

Managed service anti-spam protection

MailController anti-spam is a high performance managed service that intelligently identifies spam and blocks its delivery

How does MailController anti-spam work?

Spam filtering presents a number of complex challenges due to the dynamic nature of junk email. An effective spam filter must block the maximum unwanted email, with minimal 'false positives' (valid email, wrongly identified as spam).

MailController anti-spam solves these problems by using an 'Adaptive Spam Filtering' engine which effectively learns what an organisation considers to be spam and adapts its filters accordingly.

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

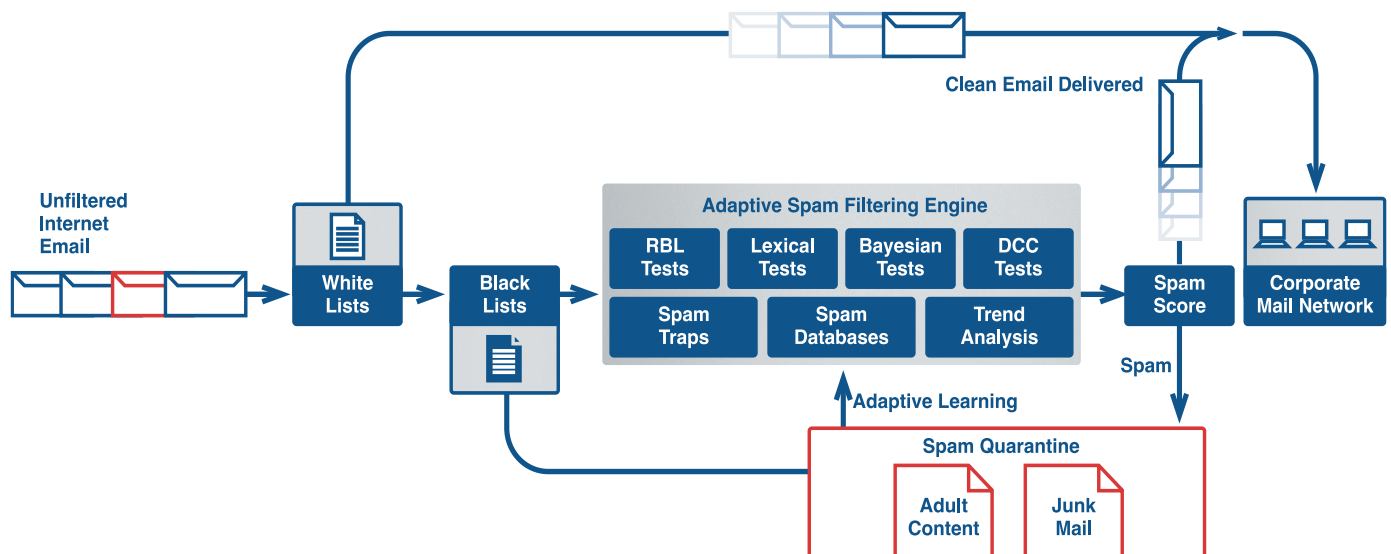
The MailController anti-spam service works by processing email through a number of filters, which include:

Black and white lists:

These are configurable lists of email addresses (or domains) that organisations explicitly block or allow through the service. The lists can be maintained at a domain level or for a specific user.

Adaptive spam engine:

The adaptive spam engine is the heart of MailController anti-spam. It uses a combination of techniques to analyse each email message and assign the message a 'spam score'. This score is used to determine the likelihood of the message being spam.



The whole scanning process takes less than one second. Once each message has been analysed 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.

Key benefits

- Increased protection, reduced operational costs
- Highest detection rates, minimal false positives
- Self-tuning adaptive spam filtering technology
- Maintain control via secure management portal
- Per-domain and per-user configuration
- Minimal helpdesk intervention

The rules used to assign a spam score include:

Real time black lists: These dynamic lists contain IP addresses of machines that are used to send spam messages. MailController anti-spam tests to see if email messages were sent from such a known source of spam.

Lexical analysis: The spam engine contains several thousand lexical tests that look for characteristics in the email that would be indicative of a junk message. These include tests that examine the header of the email looking for anomalies such as no 'from' address or badly formed headers. In addition the spam engine analyses the body of the message looking for common strings and key words indicative of spam.

Bayesian probability*: Using Bayesian techniques MailController anti-spam creates a corpus of valid email and a second corpus of spam email. Each corpus contains strings and probability weightings, used to indicate if those strings are typically associated with spam or valid email. Each new email message is analysed against the corpuses to determine the probability that the message is valid or spam.

The corpuses of email are built automatically by the service and continue to 'learn' with each new message, enabling them to adapt to the ever-changing nature of spam. The corpuses can also be manually tuned by an administrator to refine their capability. This approach enables MailController anti-spam to customise its filters to specific customer environments. As an example the string 'Viagra' is commonly associated with spam and may appear in a company's corpus of spam email. However, for a pharmaceutical company 'Viagra' may often have a valid use and as such would not appear in their corpus of spam email.

Distributed Checksum Clearinghouse: Distributed Checksum Clearinghouse: DCC is a client/server system developed by an Internet community lead by Vernon Schryver. This collaborative system works on the basis that servers using DCC create a fuzzy hash for every email processed. The fuzzy hashing logic allows emails to be compared, identifying similar messages that might contain slight variances, such as different greetings. These hashes are then collated at the Clearinghouse and counted. The highest scoring emails are the ones that have been seen most frequently across the Internet, and are likely to be spam.

*Bayesian mathematics is a branch of logic applied to decision-making and inferential statistics that deals with probability inference. Put simply, it means using the knowledge of prior events to predict future events.

Key features

- Lexical analysis, including message headers, subject and body
- White lists configured on a user basis (can be configured by users if authorised)
- Black lists configured on a user basis (can be configured by users if authorised)
- Configurable spam threshold on a user basis (can be configured by users if authorised)
- Tag spam in the subject line and deliver email
- Re-direct all spam messages to configurable email address
- Quarantine all spam email
- Company spam reports, summarising all messages processed and their spam scores
- End-user spam reports, summarising all messages processed and their spam scores (available to end-users if authorised)

Spam filtering features

- Realtime black list analysis (mail-abuse.org)
- Bayesian analysis
- Distributors Checksum Clearinghouse analysis
- White lists configured on a domain basis
- Black lists configured on a domain basis
- Configurable spam threshold on a domain basis

Management features

- Online customer portal
- Management dashboard
- Online management of quarantined email
- Online policy management
- Online message tracking
- View all message logs and delivery reports

ES-Tech delivers MailController in partnership with Opal.

For more information on **MailController** please contact ES-Tech on:

Telephone: 01869 356018

Email: sales@es-tech.co.uk