



■ MailControl Spam Technology Overview

BlackSpider MailControl Spam is a high-performance on-demand service that intelligently identifies spam and blocks its delivery. Using a variety of techniques, MailControl Spam consistently stops over 98% of all junk email.

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).

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

User Self-Service

MailControl Spam recognises that the ultimate decision on what is, or is not spam should be the users.

They can choose to receive regular message reports, to access their own quarantine area for full visibility of blocked messages, and manage their own black and white lists. Combined with the adaptive spam filtering engine, this approach removes the concern of false positives from users and email administrators for complete user confidence.

Technology Overview

The whole scanning process takes just a few seconds. Once each message has been analysed by MailControl's multiple detection techniques, the message receives an overall 'spam score'.

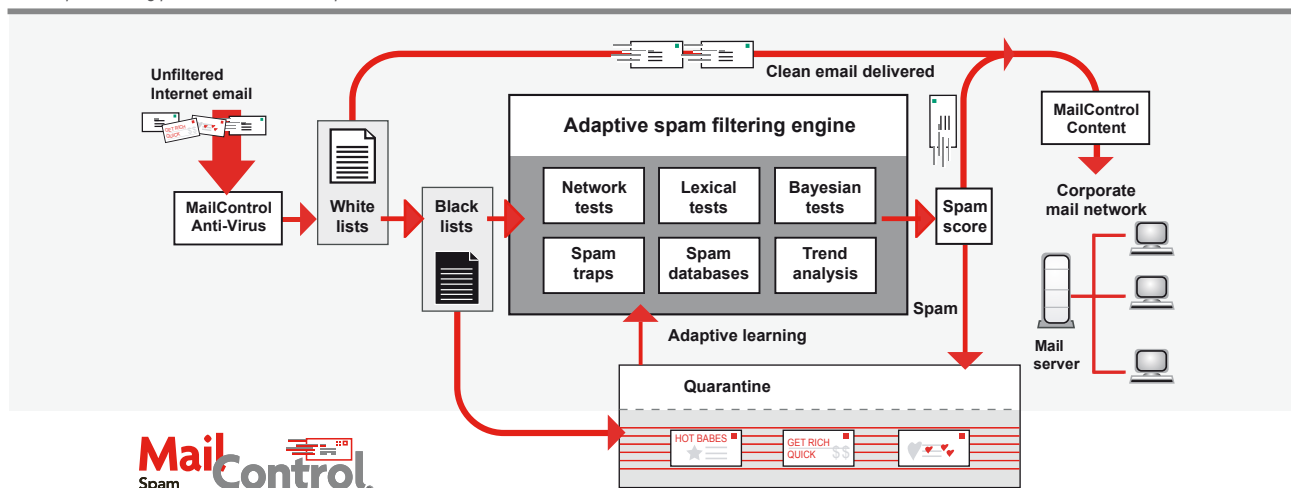
The score is then compared against a configurable spam threshold; mail scoring below the threshold is delivered as normal, whilst mail scoring above is quarantined as spam.

Adaptive Spam Engine

The adaptive spam engine is at the heart of MailControl Spam. It uses a combination of techniques to analyse each email message and assign the message its spam score, which is then used to determine the likelihood of an email being spam. The techniques used to assign a spam score include:

- **Network Tests:** These combine a number of tests including Sender Policy Framework (SPF) and Real-time Black Lists (RBLs) in order to determine the identity and reputation of an email sender.
- **Lexical Analysis:** Detailed analysis of an entire email including the message envelope, headers, subject and body text. Lexical analysis searches for key words and phrases to measure whether a message is likely to be spam.
- **Collaborative Spam Databases:** A number of Internet spam databases exist such as Vipul's Razor, that rely on a collaborative approach to identifying spam. Individual users submit spam messages to the database, where each message is given a unique signature or hash.

The adaptive filtering process of MailControl Spam





- **Bayesian Filtering:** The concept of Bayesian filtering is to create two databases or 'corpus' of email: A corpus of spam email and a second of valid email. Each corpus is 'tokenised' and analysed looking for tokens that frequently appear in each type of email. Each token is then given a probability weighting, suggesting if it is likely to appear in spam or valid email.
- **Spam Traps:** Spam traps or honey-pots are email accounts that have been set-up to collect spam. Once the same message has appeared in a very small number of spam traps it can be clearly identified as spam, with little risk of incorrect classification. Once identified, a signature (or hash) can be created and used to detect and block future instances of similar messages.

■ **Trend Analysis:** Trend analysis can be an effective technique to help mitigate false positives and improve spam detection rates. By analysing the history of email sent from an individual, trends can help assess the likelihood of an email being valid or spam.

■ **White & Black 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, group or end-user level.

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*
- *Integrates with Anti-Virus and Spam and WebDefence for total protection against email and web threats*

Key Features of MailControl Spam

Management Features

- Online customer management portal
- Online management of quarantined email
- Quarantined email held for up to 30 days
- Management spam reports, summarising all messages processed and their spam scores
- Email composition reporting
- Portal access control model, allowing different users different levels of access
- Administrator view of all message logs and delivery reports
- Customisable HTML and plain text annotations available for individual users or groups of users on inbound and outbound email
- Real-time message tracking with detailed SMTP logs via online portal
- Spam confidence threshold can be configured on a user, domain or group basis
- Integrates with all BlackSpider MailControl and WebDefence services for common policy definition, management and reporting tools

Spam Detection Features

- Network and reputation analysis, including Real-time Black Lists and Sender Policy Framework
- Lexical analysis, including message headers, subject and body
- Bayesian Filtering
- Collaborative Spam Databases
- Trend Analysis
- Distributed Checksum Clearinghouse analysis
- Spam traps (Honey Pots)
- Published spam detection rates
- White lists configured on a domain or user basis
- Black lists configured on a domain or user basis

Spam Deployment Features

- Spam mail can be quarantined and not delivered to corporate networks
- Spam mail can be tagged in the subject line and delivered
- Spam mail can be redirected to a junk mailbox

End-User Self Service Capabilities

- End-user spam reports, summarising all messages processed and their spam scores
- Authorised users are able to view quarantined messages
- Authorised end-users able to release spam messages from quarantine area through web interface
- Authorised end-users can configure their own white and black lists to tune the service



Free proof of concept
to find out more...

- Visit www.solsis.co.uk
- Call **0118 922 7938**
- Email sales@solsis.co.uk