Spam Solutions White Paper

Presented by:

Net Sense

Spam Problem Overview

What Is Spam?

AOL states that in 2003, they blocked an average of 1.5 billion spam messages each day. And this incredible glut of spam is growing more pervasive (and invasive) every day.

What exactly is spam?

Simply put, spam is unwanted email whose senders are unknown to the recipient or are inadvertent senders of an unwanted email.

Examples of inadvertent senders are:

- when email is created and sent by a virus
- sender names (often businesses) that have been spoofed by a spammer
- businesses renting an illegitimate mailing list for their email advertisements

UBE (Unsolicited Bulk Email) and UCE (Unsolicited Commercial Email) are terms that are often used to describe different types of spam.

Who Sends Spam?

Unsolicited commercial email comprises the bulk of spam, so who sends these unwanted billions of emails each day?

- Unscrupulous businesses (don't buy from them)
- Misinformed businesses (complain to them)
- Hackers attempting to compromise systems or after personal information

Buying anything from a spam email only reinforces the profit motive for a spammer. Usually, the spammer is earning a referral or affiliate commission for directing you to the product website. If they weren't making money, they wouldn't be doing it.

Occasionally, legitimate businesses send out commercial email to what they believe is a legitimate opt-in list, but it's not. Politely give them guidance on the error of their ways.

The third spam source is the most dangerous. Hackers send out bulk email trying to trick unsuspecting users to login to a phony website and reveal personal financial information. This information is then used to access their bank and/or credit card accounts.

Another trick is to include an attachment which serves as a trojan horse, granting remote system access to your computer. Avoid opening any email attachments from suspicious emails.

How Is Spam Sent?

Spam is sent by devious methods designed to conceal the source of the sender. Among the most popular methods are:

- Fraudulent accounts
- Spam-friendly ISP's
- Open relays
- Compromised hosts
    - *Open HTTP Proxy Servers*
    - *Open Socks Proxy Server*
    - *Other Open Proxies*
    - *Open SMTP Relays* - SMTP servers misconfigured as open relays)
    - *Insecure or Compromised Web Servers* - Web servers that contain insecure CGI scripts, other types of insecure scripts, or that are infected by viruses or trojans such as Code Red and NIMDA.
    - Zombie Netblocks - IPs and IP ranges that have been hijacked and are no longer controlled by the registered owners.
- *Dynamic IP Ranges* - Dynamic IP ranges used for dial-up and low-end broadband connections to the Internet that might be being used to send email directly to your server; regular users always send email via their provider's SMTP servers.

How Is Spam Identified?

Most of us would offer slightly different descriptions of spam, but each of us would agree "*I know it when I see it!*"

Spam takes many forms, so anti-spam programs zero in on these common traits:

- Originates from an email address known to belong to a spammer.
- Originates from known spam source sites, domains or hosts -- internet sites which exist solely or primarily to spam or provide services to spammers.
- Originates from irresponsible, or rogue, Internet Service Providers (ISPs), who permit spamming from their sites and fail to take appropriate action against spammers.
- Was sent using a bulk email program whose only or primary purpose is to send large quantities of junk email.
- Contains headers which match the profile of definite or probable spam.
- Contains body text strings which match the profile of probable spam.
- Contains body text strings which match the profile of a particular virus or class of viruses.

What Problems Does Spam Cause?

Spam causes tremendous expense for businesses and individuals because all the costs of spam are borne by the recipients. This is different from junk mail where the distribution costs are borne by the sender. Among these costs are:

- Overloaded mail servers
- Overloaded user accounts
- Increased archive requirements
- Excessive bandwidth consumption
- Expense of anti-spam measures
- Expense of lost employee time
- Virus exposure
- Malware exploits

Businesses and ISPs must scale their systems to handle the flood of spam that inundates their mail servers and user accounts. Ultimately, those costs are borne by consumers as those costs are added back to the end product pricing.

It also becomes more expensive for businesses to archive their email communications as legislated by the Sarbanes-Oxley Act and other federal laws.

Network bandwidth costs are also higher as spam consumes ever increasing amounts of the Internet connectivity used by businesses and ISPs.

Fighting spam requires businesses and ISPs to devote considerable manpower to implementing and maintaining anti-spam solutions. Users also have to waste their time manually deleting spam from their mailboxes every day.

Even 15 minutes a day adds up to more than two weeks time over the course of a year for a single user. Multiply that times the number of users and you begin to see just how expensive a problem spam is for businesses.

Add to that the cost of fighting viruses and malware spread by spam and other methods and the true cost of spam becomes apparent. However, there are other costs created by spam which are not readily apparent.

Legal Considerations For Business

In addition, spam can create legal complications for businesses as well:

- Hostile or unsafe workplace lawsuits
- Sexual harassment lawsuits

Defending against unsafe workplace lawsuits of this nature can be tremendously expensive for businesses. You must be able to document all efforts made to protect workers from offensive materials. Legal costs can quickly climb into the thousands without any guarantee of a favorable decision.

Similarly, employees forwarding pornographic spam can create huge liabilities for their employers. What one person might intend as a joke can be perceived by someone on the receiving end as harassment. We've all heard the old saying "perception is reality" and juries have sometimes backed that viewpoint with substantial awards.

Companies worldwide need to provide a positive work environment for their employees. For example, in the US, companies with 25 or more employees must, under federal law, provide a work environment free of gender, ethnic or racial harassment or discrimination.

That requires taking reasonable steps to eliminate harassing materials from the workplace. It may not matter whether the company knew employees were downloading pornographic images or passing racist e-mail jokes.

The test at trial could be whether well-known remedies were available to prevent abuses, whether a policy existed to apply those remedies, and whether the policy was actually enforced.

Illegal or offensive content:

- Pornographic images downloaded off the Web
- E-mail jokes (either sent or received)
- Pornographic or racially offensive e-mail attachments
- Rumors or gossip regarding a fellow employee
- Unauthorized release of personal employee information
- E-mail discussions that result in employee harassment or discrimination

Illegal or offensive content - both Web and e-mail - is a risk. It is much better from a legal standpoint to protect your business with strong spam filters and an ironclad Acceptable Use policy that is enforced every day.

What's important to stress here is that having a policy is generally not enough to establish a defense to a claim of harassment. Employers must also enforce the policy and proactively take steps to prevent employees from being exposed to harassing material. Non-enforcement implies non-commitment or, worse, disregard for accepted working conditions, while the implementation of filtering systems and perimeter protection services count as important indicators of corporate intent to enforce stated policies.

The three-pronged foundation of policy, training, and enforcement greatly reduces the potential for employment-related claims. In the event of litigation, this foundation will strengthen the employer's position in requesting a summary judgment or other motion to

terminate litigation at any early stage – saving legal costs in hundreds of thousands of dollars and substantial damages.

Anti-Spam Laws

Existing State spam legislation has been superceded by the toothless Federal CAN-SPAM Act. Information on new legislative efforts and the status of existing laws can be found at:

http://www.SpamLaws.com

CAN-SPAM Act

The CAN-Spam Act supercedes all State spam laws and the anti-spam fight has lost ground in some areas. With spam already exceeding 25% of all email traffic and that number climbing rapidly, this law is a hopeless disappointment as a spam deterrent.

The law makes it an offence to falsify message headers and use deceptive subject lines in spam, and requires the use of appropriate warnings in commercial email of a sexual nature. However, it rescinds the much tougher anti-spam laws of several U.S. states, and includes no right of private action. Now, only ISPs and State's Attorney Generals will be allowed to pursue spammers.

How To Avoid Becoming A Spam Magnet

Being careful with your online behavior is a must for anyone using a personal computer. Spammers are crafty in how they obtain email addresses. Once they have yours, they won't let up in their attempts to invade your inbox.

Tips for users:

1) Don't post your email address online

2) Don't open spam

3) Don't buy anything from spam messages

4) Don't use any spammer's "remove me" links

1) Posting your address online starts a quick journey to spam hell. Spammers rely on programs that scour the web for usable email addresses. Those harvested addresses are resold to other spammers who in turn bombard you with their own unsolicited messages.

Don't post your primary email address online. Use a free email account for any online postings, contest entries, etc. If you absolutely must use your email address, disguise it. One simple way is to add the phrase "No Spam" to it.
Example: johndoeNoSpam@xyzisp.com

2) Never open spam. Many HTML email messages return a valid email address signal to the spam senders. They know you've opened their message and now you are fair game for more spam.

Set your email client to display unread messages without the message view enabled. Simply drag the unopened spam to the trash.

3) Don't buy anything promoted by spam. Doing so just creates more spam. Spammers are only in it for the money. If the money dries up due to zero sales, they'll be out of business.

Before you succumb to a spammer's marketing pitch, ask yourself if you truly need to buy this item from this source. Remember: No sale means no spam!

4) Don't click the "remove me" link in a spam message. Doing so only confirms that your address is a live one. Your address is now upgraded to the spammer's valid delivery list. Taking no action in response to spam is always your best bet.

Note: Always use the unsubscribe link to remove your address from any legitimate opt-in mailing list to which you have previously subscribed and no longer wish to receive.

In summary, think twice before giving out your email address to anyone. It's the only way to limit your exposure.

Spam Control Methods

Blacklists (Blocklists)

Anti-spam blacklists contain the IP addresses (and, in some cases, the domain names) of the following types of servers:

- SMTP servers that are direct spam sources (usually owned by the spammers)
- Web servers that host the web sites of spammers (haven domains)
- SMTP servers that allow spammers to spam from them (spam-friendly ISPs)
- SMTP servers that relay for spammers (single- or multi-stage open relays)
- Proxy servers that allow spammers to hide behind them (open proxies)
- IP ranges that are assigned to dial-up users (dial-up lists)
- Web servers that contain insecure forms that can be used for spamming (formmail.pl and other CGI scripts)
- All servers that lack proper "whois" information or required contact addresses
- Other servers that are abused by spammers or that help spammers hide

Blocking email sent from blacklisted servers can be a highly effective way to stop spam from reaching your mailbox. In the last year, as the volume of spam on the Internet has surged, the number of blocklists has multiplied, allowing users to choose blocklists whose policies closely match their needs.

Blocklists are frequently updated, so a filter that uses them is effectively updated as often as the blocklist is, considerably more frequently than the filter itself is usually updated.

The following is a list of blocklists, sorted by these categories:

- Spam Sources
- Open Relays
- Multi-stage Open Relays
- Dynamic IP Ranges
- Insecure Web Forms
- Open Proxies
- Other Spam Support
- RFC-Ignorant.org
- All-In-One Blocklists

Spam Sources - IPs and sites listed as spam sources are persistent sources of spam that have continued to spam for a considerable length of time and despite many efforts to stop them. Many have gone through multiple ISPs, being repeatedly disconnected for breaking their provider's terms of service by spamming. Included in these lists are the SMTP servers used to send spam and the web servers that host web sites advertised by spam. Most of these lists are maintained manually.

One of these blocklists, the SpamHaus blocklist, blocks a considerable amount of spam and has a very low false positive rate. Because the most carefully maintained blocklist will make occasional errors, though, consider treating email from all blocklisted servers as suspicious rather than as outright spam, unless that email comes from a server on several blocklists or also meets your internal criteria for spam.

- ***SpamHaus.org List*** Highly respected blocklist of IP addresses used to send repeated, multiple spam runs or that host web sites advertised via spamming.

- ***NJABL Confirmed Spam Sources*** Blocklist of IP addresses used to send repeated, multiple spam runs. Slightly more aggressive than SpamHaus.org, but reasonably conservative, well-maintained, and effective.

- ***SpamCop blocklist*** List of IP addresses used to send spam or that offer spam support services. This blocklist is more aggressive than those previously listed, and is likely to result in legitimate email being blocked if you receive email from a site with a lax abuse department or that has spamming customers.

- ***MAPS Real-time Blackhole List (RBL)*** The original blocklist of IP addresses used to send repeated, multiple spam runs. Now a pay service and available only if you have subscribed.

- ***AHBL Spam Sources*** This blocklist lists hosts owned by, operated by, or under the control of spammers.

- ***AHBL Provisional Spam Source Listing*** IPs that recently have become the source of large quantities of spam, for reasons as yet unknown. The listings on this blocklist change rapidly, as blocks are either removed or moved to other categories.

- ***Spam Source Listing*** IPs that recently have become the source of large quantities of spam, for reasons as yet unknown. The listings on this blocklist change rapidly, as blocks are either removed or moved to other categories.

- ***AHBL Abusive Domains*** This blocklist lists domains (not IPs) that are owned by spammers or under their effective control.

- ***Five-Ten-SG Spam Sources*** Blocklist of direct spam sources. Similar to the NJABL Spam Sources blocklist, but more aggressive and may therefore result in blocking larger amounts of legitimate email.

- ***SORBS Spam Sources blocklist*** Blocklist of IPs and IP ranges that have sent spam to the SORBS administrators, that host web sites advertised in spam sent to the SORBS administrators, or that offer spam support services (such as email drop-boxes or DNS) to spammers. This blocklist is aggressive, and is likely to result in legitimate email being blocked if you receive email from a site with a lax abuse department or that has spamming customers.

Open Relays - Open relays are SMTP servers that accept email from any user on the Internet and deliver it to any other user on the Internet. Properly configured SMTP servers require that either the sender of the email or the recipient be a local user.

Spammers love open relays because open relays allow them to avoid spam blocks and deliver more spam, and because some open relays also hide the actual origin of the spam. The latter are called anonymizing open relays.

Blocking open relays is inherently aggressive and will block legitimate email along with spam. It is also an extremely effective way to get spam out of your mailbox, however.

- ***Relay Stop List (RSL)*** Blocklist of single-stage open relays. This is the least aggressive of the open relay blocklists; it lists only open relays that have been used to relay spam "in the recent past." The RSL tests servers to see if they are open relays only when it has "spam in hand" that appears to have come from that open relay; it does not test preemptively. It removes listings ninety days after the last reported spam from that source, or upon request. This is a good open relay blocklist for those who want to block open relays that are actively being used to send spam, but who do not approve of preemptive testing.

- ***NJABL Open Relays*** Blocklist of single-stage open relays. More aggressive than the ORDB, but well-maintained and effective.

- ***MAPS Relay Spam Stopper (RSS)*** Blocklist of single-stage open relays. Conservative -- lists only relays that have been used to spam, rather than all open relays. Now a pay service and available only if you have subscribed.

- ***Open Relay Database (ORDB)*** Blocklist of single-stage open relays. This is a "Child of ORBS" list; it tests open relays on request and lists those that are open relays. Probably the largest and most widely used list of open relays on the Internet.

- ***Five-Ten-SG Single-Stage Open Relays*** Blocklist of single-stage open relays. This is similar to the NJABL Open Relays blocklist, but more aggressive.

- ***DSBL Single-Stage Open Relays*** Blocklist of single-stage open relays -- IP addresses of SMTP servers that relay email for any user on the Internet, addressed to any other user on the Internet. This list contains the IP addresses of confirmed open SMTP relays, open proxy servers, and web sites with insecure formmail.pl scripts. Entries to this list are from trusted users only. The DSBL is a "Son of ORBZ" blocklist, and as such is somewhat aggressive.

- ***AHBL Open Relays*** Lists open SMTP relays.

- ***SORBS Open Relays blocklist*** List of IPs and IP ranges that operate SMTP servers configured as open relays.

Multi-Stage Open Relays/"Smart Hosts" - Multi-stage open relays are SMTP servers that are themselves secure; they accept email only from their own users or for their own

users. Among their users, however, are SMTP servers that are open relays. This allows a spammer to use a customer site of a multi-stage open relay to send email via that site's SMTP server, increasing the amount of spam he can deliver and further obscuring the origin of his spam.

Blocking email from a multi-stage open relay is inherently risky. Most multi-stage open relays are SMTP servers for large ISPs or companies, and most email they send is legitimate. They have been abused to send large spam runs, however. Blocking email from these relays should reduce the amount of spam you get considerably.

- ***NJABL Multi-Stage Open Relays*** Blocklist of multi-stage open relays and "smart hosts". Well-maintained and effective.

- ***Five-Ten-SG Multi-Stage Open Relays*** Blocklist of multi-stage open relays. This is similar to the NJABL Multi-Stage Open Relays blocklist, but more aggressive.

- ***DSBL Multi-Stage Open Relays*** Blocklist of multi-stage open relays -- IP addresses of SMTP servers that are themselves secure, but that relay email for other, insecure SMTP servers. Entries to this list are from trusted users only.

Dynamic IP Ranges - Blocklists of dynamic IP ranges include IP addresses assigned dynamically to dial-up users, and sometimes IP addresses assigned to DSL users and cable modem users. Most of these users are not spammers. Users with this type of connection, however, will rarely (if ever) send email directly from their computer to a recipient's SMTP server. Instead, they send outgoing email via their ISPs SMTP servers.

Spammers, on the other hand, frequently use software that sends email directly from their computer to the recipient's SMTP server, bypassing their own ISP's SMTP server. This allows them to evade security and anti-spamming measures the ISP might have taken. By rejecting email sent directly from a dial-up IP address, you are unlikely to reject legitimate email, but will catch a lot of spam.

I highly recommend that you use it or another list below; these lists catch a lot of spam.

- ***NJABL Dial-Up and Dynamic IP Ranges*** Blocklist of dynamically-assigned IP ranges, usually used for dial-up and low-end DSL and cable modem connections. Well-maintained and effective.

- ***MAPS Dial-Up List (DUL)*** Blocklist of dynamic IP addresses assigned to dial-up users. Now a pay service and available only if you have subscribed.

- ***Five-Ten-SG Dial-up List*** Blocklist of dynamic IP addresses assigned to dial-up, cable modem, and DSL users. Similar to the NJABL Dial-Up and Dynamic IP Ranges blocklist, but more aggressive.

- ***SORBS Dynamic IP Ranges blocklist*** List of dynamically-assigned IPs and IP ranges assigned temporarily to dial-up Internet users or users with low-end broadband access.

Insecure Web Forms - These blocklists list the IP addresses of web servers that have insecure web forms or scripts that allow any user to send email to any other user, such as old versions of `formmail.pl`. Email from such web servers is likely to be spam.

- ***Five-Ten-SG Insecure Web Form List*** Blocklist of web sites that run insecure web forms, such as formail.pl, which are often abused by spammers to send spam.

- ***NJABL Insecure Web Forms blocklist*** List of IP addresses of web servers that contain insecure web forms that can be used to spam. Well-maintained and effective.

- ***AHBL Formmail Spam List*** This blocklists contains the IPs of web hosts with insecure formmail.pl scripts that are abused by spammers.

- ***SORBS Insecure Web Servers blocklist*** List of web servers that host insecure CGI scripts, other types of insecure scripts that can be abused by spammers, or that are compromised by a virus or trojan.

Open Proxies - An open proxy is a proxy server that accepts anonymous connections from anyone on the Internet. Open proxys are abused by spammers to hide the origin of outgoing spam.

- ***NJABL Open Proxies*** Blocklist of IP addresses of web servers that run open proxies. Well-maintained and effective.

- ***AHBL Open Proxies List*** Lists all types of open proxies.

- ***SORBS Open HTTP Proxy Servers blocklist*** Blocklist of open HTTP proxies.

- ***SORBS Open Socks Proxy Servers blocklist*** Blocklist of open Socks Proxy servers.

- ***SORBS Other Open Proxies blocklist*** Blocklist of other types of open proxies. .

Other Spam Support - The blocklists below contain the IP addresses of sites that host bulk email servers that don't properly confirm subscriptions, and that have other spam-related problems.

- ***Five-Ten-SG Opt-Out Lists*** Blocklist of sites that host bulk email servers that don't properly confirm subscriptions.

- ***CompleteWhois Bogons blocklist*** Blocklist of unallocated IP ranges and IANA reserved IP ranges, none of which should ever appear in email.

- ***CompleteWhois Hijacked Netblocks blocklist*** List of IP ranges that have been hijacked and are controlled by users other than the registered owners.

- ***AHBL Compromised Systems List*** This blocklist lists the IPs of computers that are sources of Distributed Denial of Service (DDOS) attacks, viruses or worms, or that appear to be hacked or infected with a trojan that allows spammers to send spam through them.

- ***SORBS Zombie Netblocks blocklist*** List of IP ranges that have been hijacked and are controlled by users other than the registered owner.

- ***Five-Ten-SG Ignores Spam Complaints List*** Blocklist of sites that do not respond to spam complaints. When I last checked, most of Sprint was listed here, among other major sites -- I do not recommend using this blocklist unless you want to block a lot of legitimate email. (Sites that don't respond to spam complaints **should** be blacklisted, but it is not practical to do so at present.)

- ***Five-Ten-SG Other Issues*** Blocklist of sites with other, unspecified spam-support issues. Since I could not determine what sites were on this list or what the criteria were for inclusion, I do not recommend using this list.

RFC-Ignorant.org - These blocklists are unique -- they target computer systems and services that do not properly implement the RFCs (the "building blocks" of the Internet), rather than those that send spam.

Systems that do not implement the RFCs properly often are misconfigured in other ways and therefore easily abused by spammers. In addition, many of these systems lack any publicly available, valid email addresses that you can use to contact the system administrator when there's a problem.

There are five blocklists on rfc-ignorant.org:

- ***abuse.rfc-ignorant.org*** Blocklist of domains that have no valid abuse@ address.

- ***dsn.rfc-ignorant.org*** Blocklist of domains that reject bounces -- automatic error messages generated by mail servers when email is sent to a non-existent address or domain.

- ***ipwhois.rfc-ignorant.org*** Blocklist of IP blocks with no or invalid whois information.

- ***postmaster.rfc-ignorant.org*** Blocklist of domains that have no postmaster@ address.

- ***whois.rfc-ignorant.org*** Blocklist of domains that have no or invalid whois information.

All-In-One Blocklists - The following list is the Swiss Army knives of blocklists -- it contains multiple types of listings. SPEWS is extremely aggressive and, unless you configure your system carefully, you are likely to block legitimate email by using it. SPEWS often lists a spammer who moved to a new ISP before the other lists do.

- ***Combined Blocklist (CBL)*** The CBL is a combined blocklist that draws from a number of other blocklists, and that contains spam sources, open relays, open proxies, and other frequently abused sites. If you want a single, reliable, and relatively conservative blocklist, this or the EasyNet blocklist (discussed next) are your best bets.

- ***Spam Prevention Early Warning System (SPEWS)*** Blocklist of sites that either are spamming actively or that the SPEWS maintainers believe are likely to spam, based on past experience. This is another "Swiss Army knife" blocklist that is aggressive and may result in substantial quantities of legitimate email being classified as possible spam.

  There are actually two SPEWS blocklists. The Level 1 blocklist contain only IPs and IP ranges that the SPEWS maintainers believe belong to or are completely controlled by spammers. The Level 2 blocklist contains sites that the SPEWS maintainers believe are "spam friendly", but that also contain non-spamming users.

Whitelists

One way to ensure email messages from trusted sources are always delivered is to use a “whitelist” for automatic delivery approval.

Anti-spam whitelists contain the IP addresses (and, in some cases, the domain names) of the following types of servers:

- Private SMTP servers whose owners have guaranteed not to spam
- ISP SMTP servers that fall within a blocklists blocks through no fault of their own, and that have acceptable and enforced no-spamming AUP/TOS posted publicly on their web sites
- Bulk email sources whose owners have clear policies forbidding spam and requiring confirmed opt-in for all subscriptions

Accepting email sent from white listed servers without further filtering can be a highly effective way to reduce false positives resulting from aggressive blocklists and pattern matching filters. This also reduces load on your mail server and speeds delivery of email.

Prominent Whitelists

- ***AHBL Exemptions whitelist*** The AHBL operators maintain a whitelist of trusted email hosts and domains with strict anti-spam policies. They do not make their standards for listing on this whitelist public, but they are long-time anti-spammers with extremely strict standards about a site's policies and practices regarding spam.

- ***Habeas, Inc.*** Habeas takes a different approach to fighting spam by providing a means to identify email that is **not spam** and whitelist that email. Users either include a set of headers in their email that are trademarked by Habeas, or register their SMTP servers with the HUL. Habeas has committed to suing anyone who uses the Habeas SWE warrant mark to send spam, or sends spam via a server listed in the HUL, for trademark and copyright violations.

- ***Ironport Bonded Sender List*** The Ironport Bonded Sender program requires that participants send email only to users who have consented to receive it. It restricts the methods that may be used to obtain that consent, forbids participants to sell their email lists to third parties, and imposes a number of other requirements intended to prevent spam, including a fine of $20 per email for spam complaints.

- ***The Web-O-Trust whitelist*** The Web-O-Trust whitelist is unique, in that it contains the IPs of SMTP servers vouched for by those system administrators whom the Web-O-Trust operator considers trustworthy, *and* the IPs of SMTP servers whom those system admins consider trustworthy, and so on....

Reputation-based Control

A variation on the whitelist/blacklist approach is the use of a reputation-based control system. This provides several advantages over using content filters only.

Content filters face a natural trade-off – the more aggressive they are at blocking spam, the greater the risk of inadvertently blocking legitimate email. Content filters are also highly CPU intensive, requiring additional hardware investments and sometimes delaying the delivery of critical messages. Finally, content filters are defenseless against dictionary harvest attacks, denial of service attacks and other important risks to an enterprise.

The overall effectiveness of content-based filters can be enhanced when used in combination with a reputation-based mail flow control system. Reputation-based systems are the next generation of "identity-based" spam-fighting approaches like blacklists and whitelists and make decisions based on comprehensive information about the source of the message.

Unlike blacklists and whitelists reputation filters rely on objective data to assess the probability that a message from any given IP address is spam. This probability is based on data such as how many messages a mail server is sending, how many complaints they get, whether or not the mail server is sending to "honeypot" accounts, where the sending organization is located, how long the organization has been sending email from a given location and a number of other factors.

Using a reputation filter in combination with a content filter has numerous benefits for an organization. These benefits include:

• **Improved catch rate -** Reputation filters introduce important new sources of data tied to a sender's IP address that can be used to block egregious spam directly or as an input into third-party anti-spam systems.

• **Reduced false positives -** Because reputation-filters are probability-based (not binary like black & whitelists), receiving MTAs (Message Transfer Agent) can limit the rate they receive messages from someone without blocking their messages. This creates a prohibitive cost for spammers while ensuring that critical email still gets delivered.

• **Lower hardware costs and increased message throughput -** Research from IronPort Systems indicates that a well-designed reputation filter identifies over 50% of a typical corporation's email as either "known good" or "known bad" based on the message source. Messages from "known bad" senders can be blocked at the gateway, while messages from "known good" senders can bypass content filters. This configuration halves the number of messages that must be sent through content filters, doubling the throughput of a typical enterprise's messaging infrastructure.

• **Reduced risk from denial of service or dictionary harvest attacks -** By rate limiting based on a sender's source IP, the reputation filter can throttle senders with bad reputations, minimizing the damage from malicious attacks.

Key Components Of A Reputation-based System

When deploying reputation-based mail flow control system, there are several things companies should evaluate. Any solution should be:

• **Non-spoofable -** The email sender's reputation should be based on the IP addresses of the email sender. Because SMTP is a two-way conversation over TCP/IP, it is nearly impossible to "spoof" an IP address – the IP address presented must actually be controlled by the server sending the message.

• **Comprehensive -** The more data that is maintained about a sender's reputation, the better the decisions that can be made about a message from that source. At a minimum, any reputation-based system should track data on complaints, message volume, messages

sent to "Honeypots", sender location and open proxy status.

• **Reliable -** A reputation filter should provide fast and reliable access to network data. Where possible, reputation data should come from one source, limiting the number of threads that must be opened to process an incoming message.

• **Variable -** The richness of the data in the reputation assessment should allow for a graduated response to spam – the more suspicious a sender appears, the more restricted their access. A company may choose to block senders with terrible reputations, while limiting the number of recipients/hour for senders with bad reputations.

SenderBase™ from IronPort Systems is a powerful new sender reputation service that provides a variety of data on the identity of any sender, allowing email administrators to establish trust levels for a given sender much as a credit rating service allows a merchant to establish credit worthiness of a customer.

The data is free and can be accessed at **www.senderbase.org.** It can be used as the foundation of a reputation--based mail flow control system that can be used to determine access privileges granted to any sender.

These privileges range from unlimited delivery rates with unlimited attachment sizes and bypassed content scanning to limited delivery rates with no attachments and full content scanning to the complete refusal of incoming connections from the sender.

The next generation of spam control solutions will need to move beyond just content filtering in order to be effective. Reputation-based information makes existing filters more effective and will form the foundation of more sophisticated mail flow control systems. When used in conjunction with a content based system, the net result is a more accurate and more secure solution for incoming mail filtering.

Spam Solutions Overview

There are a tremendous number of spam solutions available today. One easy way to look at potential solutions is to categorize the solutions:

- Spam Filters
- Spam Blockers
- Spam Appliances

Spam Filters

A spam filter tags incoming spam based on its internal rules and places it into a junk mail folder for each user or, in a corporate solution, deletes known spam and places suspect mail in a folder that can be searched for false positives.

The spam analysis rules can usually be influenced by the individual or company employing this solution.

Three of the more popular spam filters for business use are:

- Surf Control
- Cloudmark Authority
- GFIMail Essentials

Surf Control

Organizations are exposed to risk each time an employee sends or receives an e-mail. Surf Control targets both email and web content and source, all e-mail - incoming, outgoing and internal.

Those risks can include:

- Viruses in e-mail attachments
- Productivity and bandwidth losses from spam
- Leakage of confidential information
- Lawsuits in response to offensive content

E-mail Filtering lets you automatically and intelligently manage the threats in e-mail as defined by your policy. By managing e-mail traffic, the risks to productivity, network resources, legal liability and security can be significantly reduced.

Content Range and Customization
User-customizable dictionaries pre-populated with keywords and phrases found in risk e-mail - covers 16 categories ranging from "adult" to "finance". It also supports Boolean language filtering.

Viruses and malicious code are serious and constant threats that plague all organizations. Viruses can run rampant through an e-mail network and a successful attack can cost an organization a great deal in lost network resources and user productivity. Surf Control's anti-virus agent used in conjunction with SurfControl E-mail Filter provides complete e-mail security management.

Protect your company from spam and junk e-mails such as chain letters, jokes, image files and screen savers that can clog your network and decrease your employee productivity. Anti-spam Agent's unique digital signature filtering ensures accuracy and efficiency thus reducing time and resources in reviewing false triggers and provides scaling performance. The single click configuration saves your time and resources.

Adaptive Reasoning Technology
Objectionable content can emerge overnight - putting your organization at risk. To prevent this, Surf Control's Adaptive Reasoning Technology dynamically updates your filtering tools as new content appears. Here's how:

Virtual Learning Agent is a unique adaptive reasoning technology that uses neural networks to filter spam mail and protect from other email risks - like confidential loss. The VLA can also be used as a content development tool to be trained on a repository of your organization's confidential data to build an extremely accurate neural network.

Virtual Image Agent - Reduce potential legal liabilities by filtering out inappropriate adult images from your e-mail network. Using intelligent scanning technology, the VIA's sensitivity settings enable filtering based on your standards.

Extensive Reporting
Precise, detailed, fully customizable and easy to use and understand. Remote capabilities, too!

Flexible, Easy to Use Rule Criteria
Apply any e-mail usage criteria: content type, file type, bandwidth allocated, time-of-day, time spent online, groups or employees affected - it's up to you!

More information is available at www.surfcontrol.com

Cloudmark Authority

Cloudmark Authority is easy to install, nearly transparent in operation, and requires only occasional updates.

Authority plugs into existing email hardware and software and seamlessly integrates with your existing email system. It requires no additional hardware, firewall configurations, costly professional services, or constant tweaking and updating like other spam fighting products.

Authority runs in memory and its lean runtime requirements only impact MTA performance by 5-10%, making it far and away the performance leader when compared to the usual impact of 40+% that competing applications consume, along with their needs for additional hardware and support.

Operationally, Authority is simple: it receives a stream of SMTP messages from an SMTP source, analyzes the messages and assigns each message a confidence level, applies an action to the message based on the confidence value, and then returns the filtered stream back to the same SMTP source.

To eradicate spam in a cost-effective way and in accordance with corporate policies requires a server-based solution that intercepts spam at the corporate gateway, preventing it from entering the corporate email system.

An appropriate server-based enterprise anti-spam solution must be scalable, capable of processing a high volume of incoming email without impeding its velocity. Migrating rules-based email filtering from the desktop to the enterprise network is inconsistent with these essential requirements.

Cloudmark Authority introduces the first-ever automated process of capturing, analyzing, and predicting spam to generate powerful spamDNA. Drawing on the advanced biotechnology techniques used to map the human genome, Authority's breakthrough third-generation Genetic Classification technology stops spam at the gateway for large enterprises.

Easily implemented, Cloudmark Authority installs into the existing network infrastructure, requires no investment in additional hardware, operates inside the corporate firewall, and preserves email and network security.

Designed to handle high-volumes of email, Authority requires minimal administrative intervention and quickly pays for itself in restored employee productivity and reduced network traffic.

Key Features:

- highly scalable software
- unparalleled accuracy
- low cost of ownership
- customizable mail-handling policies
- rich end-user management

Instead of depending on this near-continuous stream of updates, Authority only requires updating about once a month. Updating the spamDNA file, called a "cartridge," couldn't be simpler:

- **Windows** - The spamDNA cartridge is a single .dll (dynamic link library) file of about 450 Kbytes. The new cartridge is installed as an update of the previous cartridge without taking Authority out of service.
- **Linux, Solaris** - The spamDNA cartridge is a single .so (shared object) file of about 450 Kbytes. The new cartridge overwrites the previous cartridge without taking Authority out of service.

Authority is a highly cost effective solution, especially for deployment in large organizations. Authority is typically deployed in companies with greater than 1,000 mailboxes and is priced as such.

More information is available at www.cloudmark.com

GFiMailEssentials

GFI MailEssentials offers spam protection at server level and eliminates the need to install and update anti-spam software on each desktop.

GFI MailEssentials offers a fast set-up and a high spam detection rate using Bayesian analysis and other methods – no configuration required, very low false positives through its automatic whitelist, and the ability to automatically adapt to your email environment to constantly tune and improve spam detection. GFI MailEssentials will eliminate over 98% of the spam from your network.

In addition to anti-spam, GFI MailEssentials adds key email tools to your mail server: disclaimers, mail archiving and monitoring, Internet mail reporting, server-based auto replies and POP3 downloading.

GFI MailEssentials is the market-leading server-based spam solution. More than 20,000 companies worldwide use GFI MailEssentials to protect their mail servers from spam.

Server-based anti-spam
GFI MailEssentials is server-based and installs on the mail server or at the gateway, eliminating the deployment and administration hassle of desktop-based anti-spam products. Desktop-based anti-spam involves training your users to create anti-spam rules sets, and subsequently users have to spend time updating these rules. Besides, this system does not prevent your server message stores from filling up with spam.

Bayesian filtering technology
GFI MailEssentials features Bayesian filtering technology to detect spam based on message content. Rather than just checking for keywords, GFI's Bayesian filter takes the whole message into consideration as well as the content of valid emails that you send (known as 'ham').

This gives it a tremendous advantage over other anti-spam solutions that only take spam into account. Bayesian filters are widely acclaimed to be the best way to tackle spam because they use statistical intelligence to analyze the content of the mail.

Downloads updates to spam profile database
GFI MailEssentials can download updates to the Bayesian spam profile database from the GFI site, ensuring that it recognizes the latest spam and spamming techniques. GFI maintains the spam profile database by working with a number of spam collection organizations that continually supply spam samples.

Sort spam to users' junk mail folders

GFI MailEssentials gives you the flexibility to choose what to do with spam. You can delete it, move it to a folder, forward the spam mail to a public email address or folder, or send it to individual customizable folders (for example, a "junk mail" folder) in the end-users' inboxes. This allows users to easily review mail that has been flagged as spam.

3rd party DNS blacklists (DNSBL) checking
GFI MailEssentials supports third party DNS blacklists (real time black hole lists), which are databases of known spammers. If the sending mail server is on one of those lists, GFI MailEssentials marks the email as spam. GFI MailEssentials supports popular third party blacklists such as ORDB, SpamHaus, SpamCop, or RBL. GFI also supports custom blacklists.

Block foreign language spam
GFI MailEssentials can block mail that uses particular character sets. For example, you can greatly reduce spam simply by blocking all mails written in Japanese, Russian, Korean, etc.

Automatic whitelist management reduces false positives
Whitelists enable you to ensure that mail from particular senders or domains are never flagged as spam, permitting more stringent anti-spam rules. GFI MailEssentials includes a patented automatic whitelist management tool, which automatically adds all business partners to your whitelist. This greatly reduces false positives, without any need for additional administration.

Fake non-delivery reports (NDRs)
GFI MailEssentials bounces spam back to the sender with a false non-delivery report. This NDR leads them to believe that your address is invalid, and gets your organization's addresses off spam lists.

Company-wide disclaimer/footer/header text
GFI MailEssentials enables you to add disclaimers to the top or bottom of an email. Text and HTML formats are supported. You can include fields/variables to personalize the disclaimer. You can also create multiple disclaimers and associate them with a user, group or domain.

Mail archiving to a database
GFI MailEssentials allows you to archive all inbound and outbound Internet mail. This enables you to keep a back-up of all email communications and easily search for a required message. This also allows you to comply with SEC and other regulations that require you to archive email correspondence.

Reports on spam filtering and mail usage
The GFI MailEssentials reporter creates advanced reports on your inbound and outbound email. You can report on how much spam you filtered and what rules caught most spam. You can generate reports on user, domain and mail server usage.

Mail monitoring
The mail monitoring feature enables you to keep a central store of the email communications of a particular person or department. Because you can configure the mail to be copied to an email address, all email can be stored in an Exchange or Outlook store, so that you can easily search for email or content.

Personalized server-based auto replies with tracking number
With server-based, personalized replies, you can advise your customers that their message has been received and who will handle it. GFI MailEssentials assigns a tracking number to each reply and can also include attachments.

POP3 downloader
GFI MailEssentials includes a utility that can download mail from POP3 mailboxes. It supports both single and multiple recipient POP3 accounts.

Seamless integration with Exchange Server 2000/2003 & 5.5
GFI MailEssentials integrates seamlessly with Microsoft Exchange 2000/2003: It installs on the Exchange SMTP service and does not require gateway configuration. Via the SMTP protocol, it also works with Exchange 5.5, Lotus Notes and other popular SMTP/POP3 servers.

More information is available at www.gfi.com

Spam Blockers

A spam blocker system prevents the delivery of spam to your PC or network by blocking spam before email is received. Email is routed through a remote system which analyzes the messages and diverts a high percentage of the incoming spam.

The primary advantage of this approach is a higher level of protection against virus and malware attachments since they are not allowed to reach the network or user level. Similarly, offensive messages are also disposed of without exposure risks.

The spam analysis rules are controlled by the spam blocking company.

Three popular solutions are available from:

- MailControl Spam
- Brightmail
- Postini

MailControl Spam

MailControl Spam from BlackSpider Technologies is a fully managed service designed to provide companies with the highest level of protection at a cost effective price.

This adaptive approach combined with the ability to set spam thresholds on a domain and per-user basis, ensure that MailControl Spam is the most effective spam filtering technology on the market today.

The whole scanning process takes just a few seconds. Once each message has been analyzed by the different tests, the message receives an overall 'spam score'.

The score is then compared against the spam threshold defined by the customer; mail scoring below the configured threshold is delivered as normal, whilst mail scoring above is quarantined as spam.

The MailControl Spam service works by processing e-mail through a number of filters, which include:

- Black and White Lists
- Adaptive Spam Engine
- Real Time Black Lists
- Lexical Analysis
- Bayesian Probability
- Distributed Checksum Clearinghouse
- Collaborative Spam Databases
- Spam Traps
- Trend Analysis

Managing Spam
Spam thresholds can be configured at a domain level and at a user level. This approach enables administrators to 'tune' the threshold for users who receive a significant amount of spam.

E-mail messages classified as spam can be dealt with in a number of ways. Most customers choose to quarantine the e-mail automatically and send a daily or weekly report to the intended recipient listing the messages which were blocked and providing a link back to the portal where the message can be viewed and released if required.

Alternatively a customer may elect to receive spam, but have it highlighted by a comment in the subject line. e.g. 'Spam:'

In summary, MailControl Spam controls the flood of unwanted e-mail messages, increasing employee productivity, return on assets and reducing costs.

More information is available at www.blackspider.com

Brightmail

Brightmail's spam blocking solution is available as an appliance or as server-based software. It's used by six of the top ten ISP's and, as a result, filters approximately 10% of all email. While not inexpensive, it is a high-quality solution.

Catches the Most Spam
Brightmail's complete spam defense leverages a cocktail of effective technologies, a huge spam detection network, and a real-time rule delivery mechanism.

- Six separate technologies target different types of spam
- Proactive heuristic and machine learning technologies trap evolving spam
- Patented spam signatures stop real-time spam attacks
- Dynamic list of open proxy servers identifies & locks out known senders of spam
- Intelligent filters identify foreign language spam

Highest Accuracy
False positives (messages incorrectly identified as spam) cause users to lose faith in spam blocking. From day one, Brightmail has had an unwavering commitment to protecting legitimate mail. Many Brightmail customers feel comfortable deleting spam without review.

- Automated and manual safeguards
- Support for false positive submissions
- Review (by a Brightmail technician) of every false positive
- Corrected rules deployed globally within minutes
- Only introduces a new technology after it has passed rigorous accuracy standards

Zero Administration
Many anti-spam solutions place even more burden on administrators. Immediately effective out-of-the box and constantly updated, Brightmail doesn't require any tuning or training of filters by administrators.

- 24/7/365 protection from new spam attacks
- Automatic, timely, secure updates
- New filters available every 10 minutes
- Global anti-spam operations centers in the US, Ireland and Australia
- Real time visibility of new spam trends
- No ongoing tuning or training of filters

More information is available at www.brightmail.com

Postini

Postini's spam blocking service utilizes an intermediate step in email delivery, passing all incoming and outgoing mail through Postini's data center.

Postini™ services secure and manage email systems, without the need for software or hardware. Using patent-pending pass-through technology (versus store-and-forward methods), email bound for a company's email server is processed in real-time through a highly secure service architecture.

Within milliseconds, Postini's award-winning email security solution separates spam and viruses from legitimate messages. Legitimate email is instantly passed on to the destination mail server. Suspicious email can either be quarantined in a web-based, password-protected message center for administrator or end-user review, or tagged and delivered. The entire process is fully automated — valid emails pass through and cannot be physically accessed by any persons other than the recipient.

Postini™ now offers Perimeter Manager Enterprise Edition, our flagship email security service. Enterprise Edition is the next-generation in email security, utilizing revolutionary patent pending technology including Postini Industry Heuristics™, outbound and policy management, and integrated disaster recovery services. Enterprise Edition comes with the industry's best service commitment – a 99.999% service level agreement, and now also includes full 24/7 customer support.

With Enterprise Edition, you can:

- Block malicious or unwanted email messages before they penetrate the corporate firewall, improving employee productivity, minimizing IT management and maintenance costs, saving bandwidth, server and disk capacity, while keeping security threats away from the network.

- Maximize email filter accuracy and minimize false positives with patent-pending Postini Industry Heuristics™, industry and function specific heuristics-based analysis technology that enables the creation of content filters specific to industries and functions such as law and financial services, and from 'trusted networks' of senders based on proprietary Postini knowledge of SMTP content and transport patterns in these industries.

- Filter outbound email and implement policy controls with full-duplex security and content-management tools, giving IT administrators the tools to lock down and protect all aspects of the corporate email system. Filter all outgoing email communications for viruses and other policy violations.

- Maintain and protect the integrity of the enterprise email infrastructure with an integrated disaster recovery service. If your email server ever goes offline due to a break in network connectivity, or server malfunction or overload, Postini will step

in seamlessly and redirect all incoming email to a secure, architecturally redundant message store at the Postini data centers until connectivity is restored.

- Enhance productivity by providing end-users with an html-based Quarantine Summary Report. This report eliminates the need to log-in and review messages in the Postini Message Center.

- Gain exceptional management and system-level control over your email infrastructure to ensure the highest levels of trust, reliability, flexibility and security. Postini's extensive reporting and management capabilities allow email system administrators to monitor the Postini service and their entire email infrastructure in real-time, regardless of server platform or system topology.

More information is available at www.postini.com

Spam Appliances

A spam appliance can function as a spam filter or as a spam blocker and is intended for businesses with high email volume. This hardware-based solution applies filtering rules to incoming mail at the MTA (Message Transfer Agent)

The spam analysis rules are often customizable by the company receiving spam.

Three popular spam appliances are available from:

- Barracuda Networks
- Ironport Systems
- Tumbleweed Communications

Barracuda Networks

Barracuda has a spam appliance called the Barracuda Spam Firewall that is inexpensive and easy to deploy for corporate networks.

Highly scalable system
The Barracuda Spam Firewall's robust and scalable design enables it to handle email networks of over 10,000 active email users. It can process over 10 million email messages per day. There are different models for different mail loads. Multiple Barracuda systems can be employed and easily configured for redundancy or additional load capability.

No software to install and no modifications to your existing email system
Deploying the Barracuda Spam Firewall is easy. Just plug in your Barracuda Spam Firewall, accept the default settings or make any changes you'd like and you're ready to

go. There is no software to install. There are no modifications to your existing system. It's that easy. Most customers are up and running in only 5 minutes.

Independent network device dedicated to spam-blocking
The Barracuda Spam Firewall is a self-sufficient networking device that handles all your spam-blocking so it does not bog down your email servers. In fact, with the Barracuda Spam Firewall, the load on your email system is actually reduced. Your email servers will process and store less incoming email. The performance of your email servers will increase.

Blocks spam using proven methods
By using all the best methods to block spam, the Barracuda Spam Firewall provides comprehensive spam-blocking for your company. Below are the primary algorithms we employ to block spam:

- **Blacklisting of websites & domains**: Barracuda Central maintains an up to date list of the largest and most aggressive known spammers. This list is maintained by both Barracuda and other anti-spam groups. This list is automatically updated on each Barracuda Spam Firewall.

- **Keyword scanning of emails**: This can be configured on a per user basis. Our scanning methods include a scoring system such that emails are scored based on a number of criteria. If the score is above a threshold, then that email is flagged as spam. The Barracuda Spam Firewall comes with default criteria and thresholds but you may change these.

- **Checksum technology**: Barracuda uses checksum technology to keep track of the number of times a particular message has appeared on the Internet. If a message has appeared over a certain number of times, it is categorized as known spam. Checksums of known spam messages are utilized to block spam messages.

- **Message authenticity checking**: Several algorithms are utilized to verify the authenticity of a message. Some of these are simple checks to verify that the "from address" is authentic. Some are more complex relating to SMTP protocol.

- **Blacklists and Whitelists**: Domains, IP's, and email addresses can be blocked or whitelisted (allowed through). These lists may be maintained on a per user basis or on a corporate basis.

- **Rate controls**: Utilized to stop denial of service attacks as well as dictionary based spam attacks. These are integrated and automatic in the Barracuda Spam Firewall.

- **File type attachment blocking**: You can block certain types of files, such as vbl scripts, from entering your company.

User-based and corporate-based filtering
The decision on what types of emails to block can be made either at the end-user or at various corporate levels. You have the flexibility to decide where you'd like the decision to be made.

Suspect emails get quarantined
There are three main types of emails: emails that you want, emails that you do not want (spam), and emails that are suspect. The Barracuda Spam Firewall can tag suspect emails for delivery into a separate folder. You can then either have the end user or another designated person be the final judge of what to do with these suspect emails. If after 30 days no action is taken, the message is deleted.

Optional bulk mailboxes for users
Barracuda Spam Firewall provides optional bulk inboxes so that users can direct spam messages straight into these areas. This prevents spam from cluttering up their main mail system. These bulk email boxes can be checked periodically or ignored.

Automatic system updates
A team of engineers monitor the Internet for trends in spam and virus attacks. As they detect trends, updates are created for the Barracuda Spam Firewall which then automatically updates itself without any intervention. Maintaining your Barracuda Spam Firewall to deliver maximum protection is that easy.

Logs and reports on email statistics
System administrators can view logs or generate reports at any time from the desktop. It's quick, easy, hassle-free administration.

No per user charges
Barracuda Spam Firewall pricing is simple. There are three Barracuda Spam Firewall models. Each one is designed to handle different active user and email loads. Pricing ranges from $1199 for the smallest model to $3999 for the largest model. There are no per user charges. Each model comes with both spam-blocking and virus-checking capabilities.

Multiple domains & servers
A single Barracuda Spam Firewall can also be used for multiple email servers and for multiple domains.

More information is available at www.barracudanetworks.com

IronPort Systems

IronPort Systems makes both high-volume mail appliances as well as spam appliances. They also own the SpamCop filtering software.

The IronPort C-Series™ Messaging Gateway™ appliance is built on IronPort's revolutionary MTA platform. It enhances security by preventing suspicious traffic from entering the network. It also detects spam and viruses and enforces corporate policies.

MTA Platform
IronPort has built the C-Series from the ground up to address the requirements of the modern email gateway and to position our customers for the future of SMTP.

Threat Prevention
Unique Reputation Filters™ technology identifies suspicious traffic patterns. Suspect senders are throttled or blocked, preventing malicious traffic from even entering the network.

Policy Enforcement
The IronPort C-Series includes the world's fastest content scanning engine. This flexible engine allows for fine grained enforcement of corporate policies based on keyword searches of messages or attachments.

Spam Detection
Fully integrated industry leading spam detection powered by Brightmail® anti-spam. Most accurate spam detection available. Eliminates the headache of spam without false positives.

Brightmail® is the industry leader in anti-spam technology. Their technology protects over 280 million mailboxes and 1,400 businesses from the productivity loss and the IT costs of unsolicited commercial email (spam).

Brightmail on AsyncOS
The IronPort C-Series includes integrated Brightmail spam-fighting technology. Optimized for IronPort's AsyncOS™ operating system, Brightmail technology is extremely high performance and highly accurate. Automatic rule updates are integrated into the platform requiring zero administrator intervention.

Lowest False Positive Rate
False positives cost companies money in lost productivity and lost opportunities. Brightmail has the lowest false positive rate in the industry with less than one in one million messages being a false positive. This accuracy is only achievable by Brightmail because of the real-time methods they use to identify spam through their Probe Network™.

Lowest Total Cost of Administration
Brightmail runs the world's most advanced anti-spam operations center (BLOC) which delivers the most complete and up to date set of filters. The BLOC runs 24x7x365 analyzing spam, generating rules, and ensuring a low false positive rate. Brightmail writes 30,000 new rules per day so you don't have to.

Spam Handling Flexibility
Administrators have several choices on how to handle messages that are flagged as spam by Brightmail. Choices include sending the message to a per-recipient web quarantine, marking up the subject header, adding an additional "X-header", sending the message to an alternate folder in the user's mailbox, deleting or bouncing the message, or a combination of these actions.

Quality Reporting
The Brightmail system shares information with the IronPort C-Series Mail Flow Monitor making real-time and historical reports instantly available at any time.

More information is available at www.ironportsystems.com

Tumbleweed Communications

Tumbleweed's E-mail Firewall for Anti-Spam provides highly effective spam blocking and management capabilities, while easing the management burden associated with fighting the daily deluge of junk mail.

It was recently voted the #1 anti-spam solution by Network World magazine.

Developed to provide industrial-strength network protection, for corporations with over 100 mailboxes, this powerful technology exceeds the five core requirements for enterprise-level spam management:

Accurate Spam identification: Keep the "bad" email out, while letting legitimate email in. The key to minimizing the risks and costs of spam to the enterprise is successfully blocking spam while maintaining zero "false-positives."

Easily tailored for your enterprise: Different organizations define spam in different ways. Tumbleweed solutions are flexible enough to allow enterprises to easily create policies based on their unique spam definitions.

Control of anti-spam actions: You can configure your anti-Spam solution to take different actions depending on the type and content of the spam detected.
Enterprise-class gateway: Tumbleweed ensures that your mission-critical email stream remains reliable.

Minimize administrative costs: At the heart of Tumbleweed's award winning anti-spam solution is the Dynamic Anti-spam Service (DAS). DAS automates the process of analyzing and identifying spam, delivering a highly effective anti-spam solution with a low total cost of ownership (TCO).

Key Features of the email Firewall for Anti-spam:

- Stops 95% of spam
- Award winning spam analysis engine with auto-updates
- Custom Whitelists (user, group, corporate)
- Custom Blacklists (user, group, corporate)
- Realtime Blackhole Lists
- Flexible actions so each end-user gets what they need
- Reverse DNS Lookup
- Content filtering
- Anti-virus
- Anti-hacker
- In-depth reporting on email trends, spam volumes, and policy violations
- High performance SMTP Relay
- Key Benefits
- Email protection and security in one integrated solution
- Save employee time and boost productivity
- Comprehensive network protection
- Protect your intellectual property through flexible and secure email delivery
- Enforce communications policies to minimize compliance risks and liability
- Easily integrates with existing email systems (Exchange, Domino, etc)
- Easy remote administration and monitoring through a secure web-based interface
- Flexible policy actions to eliminate false positives
- Low administration with automatic updating of spam heuristics

Available as both Appliance and Software
Tumbleweed's Email Firewall for Anti-Spam comes as both an appliance and software.

More information is available at www.tumbleweed.com

Summary

The large number of spam solutions in the marketplace requires due diligence before making a decision about your preferred solution. Make a comprehensive list of your requirements, budget requirements, etc. and use it in determining which solution is best for you.

If you require assistance, Net Sense delivers IT consulting services in this and several other areas listed at the end of this document.

Net Sense Consulting Offerings

Spam Prevention
Best Practices Audit
Email Filters & Appliances
Reputation-based Control

Anti-Virus Protection
Solution Assessment
Implementation Support
Data Recovery

Wireless Networking
Security Testing & Upgrades
Authentication Strategies
New Deployments

Remote Access
Secure Dial-up
VPN Implementation
Remote Office Connectivity

Network Security & Integration
Security Audits
Firewalls
Network Intrusion Detection
Password Policies & Authentication

Network Design & Installation
Web Filters
Process Improvement
Automated Security Patch Updates
Installation Scripting

Hardware/Software Consulting
Supplier Audits
Software Licensing Compliance
Procurement RFP Design
Expense Reduction Analysis

Onsite Support & Maintenance
Support Needs Assessment
Cost/Benefit Analysis
Maintenance SLA & RFP Review

Documentation
Acceptable Use Policy
Security Policies
Server & Router Documentation

IT Strategic Planning
Technology Plans & Updates
Strategy Mapping
Function & Process Analysis

Project Management
Major Deployments
Measurement Metrics
Vendor/Staff Coordination

Email Management
Electronic Recordkeeping
Email Usage Policies
Email Security
Application Migration

Data Protection
Disaster Recovery Planning
Archive Outsourcing Guidance
Risk Analysis
HIPAA Compliance

Cost Reduction
Process Automation
Telecom Expense Analysis
Vendor Contract Issues
Enterprise Performance Planning