westcoast labs

January 2009

Anti-spam Comparison Report

Anti-spam Comparison Report

Test Laboratory Details

US Headquarters and Test Facility

West Coast Labs, 16842 Von Karman Avenue, Suite 125

Irvine, CA 92606, U.S.A., Tel: +1 (949) 870 3250, Fax: +1 (949 251 1586)

European Headquarters and Test Facility

West Coast Labs, Unit 9 Oak Tree Court, Mulberry Drive, Cardiff Gate Business Park, Cardiff, CF23 8RS, UK,

Tel: +44 (0) 29 2054 8400, Fax: +44 (0) 29 2054 8401

Test Facilities also in Delhi, Hong Kong and Sydney, Australia.

Authors: Richard Thomas, Paul Jones **Tel** : +44 (0)2920 548 400

Date: *23rd* January 2009 **Issue:** 1.1

Anti-spam Comparison Report

Contents

Anti-spam Comparison Report

Introduction

West Coast Labs performed an anti-spam comparative test on various email solutions related to spam detection rate over a series of at least 100,000 emails per solution.

The vendors that were considered were the following (alphabetically, and by deployment type):

- **Appliances**
  - Barracuda
  - Fortinet
  - Ironport
  - McAfee
- **Hosted Services (SaaS)**
  - Trend Micro
- **Software**
  - Microsoft
  - Sophos
  - Symantec
  - Trend Micro
  - Websense

Anti-spam Comparison Report

Test Configuration

Each solution in the test was configured in accordance with the solution provider's instructions, and was allowed to download the latest updates prior to the testing. During the course of the testing, signature updates were allowed. It should also be noted that no training was conducted during the testing.

All the software-based solutions were installed and configured to receive the West Coast Labs mail feed. A series of test messages were then sent through each solution in turn to determine whether they were correctly routing through to the target collection point. Once confirmed, the products were then updated to the latest releases and a forensic image was taken of each.

Simultaneously, the four appliances had the appropriate setup processes/wizards run. As with the software-based solutions, engineers then sent a series of test messages to check that the messages were correctly routing to the target collection points. Where possible, backups of the appliance configuration files were then saved.

The hosted service, InterScan Messaging Hosted Service, was then configured by engineers at Trend Micro using the network and domain information provided by West Coast Labs. The routing of traffic was then subsequently checked.

Anti-spam Comparison Report

Test Configuration (Cont.)

With the setup complete, West Coast Labs reset and deleted all previous test emails and then redirected the live corporate mail feed at each of the solutions, using in-house multiplexing systems.

Throughout testing, West Coast Labs engineers took a daily backup of each solution's mailbox. After six days, the mail feed was redirected away from the solutions and the final mailbox saved.

Anti-spam Comparison Report

Test Methodology

West Coast Labs used their live corporate enterprise spam feed, multiplexed across each of the solutions, so that each solution received the same emails. Wherever possible, the multiplexing server was designated as a known upstream server.

Testing was conducted over a total of 6 days with subsequent analysis.

The following types of email were removed from the stream prior to analysis:

- Bounced Mail
- Forwarded Mail
- Corrupted Spam
- Virus Emails
- Out of Office Notifications
- Newsletters

Following the removal of these, a series of scripts were run to ensure identical test sets across each of the ten solutions.

The table in the Test Result section is based on analysis performed against the 50,124 spam messages remaining once the types mentioned above were removed. There were also 4,249 genuine messages sent through each of the devices.

False Positive rates were calculated based on the number of genuine messages that had been incorrectly identified as spam. These genuine messages were sent through each of the solutions and originated from separate live source networks controlled and owned by West Coast Labs.

Anti-spam Comparison Report

Test Methodology (Cont.)

No externally owned email hosts or domains were used to send any of the genuine feed so that each message was coming from a known-good source.

All genuine emails replicated communications that would be expected for a corporate network. These messages were initially taken from genuine business emails, used with the original sender's consent, and subsequently anonymized so that any identifiable content was replaced.

Message counts were then taken and the catch rates calculated. The results for each were based upon the following formulae:

Spam detection rate = (spam marked as spam / total spam) * 100
False Positive rate = (genuine marked as spam / total genuine) * 100

Therefore each result can be expressed as a percentage.

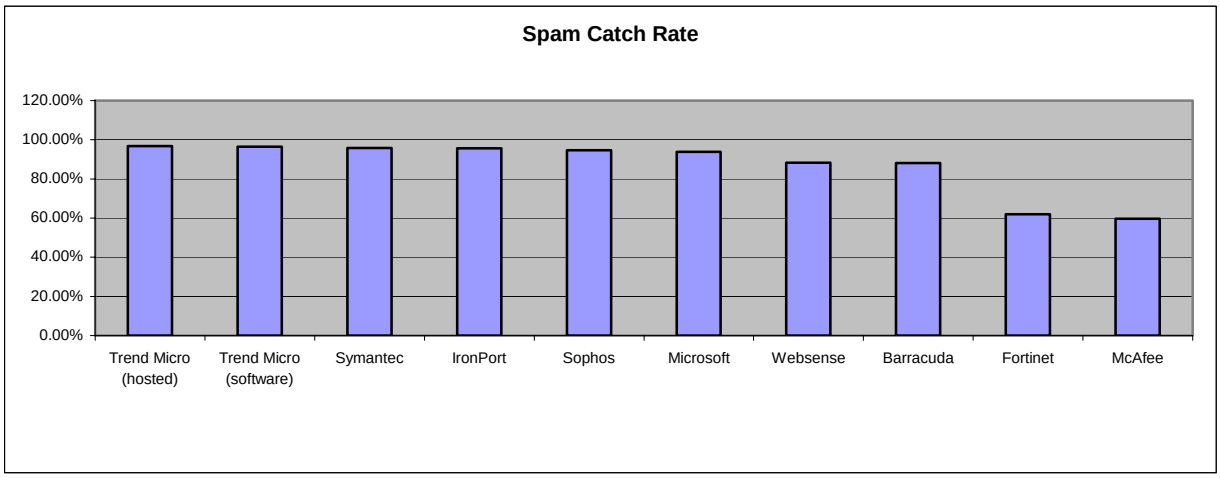
Anti-spam Comparison Report

Test Results

Direct Comparative of Catch Rates and False Positives

The following table contains the spam detection rates for the solutions tested. The False Positive detection rates were also calculated, and were negligible across each of the solutions. Only Microsoft recorded a significant False Positive rate of 0.71%.

Vendor	Spam Catch Rate
Trend Micro (hosted)	96.71%
Trend Micro (software)	96.48%
Symantec	95.73%
IronPort	95.63%
Sophos	94.63%
Microsoft	93.89%
Websense	88.25%
Barracuda	88.07%
Fortinet	61.96%
McAfee	59.66%



Anti-spam Comparison Report

Product Details

Trend Micro InterScan Messaging Hosted Security

To configure Trend Micro InterScan Messaging Hosted Security, West Coast Labs provided Trend Micro with the relevant domain and network address information needed in order to correctly redirect incoming mail along with the configuration, by Trend Micro, of an upstream server address.

Trend Micro InterScan Messaging Hosted Security service had the highest detection rate in the test with a catch rate of 96.71%.

Detection Rate: 96.71%

Trend Micro InterScan Messaging Security Suite - Version: 7.0 build 5547

Trend Micro InterScan Messaging Security Suite is a software-based gateway email security product, and the second Trend Micro product used in this test. The solution is available for Solaris, Linux, and Windows-based platforms and requires 1Gb of RAM and 500Mb of hard disk space.

InterScan Messaging Security Suite scored the second highest detection rate in the test with a catch rate of 96.48%.

Detection Rate: 96.48%

Anti-spam Comparison Report

Product Details (cont.)

Symantec - Version: 5.0

Symantec's Mail Security for SMTP is a software-based solution designed to be installed on a Windows server operating system running an SMTP mail server. The solution is available for a range of platforms including Solaris, Linux, and Windows. Minimum system requirements for this solution comprise of 1Gb of RAM and 512Mb of hard disk space. No support for 64 bit architecture was apparent at time of testing.

Detection Rate: 95.73%

IronPort - Version: 6.1.0.307

IronPort's C150 is an appliance that is specifically intended to work at the gateway level and check incoming messages for spam. The C150 is the entry level model of the 'C' series of IronPort appliances and allows throughput speeds of up to 1Gb.

Detection Rate: 95.63%

Anti-spam Comparison Report

Product Details (cont.)

Sophos - Version: 3.0.2.0

PureMessage for Exchange is a software-based solution that works in conjunction with an existing Microsoft Exchange server. The solution has a minimum recommended requirement of 256Mb of RAM and 150Mb of hard disk space. Support for both 32 bit and 64 bit architecture is provided.

Detection Rate: 94.63%

Microsoft - Version: 10.1.0746.0

Microsoft's Forefront Security for Exchange Servers is a software-based solution intended to be installed in-line with a Microsoft Exchange mail server. The solution supports both 32 bit and 64 bit architecture and requires a minimum of 1Gb of RAM and 550Mb of hard disk space.

Detection Rate: 93.89%

Websense - Version: 6.1.0

Websense Email Security is a software-based solution and required a computer running Windows 2000 Server along with Exchange 2000. The solution requires a minimum of 1.7Gb of hard disk space and 512Mb of RAM. No support for 64 bit architecture was evident at time of testing.

Detection Rate: 88.25%

Anti-spam Comparison Report

Product Details (cont.)

Barracuda - Version: 3.5.11.025

Barracuda's Spam Firewall 200 is a gateway appliance specifically designed to protect against spam and other email-borne threats. The appliance supports traffic of up to 100Mb and has a recommended user limit of 50.

Detection Rate: 88.07%

Fortinet - Version: 3.00 build 199

Fortinet's Fortimail-100 is designed to work on the gateway level and actively scan incoming messages for spam and other unwanted content. This appliance is intended to handle up to 100Mb throughput and can support up to 50 separate email domains.

Detection Rate: 61.96%

Anti-spam Comparison Report

Product Details (cont.)

McAfee - Version: 4.5

The McAfee product used in this test was the Secure Internet Gateway (SIG) 3100 appliance. The SIG supports a recommended maximum of 400 users while handling network speeds of up to 1Gb.

Secure Internet Gateway (SIG) 3100 had a detection rate of 59.66%. There were two issues noted by West Coast Labs engineers during the course of testing. The first was related to sporadic down-time that appeared to coincide with any configuration changes made by engineers. The second issues related specifically to the testing being done on 26th September – the SIG box ceased processing traffic for several hours, eventually starting to process messages again later that day. West Coast Labs can ascertain no reason for this behaviour, and log examination does not show anything unusual.

Anti-spam Comparison Report

Conclusion

The two Trend Micro solutions, InterScan Messaging Hosted Security and InterScan Messaging Security Suite, finished with the highest catch rates in the test. The hosted service had the highest catch rate at 96.71% followed by the software solution at 96.48%.

The products with the lowest detection rates were the McAfee and Fortinet solutions with catch rates at less than 80% with the Microsoft solution recording the highest False Positive rate.

It should be noted that this test was performed with no ongoing training – a step usually recommended by most anti-spam vendors. Instead this test was configured based on out-of-box configurations using the vendor's recommended settings to mimic the customer experience after initial purchase. With a period of training and ongoing maintenance, these figures are likely to be different and result in an improvement to detection rates or False Positive rates as appropriate.

Overall, both of the solutions provided by Trend Micro for this test demonstrated better protection rates for end users using this live test set against the other solutions tested. With a period of training, customers can expect to receive an even higher effectiveness from these products.

Anti-spam Comparison Report

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 the 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. West Coast Labs provide test results for any particular product tested, most relevant at the time of testing and within the specified scope of testing and relative to the specific test hardware, software, equipment, infrastructure, configurations and tools used during the 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.

Revision History

Issue	Description of Changes	Date Issued
1.0	Trend Micro Anti-Spam Comparative	01 January 2009
1.1	Layout Changes	23 January 2009

US SALES
T +1 (949) 870 3250

EUROPE SALES
T +44 (0) 2920 548400

CHINA SALES
T +86 1 343 921 7464

CORPORATE OFFICES AND TEST FACILITIES

US Headquarters and Test Facility
West Coast Labs
16842 Von Karman Avenue, Suite 125,
Irvine, California, CA92606, USA
T +1 (949) 870 3250 , F +1 (949) 251 1586

European Headquarters and Test Facility
West Coast Labs
Unit 9, Oak Tree Court, Mulberry Drive
Cardiff Gate Business Park, Cardiff CF23 8RS, UK
T +44 (0) 2920 548400 , F +44 (0) 2920 548401

Asia Headquarters and Test Facility
A2/9 Lower Ground floor, Safdarjung Enclave,
Main Africa Avenue Road, New Delhi 110 029, India.

Test Facilities also in Hong Kong and Sydney

E info@westcoast.com
W www.westcoastlabs.com