

Protect your users, your business and your brand

When it comes to your email, it's important to take control of what content is sent and received by your organisation, particularly when it could be damaging to your employees and company. In an increasingly litigious world, it is essential that organisations are able to protect themselves and their employees from internal and external email content threats. These threats include harassment of employees, defamation and obscenity, breach of confidentiality, loss of intellectual property, contractual liability, damage to business reputation not to mention wasted time and resources.

MessageLabs' Content Control service enables you to identify and control confidential, malicious or inappropriate content in inbound and outbound email. Combining technology with configurable usage rules, the service incorporates textual scanning, lexical analysis and attachment controls. Using these techniques, MessageLabs gives you control and an email policy that can be properly managed and enforced.



MessageLabs' dynamic global platform proactively scans millions of emails every day.

FULLY MANAGED

- Operates at Internet level, intercepting inappropriate content sent and received by your employees.
- Platform independent: no interoperability issues with your existing infrastructure.
- Quick and easy to setup: it frees up your IT resources and requires no additional hardware or software.
- Automated service – once configured, the service requires no intervention from individuals.
- Completely scalable – grows with your demand.
- Complements MessageLabs Anti-Virus, Anti-Spam and Image Control services.

HIGHER PROTECTION

- Uses advanced technology designed to detect confidential, malicious and inappropriate content.
- Monitors usage of specified key words and phrases and protects from email abuse.
- Uses block and approved lists to stop certain users or domains from sending/receiving emails to/from certain organisations.
- Provides additional protection to end users and also protects against legal action, loss of brand equity and network bandwidth.
- Protects against loss of employee productivity due to reduced number of time-wasting emails.
- Peace of mind knowing that email aligns with your usage policy.

COMPLETE CONTROL

- A multi-layered Content Control solution.
- Configurable to your needs: emails containing unwanted content can be tagged, logged, sent or copied to a nominated system administrator or deleted.
- Rules can be configured to control email content for individual users or groups of users specified. e.g. department, function or location.
- Controls the number, type and size of email and attachments users or groups can receive.
- Controls can be time managed so that they only apply at certain periods, e.g. large files can only be delivered during non-working hours.
- InSight™ – web-based management interface provides configuration tools, service statistics and reports.

KEY FACTS

- Over 9,000 business customers globally.
- Over 70 million business emails scanned every day.
- Sole focus on business enterprise market.

Content Analysis

The service uses MessageLabs' Content Control technology to proactively identify and stop unwanted content from reaching or leaving your organisation.

The Content Control service incorporates multiple methods – each one with its own analysis capability – to replicate an organisation's email security policy, protecting both employees and the organisation.

Deployed across our dynamic global platform, MessageLabs proactively scans millions of emails every day, helping you keep email clean and your organisation's integrity protected.

MessageLabs can replicate an organisation's email security policy via a set of defined rules. To apply different rules to different users, email senders or recipients can be defined as individuals, members of a group, a set of domains or a single domain.

Content Control can enable similar criteria and rules to be put into manageable lists in the following formats:

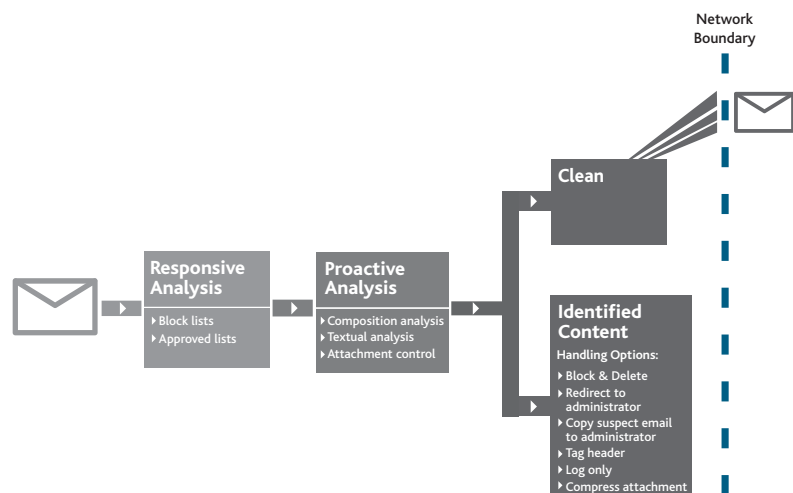
- Groups of users – sets of email addresses (either internal or external)
- Domains – sets of domain names
- Textual content – sets of words and phrases
- Message components – sets of MIME types
- File names – sets of file names or extensions

The Content Control Technology

- Determines what email is and isn't allowed to be sent in or out of an organisation by:
 - Scanning email subject and body text for words and phrases that are either user defined or pre-defined
 - Identifying message composition from MIME types (i.e. image, audio, etc)
 - Identifying file attachments against lists of file names and extensions (e.g. .doc, .jpg, .zip)
 - Identifying spoofed file attachments (e.g. executable files pretending to be text)
- Handles emails of high/low priority according to the organisation's email policy.
- Follows preset time parameters for specific rules to take place – i.e. all the time or at a specified time.
- Enables restrictions on the size of emails coming in and out according to:
 - Overall size of the email
 - Number of attachments
 - Size of attachments

How it works

- Client points MX [Mail Exchange] record to MessageLabs
- Email directed through the MessageLabs Service and handed to the client mail server.
- Proactive analysis of inbound and outbound email applies user-defined rules to process email.
- Service scans and detects inappropriate and confidential content against block and approved lists, which contain key words, phrases and file types.
- Identified suspect content controlled via multiple re-routing options including block/delete, redirect/copy to administrator, tag header, log only or compress attachment.
- Threats are managed AWAY from the client network.



To find out how you can take greater control of email to protect your organisation, please contact your regional representative or visit: www.messagelabs.com