e Indus
CleanMail

Guards your Email Kills Spam and Viruses

Do you need to...

Do you need to...

Scan your e-mail traffic for viruses?

Scan your e-mail traffic for viruses?

Reduce time wasted dealing with Spam?

Reduce time wasted dealing with Spam?

Prevent offensive material from entering your organisation?

ent offensive material from entering your organisation?

Indus CleanMail is the answer.

ICM

ICM (Indus CleanMail) gives you the power to monitor and filter e-mail traffic to protect your organisation from virus attacks, spam mails and wasted bandwidth right at the Internet level. ICM provides for virus-free and spam-free mail. All the unwanted emails (containing spam and virus) are filtered on our Internet server before they reach your mail server and the intended recipients.

Salient Features of Indus CleanMail

- Triple-level Virus Scanning

- Multi-layered Anti-Spam capabilities stops 90-95% of Spam

- Spam Analysis Engine with auto-updates and auto-learning

- Personal Whitelists and Blacklists allow/block emails from specific IDs/domains

- Real-time Blackhole Lists capture data from global spam servers to block spam

- Content filtering

- Reports on email trends, viruses detected, spam volumes, policy violations

How ICM Works
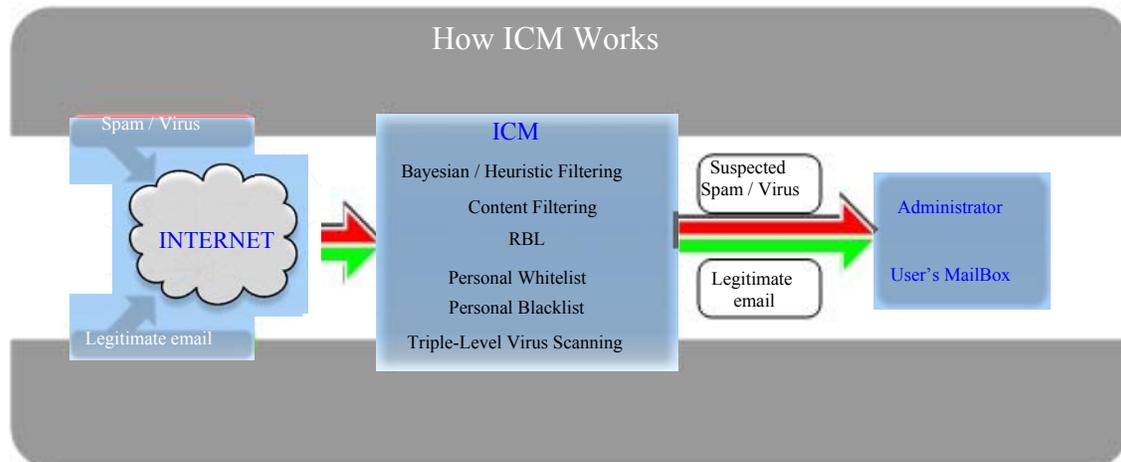
Email spam and virus are major problems, hence there is a great challenge to eliminate these twin threats. ICM provides the enterprise with excellent spam and virus filtering from an enterprise approach . In doing so , end -user productivity is increased and improved. Most importantly, security vulnerabilities can be identified, reduced and eliminated before email arrives at the corporate email servers . The primary advantage of this service is that email is examined thoroughly at the Internet level before sending it to the internal email server, hence minimising the impact of spam and viruses on the end user.

ICM

Triple-Level Virus Scanning

Scans all e-mail passing through it for viruses through three different anti-virus software to ensure maximum protection

Attachments containing viruses or other security problems are removed All safe

content is delivered untouched

While this service will remove the vast majority of known email viruses, viruses can also infect computers in other ways . For maximum protection , we therefore recommend that you also run anti-virus software on each of your computers. While no service or software can guarantee that 100% of all viruses will be caught, ICM offers an additional strong level of virus protection with its triple-level scanning.

Multi-layered Anti-Spam capabilities stops 90-95% of Spam

Completely different set of actions can be applied to spam scoring above a "High Score" threshold value.

Spam can be tagged, rejected, discarded, archived or forwarded to other addresses for inspection by administrators

With the initial, default settings, our Anti-Spam service will "out of the box" block 90 95% of all Spam. Most of the remaining Spam will actually be bypassing our service due to tricks that spammers use. The Bayesian database support in ICM tries to identify Spam by looking at what are called tokens; short phrases that are commonly found in Spam or ham. (Ham is e-mail that is not Spam.) Each token is given a small score; together these scores rate the email as Spam if above administrator defined levels.

Spam Analysis Engine with auto-updates and auto-learning

The ICM Spam Analysis is automatically updated daily with feedback from global servers. In addition, it can be trained by users who can provide it with examples of spam mai

Personal Whitelists and Blacklists allow/block emails from specific IDs/domains

An important feature of ICM is that you can create a personal "Whitelist" to ensure that your important clients and other contacts will never be blocked, even if their mail system somehow ends up blacklisted. You can Whitelist by IP address, email address and/or content. Since ICM depends partially on other organisation's " blacklists", we maintain a "Global Whitelist" for all customers, and will consider your suggestions.

The primary entries in our global Whitelist consist of :

- Major legitimate newsletters and mailing lists

- Legitimate companies in countries that are otherwise blocked

You can also create a personal "blacklist" to block email from certain sources. It does not need be Spam; it can be used to block someone who is harassing your employees. Or you might want to block recruiters who are trying to steal your employees.

- You can blacklist by IP address, email address and/or content. For example, if junk@baddomain.com is harassing you, all emails from him can be completely blocked. Such blocked emails can be re-routed to your "Spam" mailbox or completely blocked

Real-time Blackhole Lists capture data from global spam servers to block spam Content filtering

- Several organizations and companies are constantly identifying the mail servers, which are actively sending Spam. They create "real-time blacklists" (RBL) of the IP addresses of these mail servers, which are updated daily, even hourly. We have chosen four of the better known

- RBLs for selection within the ICM service. (By default, all are selected.) Our main criteria was to choose RBLs which are least likely to block legitimate email.

- A good blacklist not only quickly adds a new Spam source, but also removes it when it is no longer sending Spam. Spam is often sent through "open relays", which are legitimate mail servers, which have been (trivially) "hacked" by spammers. Typically the owner of the mail

- Server learns of this within a day and then fixes the problem. Therefore, mail systems should not be blacklisted any longer than necessary.

Content filtering

- Allows/denies attachments based on filename, providing implementation of any email security policy. Easily used to block attachments which are common ways of disguising viruses, e.g. ReadMe.doc.exe These can be varied for different users

- HTML-based Attacks

- Scans for common signs of attack such as <IFrame> and <Object Codebase=…> HTML tags. Both have been used many times to exploit vulnerabilities in Outlook (& Express) and Internet Explorer

- Dangerous HTML content can be stripped. Checks and traps added for all known Outlook, Outlook Express, Internet Explorer and Eudora security vulnerabilities.

ICM Reliability

ICM reduces the chance that you miss any email. This service uses two "relays" which will spool (i.e. "save") your email messages in the event your mail server is off-line due to power failure, system email crash, routine maintenance, or any other reason. When your mail server is back online, it will automatically receive the spooled email. (Our service will spool your mail for up to five days.)

ICM Technical Description

Email filtering is a process of monitoring incoming email and then taking the appropriate action to protect against Spam and viruses. Certain criteria are set to determine if an email is actually Spam. Each criteria has a certain weight or score. It also uses text analysis and several internet-based real-time blacklists. Tests and rules are executed on mail headers to determine and tag an email with Spam. Blocked Spam messages are logged into a database. For viruses, email messages and attachments are scanned and detected to delete and/or disinfect malicious programs.

ICM uses the following mechanisms to detect spam

Header analysis : Spammers use a number of tricks to mask their identities, fool you into thinking they've sent a valid mail, or fool you into thinking you must have subscribed at some stage. ICM tries to spot these.

Text analysis : Spam mails often have a characteristic style, and some characteristic disclaimers and CYA text. NESS can identify these tactics.

Blacklists : ICM supports many useful existing blacklists, such as mail-abuse.org, ordb.org and many, many others.

Razor : Vipul's Razor is a collaborative tracking-tracking database, which works by taking a signature of Spam messages. Since Spam typically operates by sending an nearly identical message to hundreds of people, Razor short-circuits this by allowing the first person to receive a Spam to add it to the database -- at which point everyone else will automatically block it.

Bayesian Statistics : ICM applies Bayesian Statistics against known Spam and not-Spam messages to create new rules "on the fly".

DCC : Distributed Checksum Clearing house is a system of many clients and more than 120 servers that collect and count checksums related to several million mail messages per day. ICM uses a DCC check to see if the messages have been sent to a large number of users.

All email passing through our ICM receives a "Spam score". Email below a certain score, typically 6, is not tagged as Spam and is delivered to the recipient intact. Email that typically scores between 6 and 10 is most probably Spam, but there is a very small chance that it might be real email.

ICM

There are four actions that you can take on email that is caught by our filters as Spam. These are :

Modify Subject : Specify a string to insert at the beginning of the subject line, for easy viewing or spotting of Spam messages in your regular inbox.

Forward to : Specify an email account at your domain where you would like the email message forwarded to. Instead of fully blocking Spam, it can be re-directed to a special Spam mailbox at your domain, e.g. spam@yourdomain.com. This lets you examine it to ensure that no legitimate email is being blocked. Make sure you set up the email account that you specify, before using this option. Also remember to monitor the mailbox so that it doesn't get full to where it no longer accepts any new messages and start queuing up on our server as undeliverable.

Reject : Just in case you want to be polite to the spammers, you can send them back a message saying that their email was rejected. You are no longer notified about the existence of the email, but the sender is, so they can contact you by another method. In most cases, instead of our mail server accepting the email message for delivery from the sender, we will reject the message. This results in a spammer getting the rejection message even if they are using a fake reply email address. You can customize the rejection message.

Delete : This is the recommended option, and will just delete the email message. You aren't notified, and the sender isn't notified. It's just forgotten about. We don't let the Spam message waste any of our time.

Email that scores off our limit-limit, typically over 10, is deleted, but other delivery options are available. The user never needs to be bothered by this "high scoring Spam".

It is important to note that these spam scores and delivery options can be adjusted for an entire site, allowing the site administrator to determine what is Spam and what to do with it.

1) After I sign up, how soon will the service will be activated?

Typically, within a business day. The primary reason for the delay is that any change to your domain's "MX" records do not take effect immediately, but must propagate through the Internet. Technically, your MX records have a "TTL" (Time-To-Live) value which specifies how quickly changes will take effect. A typical TTL value is one hour, but your domain may be configured with another value, such as 24 hours

2) We don't know how to change the 'MX' Record. What do we do?

That is no problem. We will email you the necessary changes and you can simply forward this email to your hosting company or IT department.

3) How is my email's security and privacy guaranteed?

ICM does not affect your email security in any way. Our service does not backup or make copies of your email messages. The log files only contain the email addresses of the sender and the recipient. We will never log the entire email message. We do not share any information with anyone else!
In the event your mail server is off-line, our service will "spool" your email messages. When your mail server is back on-line, it will automatically transfer all the spooled email messages. Even in this case, the temporarily spooled messages will not be permanently saved or backed up

4) Does ICM add any delay to my incoming mails?

Hardly! This service may delay your email by a few seconds, but not more than a minute. Email with large attachments, especially if you have anti-virus service, can be delayed up to about a minute or so because of the time it takes to do the scanning for viruses and spam.

ICM FLOW

```
Internet Mail          Message              Incoming Queue
>TCP / 25              Transfer Agent

                                            RBL tests

                                                    ┌──────────────────────┐
                       Spam                         │  Header Tests        │
                                            ┌──┐    │  Subject Tests       │
                                            │S │    │  Body Tests          │
                       Tests                │P │    │  URI Tests           │
                                            │A │    │  Misc. Tests         │
                                            │M │    │  External Processes  │
                                            │  │    │  Calculation Score   │
                                            │CHECK│  └──────────────────────┘

          ECM          Virus Tests                  Third Party Command Line
                                                    Virus Scanners

                       Attachment / HTML Tests          Quarantine
                       ( filename / filetype )

                       Message Processing       Virus
                       ( Header / subject line            Virus Actions
                         modifications )         Message
                                                               Delete

                                                    Delete
          Identified as Spam /         Spam
          Virus Free                              Delete                 Alert
                                  Spam Actions    Store

                                                 Deliver,
                                                 Bounce,
                                                 Forward

  User's MailBox    Message            Outgoing Queue      Sender / Postmaster
                    Transfer Agent                         Notificat
```