

Test Report October 2007

# InterScan Messaging Security Suite Anti-Spam Technology Report

# InterScan Messaging Security Suite

## Vendor Details

Name: Trend Micro Inc.

Address: 10101 N. De Anza Blvd.,  
Cupertino, CA - 95014, USA

Telephone: + 1 (800) 228 5651

Website: [www.trendmicro.com](http://www.trendmicro.com)

Product: InterScan Messaging Security Suite 7.0

## Test Laboratory Details

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

Telephone: +44 (0) 29 2054 8400

Date: October 2007

Issue: 1.0

Author: Chris Elias

## Contact Point

Contact name: Chris Elias

Contact telephone number: +44 (0) 29 2054 8400

---

# InterScan Messaging Security Suite

## Contents

Introduction	4
Test Network	6
Test Methodology	7
Product Test Reporting	8
Checkmark Certification	9
The Product	10
Test Report	12
Test Results	16
West Coast Labs Conclusion	17
Security Features Buyers Guide	19

# InterScan Messaging Security Suite

## Introduction

### The ever evolving spam threat

“Two years from now, spam will be solved.” Bill Gates–Jan. 2004

At the beginning of 2004, Bill Gates was addressing the World Economic Forum in Switzerland and confidently predicted that “Two years from now, spam will be solved.” Sadly his prophecy has proved somewhat wide of the mark as reports continue to emerge about the size of the problem.

Spam continues to rise dramatically with Trend Micro reporting that spam more than doubled in the third quarter of 2007, and spam now accounts for more than 90% of all email traffic on the Internet.

The nature of spam has also changed. In 2004 spam content was dominated by pornography, Viagra sales and the infamous “Nigerian scam” advance-fee fraud spam. Those types of spam are very much still with us but have been added to by phishing attacks, “Pump-and-Dump” scams (which involve artificially inflating the price of a stock in order to make a quick profit on stock previously purchased cheaply) and spam that tricks users into following URL links to web sites that download malicious code that will compromise their machines.

The methods used by spammers to launch their attacks have also transformed over time. The vast majority of unsolicited email is now being sent via vast armies of infected PCs known as botnets—often these are the machines of home users who are unaware that they are part of the problem.

This distributed system approach is making it more difficult to separate out spam emails based upon simple network-based criteria, and so companies providing anti-spam technologies are having to provide more intelligent filtering solutions.

---

## InterScan Messaging Security Suite

Trend Micro's Senior Threat Researcher, Jamz Yaneza, summarizes how spam has changed, "Spam is still the primary email security concern, but it is no longer a simple, mass-mailed advertisement. Hackers and spammers have joined forces, using botnets to optimize spam profits and applying spam techniques to send malware, phishing, and bulk mail attacks."

The spammers are also always trying to find new ways of bypassing anti-spam defenses. In early attempts, spammers tried to obscure spam words with tricks such as replacing letters with symbols (e.g. "a" with "@"), adding spaces or characters between letters, and many other variations. In late 2006, spammers began sending image spam—emails with images containing the spammer's messages. Image spam grew in prevalence throughout the first half of 2007. Peter Firstbrook, security research director for Gartner, reported that image spam went from 6 percent of all spam in Q3 of 2006 to 30 percent by Q4 and it made up almost 40% of all spam by mid-2007.

Image spam has declined as anti-spam filters have improved their image spam detection. Spammers are now turning to attachment spam. In June 2007, PDF spam flooded the Internet. In mid-August 2007, PFD spam made up over 18% of all spam according to Trend Micro and close to 30% according to Sophos. Both vendors report that PDF spam decreased to almost 0% by the end of August. Spammers have turned to other attachment types, including ZIP, XLS, RTF, and even MP3 files, playing an audio file of the spam message.

Image spam and attachment spam are not only harder to block, the spam messages are larger than simple text messages. According to some reports, the average size of a spam message has increased by 77% since September last year, from 6.62Kbytes to 11.76K) and continues steadily to grow. This adds to the cost of managing email, it wastes bandwidth and also consumes storage in quarantines and archives.

As a result, anti-spam vendors are now having to adapt to these new threats by enhancing existing techniques such as heuristics rules as well as reputation services to keep the bulk of email entirely off of the network due to the increase in both quantity and size of spam emails. Where will it all end?

# InterScan Messaging Security Suite

## **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 tests through identified email domains and changed the MX records to divert the mail stream through the hosted service.

# InterScan Messaging Security Suite

## 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 inline with the vendors 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.

## InterScan Messaging Security Suite

### 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

# InterScan Messaging Security Suite

## 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



## InterScan Messaging Security Suite

### The Product

#### Introduction

IMSS - InterScan Messaging Security Suite Version: 7.0 Build:WIN32\_5651

InterScan Messaging Security Suite (IMSS) is Trend Micro's software gateway email security solution, which is part of a family of solutions including an appliance and a hosted service. Trend Micro's commitment to performance and flexibility is reflected in these solutions, which scan email messages for spam, viruses and other mail-borne threats and provide content filtering to enforce compliance and prevent data leakage. IMSS can be deployed to a Windows 2000 server running SP4 or a



Windows 2003 server operating system, and there are \*nix distributions of the product available for Solaris or Linux. For this test West Coast Labs engineers deployed IMSS on a machine running Windows 2003 Server patched to Service Pack 2.

IMSS can be purchased directly from the Trend Micro website, and is distributed in one of two ways—either a direct download from the website or by delivery of a boxed version. For those companies who wish to evaluate the solution and experiment with how it might fit into a corporate network, there is also a 30-day free trial of IMSS which can be downloaded from the website if the interested company supplies some basic details such as address, company name and contact email address.

# InterScan Messaging Security Suite

## Installation and Configuration

The installation of IMSS is a simple process and to aid administrators Trend Micro has made available a detailed Getting Started Guide. This includes helpful sections such as a Product Overview, Installation Planning, and other configuration advice to get the system integrated within a network with minimal fuss. IMSS uses a standard Windows setup wizard to install the product, but users should be aware that the solution also requires an MSDE database server in order to function correctly. Helpfully, administrators are given the choice either to install a new MSDE database server from within the main IMSS routine, or to use an existing database server on the network.

IMSS has two main components which are installed by default. The IMSS Central Controller is a web server, which makes it possible to configure and control IMSS. The IMSS Scanner Service is the main technology base that is responsible for scanning SMTP and POP3 messages for threats.

There are also two other optional components that can be installed. The IMSS End-User Quarantine Service allows certain users to view spam that has been quarantined and also can release messages from quarantine if required. The IMSS End-User Quarantine Database logs all spam or policy violation events. Installing these extra features does require an additional 200MB of hard disk space, however, the extra functionality will be considered well worth it by many corporations.

After specifying the components to install, the setup then copies the necessary files and installs the services to the server. As with a large number of software installations, the system requires a reboot after setup has taken place.

## InterScan Messaging Security Suite

After rebooting the system and logging into the IMSS SSL-secured web interface, more advanced configuration is required in order for successful operation of the solution. Trend Micro has made this an easy process by incorporating a Configuration Wizard allowing product setup in 8 easy steps.



During the configuration the administrator is required to enter information on SMTP routing, for example, specification of the domain that IMSS will be protecting and onto what IP address or mail server the messages should be relayed. It is also possible to setup Notification Settings, such as where IMSS will send alerts or notifications, for example, to a designated email address. In the Update Source section Administrators should specify where IMSS should search for updates. By default the source is set to Trend Micro's Active Update Server. Administrators also need to specify if the network uses a web proxy server, as this could potentially be a cause of update failures.

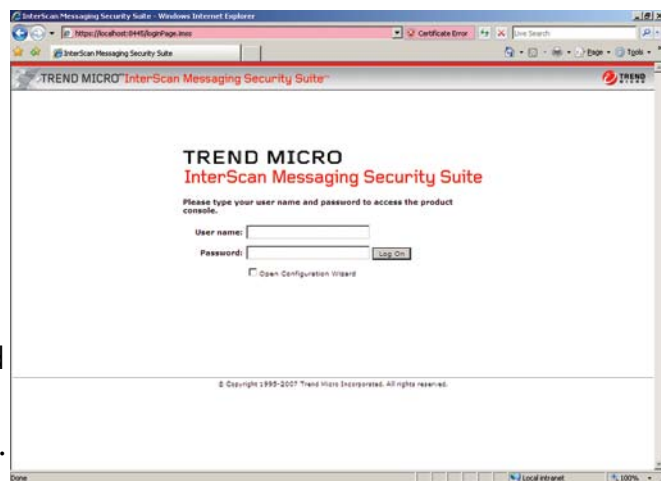
The product requires two license keys for maximum functionality –one for the Trend Micro Antivirus and Content Filter functionality and one for the Spam Prevention Solution (SPS). After completion of the Configuration Wizard, Administrators should update their corporate MX records to deliver mail to IMSS rather than the current mail server to enable scanning of the incoming mail.

Once the setup is complete users should manually start the scanning services from within the home page of the web administration console. These are clearly labeled buttons at the bottom of the first page.

## InterScan Messaging Security Suite

### Operations and Features

As with most products of this genus, IMSS uses an SSL-encrypted web interface to allow secure and easy administration. After successfully logging into the GUI by entering a user name and password, the administrator is greeted by a summary page showing the product status. This displays important information, such as the updates most recently applied and which services are currently running.

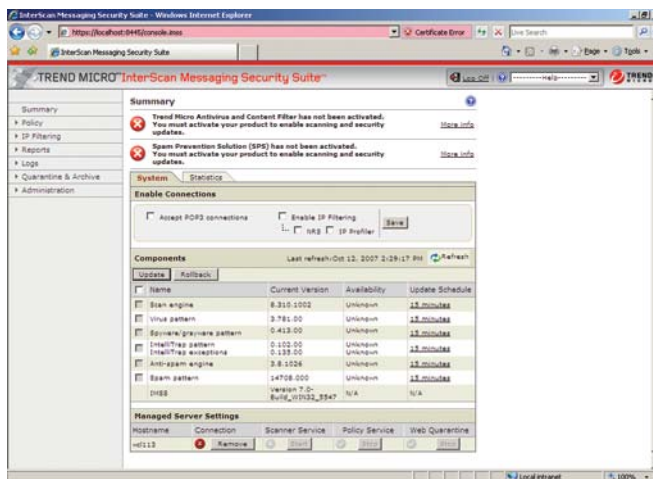


Separate to this web interface, the solution also has a convenient real-time monitor running on the server on which it is installed. This allows the administrator to see exactly what mail is coming in at any particular time and also if there are any problems with mail traffic. The monitor also shows further important data including counters that display virus threats, spam and queued messages.

IMSS has 2 detection engines coupled with 4 databases that provide a multi-layered standard of protection. The main scanning engine protects against malware and there is a distinct and specific anti-spam engine. The databases are broken down into Virus, Spyware/ Grayware, IntelliTrap and IntelliTrap exceptions, and Spam. This wide ranging detection capability is complemented by Email Reputation and IP filtering.

## InterScan Messaging Security Suite

There are two main policies set by default—a “Global Antivirus” rule and a “Default Spam” rule. These policies automatically quarantine any detected incoming malware or spam. Further policies can be created and customised to suit any individual organizational need.



The “Default Spam” rule can be altered not only to nullify spam messages and phishing emails, but also to react to messages based upon keyword expressions. Examples of keyword expression categories include Hoaxes, Profanity, Sexual Discrimination, Racial Discrimination, and Chain Mail. The spam detection settings within this rule may be configured to low, medium, or high settings. It is also possible to enhance these basic settings further by using a user-specified level of filtering. This ranges on a numeric scale between 3 and 10 with 3 being the lowest level of filtering.

IMSS also includes blacklist functionality called Blocked List that is based upon sender email addresses. Conversely, it is also possible to whitelist known good senders using the Approved list.

# InterScan Messaging Security Suite

## Reporting

Reports can be scheduled at daily, weekly, or monthly intervals, and there is a wide range of reports available. The administrator can specify what content to include within these reports, for example, virus and malicious code summaries, spam summaries, and top 10 spam recipients. Given the scope of reporting options, administrators should be able to easily find any information required.

Within the summary page there is also a statistics section and from here the administrator can gain an informed overview of what types of messages and volumes are being processed.

There are 3 main statistical overviews. Performance overview displays the incoming and outgoing mail in both graphical and tabular format. Scan performance shows catch rates and overviews related to various types of mail that have been processed, including malicious code, spam, phishing mail, and viruses. The final statistical overview is IP filtering performance and this displays IP addresses that have been blocked for spam policy violations, Directory Harvest Attacks, zombie-based attacks caught by the Email Reputation , and bounced mails. Administrators are given the ability to view these statistics from 1 day up to the past 7 days.

## InterScan Messaging Security Suite

### Results

<u>Type of Mail</u>	<u>Detected as Genuine</u>	<u>Detected as Spam</u>
GENUINE	100%	0%
SPAM	3%	97%

Trend Micro's IMSS solution performed well, delivering 100% of the genuine mail correctly and correctly classifying 97% of spam mail.

It is also worth noting that IMSS 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.

# InterScan Messaging Security Suite

## Conclusion

IMSS has a lot to offer organizations wishing to manage their mail flow. The product has good spam blocking capabilities as well as effective scanning engines for stopping malware.

The setup and configuration on Windows is a simple process and ensures that the solution can be in place rapidly. This is due to the well-written Getting Started Guides and walk-through setup wizards that accompany IMSS. The quality of detection combined with the flexibility of rule creation and implementation provides a solid platform with which to filter mail.

The reporting options mean that administrators have a thorough overview of mail traffic on their network. Given that the reporting takes place through the familiar medium of a web interface, the pool of potential administrators is widened.

Overall IMSS performed solidly and consistently under test and the scalability of the product ensures that the solution can be deployed in a range of business sizes up to enterprise level.

## InterScan Messaging Security Suite

### Security Features Buyers Guide

#### InterScan Messaging Security Solutions

The Trend Micro InterScan™ Messaging Security solution family integrates anti-spam, antivirus, anti-phishing, and anti-spyware with content filtering to enforce compliance and prevent data leakage.

#### InterScan Messaging Security Suite

Offered on the leading operating systems, this flexible software solution is delivered on a single, highly scalable platform with centralized management for easy, comprehensive email security at the gateway.

#### InterScan Messaging Security Appliance

Optimized for high performance and continuous security, this easy-to-install appliance provides comprehensive gateway email security.

#### InterScan Messaging Hosted Security

This cost-effective hosted email security solution features high availability, reliability, and scalability. Organizations can choose the management level that best suits their security needs with either streamlined administration or granular access and control.

#### Spam Prevention Solution

Trend Micro Spam Prevention Solution provides comprehensive anti-spam in a flexible software solution. Email Reputation and IP Profiler stop most threats before entering the gateway and the composite engine keeps remaining threats out of the inbox.

url : <http://us.trendmicro.com/us/products/enterprise/interscan-messaging-security-suite/index.html>

<http://us.trendmicro.com/us/products/enterprise/interscan-messaging-security-appliance/>

<http://us.trendmicro.com/us/products/enterprise/interscan-messaging-hosted-security/>

<http://us.trendmicro.com/us/products/enterprise/spam-prevention-solution/index.html>

# InterScan Messaging Security Suite

## Security Features Buyers Guide

### Business Benefits....as stated by Trend Micro

The InterScan Messaging Security solutions integrate protection against all email threats, securing the network against standalone, blended and targeted email attacks. This comprehensive protection increases employee productivity as well as the security, availability, and reliability of critical IT infrastructure. The solutions also provide content filtering to enforce regulatory compliance and prevent data leakage through email and attachments. This integrated email security reduces costs by consolidating infrastructure and streamlining management through a single, centrally managed platform. The InterScan Messaging Security solutions reduce the risks to business continuity, employee productivity, and data privacy and security while enabling critical business communications.

url :

<http://us.trendmicro.com/us/products/enterprise/interscan-messaging-security-suite/index.html>

<http://us.trendmicro.com/us/products/enterprise/interscan-messaging-security-appliance/>

<http://us.trendmicro.com/us/products/enterprise/interscan-messaging-hosted-security/>

<http://us.trendmicro.com/us/products/enterprise/spam-prevention-solution/index.html>

## InterScan Messaging Security Suite

### Security Features Buyers Guide

#### Technical Benefits....as stated by Trend Micro

As the leader in gateway security, Trend Micro offers industry-leading anti-spam effectiveness and award-winning antivirus. The InterScan Messaging Security solutions provide an anti-spam solution that is strategically configured to keep the majority of email threats completely off of the network, preserving valuable network resources. These solutions also provide antivirus with zero-day protection and broader malware security, including anti-spyware to defend against targeted email attacks. The flexible content filtering identifies content by attachment characteristics, dictionaries, keywords, lexicons, and customized data rules. This comprehensive protection is provided in a highly scalable solution with a centrally managed, Web-based administrative console for easy management.

url:

<http://us.trendmicro.com/us/products/enterprise/interscan-messaging-security-suite/index.html>

<http://us.trendmicro.com/us/products/enterprise/interscan-messaging-security-appliance/>

<http://us.trendmicro.com/us/products/enterprise/interscan-messaging-hosted-security/>

<http://us.trendmicro.com/us/products/enterprise/spam-prevention-solution/index.html>

---

# InterScan Messaging Security Suite

## Security Features Buyers Guide

### InterScan Messaging Security Suite—developments in the last 12 months

The InterScan Messaging Security solutions and standalone Spam Prevention Solution include three distinct anti-spam techniques integrated into one solution.

- **Email Reputation**

Email Reputation provides the initial tier of defense by stopping spam and phishing prior to entering the gateway—before they can flood the network, overload mail servers, and burden IT resources. Email Reputation uses two types of reputation services to stop spam. The first verifies IP addresses of incoming email against the world's largest, most trusted reputation database and the second provides a dynamic reputation service, which identifies new spam and phishing sources, even stopping threats from zombies and botnets when they first emerge.

- **IP Profiler\***

IP Profiler is a patent-pending approach that creates a firewall against Directory Harvest Attacks (DHA) and bounced mail attacks and provides customer-specific reputation services based on the organization's email traffic. Working together, Email Reputation and IP Profiler keep email threats completely off of the network, securing the network and preserving bandwidth, storage, and other network resources.

- **Trend Micro anti-spam composite engine**

The robust anti-spam composite engine provides the final tier of protection by filtering spam and phishing emails at the gateway through statistical analysis, advanced heuristics, signature filtering,

# InterScan Messaging Security Suite

## Security Features Buyers Guide

whitelists, blacklists, and multi-lingual spam detection, catching any remaining threats before they reach the inbox. The anti-spam composite engine includes patent-pending image spam detection technology, embedded URL reputation, and other cutting-edge approaches to protect customers as spam and other threats evolve.

*\*The hosted service does not contain IP Profiler because the tuning is conducted by Trend Micro and the customer-specific protection offered in IP Profiler is not required.*

## InterScan Messaging Security Suite

### **Additional Noteworthy Product Features**

Features included in the InterScan Messaging Security solutions

- Powerful email threat protection
- Industry-leading, award-winning antivirus with zero-day protection
- Extended malware protection for spyware in email and other malware threats
- Content filtering to enforce compliance and prevent data leakage
- Multi-tier anti-spam with Email Reputation, IP Profiler, and Trend Micro's anti-spam composite engine
- Anti-phishing technologies, including sender reputation, signatures, heuristics, and embedded URL reputation
- Predictive techniques to combat targeted attacks including zero-day protection, heuristics, and behavioral analysis
- Integrated management
- Highly scalable solution allows the use of multiple servers or appliances and the hosted service will scale to meet the needs of any organization.
- A single, Web-based management console centralizes policy, quarantine, archive, logging, and reporting
- Auto-updates provide hands-off, up-to-date threat protection
- Protection optimized to keep threats off the network, not just out of the inbox
- LDAP integration, delegated administration, and message tracking simplify administration
- Web-based End-User Quarantine and quarantine notification emails enable end users to manage their own spam
- Trend Micro Control Manager provides centralized management between the appliance and software solutions and other Trend Micro products

# westcoast labs

## **US SALES**

T +1 (717) 243 5575

## **EUROPE SALES**

T +44 2920 548 400

## **GLOBAL HEADQUARTERS**

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