or posted as part of a larger collection of messages, all having substantially identical content.”

In practice, whereas a virus is a virus, each organization has a different view of what constitutes spam. Many instances of spam would fit everyone’s definition; let’s term this “dark” spam. Other instances are less clear; think of this as “gray” spam.

The impact of spam

Spam is more than just an irritation for a majority of organizations. It has grown into an issue that seriously affects organizational productivity. First consider the impact to network productivity. According to Meta Group [Meta 1122] between 2% and 10% of inbound Internet corporate email can currently be classified as spam, with that number expected to grow to 10%-20% during the next five years (consumer e-mail already comprises about 25% spam). When factoring in these additional messages to an organization’s network infrastructure, the end result is serious costs related to network hardware for storing and handling the messages and bandwidth costs for processing each message.

Secondly, factor in the impact to employee productivity. Consider the cost of each employee managing spam at their desktop. In addition, much of the material sent via spam can be considered offensive, containing pornographic images and text that is laced with profanity. Such materials can lead to issues related to harassment and legal liability.

How bad is the problem?

Date	Unauthorised mass mailings – i.e. spam attacks (by email volume)
Apr 01	0.70 Million
Jun 01	0.85 Million
Aug 01	1.5 Million
Oct 01	1.7 Million
Dec 01	1.98 Million
Feb 02	3.25 Million

The volume of spam is rising rapidly with little relief in site. Data presented in a Business Week article (Apr 2002) shows an alarming increase in spam attacks over the last year.

Organizations cannot expect regulatory relief to combat spam. Although legislation has appeared around the globe to regulate spam, tracking down the people who send spam can be a difficult task. Most spammers make a great effort to conceal themselves, often routing email through one or more foreign countries before the message arrives in the intended recipient’s inbox.

Opting out of spam mailing lists is also ineffective. While most spam includes instructions on how to be removed from the sender’s mailing list, more often than not following these instructions only encourages more spam to be sent, as the sender now has validation that the receiving address is valid.

How is spam identified?

By where it comes from

One technique to reduce the incidence of spam is to block the reception of any email from specific sources known to originate spam email. This technique is commonly based upon:

- Locally managed block lists of domains and senders
- Remote service that manages a broad list of domains/addresses

By what it contains

By analysis of individual messages, it is possible to identify spam. This analysis may take the form of:

1. Identifying reoccurrences of known spam messages
2. Looking for the generic traits and common language of spam messages
3. Examination of all aspects of a message to see if it fits a statistical profile of spam

What to look for in identifying spam

Spammers use different tricks and techniques to attempt to bypass security measures and encourage recipients to open the message. The following lists some of the more common methods used by spammers when sending out their email:

1. Phoney subject line: Some spam tries to bypass security looking for specific headers, by misspelling some words i.e. - "re: you are this months priz winer" or "Loose weght in only 7 days"
2. Numeric address formats: Often spam emails will use addresses with numeric versions to avoid blocking based on previous spam email recognition i.e philr1210@hotmail.com; philr1211@hotmail.com; philr1212@hotmail.com
3. Celebrity subject headers: If a message header refers to celebrities such as J Lo, Kylie Minogue, Britney Spears etc in most instances this will be spam
4. Dictionary spam: If a message's "To:" field is crowded with email addresses containing names similar to yours, you've got dictionary spam. This is where spammers send messages to every address that looks like yours at several different email domains.
5. Spurious content: If an email says you can get rich working from home while enlarging your breasts, or earn a million in one day, it's spam.
6. Bogus unsubscribe links: Legitimate marketers honour unsubscribes requests. Spammers (at worst) use them to verify your address and send more spam. Just delete spam, never reply unless you want to respond to the offer
7. Fake return address: Most bulk emailers can generate random false return addresses--sometimes even using your own email address.
8. Forged headers: Spammers falsify routing headers--the breadcrumb trail left by mail servers as email passes through--to hide their location.
9. Common Spam Categories: The following categories are normally a good indicator of spam mail, Pornography, Money Making, Direct Products, Become a spammer, Gambling/Sweepstakes, Healthcures/Weightloss

Once identified, what options are available to manage spam?

Use of a block list can give rise to only one response – to block reception. This technique cannot differentiate between individual emails; all email from the named source will be blocked. However, for some sources of ‘dark spam’ e.g. known pornographic spammers, blocking is typically the best approach.

Identifying spam based upon the content of the message gives a broader choice of responses, allowing organizations to customize their approach to:

- Tag the message as spam and deliver to the recipient
- Quarantine the message for administrative review
- Block the message

For some companies it is important to be able to tailor spam handling by roles (e.g., executives get messages tagged and delivered; line workers get administrative review).

Consequently, an ideal spam solution should incorporate the full range of technologies to detect spam at the gateway and provide multiple, flexible and customizable policy actions to be applied to a suspected spam message.

The Clearswift approach to combating spam

The problem of spam is similar in nature to the problem of viruses, in that the problem has become increasingly sophisticated as spammers have refined and improved their techniques. Clearswift believes defense-in-depth is the only effective way to combat and manage spam, and therefore developed its solution based on the [3 Elements of Effective Spam Management](#). The Clearswift approach is based on combination of Policy, Products and Proactive Services.

1. Policy
2. Product
3. Proactive Services

Using our integrated approach, organizations can get their spam problem under control by working with Clearswift to implement:

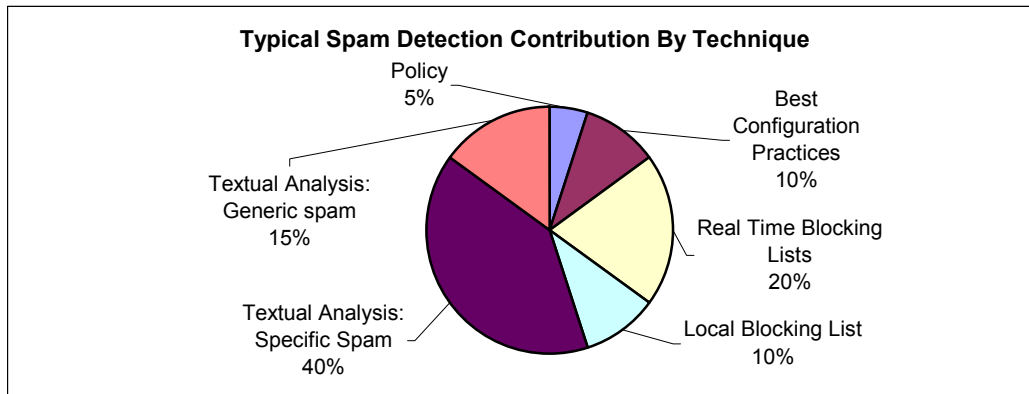
- 1) Sound email usage **policies** (e-policies) so that employee’s are aware of their responsibility for preventing spam from entering the organization and knowing how to deal with any spam that makes it to their desktop.
- 2) Clearswift’s gateway email **products** to provide organizations with best configuration practices for their gateway as well as reactive and proactive techniques to stop spam using a combination of blocking lists and content analysis to identify spam senders and spam content at the gateway.
- 3) **Proactive services** such as Threatlab Active that keeps spam defenses current with minimal administration overhead.

A combination of techniques will maximize the overall “effectiveness” (i.e. maximize spam removal). While the techniques have some degree of overlap in terms of spam detection, using the above approaches together can yield significant reductions in spam.

“IDC analyst Mark Levitt recommends blocking the most offensive and common spam at the server...”

**Network World-
Fighting Back
Against Spam,
05/13/02**

The relative combination of any given technique will vary from organization to organization, however a “typical” customer might expect to receive the following contributions from each technique.



Clearswift currently offers the most comprehensive mix of products and services to provide organizations with strong reactive and proactive defenses against the growing spam menace. Clearswift is committed to providing organizations with the flexibility to craft a custom and nimble defense against spam while providing organizations with the support and services necessary to make administering the solution as painless as possible. Over the long term, Clearswift is committed to the improvement of the anti-spam techniques and services available to customers.

Organizations that select Clearswift not only get a best of class anti-spam solution but also the capabilities to create and manage centralized e-policies for any issues related to protection (i.e. malicious threats, viruses, legal liability & confidentially breaches), compliance (secure messaging, regulatory compliance, auditing & archiving) and productivity (network & employee).

81% of organizations have written e-policies in place

47% monitor email

51% require written employee acknowledgement of e-policies

24% actively educate employees about email risks and email responsibilities

**ePolicy Institute,
US News, AMA
2001 Survey**

Element 1: Policy

The first step in combating spam (prior to implementing any type of software or technology solution) is to ensure an appropriate usage policy (e-policy) for email is implemented. While most organizations have written e-policies in place, many e-policies lack the specific detail required to instruct employees how to deal with inappropriate email. A good e-policy will specify whether or not employees can sign up for newsletters and online sites that require email addresses. If allowed, the e-policy should state the conditions in place for selecting a newsletter to sign up for (i.e. to ensure it is business related and meets the guidelines required by the organization). The e-policy also will state what is considered appropriate and inappropriate content for e-mail and how employees are to handle inappropriate and unsolicited content.

Employees must be properly educated about the e-policies to ensure they fully understand them. Education should require written acknowledgement of the policy and should involve frequent e-policy reinforcement.

A strong e-policy is an important component in the battle against spam. Clearswift's e-policy services are structured to assist organizations in establishing effective e-policies, educating their employees and enforcing e-policies using technology. Templates for translating written email and Web usage policies into enforceable policies using Clearswift software are available specifically for creating anti-spam policies.

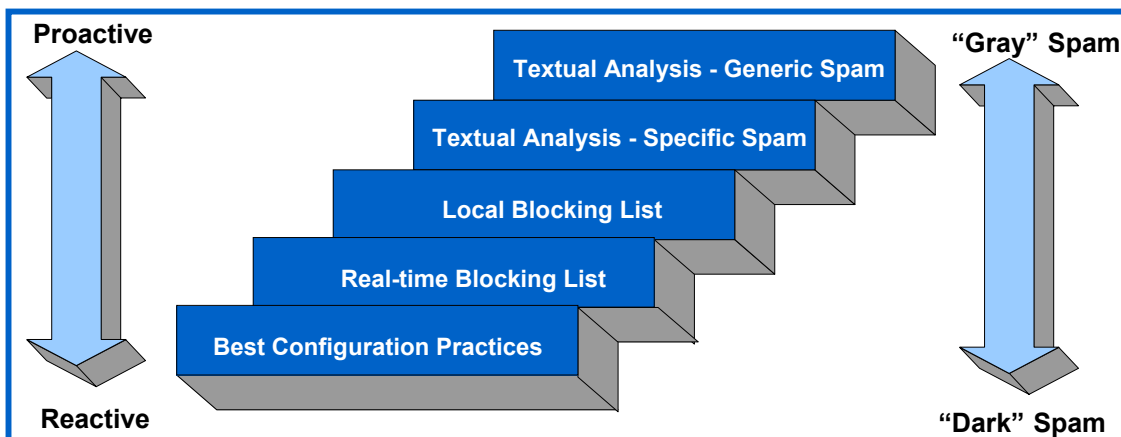
Clearswift's e-policy services are part of the broad family of Clearswift Enterprise Services, which consists of technical and consultancy services aimed at providing organizations with the benefits of expert advice and proactive analysis.

For more information, proceed to www.Clearswift.com/epolicy or email at epolicy@Clearswift.com.

Element 2: Product

Clearswift's products and solutions provide a range of techniques to combat spam. These techniques can be layered together to build defense in depth:

- The base layers are aimed at dealing with "dark" spam (spam that fits everyone's definition). These approaches can be considered to be "reactive" in nature, dealing with known spam and spam sources.
- The higher layers provide closer tailoring for handling organization-specific "gray" spam (instances where the definition is less clear). These approaches are more "proactive", handling existing and new instances of spam.



Best Configuration Practices

Clearswift spam protection starts with the configuration of our products. The following methods each contribute in a small way to the overall effectiveness of our solution to protect against spam and spoofed email:

- **Validating the Sender's Address:** Prevents spammers from using arbitrary 'from' addresses within the message by ensuring the sending address is indeed a valid address
- **Limit the Number of Message Recipients:** A lot of spam mail contains multiple address entries in the To: or CC: fields. This option allows organizations to limit how many addresses are allowed in these fields for incoming messages.
- **Relay Host:** Allows organizations to prevent their gateway from being used as a third-party mail relay by specifying that only trusted sources are allowed to use the gateway as a mail relay. This hinders an unsuspecting organization from relaying spam mail to the intended recipient.
- **Auditing and Reporting:** Clearswift supports a variety of different ways to report on mail entering the Internet gateway. Knowing how mail is entering the organization empowers a flexible and real-time response to spam problems.

Effectiveness and accuracy

- Overall spam removal (true-positive) – Moderate
- Miss-hits (false-positive) – Low
- Clearswift Proactive Services and Product Training are available to provide assistance with best practice configuration.

Maintenance

- Low

Bottom Line

- Whereas the overall contribution of these configuration practices is relatively low to the overall spam solution, they should be implemented because they require minimal set-up and maintenance.

Real-Time Blocking Lists

Real-time Blocking Lists (RBLs) are Internet services that provide a way to block mail that is sent via open mail relays (basically when a message is transferred through a third party relay to help mask the true sending address) and known spam sources. The MAPS RBL (www.mail-abuse.org) is probably the most well known, and offers a fee-paying service, whereas others are provided free. All are operated by “not for profit” organizations. Many ISPs (such as Hotmail) use the services of the RBLs.

Clearswift allows RBL services to be fully integrated into an overall anti-spam policy. The RBL services that are accessible by Clearswift are often referred to as DNSBL lists. These services make DNS lookups (matching the sender’s address to the host/IP address) to the services’ database of spam senders. Information on sites that offer such RBL services can be found at www.openrbl.org (OpenRBL) and www.spews.org (Spews).

When leveraging a RBL service, part of the control of an organization’s messaging system is turned over to the RBL service. As such, it is important to monitor the integrity and quality of the chosen RBL. A newsgroup such as news.admin.net-abuse.email can assist in this process. Clearswift ThreatLab Active maintains a list of recommended RBL services.

Use of an RBL alone is not likely to provide an acceptable rate of spam reduction. Clearswift recommends that RBL use should be used in combination with one or more of the other techniques mentioned in this paper.

Effectiveness and accuracy

- Overall spam removal (true-positive) – Moderate- varies with list used
- Miss-hits (false-positive) – Low to Moderate - depending on the accuracy of the list provided by the DNSBL supplier. Some list providers admit to being aggressive and may block legitimate mail domains
- Clearswift ThreatLab Active can advise you on the most appropriate RBL and ongoing monitors the RBL suppliers that our customers generally find most useful and alerts customers if we are recommending they change RBL supplier
- Choice of list – focus varies; open relays, open proxies, known spam sources, combinations – some are managed, others are automated – some are “aggressive” others “low risk”
- With so many lists available tracking which is the most up-to-date and accurate source
- Different lists may use a different implementation of reporting if a site is a known spam location

Maintenance

- Low – Organization’s need to keep a watch on list quality

Bottom Line

- RBL lists can provide an important first line of defense and detects new spam from well-known spammers more effectively than most other techniques. Choosing between the 150 plus RBLs on the Internet can be a daunting task. Clearswift can recommend the best RBL for your environment and alert you of any changes that would impact that choice.

Local Blocking List

A **local block list** is a set of domains or message sources from which an organization chooses to block the reception of email. The technique is equivalent to use of an RBL, except the organization manages the blocking list themselves. The local block list can augment use of an RBL service – enabling a less aggressive RBL service to be used effectively. Particular nuisance message sources can be successfully managed through a local block list.

The Spews website has links to sites containing up to date “nuisance” email addresses and relay host addresses that organizations can add to their local lists.

Effectiveness and Accuracy

- Overall spam removal (true-positive) – Low – targeted to specific nuisance mailers
- Miss-hits (false-positives) – Low
- May require investigation to determine the source addresses to block

Maintenance

- Low – infrequent additions/deletions would be the norm

Bottom Line

- The ability to provide local customization is key to any good spam management solution; local blocking lists can therefore be critical in some environments.

Textual Analysis- Specific Spam

This technique involves textual analysis to identify specific instances of known spam. In this method an expression list of textual words and phrases is compiled, where typically each entry represents a particular spam instance or class of spam. This technique is particularly effective for dealing with repetitive spam, such as chain mail and fraudulent offers. Spam of this nature often is tracked and documented on web sites e.g. <http://hoaxbusters.ciac.org/>.

The expression list for this technique is relatively simple in its construction. Each entry acts as a trigger and there is little or no interrelation between the different entries.

For example, consider the phrase: *"Could you sell billions of hamburgers using only a single restaurant?"* This could be used as an instant trigger for this particular “get rich quick” scheme.

Effectiveness and Accuracy

- Overall spam removal (true-positive) – Moderate-to-High - but requires frequent expression list update.
- Miss-hits (false-positive) – Low
- Best to “age out” entries to minimize the size of the expression list
- Essentially a reactive approach – based upon known spam “in the wild”

Maintenance

- Moderate – if expression lists locally managed
- Low – if the Clearswift [Threatlab Active](#) managed anti-spam service is leveraged.

Bottom Line

- Looking for known spam is one of the core techniques of any good spam management system. However, 'known spam' from the wild is always by nature out of date and is not reflective of "local" spam. Leveraging an actively managed service, such as Clearswift [Threatlab Active](#), will keep an organization up to date in defending against specific spam.

Textual Analysis- Generic Spam

This technique involves using textual analysis to identify the generic traits of spam content. In this way an expression list is compiled to identify the typical characteristics of a spam message. Adjusting the sensitivity (or threshold) of the expression list can be used to tune the aggression of the detection. The more aggressive the setting the more spam is detected, but this increases the chances that false-positives will result.

For example, consider the following expression list:

Weighting	Phrase
5	"You can't lose"
5	"You could be making a killing"
2	"You make money"
5	"You may never have to pay"

In this example the list may have a threshold of 10 and therefore a message would require phrases that when detected matched or exceeded that threshold.

This technique can be further refined by use of multiple expression lists, where each list is established to recognize a particular type of spam (e.g. offensive spam, chain mail, etc). An organization can then fine tune the sensitivity applied to each type of spam.

This technique provides a more proactive defense as it does not require the previous identification of specific instances of spam. Therefore *Textual Analysis – Generic Spam* complements the techniques described above, each of which are reactive.

Effectiveness and Accuracy

- Overall spam removal (true-positive) – Moderate-High – depends on expression list granularity and sensitivity settings
- Miss-hits (false-positive) – Moderate - depends on sensitivity settings

Maintenance

- Moderate – if expression lists locally managed
- Expression lists are complex to modify – relying on the interrelation of entries
- Relies on the administrator understanding the syntax and building the entries with appropriate weightings

Bottom Line

- Expression lists to block generic spam provides organizations with a proactive approach to stop spam, however building and maintaining these list can be difficult. Clearswift makes lists of generic spam expressions available for customers to get them up and running quickly meaning reduced list administration.

Element 3: Proactive Services

Clearswift Threatlab Active

Keeping up with the tactics and methods employed by those who send spam is a difficult task. To assist organizations in keeping their spam defenses current, Clearswift provides a managed spam list service available for all customers who subscribe to Clearswift Threatlab Active. This service provides:

- Actively updated lists of spam expressions, posted to Clearswift's website daily for Clearswift customers to use in place of internally managed expression lists for Specific spam.
- Provision of automated processes to facilitate seamless updates of the new spam patterns
- Clearswift has 15 offices around the World providing a truly global reach, which allows for the preparation of spam expression lists specific for different regions across the globe. Lists are tested extensively before publishing to ensure that accuracy remains high while false positives remain low. Clearswift Threatlab Active takes the burden of maintaining expression lists containing spam terminology away from the organization.

Spam is an ever-moving target. You need active support to battle the problem; Clearswift ThreatLab with its global reach (Europe, North America and Asia Pacific) is working 24x7 to keep our solutions current.

Clearswift Product Support

In addition to Threatlab Active, Clearswift makes available to any customer tools and documentation to help configure and maintain their spam defenses.

This includes:

- Lists of Generic spam expressions
- Updated advice on the use of the best RBL list
- Best Practice Configuration advice for Clearswift's gateway products
- Anti-spam modules within product training courses that cover product configuration and ongoing maintenance

"IDC's Mark Levitt recommends that IT departments partner with an anti-spam product vendor or service provider rather than trying to program rules and algorithms on their own. 'You can't build your own spam engine. You don't have time', he says."

**Network World-
Fighting Back
Against Spam,
05/13/02**

Summary

The problem of spam is similar to the problem of viruses – the problem has become increasingly sophisticated as spammers refine and improve their techniques. At the same time many of solutions to the problem of spam have grown increasingly complex. However, the solution does not necessarily require significant administration. The following summarizes how Clearswift can help organizations stop spam without significant administrative overhead.

Element 1: POLICY

Clearswift can help you develop, deploy and manage effective policies to help your staff minimize the spam they bring into the organization

Element 2: PRODUCT

BEST CONFIGURATION PRACTICES: Clearswift will help you configure your Clearswift perimeter defenses using field proven best practices

REAL TIME BLOCKING LISTS: There are more than 150 real-time blocking lists available on the market. Many are free, some require an annual subscription. We'll help you pick the best list for your organization

LOCAL BLOCKING LISTS: Clearswift products allow for the customization of a local block-list to include spam sources that are a particular nuisance to your organization

TEXTUAL ANALYSIS- SPECIFIC SPAM - Much like an anti-virus signature, repetitive specific-spam is identified by specific titles and phrases and blocked using Clearswift products and services

TEXTUAL ANALYSIS- GENERIC SPAM -The generic-spam textual analysis looks for the characteristics and generic traits of spam messages to block spam

Element 3: PROACTIVE SERVICE

Clearswift's [Threatlab Active](#) will make sure your defenses remain current to address the ever moving spam threat, as well as minimize your ongoing management burden by keeping you abreast of issues in the outside world that can effect your policies. Clearswift will then provide you with the tools and services to make the maintenance of policy simple.

A combination of techniques will maximize the overall “effectiveness” (i.e. maximize spam removal). While the techniques have some degree of overlap in terms of spam detection, using the above approaches together can yield significant reductions in spam.

Clearswift currently offers the most comprehensive mix of products and services to provide organizations with strong reactive and proactive defenses against the growing spam menace. Clearswift is committed to providing organizations with the flexibility to craft a custom and nimble defense against spam while providing organizations with the support and services necessary to make administrating the solution as painless as possible. Over the long term, Clearswift is committed to the improvement of the anti-spam techniques and services available to customers.

Organizations that select Clearswift not only get a best of class anti-spam solution but also the capabilities to create and manage centralized e-policies for any issues related to protection (i.e. malicious threats, viruses, legal liability & confidentially breaches), compliance (secure messaging, regulatory compliance, auditing & archiving) and productivity (network & employee).

Bottom Line: More customers have purchased Clearswift for spam management than any other solution on the market. IDC notes Clearswift is the market share leader for email content filtering

About Clearswift

Clearswift is the world's leading provider of software for managing and securing electronic communications, with a 23% share of the global content filtering market. Clearswift delivers the capabilities for organizations to protect themselves against email and web-based threats, meet legal and regulatory requirements, implement productivity-saving policies and manage intellectual property passing through their network.

The company's expertise lies in establishing and enforcing e-policies. Content security threats include the circulation of inappropriate images and text, spam and oversized files, loss and corruption of data, breaches of confidentiality, as well as viruses and malicious code. Clearswift's software portfolio includes Clearswift MIMESweeper, a product family for email and web e-policies and Clearswift ENTERPRISEsuite, a software infrastructure for managing e-policies in complex environments. More information about Clearswift, its products and services is available at www.Clearswift.com.

About Clearswift MIMESweeper

MIMESweeper is the market leading family of products designed to implement email and web communication e-policies. MIMESweeper delivers the capabilities for organizations to protect themselves against email and web based threats, meet legal and regulatory requirements, implement productivity saving policies and manage the intellectual property passing through their network.

Within the Clearswift MIMESweeper family there are two products available for combating spam at the Internet gateway: **CS MAILsweeper for SMTP** analyzes incoming and outgoing email at the Internet gateway; **CS eSweeper** analyzes incoming and outgoing email in a hosted or managed service environment.

About Clearswift ENTERPRISEsuite

Clearswift ENTERPRISEsuite (ES) meets the needs of enterprises and government organizations with complex environments and premium value communications. ES delivers the e-policy infrastructure and the enforcement technology required to deploy a comprehensive management and security solution.

Within Clearswift ENTERPRISEsuite are inter-related products for gateway email policy enforcement, internal email policy enforcement and Web policy enforcement. ES ClearEdge provides protection at the Internet gateway and enables large, complex organizations to enforce e-policy management for inbound and outbound email communications at the Internet gateway.

Clearswift MIMESweeper Family:

*CS MAILsweeper for
SMTP*

*CS MAILsweeper for
Exchange*

*CS MAILsweeper for
Domino*

CS WEBSweeper

CS eSweeper

ClearSecure

Clearswift ENTERPRISEsuite:

*ES ClearPoint PMI –
Policy Management
Infrastructure*

ES ClearEdge

ES ClearSurf

ES ClearSecure

*Intelligent Interface
Design*



CLEARSWIFT™

Managing and securing
electronic communications

EUROPE

United Kingdom

1310 Waterside
Arlington Business Park
Theale, Reading
Berkshire, RG7 4SA
UNITED KINGDOM
Tel: +44 (0) 11 8903 8903
Fax: +44 (0) 11 8903 9000

Germany

Amsinckstrasse 67
Poseidonhaus
Hamburg, 20097
GERMANY
Tel: +49 402 399 90
Fax: +49 402 399 9100

France

54-56 Avenue Hoche
75008, Paris
FRANCE
Tel: +33 1 56 60 58 00
Fax: +33 1 56 60 56 00

AMERICA

US West Coast

15500 SE 30th Place
Suite 200
Bellevue
Washington, 98007
UNITED STATES
Tel: +1 425 460 6000
Fax: +1 425 460 6185

US East Coast

1050 Winter Street
Suite 1000
Waltham
Massachusetts, 02451
UNITED STATES
Tel: +1 781 839 7321
Fax: +1 781 522 7488

ASIA PACIFIC/JAPAN

Australia

Ground Floor
165 Walker Street
North Sydney
New South Wales, 2060
AUSTRALIA
Tel: +61 2 9424 1200
Fax: +61 2 9424 1201

Japan

Eisho Takanawadai Bldg 6F
2-11-8,
Minato-ku Shiroganedai
Tokyo-to, 108-0071
JAPAN
Tel: +81 (3)5423 8171
Fax: +81 (3) 5423 1274

www.clearswift.com

© 2002 Clearswift Ltd. All rights reserved. The Clearswift Logo and Clearswift product names including ES™, ENTERPRISEsuite™, ES ClearPoint™, ES ClearSecure™, ES ClearEdge™, ES ClearBase™, ES ClearSurf™, ES DeepSecure™, CS Bastion II™, CS X.400 Filter™, CS MIMESweeper™, CS MAILsweeper™, CS WEBSweeper™, CS e-Sweeper™, CS IMAGEmanager™, CS SECRETSweeper™ are trademarks of Clearswift Ltd. All other trademarks are the property of their respective owners. Clearswift Ltd. (registered number 3367495) is registered in Britain with registered offices at 1310, Waterside, Arlington Business Park, Theale, Reading, Berkshire RG7 4SA, England

Managing and securing electronic communications™