



ANTI SPAM SOLUTIONS TECHNOLOGY REPORT

SurfControl MailControl



JANUARY 2007

CONTENTS

SurfControl MailControl

SurfControl, Inc., 5550 Scotts Valley Drive, Scotts Valley CA, 95066, USA
Tel: (831) 440-2500 • www@surfcontrol.com

SurfControl plc., Riverside, Mountbatten Way, Congleton, Cheshire, CW12 1DY, UK
Tel: +44 (0) 1260 296 200 • www@surfcontrol.com



- Introduction3
- Test Network4
- Test Methodology5
- Product Testing Reporting6
- Checkmark Certification7
- The Product8
- Test Report9
- Test Results14
- West Coast Labs Conclusion15
- Security Features Buyers Guide16



INTRODUCTION



As the war for corporate inboxes intensifies, and unmonitored emails disrupt effective and secure working practices, Anti-Spam solutions continue to evolve to deal with this menace.

In this, the second Anti-Spam Technology Report, we examine the functionality and performance of the leading products in this market, which are aimed specifically at the SME network environments.

A key objective of the testing is to replicate the installation, configuration and use of the solutions in a real-world business environment to enable readers of the White Paper – prospective buyers – to make a meaningful assessment of the product that is right for protecting their corporate email environment.

Test Engineers have evaluated how the solutions install to ensure timely and effective spam protection. Consideration has also been given to the level of security administrator expertise and technical support required to facilitate both out-of-the-box operation and thereafter product training to ensure maximum effective spam protection.

This reports provides an independent assessment of effectiveness with regard to:

- The features and functionality of the solution.
- Integration into a network infrastructure.
- The level of user administration required to operate the product effectively.
- Spam detection capability and rates of detection.

TEST NETWORK

WCL has a number of domains that collect genuine spam. These domains receive varying levels of spam and are consistent with different email environments.

To reflect the email usage within a corporate environment, within each domain are a number of designated user accounts with a variety of email practices and needs including some that are subscribed to a variety of newsgroups and mailing lists. Some user accounts actively contribute to mailing lists.

The multiple domains designated for testing purposes were those that, between them, receive spam at a level consistent with the defined requirements of testing.

Software solutions included in the test program were installed on servers that meet the minimum specifications required by the vendor. Appliance-based solutions were installed on the network according to the vendor's recommended placing.

For hosted services, WCL testes through identified email domains and changed the MX records to divert the mail stream through the hosted service.

TEST METHODOLOGY



WCL initially performed the testing with an “out-of-the-box” configuration, changing only those settings on the solution needed to ensure correct operation in line with the vendor’s recommended installation and configuration procedures.

Further testing was then performed following the vendor’s advice for the tuning or training of the solution under test. WCL fine-tuned the solution each day of the test, spending no more than half an hour per day undertaking such work.

Throughout the course of testing, a mixture of email was sent to the test domains from other email addresses and domains controlled by WCL to mirror genuine email activity common in business, for example, requesting meetings, sending notifications to groups and non-business related social emails.

Emails were also sent from web-based accounts such as Hotmail and Google’s Gmail in order to simulate external users sending non-business related social emails, and home workers.

Thus, during the testing period the domains received some spam, some list/newsgroup mailings and “genuine” individual emails.

PRODUCT TEST REPORTING

Product evaluation addresses three specific areas* - Management/Administration, Functionality, Performance plus Additional Feature Testing.

1. MANAGEMENT/ADMINISTRATION

- Ease of Setup/Installation
- Ease of Use
- Logging and reporting function
- Rule creation
- Customization
- Content Categories

2. FUNCTIONALITY

- Email Processing Steps
- Allow/Blocking of Email
- Quarantine Area
- Additional functionality reporting
- Steps to Process Email
- Block Email Addresses
- Blacklist/Whitelist
- Allow Email Addresses

3. PERFORMANCE

- Volume or Percentage of spam detected
- False positive rate
- Spam incorrectly passed through
- Legitimate mail blocked
- Legitimate subscription mail blocked

CHECKMARK CERTIFICATION

Upon completion of the testing, individual product results are analyzed, resulting in accreditation to one of the two Checkmark Certifications for Anti-Spam subject to achieving the following catch rates:-

- Checkmark Anti-Spam Certification - Premium - 97% and over Catch Rate.
- Checkmark Anti-Spam Certification - Standard - 90% and over Catch Rate.



THE PRODUCT



SURFCONTROL MAILCONTROL

SurfControl MailControl is an integrated set of on-demand e-mail security solutions; protecting against viruses, spam and unwanted content and enabling secure e-mail communications to the extended enterprise.

http://launch.surfcontrol.com/us/global/e-mail_protection/on-demand/mailcontrol_overview.html

SURFCONTROL SAYS ABOUT THE SERVICE'S BUSINESS BENEFITS...

The MailControl on-demand e-mail security solution is one of a number of threat prevention solutions from SurfControl. With threats from Web and e-mail now converging, it is more important than ever to have a unified strategy on threat prevention. With SurfControl's suite of products and technology leadership, SurfControl can provide unrivalled protection against Internet and e-mail threats and help reduce business risk.

SurfControl MailControl delivers lower cost of ownership by reducing productivity costs. As an on-demand service it also offers unlimited scalability and with SurfControl's global delivery network, customers are guaranteed an uninterrupted service with no single point of failure.

http://launch.surfcontrol.com/us/global/e-mail_protection/on-demand/mailcontrol_overview.html

SURFCONTROL SAYS ABOUT THE SERVICE'S TECHNICAL BENEFITS...

SurfControl's MailControl is an integrated suite of solutions that provides comprehensive e-mail protection against the threat of viruses, spam and other unwanted content as well as enabling the securing of e-mail communications. SurfControl's world-class reputation services and heuristics technology complemented by Global Threat Experts ensures that e-mail threats are analyzed and defences updated immediately.

The real-time online management portal makes it more straightforward to define and enforce security policy. Powerful end-user quarantine management tools help relieve the burden on IT administrators and on-demand statistics and message reporting give you control, by helping you understand what's happening in your network.

http://launch.surfcontrol.com/us/global/e-mail_protection/on-demand/mailcontrol_overview.html

TEST REPORT



INTRODUCTION

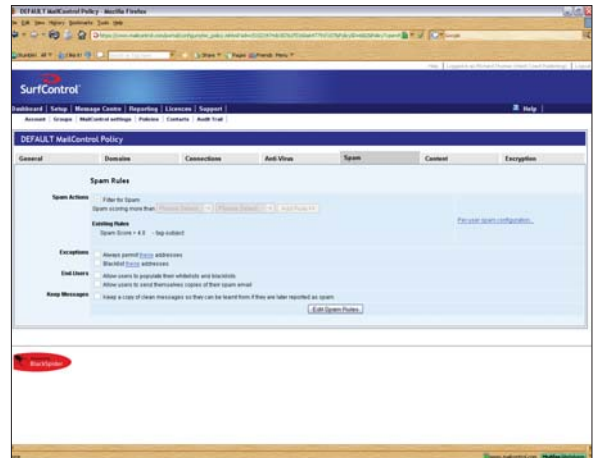
SurfControl's MailControl is a managed service aimed at organizations looking to outsource antispam protection. Messages can be routed through MailControl before they are received by the organization's own mail servers. This reduces the strain on bandwidth, potentially increasing server stability, while reducing the time-consuming manual removal of spam.

By opting to use the MailControl hosted service, an organization can avoid the cost of acquiring new server hardware. However, potentially the greatest benefit from using this hosted service is the time saved by an administrator, who would otherwise have to assume responsibility for the running and day-to-day maintenance of yet another piece of hardware.

TEST REPORT

INSTALLATION AND CONFIGURATION

As this is a managed service, most of the initial configuration is carried out by SurfControl, reducing the workload on the administrator while ensuring the correct setup of the account. Work required of the administrator in order to get the service running, is limited to the configuration of the organization's domain and mail routing settings. This is a quick process and in very little time the service is ready to begin scanning mail. It can then be further customized to best suit the needs of the organization.



The first step in this process is to set up the domain information, which can be accessed from the Domains tab in the Policy Setup screen. The administrator can choose to add a new domain or to edit one that has already been created. When selecting to add a new domain the administrator is prompted to enter the domain name that is to be protected by MailControl, along with the option of including any possible sub-domains.

Once this information has been entered, and the submit button clicked, MailControl will then manually check the domain name. During this time the administrator is warned not to redirect mail through the service, as this will result in email being lost. The administrator may view the current status of the domain by viewing the Status field within the Domain tab. Once this displays the status of the domain as checked, the administrator may begin redirecting mail through the service.

Information relating to which mail servers should be allowed to send and receive email through the MailControl service may be entered using the Connections tab. Using this screen the administrator may enter the IP addresses of the mail servers that are currently in use by the company, along with priority values that define the order in which MailControl should use the servers.

While not necessary to begin benefiting from the MailControl service, the administrator may also choose to create groups of users. This may be carried out from the Groups tab in the Setup menu. Within this screen is an Add Group function. When using this the administrator is prompted to enter a name for the group and may also add a brief description. Once the group has been created, the administrator may begin to populate the group with users' email addresses.

Use of this function allows an administrator to organize users, for example by departments or locations. The creation of groups also enables the administrator to assign different rules for blocking spam to different people. For example, a medical department may require emails with words such as pharmaceuticals, drugs, or prescription, to be allowed through.

TEST REPORT

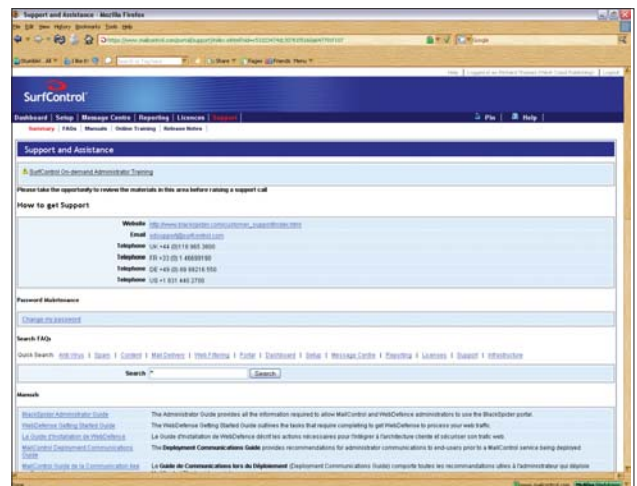
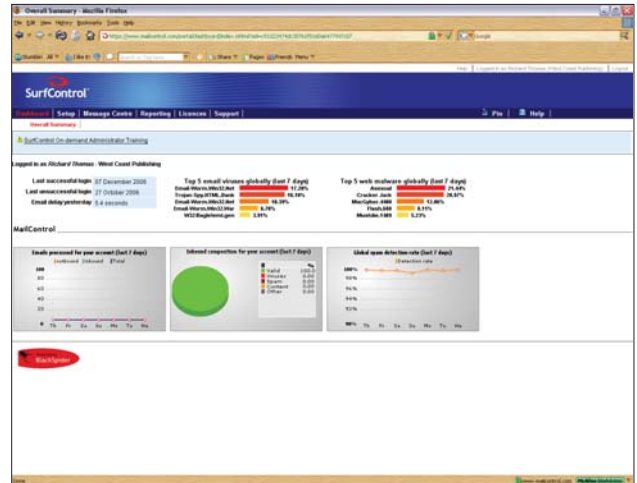
INTERFACE

Access to the service is provided over a secure web connection. Once logged in, the administrator is presented with a clear, colorful, and well presented interface. The screen initially presented to the user provides all the support information required to get the most from the service. This information includes contact details for the support team, links to user manuals in various languages, a series of setup demonstrations, and a list of FAQ categories.

The wealth of information provided greatly aids the administrator in the customization of the service and ensures that any questions regarding the use of MailControl can be answered quickly. This same level of information is provided throughout the use of MailControl and provides the administrator with all the information required to best configure the service.

Further configuration of the service is carried out via the Policies window in the Setup area of the interface. It is from here that changes to domain settings may be carried out, such as altering target mail servers. Any new configurations can be quickly applied and enable the service to offer continuous email protection to an evolving organization.

Messages received by the MailControl service are subject to an array of tests designed to thoroughly examine the message for common spam phrases, content, and behavior. These tests are carried out by various technologies such as Bayesian filters, checksums, white and black lists, and lexical analysis. This last is responsible for the scanning of header information and message content.



TEST REPORT

When dealing with mail that is detected as spam, the administrator is free to choose from a number of different actions to take. Included amongst these are prepending a spam tag to the subject line and then allowing the message through, or blocking the message outright. Both of these options have their merits and allow the organization to choose how to merge MailControl with their network policy. By default MailControl prepends a spam tag to the subject line, which allows users to monitor their mail for potentially misdiagnosed spam.

MailControl also has the ability to scan for infected messages and attachments, and this is provided through the use of three individual antivirus technologies. One of these is SurfControl's Huntsman scanner, which is designed to detect zero-day viruses which have yet to be classified. The provision of antivirus scanning adds yet another layer of defense.

TEST REPORT

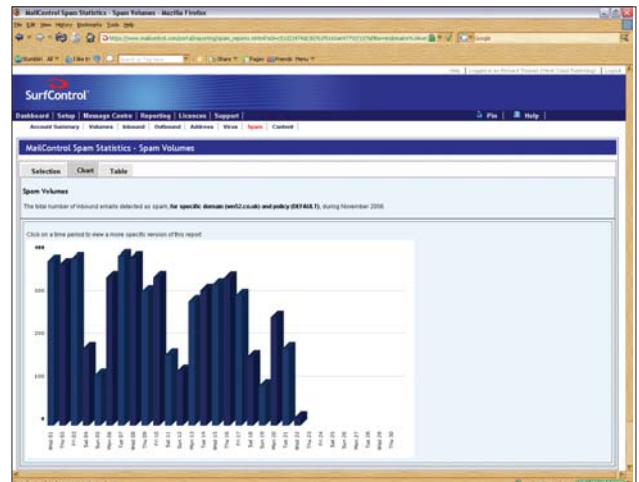
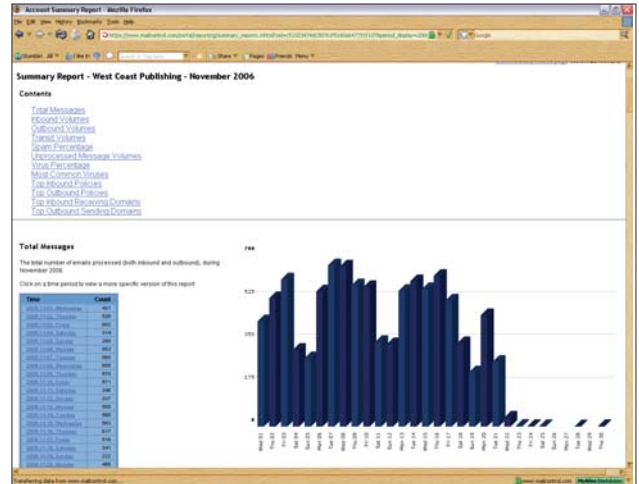
REPORTING

When using the Reporting function of MailControl, the administrator has the choice of eight different report types: account summary, volumes, inbound, outbound, address, virus, spam, and content. Each category enables the administrator to break down the relevant information so that a detailed picture of all mail traffic may be established.

Viewing an Account Summary Report displays data covering either specific months or over a given number of weeks. Each of the reports generated contains fourteen categories, breaking the data down into a range of different viewpoints including total messages, virus information, policy information, and various volume categories. Several of these categories, such as Top Inbound Policies and Most Common Viruses, contain graphs and charts which require the installation of a Flash player onto the browser being used to view the interface.

The other seven categories all share a common design, which is different to that of the Account Summary. An initial page allows the administrator to select from various fields, including dates, user groups, policies, and traffic direction. Once the administrator has specified the criteria on which to report, MailControl retrieves the matching information. The results are split over two pages, chart and table; the former displays a bar chart while the latter displays a count of traffic in a table format.

Information displayed in any of the tables, including those within the Account Summary screen, may be saved to a local disk in .CSV format. This allows for data to be imported into a variety of spreadsheet tools for further examination or to aid in data comparison. Also included is a link to a printer-friendly page, which displays the all the information but without the menu or title bars.



TEST RESULTS

<u>Type of mail</u>	<u>Detected as genuine</u>	<u>Detected as SPAM</u>
GENUINE	100%	0%
SPAM	1%	99%

SurfControl's MailControl performed well, delivering 100% of the genuine mail correctly and correctly classifying 99% of the spam mail.

It is also worth noting that MailControl delivers a good proportion of grey and list mail as genuine. This gives an organization the flexibility and opportunity to define policies during a training period without missing mail that could potentially be business critical.

West Coast Labs is pleased to award MailControl the Premium Anti-Spam Checkmark.



WEST COAST LABS CONCLUSION



SurfControl's MailControl is an impressive managed service that provides an organization with the tools and information necessary to defend their network from the impact caused by spam. This should be recommended to companies looking for a managed service that offers a high degree of customization.

Reporting functionality is also available that offers an impressive range of searchable data. The service allows an administrator to view data over large timeframes or down to a specific date. This data is well presented and accurately portrays traffic trends and patterns.

West Coast Labs Disclaimer

While West Coast Labs is dedicated to ensuring the highest standard of security product testing in the industry, it is not always possible within the scope of any given test to completely and exhaustively validate every variation of the security capabilities and/or functionality of any particular product tested and/or guarantee that any particular product tested is fit for any given purpose.

Therefore, the test results published within any given report should not be taken and accepted in isolation. Potential customers interested in deploying any particular product tested by West Coast Labs are recommended to seek further confirmation that said product will meet their individual requirements, technical infrastructure and specific security considerations.

All test results represent a snapshot of security capability at one point in time and are not a guarantee of future product effectiveness and security capability. When West Coast Labs provide test results for any particular product tested, said results are most relevant at the time of testing and within the context of the specific scope of testing and relative to the specific test hardware, software, equipment, infrastructure, configurations and tools utilized during that specific test process.

West Coast Labs is unable to directly endorse or certify the overall worthiness and reliability of any particular product tested for any given situation or deployment.

SECURITY FEATURES BUYERS GUIDE

DEVELOPMENTS IN THE PRODUCT OVER THE LAST 12 MONTHS AS STATED BY SURFCONTROL...

During the last twelve months SurfControl MailControl has been significantly enhanced to better address the ever growing and evolving spam problem. One of the key enhancements has been the addition of specific protection against both static and animated image-based spam which has become much more prevalent. This has brought significant benefits to customers, including improved productivity and reduced network load as a greater percentage of spam is blocked before it reaches their network.

Spam detection development and tuning is an on-going aspect of the MailControl on-demand spam service. Resources are dedicated to investigating new spam threats and developing and tuning spam detection capabilities. Aside from continuous tuning, the following enhancements to processing and managing spam have been made over the last twelve months:

- Detection of static image-based spam using optical character recognition (OCR)
- Detection of animated image-based spam
- Global spam detection rate graph displayed in the dashboard section of the on-demand portal. This allows customers to monitor the MailControl spam detection rate and trends
- Searchable black/white lists allow administrators to search black and white lists set by individual end users
- Black and white list reporting available to administrators to help with troubleshooting.
- Black/white list changes identified in audit trail helping with traceability
- End user message reports and notifications provided in a further nine languages (total now fourteen) improving ease of use of spam and quarantine reporting
- Further usability improvements to end user message reporting to help identify borderline spam

ADDITIONAL NOTEWORTHY PRODUCT FEATURES

SPAM FILTERING

- Real-time black list analysis
- Collaborative spam databases
- Lexical analysis, including message headers, subject and body
- Trend analysis
- Reputation filters
- Checksum databases
- Bayesian analysis
- Spam traps

SECURITY FEATURES BUYERS GUIDE

- Black and white lists configured on a domain and per user basis
- Image spam detection (static and animated images)
- Configurable spam threshold on a domain basis
- Optionally tag spam in the subject line and deliver e-mail
- Optionally re-direct all spam messages to configurable e-mail address (junk mailbox)
- Optionally quarantine all spam e-mail

END-USER SELF-SERVICE

- End-users able to safely view - and release - quarantined messages through a Web interface in real-time

REPORTING

- Management reports on the volumes of messages processed
- Management reports, summarizing all messages processed and their spam scores

MANAGEMENT AND GENERAL FEATURES

- Online customer management portal
- Online real-time policy management
- Portal access control model, allowing different users different levels of access
- Management dashboard providing a snapshot view of the service
- Online management of quarantined e-mail
- Quarantined e-mail held for up to 30-days
- Quarantined e-mail can be viewed and released by the administrator
- Administrator view of all message logs and delivery reports
- Customizable annotations on all inbound and outbound e-mail
- Configure different annotations based on users and domain names
- Annotations can be placed at the top, bottom or wrapped in a message
- Administrators can view quarantined messages & release, forward or delete through the customer portal
- Service guarantees for key aspects of service performance including spam detection rate.

http://launch.surfcontrol.com/us/global/e-mail_protection/on-demand/mailcontrol_overview.html