

Mercury Technologies
Anti-Spam / Anti-Virus Solution

*A Mercury Technologies White Paper
August 2003*



Mercury's Anti-Spam/Anti-Virus Solution

Wouldn't it be nice to not worry about another Sobig Virus? Don't you hate having to go through all that junk email? Mercury's integrated Anti-Spam/Anti-Virus service for corporate email hosts keeps your productivity high at a low cost that simply can not be achieved using most in-house solutions yet provides features and quality surpassing virtually any other similar solution. We mean it - we've looked at them all!

Mercury's Anti-Spam filters are updated daily and are packaged with all the essential self-management features such as white-list and blacklist management. The Anti-Virus service combines two industry leading anti-virus engines that are updated every ten minutes. Contact us for a free thirty day demonstration.

This is an overview of the features supported by our service.

Features

Spam Filtering

Our spam filter automatically eliminates "junk" e-mail or "spam" from each users mailbox, protecting workers from unwanted distractions and interruptions. With the ever-increasing amount of unsolicited e-mail arriving daily, protection is an important means of saving time and staying focused on important work at hand.

As e-mail passes through our mail routers, our proprietary spam filter automatically scans inbound e-mail and separates out any spam found.

Spam is filtered in a three-step process. The first step is a collection of thousands of "bait" e-mail addresses. These e-mail addresses are used to actively look for spam. Spam is captured and run through a process in which a fingerprint is created and added to a master database for each message.

The second step is a process in which each new e-mail message that enters the network is fingerprinted and cross-reference in the database to see if there is a match. If there is a match, the message is marked as spam. If there is no match, the message proceeds to step three in which it is run through a series of tests where different aspects of the message including the header, subject, and content of the message are analyzed. These tests give the message a score that in turn determines if the message is spam. Spam messages are fingerprinted and added to the database. Clean messages are queued for delivery to the client. This whole process, on average, takes less than a second to perform.

Administrators have four options in regards to the spam:

- 1) The first and most popular is called SpamTank. With this option, spam is held on the Gateway servers. As spam is identified, temporary junk e-mail boxes are created for each user. Users are notified that they have junk e-mail on the server and are given a link to a web-based control panel where they can check it. The administrator sets

the notification interval. Spam is held on the Gateway Servers for 30 days before it is deleted.

- 2) The second choice is to redirect all spam to a single e-mail address. For example, spam@yourcompany.com
- 3) The third option is to insert an x-header. Rules can be written on the destination mail server to reroute mail via the x-header variable.
- 4) The fourth option is a subject modification. For example, the word JUNK could be inserted before the subject so that the individual users could easily identify Spam messages

Spam Accuracy Metrics:

Percentage of Spam Caught: 98%

False Positives: .001% (1 in 100,000)

Virus Scanning

Mercury's Virus Filter detects and eliminates viruses before they enter the client's network. The system utilizes two leading virus scanners on the market: Trend Micro and Sophos. Mercury's network receives virus definition updates every 10 minutes. All inbound e-mail as well as attachments are scanned through both engines insuring the most complete protection possible. Each anti-virus partner maintains global research and solution centers to ensure viruses are identified as early as possible and solutions are implemented as quickly as possible. Mercury's anti-virus libraries are updated far more frequently and more efficiently than is possible within a typical company.

Attachment Blocking & Filtering

The Attachment Filter is positioned to reject messages with certain types of file attachments before they enter the corporate e-mail system. This feature is the first layer in of defense to insure potentially destructive files, such as ".vbs" and ".exe", do not gain access to the customer's e-mail infrastructure.

This feature is defined by domain. Customer's can add or delete file types as well as file names in order to fine-tune the filter. E-Mails with blocked attachments are sent to Quarantine for administrative review.

Content Filter

The Content Filter gives administrators the ability to block messages based on content found in the message subject as well as the message body. Messages can also be blocked based on character sets (i.e. language types). Any blocked messages are delivered to Quarantine for administrative review.

Policy Filter

The Policy Filter allows administrators to block messages based on message size as well as number of recipients.

This feature is defined by domain. E-Mails with policy violations are sent to Quarantine for administrative review.

Black & White Listing

The Black and White lists give customers the ability to block or allow e-mail messages based on domain name, e-mail sender and/or e-mail recipient. Mercury offers domain wide black/white lists at the administrative level. Clients also have the option to let individual users set up their own custom black/white lists.

User Level & User Controlled Black & White Listing

We have found that this single feature is one of the most popular reasons clients choose Mercury's service over competitive solutions. This option gives each user their own personal login to the system where they can control their personal white and black lists. This relieves mail administrators from having to deal with the particular needs of every user. Putting this feature in the hands of users has been shown to produce a distinct positive perception of the services provided by the internal mail administration staff. This eases adoption by the user community since it is perceived as a positive change in their environment.

Black listed e-mails are sent to Quarantine for administrative or user-level review.

Store & Forward

The Store & Forward feature operates as a backup server, protecting the customer's network from lost or bounced e-mail. Each day, corporate e-mail servers refuse messages for a variety of reasons including: unscheduled downtime, server overload, server crashes, maintenance windows and connectivity problems - locally or to the Internet. If you currently contract for backup MX service, you will no longer need a separate backup mail service. This may decrease your operating expenses even further.

The Store & Forward feature is based upon Mercury's distributed network providing customers with unparalleled uptime and system redundancy. Undelivered e-mail is held on the network for up to ten days or longer if necessary.

Outbound SMTP

The Outbound Virus Filter scans all outbound e-mail and attachments prior to delivery. Using proprietary tools and two leading virus-scanning engines, Trend Micro and Sophos, this service enhances the capability of a company to catch and kill viruses.

Simple outbound e-mail relaying is also available for customers who want to mask their e-mail server and network information to outsiders further securing their e-mail messaging network. This service ensures the e-mail server will be masked, protecting it from unsolicited e-mail and mail bomb attacks.

Detailed Reporting

Mercury provides a unique range of web-based reporting services allowing e-mail administrators an unparalleled view into the use or abuse of their e-mail servers. Mercury provides each customer with a wide variety of online reports in order to help manage internal e-mail usage.



Mercury Technologies Anti-Spam / Anti-Virus Solution – White Paper
August 2003
Author: Philip Meese

Mercury Technologies, Inc.
32 Old Slip
11th Floor
New York, NY 10005

Inquires:
VOX: +1.212.483.0300
FAX: +1.212.483.0400
www.mercurytech.com/collaboration
collaboration@mercurytech.com

Copyright © 2003 Mercury Technologies
All Rights Reserved