

Lab Testing Summary Report

July 2010

Report 100607

Product Category:
Email Security Solution

Vendors Tested:

Cloudmark
MessageLabs/Symantec
MxLogic/McAfee SaaS
Proofpoint
Red Condor

Products Tested:

Cloudmark - Cloudfilter;
MessageLabs/Symantec
Email AntiSpam,
AntiVirus, Image Control
Services;
MxLogic/McAfee SaaS
Email Defense Service;
Proofpoint - P340;
Red Condor - MAG2700



Key findings and conclusions:

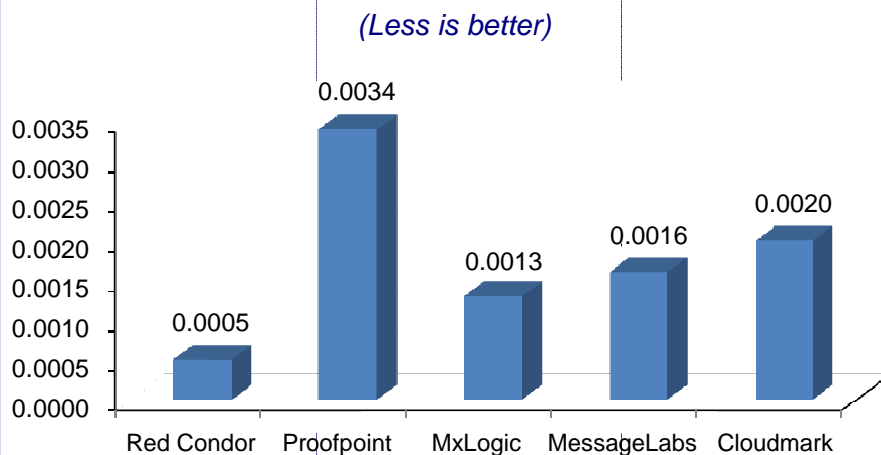
- Red Condor had the lowest misclassification rate among the five filtering solutions
- MAG2700 blocked 99.9% of received spam messages during testing
- During a one-week deployment, zero false positives were generated by the MAG2700
- Vx Technology enabled network load sharing and high availability on the MAG2700

Red Condor Message Assurance Gateway 2700 was evaluated in an ongoing assessment of email security products. We tested Cloudmark Cloudfilter, MessageLabs (now Symantec Hosted Services) Email AntiSpam, Email AntiVirus and Email Image Control services, MxLogic (now McAfee SaaS) Email Defense Service host-based solutions and the Proofpoint P340 and Red Condor MAG2700, on-premise non-SaaS appliances.

A large and growing population of spammers, using sophisticated tools, generate a huge amount and variety of spam. Ninety to ninety-five percent of all incoming email consists of spam, phishing attempts, and virus threats. In this environment, getting the five to ten percent of good mail to user inboxes and keeping out the bad demands an email security solution with a high filter accuracy rate.

Companies have dozens of choices, many of them touting similar features and claims, to solve this problem. To help decision makers make the right choice, Miercom ran five email security solutions through the paces during one week of lab testing. The hosted solutions were: Cloudfilter from Cloudmark; Email AntiSpam, Email AntiVirus and Email

Figure 1: Spam Filter Misclassification Rate
Percentage of Messages Incorrectly Identified



Source: Miercom, July 2010

Misclassification Rate calculates the rate of incorrectly identified messages, that is, false positives and false negatives. Red Condor achieved the lowest misclassification rate among the email security solutions tested.

Image Control services from MessageLabs; Email Defense Service from MxLogic. The on-premise non-SaaS appliances were: P340 from Proofpoint and MAG2700 from Red Condor.

Each product was evaluated for spam filtering effectiveness based on content analysis accuracy and the ability to protect against email-borne threats, including virus, adult content and phishing. The five solutions were subjected to a production email stream of approximately 3,000 messages a day for one week. After reviewing the missed spam (false negatives) and the quarantined legitimate messages (false positives), we determined that the Red Condor appliance had the lowest misclassification rate. Red Condor and MxLogic had the highest spam block rates. Red Condor MAG2700 and MessageLabs, meanwhile, generated zero false positives during the test week.

See *Figure 1 on page 1* for misclassification rates, *Figure 2 on page 2* for block rates, *Figure 3 on page 4* for false negatives and *Figure 4 on page 4* for false positives.

The Problem of Misclassified Mail

Email is an essential communications tool. Legitimate messages classified as spam can cause deals to be lost, a decline in customer satisfaction and other business problems. Spam messages incorrectly classified as legitimate mail are annoying and potentially dangerous if they contain a virus.

Most spam filters force a sacrifice: A high spam capture rate – or block rate – at the expense of a high false positive rate, and vice versa.

The most effective filter offers the best of both worlds – a low misclassification rate, which counts both false positives *and* false negatives. Red Condor had the lowest number of misclassified messages among the solutions tested. See *Figure 1 on page 1*.

Deployment Options: SaaS, Appliance and Hybrid

To protect against email-borne threats, email security solutions can be deployed as SaaS (Software as a Service), on-premise appliance, or a combination of both for a hybrid solution.

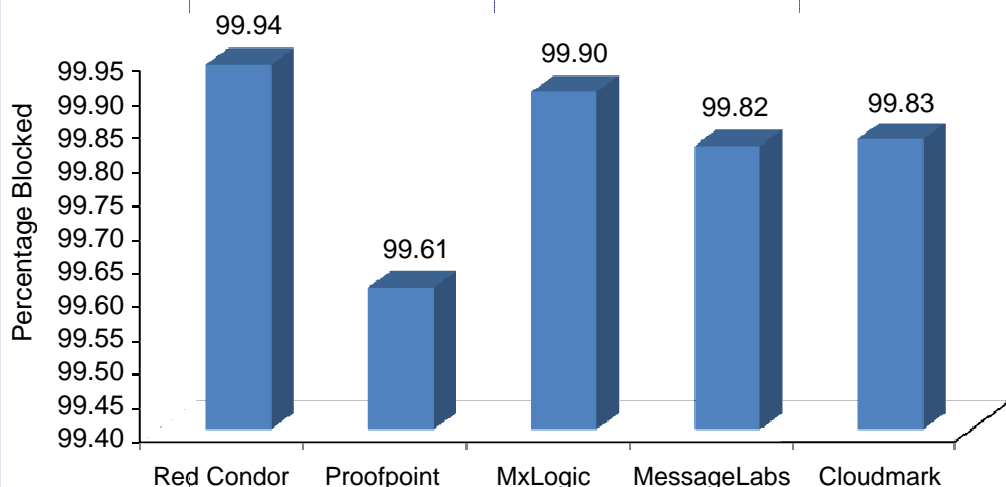
The advantage of a SaaS-based spam filter is the reduction of email allowed into the internal network. Only filtered or good email is received by the production Message Transfer Agent (MTA). This increases overall network performance and decreases bandwidth utilization. We tested SaaS solutions from Cloudmark, MessageLabs, and MxLogic. On-premise solutions offer more granular control options and flexibility to secure information and message systems. The on-premise, appliance-based solutions we tested were the Proofpoint P340 and the Red Condor MAG2700.

For built-in redundancy and cost savings, an inbound hybrid solution can be deployed. An

Figure 2: Spam Filter Block Rate

Percentage of Spam Messages Successfully Blocked

(More is better)



Source: Miercom, July 2010

When more spam - false negatives - are allowed into a mail server, the entire system can become overloaded, slowing down delivery of legitimate messages. Keeping these emails from delivery is critical. Red Condor had the lowest number of false negatives and the highest block rate.

Table 1: Email Security Solutions Test Results

	Red Condor	Proofpoint	McAfee	MessageLabs	Cloudmark
Emails received	23,651	22,402	21,367	23,971*	28,465
Spam (includes blocked sessions)	21,357	19,356	19,308	21,644	27,224
Messages Delivered	2,294	3,046	2,059	2,327	1,241
False Negatives (FN)	12	75	20	39	47
False Positives (FP)	0	2	8	0	11
Missclassified Messages (FN + FP)	12	77	28	39	58
Misclassification Rate	0.00050	0.0034	0.0013	0.0016	0.0020
Block Rate	99.94	99.61	99.90	99.83	99.83

**Estimate - MessageLabs does not record blocked/dropped email stopped at the outer security gateway.*

Definitions Used:

False Negative: Spam that was misclassified and delivered as good mail

False Positive: Legitimate email that was misclassified as spam and blocked

Missclassified Messages: Total of False Negatives and False Positives

Misclassification Rate: Missclassified Messages/Emails Received

Block Rate: Total of (Spam less False Positives) / (Spam plus False Negatives less False Positives)

onsite appliance is deployed in combination with a hosted system to support load sharing and failover mail traffic. The Red Condor MAG2700 with Vx Technology was the only product tested that offers this feature.

Email Filtering Effectiveness

Effective email security requires a high filtering rate and accurate content analysis of the email stream. We measured the accuracy of the spam and virus engines' identification of spam, and the frequency of misclassified messages as spam. In this report, spam messages delivered to the inbox are referred to as false negatives. Legitimate emails identified as spam and not delivered are called false positives. Each spam filtering product received between 22,000 and 29,000 emails for the week.

Block rates were calculated for overall filtering effectiveness in blocking malicious email. Test results show Red Condor had the least number of false negatives and the highest block rate. See [Figure 2 on page 2](#). Red Condor and MessageLabs generated zero false positives. See [Figure 4 on page 4](#).

Email security solutions apply a number of filters for each inbound message. The first filter looks

for invalid recipient and poor reputation, thereby effectively blocking 80 to 90% of bad email.

Some vendors, such as MessageLabs, do not report email blocked/dropped at this first filtering level. So the spam count for MessageLabs contained only messages that passed through this first filter, while the spam count for all the other solutions included all rejected emails due to bad reputation and invalid recipients. In order to make a fair comparison of block rates for all solutions, the spam count for MessageLabs was estimated as an average of all spam received for the products tested. Therefore the block rate is an average/estimate for MessageLabs.

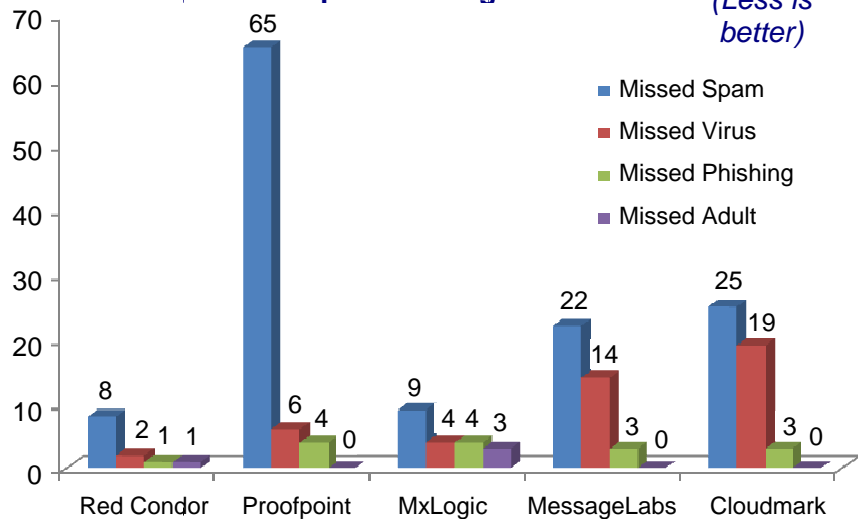
High Availability and Redundancy

Red Condor offers a hybrid spam filtering solution, Vx Technology, which combines a cloud-based hosted service with an on-premise spam filtering appliance.

The setup of Vx Technology was easily accomplished by opening the firewall on port 25 with the destination set to the production MTA and the source set to the Red Condor data center IP range.

The Lightweight Directory Access Protocol (LDAP) port was opened at the firewall for the

Figure 3: Spam Filter False Negatives
Number of Spam Messages Missed



Source: Miercom, July 2010

False negatives, or spam delivered to the inbox, can be potentially dangerous if they contain a virus. Red Condor had low false negative counts in all the categories tested.

Red Condor data center to access the user directory. The MX records were modified with the primary MX record pointing to the appliance, and the secondary and tertiary MX records pointing to the Red Condor data center IPs.

Vx Technology not only reduces the load on the production network, it also provides automatic failover to sustain continuity of the email stream in the event of network attacks or power failures. Our experts observed that 14% of email traffic was processed by the Red Condor cloud services, thereby providing load sharing.

To test high availability and redundancy of the MAG2700, we turned the appliance offline

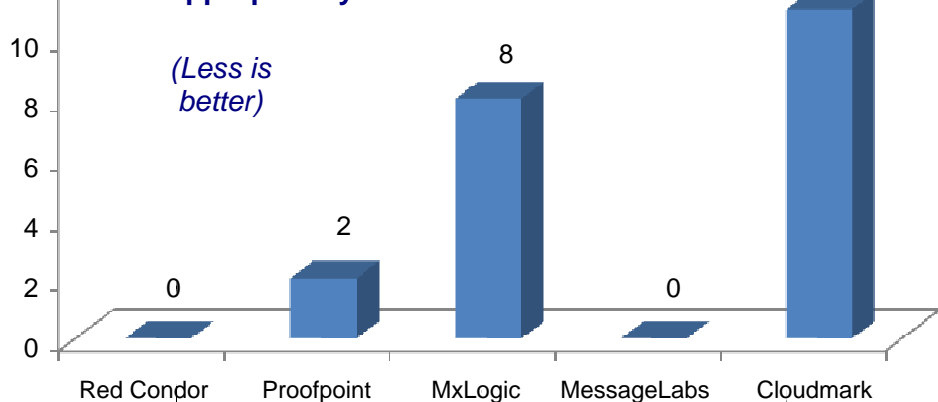
periodically during testing and verified email continuity for production environment under test.

Bottom Line

All spam filters block unwanted email, using various techniques to achieve a high spam block rate. But when all errors were taken into consideration, we found Red Condor had the lowest misclassification rate of all solutions tested; one mistake out of 1,970 messages received. Their hybrid approach of SaaS and a locally deployed appliance proved a highly available and redundant filtering system.

Based on the filtering and blocking test results of the MAG2700, Red Condor provides an effective email security solution.

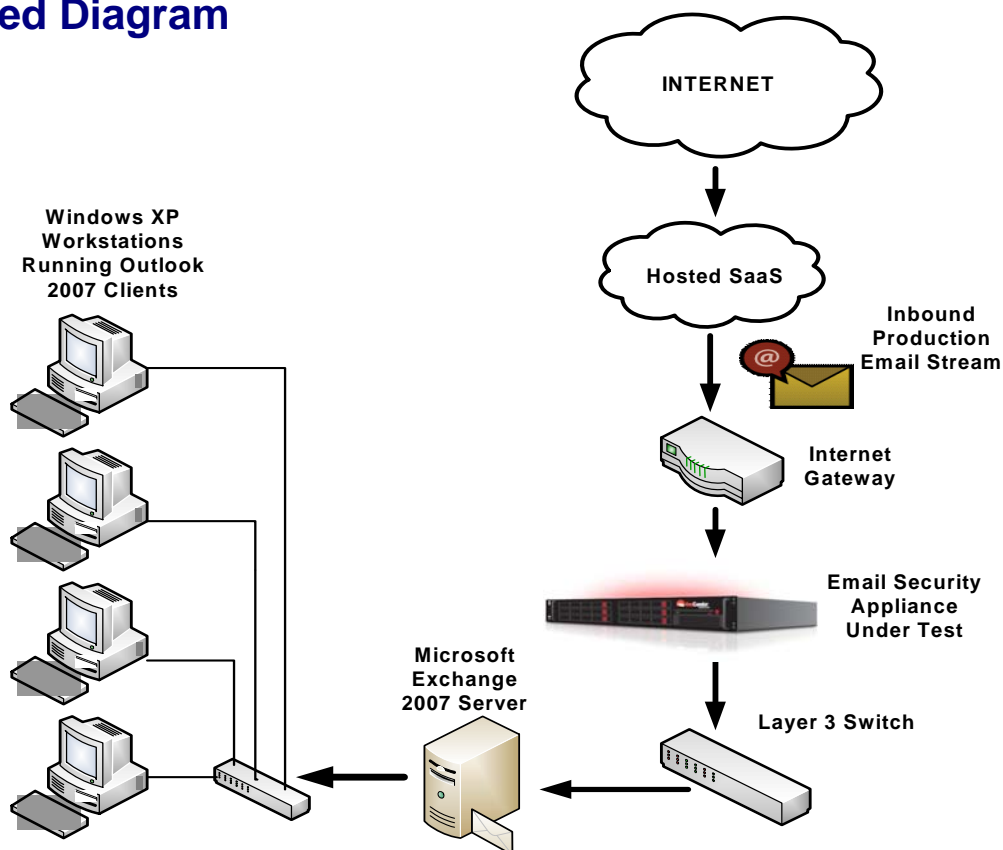
Figure 4: Spam Filter False Positives
Number of Legitimate Messages Inappropriately Blocked



Source: Miercom, July 2010

False positives, or the blocking of legitimate email, can disrupt critical business communications. Red Condor and MessageLabs recorded no false positives during the test period.

Test Bed Diagram



Devices Under Test

Cloudmark - Cloudfilter Solution; MessageLabs/Symantec Email AntiSpam, Email Antivirus and Email Image Control; MxLogic/McAfee Email Defense Package; Proofpoint P340, Version 6.0.2.105; Red Condor MAG2700 R05.00.02 with Vx Technology 7.0. All spam engines, antivirus engines, spam fingerprints, virus definitions and signature sets were current at the time of testing.

How We Did It

All testing was conducted at Miercom Labs. Each email security solution was deployed in a production environment receiving 3,000 to 4,000 emails each day. Each solution under test received emails coming directly from the Internet with no relay between the sender of the message and the solution under test. The domains used for testing have existed for the past 20 years with all real user mailboxes receiving spam and legitimate emails. Testing was conducted with each solution for one week. Red Condor/MAG2700 was tested from 15 March to 22 March 2010, MxLogic-McAfee/Email Defense Package was tested from 25 March to 1 April 2010, MessageLabs-Symantec/Email AntiSpam, Email Antivirus and Email Image Control was tested from 2 April to 9 April 2010, Cloudmark/Cloudfilter was tested from 15 April to 22 April 2010 and Proofpoint/P340 was tested from 30 April to 7 May 2010.

The setup included production Windows Exchange Server 2007 running on Windows Server 2003 R2. The MX records were changed to point to the email security solution under test. Once the DNS update was propagated properly throughout the Internet, the production email server was then locked down to receive email only from the solution under test.

Ixia (www.ixiacom.com) IxLoad and XM2 chassis were used to generate SMTP traffic for protocol verification. IxDefend is used in protocol integrity verification.

The tests in this report are intended to be reproducible for customers who wish to recreate them with the appropriate test and measurement equipment. Contact reviews@miercom.com for details on the configurations applied to the System Under Test and test tools used in this evaluation. Miercom recommends customers conduct their own needs analysis study and test specifically for the expected environment for product deployment before making a product selection.

Miercom Performance Verified

Based on our assessment of email security products, the Red Condor MAG2700 is awarded the Performance Verified certification for its achievements of producing the lowest message misclassification rate among the solutions tested.

The MAG2700 with Vx Technology is the only email security solution that acts as a hosted service, a network appliance, or as a hybrid, combining the best features of each platform. We found Red Condor an impressive email security solution that provides load sharing and delivers high availability.



MAG2700
Email Security
Appliance



Red Condor
1300 Valley House Drive
Rohnert Park, CA
1-888-966-7726
www.redcondor.com

About Miercom's Product Testing Services

Miercom has hundreds of product-comparison analyses published over the years in leading network trade periodicals including Network World, Business Communications Review - NoJitter, Communications News, xchange, Internet Telephony and other leading publications. Miercom's reputation as the leading, independent product test center is unquestioned.

Miercom's private test services include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: [Certified Interoperable](#), [Certified Reliable](#), [Certified Secure](#) and [Certified Green](#). Products may also be evaluated under the [NetWORKS As Advertised](#) program, the industry's most thorough and trusted assessment for product usability and performance.



Report 100607

reviews@miercom.com

www.miercom.com

 Before printing, please
consider electronic distribution

Product names or services mentioned in this report are registered trademarks of their respective owners. Miercom makes every effort to ensure that information contained within our reports is accurate and complete, but is not liable for any errors, inaccuracies or omissions. Miercom is not liable for damages arising out of or related to the information contained within this report. Consult with professional services such as Miercom Consulting for specific customer needs analysis.