



February 2009

Trend Micro™
Worry-Free™ Business Security
Comparative Testing Report

Trend Micro™ WFBS Comparative Testing Report

Vendor Details

Vendor:

Trend Micro™, 10101 N. De Anza Blvd, Cupertino, CA 95014, USA

Tel: + 1 (800) 228 5651

Products:

Trend Micro™ Worry-Free™ Business Security and competitor products.

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, Chris Elias, Matt Garrad, Lysa Myers**

Tel : +44 (0)2920 548 400

Date: **20th February 2009**

Issue: **1.0**

Trend Micro™ WFBS Comparative Testing Report

Contents

Introduction	5
Executive Summary	6
Results	
1. Installation	10
2. Memory Footprint: Kernel vs User Mode	14
3. Web Threat Protection	19
4. Location Awareness	21
5. Firewall and IDS / IPS	23
6. Transaction Protector: Keylogger Protection	27
7. Transaction Protector: Wi-Fi Advisor	30
8. TrendProtect	33
9. Behaviour Monitoring: QuickBooks Protection	38
10. Security Dashboard	40
11. Email Protection Vector	42
12. File Protection Vector	45
13. Data Leakage	47
14. IM Content Filtering	49
15. Outbreak Defence	51
16. Vulnerability Assessment	54
17. Damage Cleanup	56
Conclusion	58
Appendix A: References	59
Appendix B: Suggested Quickbooks methodology	60
Appendix C: Test Tool Identification	61
Appendix D: Software Specification	63

Trend Micro™ WFBS Comparative Testing Report

Appendix E: Hardware Specification	66
Appendix F: Component Comparison	67
West Coast Labs Disclaimer	75

Trend Micro™ WFBS Comparative Testing Report

Introduction

Trend Micro Inc commissioned West Coast Labs to carry out a series of independent performance evaluations through comparative tests on the Trend Micro Worry-Free™ Business Security package comparing it to an industry average made up of other leading vendors.

As agreed with Trend Micro at the outset of the project, this technical report forms the basis for a narrative document based on the comparisons drawn between the Trend Micro solution and the solutions from McAfee and Symantec.

All testing was conducted at West Coast Labs' UK test facility from September to December 2008.

Trend Micro™ WFBS Comparative Testing Report

Executive Summary

The goal of these tests was to establish the availability, and where possible the effectiveness, of various security technologies within three of the leading vendors' solutions. Contained in the following pages are the results of these tests, laying out the methodology followed to obtain them and descriptions of any issues that were encountered at that time.

The methodologies used, as described later in this report, were adhered to for each solution and not weighted in favour of any one vendor - in accordance with West Coast Lab's ISO17025 certification. However, some tests are against technologies not available on each solution; where applicable this has been stated. In keeping with this, a document has been drawn up separately that provides a means of cross-referencing the available technologies for each solution.

The solutions, as selected by Trend Micro for this comparison, are as follows:

Trend Micro Worry-Free™ Business Security Advanced

Symantec Endpoint Protection

McAfee Total Protection Advanced

More detailed information is laid out in the Software Specification section of this report.

Trend Micro™ WFBS Comparative Testing Report

Executive Summary (Cont.)

West Coast Labs were specifically asked to examine the following technologies and features:

1. [Installation](#)
2. [Memory Footprint: Kernel Vs User Mode](#)
3. [Web Threat Protection](#)
4. [Location Awareness](#)
5. [Firewall and IDS / IPS](#)
6. [Transaction Protector: Keylogger Protection](#)
7. [Transaction Protector: Wi-Fi Advisor](#)
8. [TrendProtect](#)
9. [Behaviour Monitoring: QuickBooks](#)
10. [Security Dashboard](#)
11. [Email Protection Vector](#)
12. [File Protection Vector](#)
13. [Data Leakage](#)
14. [IM Content Filtering](#)
15. [Outbreak Defence](#)
16. [Vulnerability Assessment](#)
17. [Damage Cleanup](#)

The descriptions of each test, along with the methodology used, rationale, and the result are found in the Report Section of this document.

In order to ensure consistency between all installations, a base installation was made of one each of the servers and clients, and these were then forensically imaged over a network connection to give bit-for-bit exact images on each machine prior to the installation of the solutions.

Trend's Worry-Free™ Business Security Advanced product as supplied has shown that it competently handles most of the areas considered here for testing, and certainly seems to have more generalised coverage than the immediate competitors considered here.

Trend Micro™ WFBS Comparative Testing Report

Executive Summary (Cont.)

However, there are notable exceptions that need to be considered by Trend Micro in light of some of the results – these are detailed in the report. In review of the data gathered during the tests, West Coast Labs assigned a score of between one and five for each of the technology sets examined in this test.

Key Technical Requirements	Trend Micro Worry-Free™ Business Security Advanced v5.0	Symantec Endpoint Protection v11.0	McAfee Total Protection Advanced v4.5
Web Protection Technologies			
Test Rating	4 stars	Not tested	3 stars
Email Protection Technologies ⁱ			
Test Rating	4 stars	Not tested	Not tested
File Protection Technologies			
Test Rating	4 stars	4 Stars	4 stars
Perimeter Protection Technologies			
Test Rating	5 stars	4 Stars	4 stars
Data Protection Technologies			
Test Rating	4 stars	4 Stars	3 stars
Mobile Protection Technologies			
Test Rating	5 stars	5 stars	Not tested
Outbreak Protection Technologies			
Test Rating	4 stars	3 Stars	Not applicable

Trend Micro™ WFBS Comparative Testing Report

Executive Summary (Cont.)

Key Business Requirements	Trend Micro Worry-Free™ Business Security Advanced v5.0	Symantec Endpoint Protection v11.0	McAfee Total Protection Advanced v4.5
Installation			
Test Rating	Not applicable	Not applicable	Not applicable
Memory Footprint			
Test Rating	4 stars	3 Stars	3 stars
Management			
Test Rating	5 stars	5 stars	5 stars

The scores attributed to Trend Micro, in each of the Key Technical Requirements fields, are based on ratings given to the following Trend Micro technologies. Further details can be found in the accompanying Narrative document.

Web Protection Technologies: Web Threat Protection, Trend Protect

Mobile Protection Technologies: Location Awareness, Wi-Fi Advisor

Data Protection Technologies: Transaction Protector, Data Leakage, IM

Content Filtering

File Protection Technologies: Behavior Monitoring: QuickBooks, File Protection Vector

Outbreak Protection Technologies: Outbreak Defense, Vulnerability

Assessment, Damage Cleanup

Trend Micro™ WFBS Comparative Testing Report

1. Installation

Executive Summary:

By installing the solutions on a variety of operating systems and processors, engineers noted the changes made by each product. The footprint on the machine, and steps required to install the products were all considered, and results varied significantly.

Trend Micro's product showed the lowest number of changes, however took the most number of clicks to install. However, it was noted that Worry-Free™ Business Security Advanced provided all setup and deployment technologies within one interface.

Rationale:

To observe the installation process, including how many changes each makes to the server and client machines.

Test Results:

Trend Micro Worry-Free™ Business Security Advanced:

It took 19 clicks to install the server for this product. The clients could then be installed remotely from a LAN. It made the following file system and registry changes to the server:

5056 files added

1 file deleted

20 files updated

Trend Micro™ WFBS Comparative Testing Report

1. Installation (Cont.)

2373 registry entries added

88 registry entries deleted

169 registry entries updated

It took a total of 16 clicks to deploy the client via LAN deployment. Once the client had been installed it made the following changes to the system:

1030 files added

4 files deleted

39 files updated

6567 registry entries added

211 registry entries deleted

138 registry entries updated

Symantec Endpoint Protection:

It took 17 clicks to install the server version of this product. The clients could then be installed remotely from a LAN. It made the following file system and registry changes to the server :

4029 files added

3 files deleted

90 files updated

6437 registry entries added

586 registry entries deleted

92 registry entries updated

Trend Micro™ WFBS Comparative Testing Report

1. Installation (Cont.)

It took 17 clicks to deploy the client remotely via LAN and once installed it made the following changes to the system:

1171 files added
12 files deleted
50 files updated
16194 registry entries added
358 registry entries deleted
175 registry entries updated

McAfee Total Protection Advanced:

There was no need to install a server version of this product as it is a managed service. A link is sent from McAfee via email, which provides an Executable file for download. Launching the Executable starts an automatic download of the product complete with the latest updates. The user is then prompted to reboot the machine.

The product made the following file system and registry changes to the client:

733 files added
7 files deleted
50 files updated
6947 registry entries added
322 registry entries deleted
177 registry entries updated

Trend Micro™ WFBS Comparative Testing Report

1. Installation (Cont.)

Test Methodology:

Not included in formal test plan

Implementation of Methodology:

Trend Micro Worry-Free™ Business Security Advanced server was installed on a 64-bit version of Windows 2003 Small Business Edition. The client was installed remotely by LAN on 32-bit versions of Windows XP SP3.

Symantec Endpoint Protection 11.0 Small Business Edition server was installed on a 32-bit version of Windows 2003 Standard Server. The client was installed remotely by LAN on 32-bit versions of Windows XP SP3.

McAfee Total Protection Service for Small Business is delivered via a managed service component; thus there is no server product to install. The protection can be managed online using a username and password which is sent via email by McAfee. The clients were installed on 32-bit versions of Windows XP SP3, via a link sent in email to download the product.

Tools Used:

Installrite ⁽¹⁾

Trend Micro™ WFBS Comparative Testing Report

2. Memory Footprint: Kernel vs User Mode

Executive Summary:

The Kernel mode and User mode figures are provided below for each of the solutions at two points as per the recommendations from Trend Micro – these points are 5 minutes after boot (idle state) and at a random point 3-5 minutes into a full system scan (busy state). Results varied between the solutions, with no overall solution being considered best.

It should be noted that only the default technologies were active while the memory usage measurements were taken. The results for each solution should be taken with this in mind and not as a function-by-function memory comparison.

Rationale:

To observe how each of the solutions allocates memory.

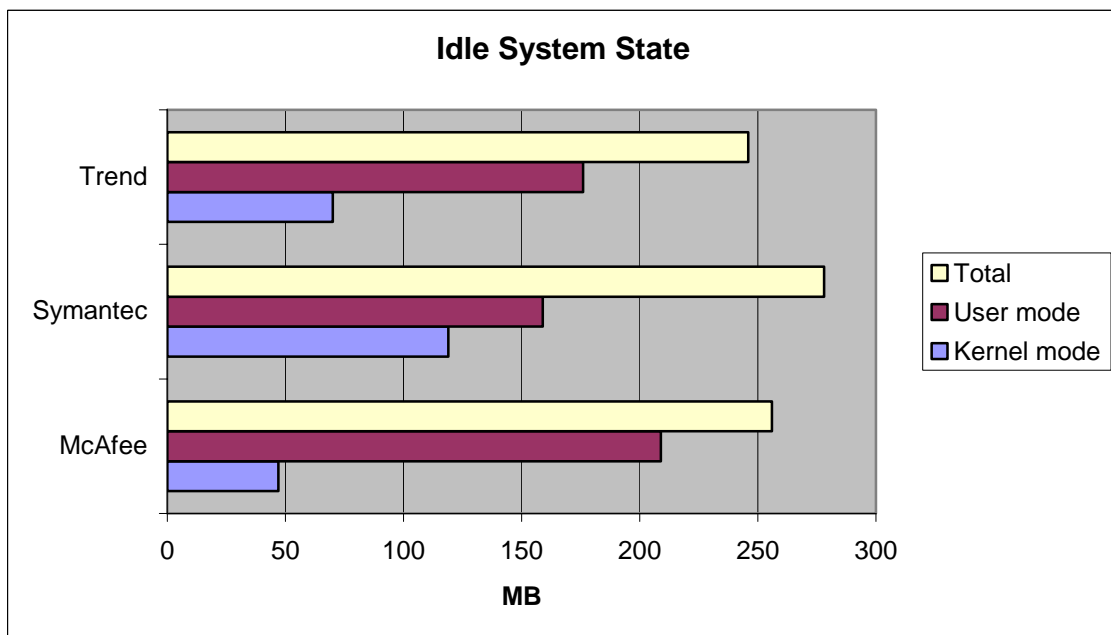
Trend Micro™ WFBS Comparative Testing Report

2. Memory Footprint: Kernel vs User Mode (Cont.)

Test Results:

Idle System State

Product	Kernel mode	User mode	Total
Trend	70MB	176MB	246MB
Symantec	119MB	159MB	278MB
McAfee	47MB	209MB	256MB

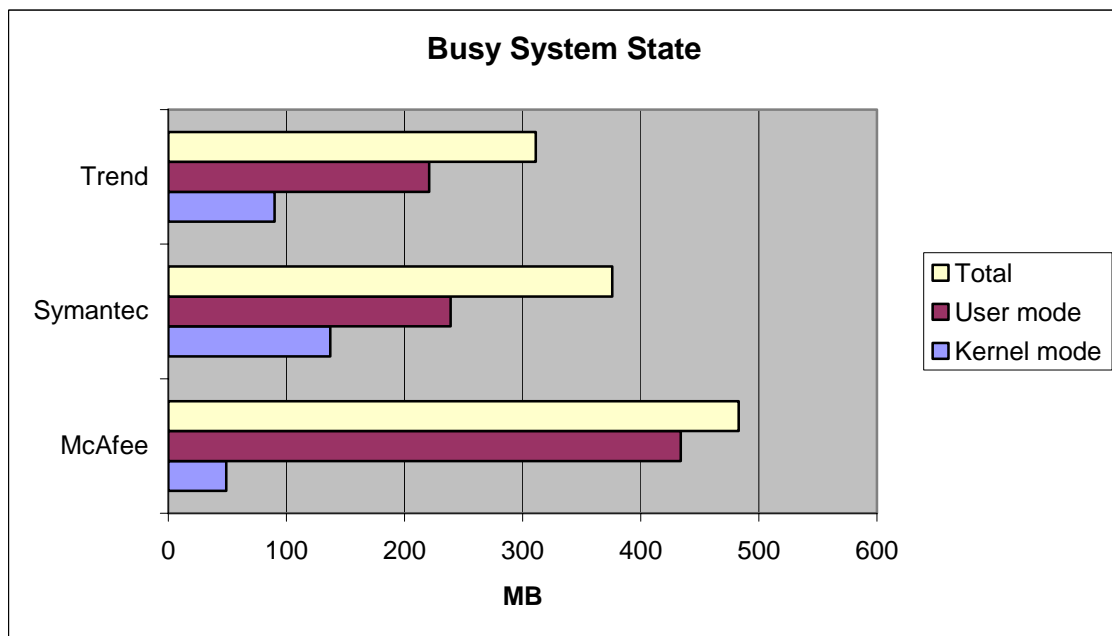


Trend Micro™ WFBS Comparative Testing Report

2. Memory Footprint: Kernel vs User Mode (Cont.)

Busy System State

Product	Kernel mode	User mode	Total
Trend	90MB	221MB	311MB
Symantec	137MB	239MB	376MB
McAfee	49MB	434MB	483MB



2. Memory Footprint: Kernel vs User Mode (Cont.)

Trend Micro™ WFBS Comparative Testing Report

Trend appears to have the second highest amount of Kernel mode memory usage when in both an idle and a busy state, with only Symantec using a higher amount of Kernel memory.

When considering the overall usage of the User mode and Kernel mode added together for Trend, it is lower than the other solutions during an idle state.

During a busy state, the results obtained for Trend Micro again place them first out of the solutions tested

Symantec has the highest Kernel usage during both system states and overall has the highest memory usage in an idle state and second highest in a busy state.

McAfee has the lowest kernel usage in an idle state (figures shown are subject to rounding to convert from bytes to Mb). McAfee also shows the highest use of User mode memory in both system states. The overall results show that McAfee has second highest usage during an idle state and highest during a busy system state.

Trend Micro™ WFBS Comparative Testing Report

2. Memory Footprint: Kernel vs User Mode (Cont.)

Test Methodology:

Not included in originally agreed test plan.

Implementation of Methodology:

To perform this testing, West Coast Labs used various tools to work out the overall memory used by the system with each solution. Pooltag was used to ascertain the Kernel Memory usage and West Coast Labs proprietary memory usage code was used to measure the overall memory usage, from which the user mode allocation could be deduced.

Tools Used:

Pooltag⁽¹⁴⁾

West Coast Labs Proprietary code

Trend Micro™ WFBS Comparative Testing Report

3. Web Threat Protection

Executive Summary:

Engineers tested a list of URLs sourced both from West Coast Labs' feeds and from Trend Micro themselves against the Trend Micro solution to test whether access to the given website would be restricted based on Trend Micro's URL Reputation technology whereby each URL is referred to Trend's In-the-cloud servers for a block/allow decision. Of the other solutions tested in this report, none appeared to provide a comparable technology. Trend Micro's Reputation filtering proved to be effective against the URLs tested.

Rationale:

To observe what protection mechanisms were in place in each product to prevent access to potentially malicious sites.

Test Results:

Trend Micro Worry-Free™ Business Security Advanced:

Trend Micro Worry-Free™ Business Security Advanced sends each website address for checking against their In-the-Cloud servers before access to the site is granted. Should the address come back as known-bad or suspicious then access to the site will be denied.

Symantec Endpoint Protection:

No comparable technology was apparent on this product.

McAfee Total Protection Advanced:

No comparable technology was apparent on this product.

Trend Micro™ WFBS Comparative Testing Report

3. Web Threat Protection (Cont.)

Test Methodology:

Within the context of this test, the Web Threats included in the test environment are defined as those sites that have been reported to, or discovered by Trend, along with being subsequently validated by them as having some malicious content attached.

Implementation of Methodology:

To perform this testing, West Coast Labs used a cross-section of its URL list, passing them through the Trend Micro solution. The URL list includes a mixture of genuinely safe websites, and sites which contain drive-by downloads, iframe exploits, and malicious downloadable content.

URLs were visited using a West Coast Labs proprietary tool based around a well known Internet browser that loads all sites exactly as a user would see them, and the resulting network traffic was captured by using a publicly available sniffing application, Wireshark. The recorded traffic was then analyzed to determine the ability of Worry-Free™ Business Security Advanced to check the reputation of each URL.

Tools Used:

Wireshark (2)

Trend Micro™ WFBS Comparative Testing Report

4. Location Awareness

Executive Summary:

The Trend Micro solution was moved onto a new network setup that was previously unknown to each of the solutions. West Coast Labs then studied the security changes made by Trend Micro Worry-Free™ Business Security Advanced, to determine the ability of the solution to adapt to the new network environment.

Trend Micro Worry-Free™ Business Security Advanced was the only solution in this test to offer adaptability across multiple security technologies. Symantec Endpoint Protection provides the ability to define specific policies for known and unknown networks.

Rationale:

To determine any disparity in protection levels once removed from the known-good network containing each solution's server base.

Test Results:

Trend Micro Worry-Free™ Business Security Advanced:

Trend's Worry-Free™ Business Security Advanced solution accurately identified the transition from the known-good network to that of the new one. Once moved, the security settings on the client machine were adjusted to provide greater protection on the unknown network. Included within this protection mechanism, is the level of security provided by the Firewall, Web Reputation, and TrendSecure Toolbars technologies.

Trend Micro™ WFBS Comparative Testing Report

4. Location Awareness (Cont.)

Symantec Endpoint Protection:

SEP contained a similar technology, entitled Location Manager, which allowed the administrator to specify the range of expected IP addresses on which a client should reside. If the client address falls outside this range then SEP makes it possible for the administrator to assign varying levels of rights to that system/user.

McAfee Total Protection Advanced:

McAfee Total Protection Advanced did not appear to have any comparable functionality.

Test Methodology:

For this service, West Coast Labs monitor the security settings of the client machine with the aim of detecting a shift in security stance once it leaves the known-good network.

Implementation of Methodology:

To perform this testing, West Coast Labs' engineers created a separate test network to that used in the installation and deployment of the solution's server-base. Each solution was subsequently transferred to this network, whereupon engineers then examined the various security settings on each solution to determine what, if any, had been changed.

Tools Used: N/A

Trend Micro™ WFBS Comparative Testing Report

5. Firewall and IDS/IPS

Executive Summary:

Engineers ran various port scans and malformed packet attacks on the three products using default settings to see whether the machines showed any sign of network-based vulnerabilities or open services not protected by the firewall. Results were similar across the range of products, with one or two exceptions (shown in results section). West Coast Labs also used specialist hardware to test for the existence, and effectiveness, of IDS/IPS protection on each of the three vendor products.

Rationale:

This test was conducted to ascertain the level of basic protection afforded by each solution, including whether the client with the solution installed advertised its presence after the installation of the firewall. Further tests were conducted to determine the ability of each product to block intrusion attempts.

Test Results:

Trend Micro Worry-Free™ Business Security Advanced:

Trend Micro's product is delivered with a desktop firewall packaged in. It appeared to WCL that the firewall had to be enabled from the Trend Micro Worry-Free™ Business Security Advanced server before it could become active.

Based upon a stealth scan using SYN packets, WCL noted that ports 139 and 445 were shown in an open state on the target machine.

Trend Micro™ WFBS Comparative Testing Report

5. Firewall and IDS/IPS (Cont.)

Trend Micro's product allowed the user to configure access on a per port basis after enabling Advanced security from the server, but did not appear to allow for blocking by program or executable as the other solutions do.

Trend Micro Worry-Free™ Business Security Advanced contains an IDS filter that actively scans for Intrusion attempts against the client machine. During testing, engineers noted that approximately 30,000 attacks were blocked and reported by Trend's Worry-Free™ Business Security Advanced solution.

Symantec Endpoint Protection:

Symantec's solution, using the same Stealth SYN scan, showed the 135, 139 and 445 as open. Further, when conducting a UDP scan, Symantec's solution showed ports 123,137,138, 445, 1500, 1034, 1039, 1198, 1900 and 4500 as open.

Symantec Endpoint Protection 11.0 contains built-in IDS protection that was sufficient to block the scans/attacks used by West Coast Labs. However, it should be noted that only one log entry was reported related to a possible DOS attack.

McAfee Total Protection Advanced:

The McAfee solution showed similar results to the Trend Micro solution, giving ports 139 and 445 as open on a stealth scan using SYN packets.

Trend Micro™ WFBS Comparative Testing Report

5. Firewall and IDS/IPS (Cont.)

McAfee Total Protection Service for Small Business blocked all mutated attacks run by West Coast Labs' engineers. However, this is primarily the result of the integrated firewall protection, as no evidence of IDS warnings could be found in the solution's log files.

Test Methodology:

To validate the Security Level features, WCL will test the Firewall with various and appropriate settings to confirm policy adherence. In testing the Intrusion Detection System, WCL will also run various proprietary and commercial scripts and tools to confirm that any intrusion attempts are properly reported. Various Protocol Exceptions will be added and policy adherence will be confirmed as appropriate.

Implementation of Methodology:

To perform this testing, West Coast Labs used a combination of publicly available tools and proprietary scripting designed to test a firewall's effectiveness. Scans were launched from a third party machine running a proprietary build of Linux. Traffic was observed using the well known tool Wireshark.

To perform the IDS/IPS testing, West Coast Labs used an MU 4000 appliance supplied by Mu Dynamics to launch a series of scans against each of the three vendors in turn. These scans included a variety of mutation attacks and protocol exceptions, designed to specifically target services running over the

Trend Micro™ WFBS Comparative Testing Report

5. Firewall and IDS/IPS (Cont.)

IPv4 protocol. This includes both TCP and UDP data. The various mutation attacks were targeted against each vendor with the resulting traffic monitored and log files inspected.

Tools Used:

Wireshark ⁽²⁾

Proprietary scripting from WCL ⁽⁴⁾

Proprietary linux live CD (based around Knoppix STD) ⁽⁵⁾

Mu Dynamics' Mu 4000 ⁽⁶⁾

Trend Micro™ WFBS Comparative Testing Report

6. Transaction Protector: Keylogger Protection

Executive Summary:

For this test West Coast Labs engineers attempted to install a selection of keyloggers on each of the systems in order to steal users' passwords.

Detection of most products was good, but prevention of keylogging activity varied considerably between products.

Symantec was the only product to block all keyloggers on the initial test.

Trend Micro now blocks the one missed keylogger upon submission to their engineers.

Rationale:

To observe how effectively the products prevented data loss caused by keylogging programs.

Test Results:

Trend Micro Worry-Free™ Business Security Advanced:

Trend Micro detected 11 out of 12 keyloggers. It failed to detect refog_setup_457.exe. Its firewall did not stop the application from sending screenshots and keystrokes to a remote SMTP mail server. It did however encrypt keystrokes entered into Internet Explorer, but it was still possible to see screenshots sent via this keylogging program, and monitor what sites had been visited. Upon a retest subsequent to notification of this failure to Trend, the Keylogger was detected and nullified.

Trend Micro™ WFBS Comparative Testing Report

6. Transaction Protector: Keylogger Protection (Cont.)

Symantec Endpoint Protection:

Symantec was able to detect and nullify all 12 of the keyloggers.

McAfee Total Protection Advanced:

McAfee detected 11 out of 12 keyloggers. It also failed to detect refog_setup_457.exe. Using this keylogger it was possible to log keystrokes but the firewall denied this program access to the Internet when attempting to send this data out via SMTP.

Test Methodology:

In the context of Transaction Protector, WCL will test Keystroke Encryption by putting keyloggers on devices on which the Trend solutions are installed and examine the keylogger logs to see if any usable data has been extracted.

Implementation of Methodology:

Engineers tested 12 different keyloggers against the three solutions to see how much keylogging behaviour they could prevent.

The 12 keyloggers were run against the solutions, including their full range of behaviour, to see which behaviours could be stopped by the product.

Trend Micro™ WFBS Comparative Testing Report

6. Transaction Protector: Keylogger Protection (Cont.)

Tools Used:

actualspy.exe	rkfree_setup.exe
ek_setup.exe	SpyEx.exe
i_bpk_lite.exe	CLogger.exe
klog.exe	SETUP.exe
powered_keylogger.exe	FamilyKeyLogger-setup.exe
refog_setup_457.exe	HomeKeyLogger-setup.exe

N.B. Trend Micro has removed the keylogging encryption function in post-5.0 versions of Worry-Free™ Business Security Standard and Advanced.

Trend Micro™ WFBS Comparative Testing Report

7. Transaction Protector: Wi-Fi Advisor

Executive Summary:

By connecting to various wireless networks and launching a number of attacks, engineers attempted to gauge the level of mobile protection available on each product. All products behaved as expected on the public hotspots. Trend Micro's Wi-Fi Advisor offered warnings that the safety of some wireless networks was uncertain. Symantec was the only solution to detect the ARP spoofing attempt, and this was only when a non-default option was enabled.

Rationale:

To observe whether the solutions would compensate for wireless-based network attacks that could lead to a mobile machine being compromised.

Test Results:

When connected to various public hotspots, each product behaved in accordance with expectation.

Trend Micro Worry-Free™ Business Security Advanced:

Trend appears to be the only product that caters specifically to using wireless devices. However, when connected to the third party unsecured wireless network it was possible to spy on network traffic and so a Man in the Middle attack was possible across all four of the products. Trend's Wi-Fi Advisor did, however, state that the safety of the Wireless network was uncertain.

Trend Micro™ WFBS Comparative Testing Report

7. Transaction Protector: Wi-Fi Advisor (Cont.)

Symantec Endpoint Protection:

When connected to the in house "bad" network, all products failed on the ARP spoofing when set in default mode. The only product that detected the attack was SEP, but only when the "Enable Anti MAC spoofing" option (disabled by default) was turned on.

McAfee Total Protection Advanced:

This solution did not provide a comparable technology.

Test Methodology:

The Wi-Fi Advisor functionality will be tested by testing to various known good and wireless networks and hotspots. WCL will also set up a bad wireless network and observe the behaviour of the solutions when attempting to connect to it.

Implementation of Methodology:

Engineers connected a device with each solution installed to a series of public networks in differing UK cities to ensure that they acted in accordance with differing network profiles.

Further to this, engineers constructed a wireless network with a restricted IP address pool allocated by DHCP and a WPA/TKIP passphrase required to gain access to the network. Network packet captures were performed using Wireshark, a well-known sniffer. Each client attached to the network was

Trend Micro™ WFBS Comparative Testing Report

7. Transaction Protector: Wi-Fi Advisor (Cont.)

tested against a number of known good external websites to prove the functionality.

Using scripts and services on the Backtrack 3 CD, engineers launched a series of DNS spoofing attacks by sending specially crafted ARP packets to the clients. If successful, the attack would be used to redirect an otherwise innocuous request for a web page to first an internal and then an external web server.

Further to this, WCL managed to locate an unsecured third party wireless network and attempted to use the Cain & Abel tool to perform a Man in the Middle attack. If successful WCL would be able to intercept network traffic and spy on the clients network activities.

Tools Used:

Wireshark ⁽²⁾

Backtrack3 Live CD ⁽⁷⁾

Cain & Abel ⁽⁸⁾

Trend Micro™ WFBS Comparative Testing Report

8. TrendProtect (Browser Page Rating Service)

Executive Summary:

Search terms were entered into various search engines in order to evaluate how the browser plug-ins for each solution worked and to look at the overall results that were returned. Only Trend Micro and McAfee provide Browser Page Rating plug-ins.

Trend Micro's product classified more URLs on Google than McAfee, however it classified slightly less on Yahoo and did not work with MSN on the day of testing. Both solutions provided higher levels of classification than the third party solution, the data of which is not recorded here.

Rationale:

Solutions that offer browser and search engine products should be able to warn users before they visit a site that may either be compromised or have potentially inappropriate content. The ability of each product was tested to warn users about websites that may compromise security.

Test Results:

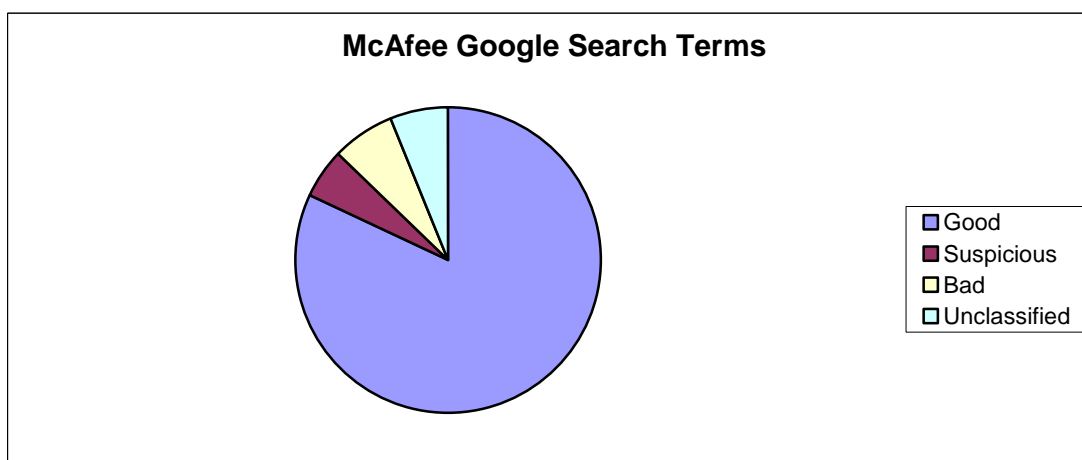
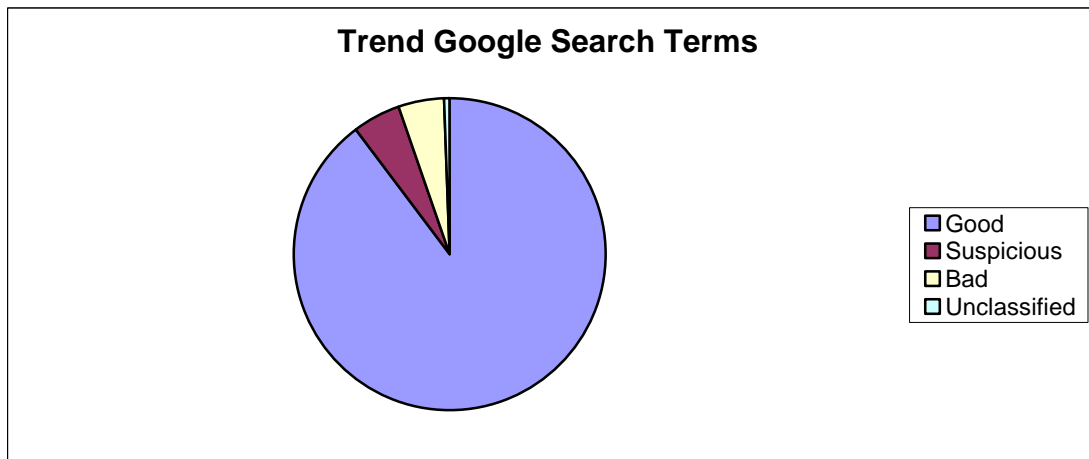
Only two of the four products supported the functionality to classify the results returned from search engines - TrendProtect and McAfee's SiteAdvisor. Symantec Endpoint Protection does not appear to have a website classification tool as part of their core functionality. At the time the testing was conducted (03 Oct 2008), it was found that TrendProtect was not compatible with the MSN Live Search engine, either at the central msn.com or the regional msn.co.uk.*

Trend Micro™ WFBS Comparative Testing Report

8. TrendProtect (Browser Page Rating Service) (Cont.)

Google

Product	Good	Suspicious	Bad	Total Classified	Unclassified
Trend	89.69%	4.90%	4.98%	99.57%	0.43%
Symantec	N/A	N/A	N/A	N/A	N/A
McAfee	82.04%	5.07%	6.79%	93.90%	6.10%

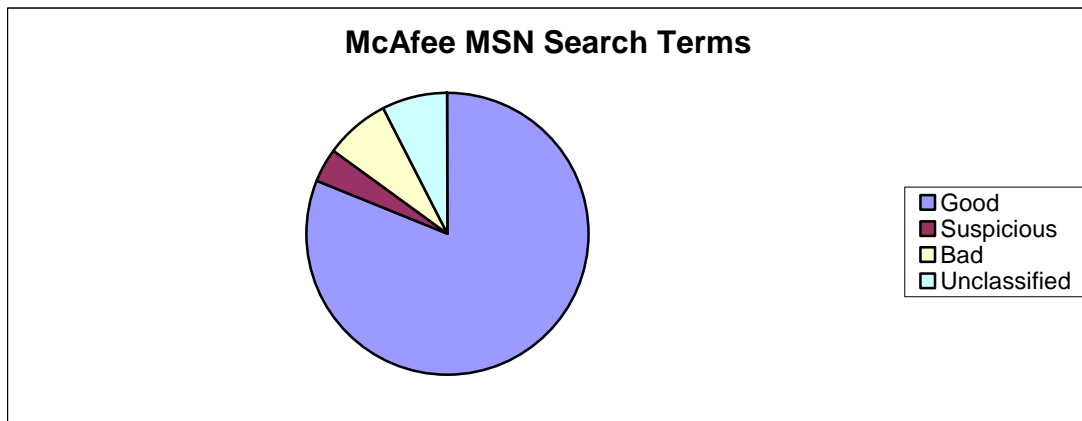


Trend Micro™ WFBS Comparative Testing Report

8. TrendProtect (Browser Page Rating Service) (Cont.)

MSN

Product	Good	Suspicious	Bad	Total Classified	Unclassified
Trend	N/A	N/A	N/A	N/A	N/A
Symantec	N/A	N/A	N/A	N/A	N/A
McAfee	85.37%	4.12%	7.79%	92.13%	7.87%

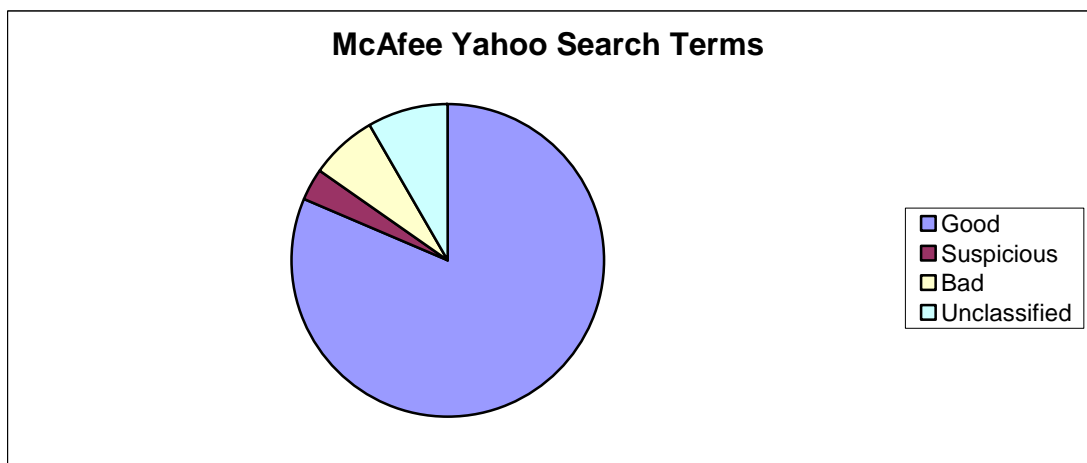
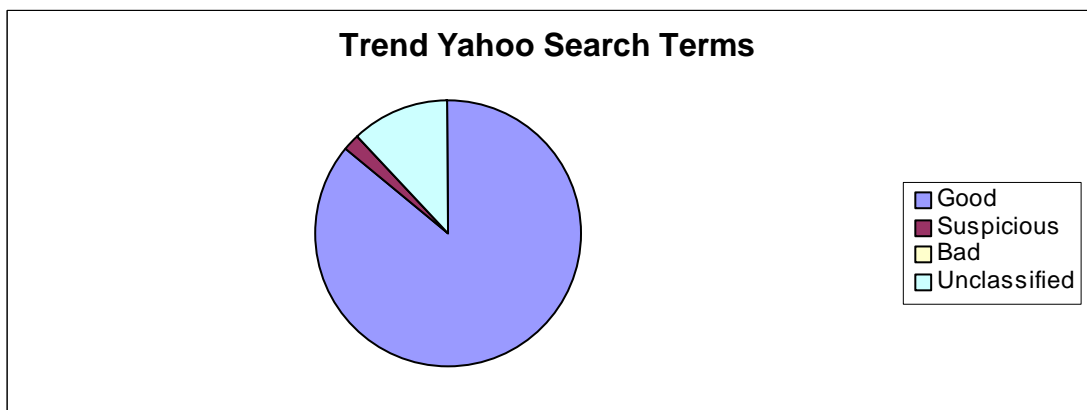


Trend Micro™ WFBS Comparative Testing Report

8. TrendProtect (Browser Page Rating Service) (Cont.)

Yahoo.com

Product	Good	Suspicious	Bad	Total Classified	Unclassified
Trend	85.95%	2.24%	0.00%	88.19%	11.81%
Symantec	N/A	N/A	N/A	N/A	N/A
McAfee	81.26%	3.53%	6.99%	91.79%	8.21%



Trend Micro™ WFBS Comparative Testing Report

8. TrendProtect (Browser Page Rating Service) (Cont.)

Test Methodology:

For TrendProtect West Coast Labs will enter a number of search terms into various web search engines and compare the results reported back by the Trend solutions to that of a third party application which offers the same functionality.

Implementation of Methodology:

To perform this testing WCL obtained a list of search terms that may result in search engines returning malicious and/or unsafe websites. Each of the search terms was entered into 3 major search engines (Google, Yahoo and MSN Live search) and the results were recorded.

Tools Used:

N/A

*Since the time of testing, Trend Micro has released a patch that resolves the error seen with MSN. However, as this was released post-test, no classification score can be given.

Trend Micro™ WFBS Comparative Testing Report

9. Behaviour Monitoring: QuickBooks

Executive Summary:

Engineers installed Intuit QuickBooks SimpleStart 2008 on each of the client machines in order to test and validate each product's abilities to protect and block any unauthorised changes to the QuickBooks Application files. Against the files used, no product seemed to provide full protection.

Rationale:

To observe each of the product's abilities to protect the application files used by the Intuit QuickBooks application.

Test Results:

Trend Micro Worry-Free™ Business Security Advanced:

WCL found that when using Trend to protect QuickBooks it was possible to append and overwrite files using both the proprietary tool and UltraEdit. Trend blocked the proprietary tool from performing copy/rename/delete operations, however it was still possible to perform these operations through a command prompt.

Symantec Endpoint Protection:

No comparable technology was present on this solution.

McAfee Total Protection Advanced:

No comparable technology was present on this solution.

Trend Micro™ WFBS Comparative Testing Report

9. Behaviour Monitoring: QuickBooks (Cont.)

Test Methodology:

The original test methodology relied on Trend supplying a piece of QuickBooks specific malware, which proved to be difficult. In light of this, they suggested an alternative test methodology, recreated in Appendix C. At the time of writing, the only version of UltraEdit that could be found was version 14 rather than the recommended version 11, so this was used.

Implementation of Methodology:

Further to the use of UltraEdit, West Coast Labs wrote an executable which targets an executable file TechHelp.exe in the Quickbooks program directory (C:\Program Files\Intuit\Quickbooks 2008), thus simulating behaviour which might have been caused by malware. West Coast Labs also used other approaches such as use of the Windows command prompt to attempt to append, overwrite, create, copy, rename, or delete the application files.

Tools Used:

UltraEdit ⁽⁹⁾

Proprietary scripting ⁽¹⁰⁾

Proprietary tools ⁽¹¹⁾

QuickBooks SimpleStart 2008 ⁽¹²⁾

Trend Micro™ WFBS Comparative Testing Report

10. Security Dashboard

Executive Summary:

West Coast Labs examined the Dashboard (or equivalent) for each product to ensure that all products were reporting back those incidents that they had noted.

Rationale:

In order to ensure audit functionality from a security solution, all transgressions that are found should be noted in the logs.

Test Results:

Trend Micro Worry-Free™ Business Security Advanced:

Trend Micro's Security Dashboard showed all the relevant and appropriate data that had been created during the ongoing testing covered in all other sections of this report. The data was correct and gave an accurate depiction of the network.

Symantec Endpoint Protection:

Symantec Endpoint Protection's interface updated its information regularly and provides the administrator with a good overview of the current status of protected computers.

McAfee Total Protection Advanced:

McAfee Total Protection may be monitored through the use of a web-based interface. Included within is a statistical breakdown of the machines running the Total Protection client. All data was found to be accurate.

Trend Micro™ WFBS Comparative Testing Report

10. Security Dashboard (Cont.)

Test Methodology:

This feature will be validated in the context of the Malware, Spam, Web Reputation, Behaviour Monitoring and Licensing functionalities

Implementation of Methodology:

Observations were made during the course of testing.

Tools Used:

N/A

Trend Micro™ WFBS Comparative Testing Report

11. Email Protection Vector

Executive Summary:

West Coast Labs directed a large number of email messages at the available email protection services to determine each solution's ability to detect unwanted email.

Rationale:

To test the effectiveness of the email protection offered by each solution.

Test Results:

Trend Micro Worry-Free™ Business Security Advanced:

Trend Micro Worry-Free™ Business Security Advanced utilizes a multi-layered approach to Anti-Spam protection. Contained within this solution are various engines and technologies designed to target specific types of Spam and reduce the number of unwanted messages hitting the network.

Messages are scanned at four distinct transfer phases. The first layer of protection is in-the-cloud and includes scans for malware and spam as well as performing content filtering and IP reputation. The second is at the SMTP layer and includes further IP reputation scans, while at the Exchange layer Trend Micro Anti-spam Engine (TMASE) provides heuristic and signature-based protection.

Trend Micro™ WFBS Comparative Testing Report

11. Email Protection Vector (Cont.)

Messages that arrive via the POP3 protocol are then scanned by client-based TMASE engines. The in-the-cloud policy-based content scanning features, provided by the IMHS service, were not enabled for this test.

Using just Worry-Free™ Business Security Advanced's POP3 plug-in, the solution was able to successfully block 89% of the incoming Spam feed. However, with additional technologies enabled, this catch rate increased to 96%.

Symantec Endpoint Protection:

While Symantec Endpoint Protection 11.0 provides the same ability to scan for malicious programs within email as Worry-Free™ Business Security Advanced, it appears to require additional licensing in order to activate the Symantec Premium AntiSpam technology.

McAfee Total Protection Advanced:

McAfee Total Protection Service for Small Business appeared to provide no on-premise Anti-Spam support from within the tested solution.

Test Methodology:

The Anti-Spam protection is to be validated, evaluated and compared in the context of the following: Ability to block emails based on blocked IPs, scan for image and PDF spam, and the availability of an outlook plug-in for POP3 mail clients.

Trend Micro™ WFBS Comparative Testing Report

11. Email Protection Vector (Cont.)

Implementation of Methodology:

West Coast Labs' engineers directed a large mail feed at the Exchange server and then forensically imaged the box. Each solution was then connected up to the server and the messages were downloaded then analysed for detection and blocking levels.

A second test was then run, again targeting the Exchange server, with the messages passing through Exchange and onto the client machine. Any applicable exchange level protection was installed along with any client-based protection.

Tools Used:

In-house mail feeds

Microsoft Exchange 2000

Microsoft Outlook connected via POP3

Trend Micro™ WFBS Comparative Testing Report

12. File Protection Vector

Executive Summary:

West Coast Labs scanned malware samples, used in the Checkmark Certification programme, to determine the effective detection rate for each solution.

Based on our results, all products performed comparably on File Protection Vector, with McAfee in front by just 0.59%.

Rationale:

To test the effectiveness of each solution to detect known-infected files when scanned using their Anti-Virus technologies.

Test Results:

Trend Micro Worry-Free™ Business Security Advanced:

Trend Micro Worry-Free™ Business Security Advanced successfully detected 97.13% of West Coast Labs' malware test suite.

Symantec Endpoint Protection:

Symantec Endpoint Protection 11.0 successfully detected 97.89% of West Coast Labs' malware test suite.

McAfee Total Protection Advanced:

McAfee Total Protection Service for Small Business successfully detected 98.48% of West Coast Labs' malware test suite.

Trend Micro™ WFBS Comparative Testing Report

12. File Protection Vector (Cont.)

Test Methodology:

The File Reputation / IntelliScan file identification functionality of Trend Worry-Free™ Business Security Advanced is to be compared against the two competitor solutions.

Implementation of Methodology:

The selected files were placed onto the hard drives of each machine containing one of the three solutions. These files were then scanned and any remaining files analyzed in order to determine whether any infection remained on the computer. Real-time scanning capabilities were disabled during this test, with a focus on the On-Demand scanning.

Tools Used:

Cross-section of West Coast Labs' malware catalogue

Trend Micro™ WFBS Comparative Testing Report

13. Data Leakage

Executive Summary:

In order to test the ability of each solution to prevent the leaking of sensitive or private information, West Coast Labs attempted to transmit particular types of data such as credit cards numbers, US SSNs and bank account numbers through email communication channels.

Rationale:

To observe that Trend WFBS could prevent data from leaking from the client machines.

Test Results:

Trend Micro Worry-Free™ Business Security Advanced:

Worry-Free™ Business Security Advanced allows an administrator to use regular expressions and filter out sensitive, or critical, information such as bank account numbers, social security numbers, and credit card details.

This ability was found to be available from within the Message Transport Agent configuration screen within the administrative console. The use of regular expressions allows for particular information to be prevented from leaving the corporate network.

Symantec Endpoint Protection:

No comparable technology could be found on this solution.

Trend Micro™ WFBS Comparative Testing Report

13. Data Leakage (Cont.)

McAfee Total Protection Advanced:

No comparable technology could be found on this solution.

Test Methodology:

By entering a series of regular expressions and testing using email, West Coast Labs validated that Trend Micro has the capability of stopping sensitive data from leaking out from a network.

Implementation of Methodology:

In order to assess the strength of data leakage protection in the various products, a variety of data relating to credit card numbers, social security numbers, etc, was sent via the Microsoft Outlook email client.

Tools Used:

Microsoft Outlook

Trend Micro™ WFBS Comparative Testing Report

14. IM Content Filtering

Executive Summary:

West Coast Labs tested four different IM clients to determine which products were capable of blocking inappropriate content. While some products were able to block IM applications, only the Trend product was able to filter specific content.

Rationale:

By sending a mix of profane and benign words through the IM clients, this would test the products' IM content filtering capabilities.

Test Results:

Trend Micro Worry-Free™ Business Security Advanced:

Trend Worry-Free™ Business Security Advanced allowed West Coast Labs to enter a list of words into its database, which were then successfully filtered out when an attempt was made to transmit these via the IM applications.

Symantec Endpoint Protection:

Symantec Endpoint Protection contains an application designed to block Internet-based applications from running. During testing this feature appeared unable to block the IM applications being used. As a result, SEP neither filters conversations nor blocks the application.

Trend Micro™ WFBS Comparative Testing Report

14. IM Content Filtering (Cont.)

McAfee Total Protection Advanced:

McAfee Total Protection does not provide the ability to filter either incoming or outgoing IM traffic. However, Total Protection does allow for certain applications to be blocked from accessing the Internet.

Test Methodology:

WCL will attest to the availability of this functionality.

Implementation of Methodology:

Each product was tested for its ability to block specific IM content. To perform this test, four Instant Messaging (IM) applications were installed on a client box containing one of the three solutions under test. An external machine was also configured with the four IM solutions in order to provide a source of two-way communication.

A list of selected words, both profane and otherwise, were sent from the client machine to the external client via each IM solution in turn. A record was then kept of what, if any, words were successfully blocked.

Tools Used:

AOL Instant Messenger 6.8.12.4

ICQ 6

Messenger Live 8.1

Yahoo! Instant Messenger 9.0.0.1912

Trend Micro™ WFBS Comparative Testing Report

15. Outbreak Defense

Executive Summary:

This test was designed to test the ability of Trend Micro Worry-Free™ Business Security Advanced to prevent the spread of malware using its policy-based technologies. West Coast Labs will attempt to infect the client machine with a malware sample and then analyze the machine to detect any trace of malware activity.

The Outbreak Prevention Policies, provided by Trend Micro labs, are designed to specifically close off and protect the machine from the specific methods a given malware samples uses to infect the machine. As opposed to using a standard signature to watch for, the policy pro-actively closes ports known to be targeted by the malware sample, alters permissions on specific files, and generally attempts to prevent the sample from gaining any foothold on the client machine.

These policies are provided in two categories – Yellow Alert and Red Alert. Red Alert policies have the ability to block all incoming access to the target network, should the malware outbreak warrant such action.

Outbreak Defense is a feature unique to Trend Micro in this test; as such, no comparison can be provided for the other solutions being tested.

Rationale:

This test is designed to test the ability of Worry-Free™ Business Security Advanced to prevent further outbreak of malware.

Trend Micro™ WFBS Comparative Testing Report

15. Outbreak Defense (Cont.)

Test Results:

Trend Micro Worry-Free™ Business Security Advanced:

Upon downloading the Outbreak Prevention Policy, created specifically for this malware sample, the malware sample proved unable to infect the machine. No trace of malicious activity was detected on the machine after the file was executed and analysis performed.

Symantec Endpoint Protection:

No comparable technology could be found on this solution.

McAfee Total Protection Advanced:

No comparable technology could be found on this solution.

Test Methodology:

Prevent the spread of malicious files and infection of client machines.

Implementation of Methodology:

A malware sample was provided to Trend Micro's labs who, in turn, developed an outbreak policy specific to the sample. This policy was subsequently downloaded and installed to a client machine and a forensic image taken. Engineers at West Coast Labs then attempted to run the malware sample and look for signs of either the executable successfully

Trend Micro™ WFBS Comparative Testing Report

15. Outbreak Defense (Cont.)

running or for any typical signs of malicious activity. A fingerprint was the taken of the machine and compared to that of the known-good state, any differences were noted and analyzed.

Tools Used

To perform this testing WCL used various pieces of malware that were sourced from West Coast Labs' worldwide honeypots.

Trend Micro™ WFBS Comparative Testing Report

16. Vulnerability Assessment

Executive Summary:

West Coast Labs tested the ability of each solution to identify potential host-based vulnerabilities on a Windows XP Installation, containing Service Pack 3.

Only Trend offered the ability to scan for patch levels as a third-party solution. Trend Micro's results also included links to the available patches along with remediation advice.

Rationale:

To identify the ability of each solution to warn of missing patches or system vulnerabilities.

Test Results:

Trend Micro Worry-Free™ Business Security Advanced:

Trend Micro Worry-Free™ Business Security Advanced allowed West Coast Labs' engineers to perform VA scans from the Administration console. The resulting reports for these scans included links to Microsoft pages that contained remediation advice and links to any required patches. It was also noted that Worry-Free™ Business Security Advanced allowed engineers to start vulnerability scans across all client machines from the administrative interface.

Symantec Endpoint Protection:

Symantec Endpoint Protection 11.0 appeared to provide no Vulnerability Assessment ability.

Trend Micro™ WFBS Comparative Testing Report

16. Vulnerability Assessment (Cont.)

McAfee Total Protection Advanced:

McAfee Total Protection Service for Small Business appeared to provide no Vulnerability Assessment ability.

Test Methodology:

Checks vulnerability / patch recommendations

Implementation of Methodology:

Scans will be run using any available vulnerability assessment tools, included within the solutions, to determine the existence of any potential system vulnerabilities and patch levels. Engineers will also check for the existence of remedial advice to correct any detected Issues. Each vendor's product was asked to perform the appropriate scans and report on vulnerabilities.

Tools Used: N/A

Trend Micro™ WFBS Comparative Testing Report

17. Damage Cleanup Services

Executive Summary:

Malware samples will be used to infect a client machine, the samples will then be submitted to Trend Micro's labs in order to create a Damage Cleanup policy. West Coast Labs will then report on the ability of the Damage Cleanup Policy to successfully remove all trace of the infection.

Damage Cleanup Services is a Trend Micro specific technology, as such only Trend Micro Worry-Free™ Business Security Advanced could be reported on. A similar service was found to be available from within the Symantec Endpoint Protection solution, however this does not receive tailored policies as per the Trend Micro solution.

Rationale:

This test was conducted to ascertain each solution's ability to clean up damage caused by malware that had been executed whilst the protection had been disabled for some reason (for example an installation that requires AV disabled).

Test Results:

Trend Micro Worry-Free™ Business Security Advanced:

The Trend Micro solution was found to be capable of removing, or cleaning, files that were found to be infected on the client machine as a result of malware activity.

Trend Micro™ WFBS Comparative Testing Report

15. Damage Cleanup Services (Cont.)

Symantec Endpoint Protection:

While not directly comparable to the Trend Micro offering, Symantec Endpoint Protection does include a remote scanning utility that provides a means of scanning and cleaning an infected client machine.

McAfee Total Protection Advanced:

No comparable technology could be found on this solution.

Test Methodology:

Cleanup and removal of client infection.

Implementation of Methodology:

A client machine will be infected with a known-good malware sample. The sample will be submitted to Trend Micro who will subsequently create a Damage Cleanup policy designed to remove all trace of infection from the client machine. West Coast Labs will then analyze the client, using various tools and scripts, to verify that the infection has been successfully removed. Forensic images will be taken before and after the infection and cleanup stages to provide a means of comparison and to aid in the analysis process.

Tools Used

To perform this testing WCL used various pieces of malware that were sourced from West Coast Labs' worldwide honeypots.

Trend Micro™ WFBS Comparative Testing Report

Conclusion

The testing described above has produced a variety of results.

Trend's Worry-Free™ Business Security Advanced product as supplied has shown that it competently handles most of the areas considered here for testing, and certainly seems to have more generalised coverage than the immediate competitor products considered in this report.

The points where some issues appear to have arisen are as follows:

QuickBooks testing - it appears that this is not working as it should against the particular version of the QuickBooks application that was tested.

It should be noted that there were no statistically significant differences in scores among the products tested in the File Protection Vector.

These issues should, however be relatively easy to fix as they appear to be minor and would seem to be related to product range or versioning of the end applications.

Trend Micro™ WFBS Comparative Testing Report

Appendix A: References

- 1 <http://www.epsilon squared.com/>
- 2 <http://www.wireshark.org/>
- 3 Content filtering script developed by WCL engineers
- 4 Firewall script developed by WCL engineers
- 5 <http://www.knoppix-std.org/>
- 6 <http://www.mudynamics.com/products/mu-4000.html>
- 7 http://www.remote-exploit.org/backtrack_download.html
- 8 <http://www.oxid.it/cain.html>
- 9 <http://www.ultraedit.com/>
- 10 Quickbooks script developed by WCL engineers
- 11 Proprietary QuickBooks tool developed by WCL engineers
- 12 <http://quickbooks.intuit.co.uk/accounting-software/products/simplestart.jsp>
- 13 <http://www.firewallleaktester.com>
- 14 <http://www.osronline.com/article.cfm?article=98>

Trend Micro™ WFBS Comparative Testing Report

Appendix B: Trend Micro's Test Plan for QuickBooks

We select Ultraedit v11 as our testing tool (a.k.a. malware tool) since it doesn't have a sign key and is not added into the AEGIS exception list yet.

1. Tests (cases):

Default settings (including UI):

i. SS console:

Default is disable and able to enable at SS console's page [Security Settings] -> [Behavior Monitoring], then setting will deploy to clients

AEGIS of Client Privilege setting

ii. CSA: Disabled (default) and enabled when server enabled

II. Main functionality:

(Testing tool: Ultraedit_v11_10)

i. Lock QB's EXE and DLL files:

Modify or delete the exe or dll files under QB path is not allowed.

Result: Popup warning message and logs at both CSA and SS console (QB's exe and dll files are not able to be modified and deleted)

ii. AEGIS priority execution:

Add a process (Ultraedit) into Server's exception list with trust and then use it to modify or delete the exe or dll files under QB path again

Result: Popup warning message and logs at both CSA and SS console (QB's exe and dll files are not able to be modified and deleted)

Taken from email from W. Kam Mon 03/11/2008 03:03

Trend Micro™ WFBS Comparative Testing Report

Appendix C: Tools Used

6. Transaction Protector

Tools used:

e5671aece96f7f95541c8c7a11ebbc4b actualspy.exe
821b16ce52a0c28ce97c21ab73ce0e35 ek_setup.exe
f643876d67f34219fc2e98e5a832ba54 i_bpk_lite.exe
43a5f04e751f98d6ee6491da8ba89574 klog.exe
6f8fabc8980415ac807ababa612a5d4d powered_keylogger.exe
8bb8f5d3db1c7bd6ae889b58c2161aec refog_setup_457.exe
a19c96aad725fb67ab3a499f97b25a89 rkfree_setup.exe
2f37948a886b46d35087c1f9f9ceeb1a SpyEx.exe
6917408777ea4263b3683bdcc8c7392b CLogger.exe
2f769455606099e8447b0300912f2f0d SETUP.exe
19495b25122ddd5624642dd70e554d48 FamilyKeyLogger-setup.exe
301b76bccca77855ca1d44136fb2fd435 HomeKeyLogger-setup.exe
b936c243fded4390fbc7e512850d0820 W32SillyFDC!itw#10.exe
a230185af1b502e296386c459a319fed W32VBlitw#160.exe
b4034ad92b4cd7829a190dfe3652ee97 W32VBlitw#161.exe
caaf45327eca87b903b61add62c3201 W32!itw#162.exe
c752c28b5a8547587d18f8425451b5d9 W32SillyFDC!itw#1.vxe
6452e3c7d51483e365e0cf2406937e5c W32SillyFDC!itw#24.vxe
73894e52fd1d9c1be63cac4389a27e3f OnlineGames!itw#590.vxe
a71e97372d227855287768263a02db72 OnlineGames!itw#591.vxe
889102bb99768b1b1115e0fde2493c1e W32VBlitw#59.vxe
af4e42b857fa4a3ec7a8f693edbd5e12 W32VBlitw#72.vxe
5f85dc4d417c7aa7e49652d89cd6568a W32KolabC!itw#7.vxe
cd2f0aff90181459e083711c16055a54 W32Vanbot!itw#84.vxe

Trend Micro™ WFBS Comparative Testing Report

Appendix C: Tools used

Remediation technologies:

15. Outbreak defence (Cont.)

Tools Used:

af9f7dbf2e25b3b81dcde54b58aeb3db W32Bagle-HK.vxe
6adb096262c3da36d5b449ade51b8410 W32EmailWorm-INF.vxe
6ab3e6fc4931208eb2796148a37a0ef2 W32Emailworm-IYX.vxe
910721cf2827bb5bc6df42aa4a5d3692 W32Emailworm-IYZ.vxe
6e671378de9c1a2d0adf7e3652fb244a W32Emailworm-JAJ.vxe
f960202f669b4799c00828700a69d720 W32EmailWorm-JJZ.vxe
548e2d23f88bf4fec2528faf327d52b4 W32EmailWorm-JMX.vxe
4f845e7e813a1f88d020ee763a78df25 W32EmailWorm-KC.vxe
c2ca2d6e112ba1d8f4b0b5adb6e7e44e W32EmailWorm-KDR.vxe
3ee3e775b83c46801b9577182c8fc060 W32EmailWorm-KML.vxe
e16e39b008e61f3fb5ef1a46c5e0410a W32EmailWorm-KOQ.vxe
178014da44a79fc496fc26b0a13fb6b1 W32EmailWorm-KPV.vxe
9fce73bb786d97a464b9c6256603e6f8 W32EmailWorm-MXW.vxe
aa3be82ae1c2b792c28f56c3e8997572 W32SillyWorm-WI.vxe
ad1f3f13291a71d3de52bf26b40b2306 W32SillyWorm-WR.vxe
cb73f0c6d0a20e191c21cc47dff1e471 W32Sober-X.vxe
549af6c1265ad921c582078f19508e2c w3baglef.exe
1aec7aebd916c3862131af0f7fe46da2 W3Myd!!67.exe
d5a1b82f4eebb86517fbbc49462b5142 W3MydoAM.exe
d3d01fa0a3eb3cc5f8c9ae7dffbd2c7f W3MyDoll66.exe

Trend Micro™ WFBS Comparative Testing Report

Appendix D: Software Specification

Trend



Version: 5.0

Trend Micro Inc supplied West Coast Labs with an initial version of their Worry Free Business Security Advanced (Worry-Free™ Business Security Advanced) software, detailed as below. It is understood by West Coast Labs that this version had been compressed and packaged with a new engine specifically for West Coast Labs.

Filename: Worry-Free™ Business Security Advanced

50_Advanced(CSM)_B1307_Repack1_EN.zip

MD5 Checksum: b434e1bb1ec56b13fe546fba4fc1249c

License key: CM-S4QL-KS6EU-8PDWG-PJQHZ-9W2MK-HGSSB

West Coast Labs have been informed that this license key refers to the Advanced version of the product and that there is no difference in the binaries between Advanced and Standard.

This solution was installed first to a server machine, running Windows 2003 SBS, and then subsequently deployed to multiple client machines running Windows XP. All installation steps were carried out following the best practices laid out in the setup documentation.

System requirements for the server machine include 512Mb of RAM and 1.2Gb of available disk space. The client software requires 256Mb of RAM and 200Mb of disk space.

Trend Micro™ WFBS Comparative Testing Report

Appendix D: Software Specification

Symantec Endpoint Protection



Version: 11.0

Symantec Endpoint Protection (SEP) 11.0 Small Business Edition, was purchased by West Coast Labs from a reseller in the UK, and arrived as a boxed version.

Serial Number: M5510287134

The SEP server and management software was first installed to a machine running Windows 2003 Server and then deployed to client machines running Windows XP. Deployment was carried out using SEP's the Migration and Deployment Wizard contained within the server solution.

The requirements of the server consisted of 2Gb of RAM and 1Gb of hard disk space. The client software required 256Mb of RAM and 180Mb of hard disk space. It should be noted that SEP's documentation states the requirement of an additional 440Mb of hard disk space during the installation.

Trend Micro™ WFBS Comparative Testing Report

Appendix D: Software Specification

McAfee Total Protection Advanced



Version: 4.7.0.538

McAfee's Total Protection Advanced solution was licensed by West Coast Labs from a reseller in the UK. The solution may be downloaded to each client manually.

Location:

<http://vs.McAfeeasap.com/MC/enu/rd.asp?P=UC&CK=0005040005060300000f000001>

Filename: TOPSBDM.exe

MD5: 4B20088B30C97626CE855EF64013FE09

Total Protection is a managed service that may be centrally controlled via a web-based console accessed from the McAfee portal. Installation may be performed manually by downloading the product from a link emailed directly from McAfee .

The client package requires a minimum of 64Mb of RAM and also provides support for 64 bit architecture. No minimum requirement for hard disk space could be determined at time of reporting.

Trend Micro™ WFBS Comparative Testing Report

Appendix E: Hardware Specification

In order to make sure that the tests were comparable, hardware of equivalent specification was used for each of the solutions. Therefore, machines with the following specification were used in the labelled roles.

Servers

Model: Acer Aspire M3200

Processor: AMD Athlon 64 X2 5000

Hard Disk: 1TB HDD

Memory: 2GB RAM

Network Card:

Installed OS: Windows (as appropriate, see Installation, pp.12)

Clients

Model: Acer Aspire M1640

Processor: Dual Core E2160

Hard Disk: 160 GB HDD

Memory: 2 x 512MB RAM

Network Card: Gigabit Ethernet (onboard), generic wireless NIC.

Installed OS: Windows XP SP3

Trend Micro™ WFBS Comparative Testing Report

Appendix F: Component Comparison

	Trend Micro	Symantec	McAfee
Subscription Services	Availability	Availability	Availability
Virus	YES	YES	YES
Browser Protection	YES	YES	YES
Firewall	YES	YES	YES
Spyware	YES	YES	YES
Managed-Email Service	YES	YES	YES
Installation/Deployment			
Operating System/System Requirements			
Management Server	Appendix E	Appendix E	Appendix E
Client	Appendix E	Appendix E	Appendix E
64 Bit OS Support	YES	YES	YES
64 Bit aware installer	YES	YES	YES
Itanium Support	YES	NO	NO
Client Installation Method			
Web Install	YES	YES	YES
Login script	YES	YES	NO
Remote Install	YES	YES	YES
Group Policy	YES	YES	YES
Client Packager Support	YES	YES	NO
Remote Uninstallation	YES	NO	NO
Management Console Installation			
Pre-installation requirements	Appendix E	Appendix E	Appendix E
No. of steps to install server	1. Installation	1. Installation	1. Installation
No. of management consoles	1	4	1
Web server support	YES	NO	NO
Active Directory Support	NO	YES	NO
Messaging Protection Installation			
Microsoft Exchange auto detection	YES	NO	NO
Remote install	YES	NO	NO
Manageable using a single console	YES	NO	NO
Client Protection Installation			
Silent installation	YES	YES	YES
No. of steps to install clients	1. Installation	1. Installation	1. Installation
No client reboot required	YES	YES	NO
Active Directory Integration of accounts	NO	YES	NO
Plug-in Manager/Architecture	YES	NO	NO

Trend Micro™ WFBS Comparative Testing Report

Appendix F: Component Comparison (Cont)

Endpoint Protection			
Antivirus scanning			
Heuristic detection	YES	YES	YES
Scan mapped drives/shared folders	YES	YES	YES
Scan by file type	YES	YES	YES
Scan All	YES	YES	YES
Scan by extension	YES	YES	YES
File exclusion	YES	YES	YES
Directory exclusion	YES	YES	YES
Backup files before cleaning	YES	YES	NO
Configurable alert dialogs	NO	YES	NO
Rootkit detection	YES	YES	YES
Web Reputation			
SiteAdvisor	YES	NO	YES
Wi-fi Advisor	YES	NO	NO
Keystroke Encryption	YES	NO	NO
Instant Messaging	YES	NO	NO
Wireless Protection	YES	NO	NO
Software protection			
Intuit Quickbooks	YES	NO	NO
Antispyware scanning			
Spyware/Grayware Approved List	YES	YES	YES
Real-time/manual/scheduled scan protection	YES	YES	YES
Centralized anti-spyware management	YES	YES	YES
grant client privilege to configure anti-spyware settings	YES	YES	YES
Spyware action	YES	YES	YES
Spyware Reports	YES	NO	YES
Presents spyware description	YES	YES	YES
Customizable action depending on threat/risk	YES	YES	NO
Automatic spyware pattern updates	YES	YES	YES
Preconfigured scan action	YES	NO	YES
Compressed file scanning	YES	YES	YES
Central Quarantine	YES	YES	YES
Service reloading	YES	YES	NO
Grant/limit privilege to antivirus client	YES	YES	NO
Macro detection	YES	YES	YES
System Utilization throttling	YES	YES	NO

Trend Micro™ WFBS Comparative Testing Report

Appendix F: Component Comparison (Cont)

Process scanning	YES	YES	YES
Email Reports	YES	YES	YES
Configurable of above	YES	NO	YES
Configurable action per malware type	YES	YES	YES
Commercial Application detection	NO	YES	NO
Personal Firewall			
Firewall Rule creation wizard	NO	YES	YES
Rule Type			
Application	NO	YES	YES
Service	YES	YES	YES
Schedule	NO	YES	NO
Actions	YES	YES	YES
Notification	YES	YES	YES
Rule Severity/Security Level	YES	NO	NO
Intrusion Protection			
Network Attack Detection	YES	YES	YES
Network Virus Detection	YES	YES	NO
Location Awareness	YES	YES	YES
Behavior Monitoring	YES	YES	NO
Proactive Threat/Outbreak Prevention			
Automated response to threat/outbreak	YES	NO	NO
Damage Cleanup			
Initiate cleanup on infected hosts	YES	NO	NO
Vulnerability assessment			
Checks for Microsoft vulnerabilities	YES	NO	NO
Detect unprotected hosts	YES	YES	NO
Client Mail Scan			
POP3 mail scanning	YES	YES	NO
Supported mail clients	OUTLOOK	YES	N/A
Client Control			
Application Control	YES	YES	YES
Device Control	NO	YES	NO
Messaging Protection			
Security Dashboard	YES	N/A	YES

Trend Micro™ WFBS Comparative Testing Report

Appendix F: Component Comparison (Cont)

Antivirus			
Scan by file type	YES	N/A	YES
Scan All	YES	N/A	YES
Scan by extension	YES	N/A	YES
Packer Detection	YES	N/A	YES
Heuristic Detection	YES	N/A	YES
Scan Message Body	YES	N/A	YES
Antispam			
Does not require additional license/subscription	YES	No	YES
Spam categories	YES	N/A	YES
Detect phishing attempts	YES	N/A	YES
Approved senders	YES	N/A	YES
Blocked senders	YES	N/A	YES
Image Spam Protection	YES	N/A	YES
Quarantine			
Search	YES	N/A	YES
Resend	YES	N/A	YES
Maintenance	YES	N/A	YES
End User Quarantine			
Automatic user level spam folder maintenance	YES	N/A	NO
User inclusion/exclusion to EUQ	YES	N/A	NO
Management/Administration			
Management Console			
Centralized management console	YES	NO	YES
Web-based management console	YES	NO	YES
Consoles used for routine tasks	1	4	1
Security dashboard	YES	YES	YES
Real time status	YES	YES	YES
Configurable dashboard	NO	YES	NO
Vital status summary	YES	YES	YES
Silent Installation	YES	YES	N/A
Threat Status			
Outbreak Defense	YES	NO	NO
Antivirus	YES	YES	YES
Anti-spyware	YES	YES	YES
Anti-spam	YES	NO	YES
Network Viruses	YES	NO	NO

Trend Micro™ WFBS Comparative Testing Report

Appendix F: Component Comparison (Cont)

Browser Protection	YES	NO	YES
Behavior Monitoring	YES	NO	NO
Email Protection	YES	YES	YES
System Status			
License	YES	NO	YES
Updates	YES	NO	YES
System	YES	NO	NO
Security Indicators			
Internal Virus Outbreak	YES	YES	YES
Virus Infection	YES	YES	YES
Spyware Infection	YES	YES	YES
Outdated Virus Pattern	YES	YES	YES
Outdated Spyware Pattern	YES	YES	YES
Policy Management			
Endpoint grouping via policy	NO	YES	YES
Nested groups	YES	YES	YES
Policy inheritance	NO	YES	NO
Location specific policy	NO	NO	YES
Active directory support	NO	YES	NO
Group Administration			
Read Only	NO	YES	YES
Read & Modify Reports	NO	YES	YES
License Information			
Service/Product name	YES	YES	YES
License status	YES	NO	YES
Activation code	YES	NO	YES
Threat Management and Policy Enforcement			
Outbreak defense			
Outbreak Prevention	YES	NO	NO
Provides automatic vulnerability assessment	YES	NO	NO
0day protection without updated signature file	YES	NO	NO
Automatic Damage Cleanup Service	YES	NO	NO
Vulnerability assessment	YES	NO	NO
Client Control			
Application Control	YES	YES	YES
Device Control	NO	YES	NO
Policy Enforcement	YES	YES	YES

Trend Micro™ WFBS Comparative Testing Report

Appendix F: Component Comparison (Cont)

Update Components			
Version	YES	YES	YES
Last Updates	YES	YES	YES
Virus Pattern	YES	YES	YES
Common Firewall Pattern	YES	YES	YES
Spyware Pattern	YES	YES	YES
Anti-spam pattern for Messaging Security Agent	YES	NO	NO
Intellitrapp Exception Pattern	YES	NO	NO
Intellitrapp Pattern	YES	NO	NO
Vulnerability Pattern	YES	NO	NO
Advanced Settings			
Display support notifications on client computers	YES	YES	YES
Advanced Virus Protection Settings			
Outbreak Response	YES	NO	NO
Buffer Overflow Protection	YES	YES	YES
Scan Email before delivering to outlook	YES	YES	YES
Scan w/in archives during on-access scanning	YES	YES	YES
Scan w/in archives during on-demand scanning	YES	YES	YES
Advanced Spyware Protection Settings			
Detect remote Admin tools	YES	YES	YES
Detect spyware	YES	YES	YES
Detect dialers	YES	YES	YES
Detect password crackers	YES	YES	YES
Detect adware	YES	YES	YES
Detect potentially unwanted programs	YES	YES	YES
Detect Key loggers	YES	YES	YES
Reports			
Report Type	PDF	HTML	HTML
Send report via email	YES	YES	YES
Automatically send report	YES	NO	YES
Domain Overview			
Desktop/Servers			
Patterns Current to Security Servers	YES	YES	NO
Patterns Current to Monitoring Server	YES	YES	NO
Security Agents current to Security Server	YES	YES	NO

Trend Micro™ WFBS Comparative Testing Report

Appendix F: Component Comparison (Cont)

Exchange Servers			
Patterns Current to Security Servers	YES	NO	NO
Patterns Current to Monitoring Server	YES	NO	NO
Virus Infection	YES	YES	YES
Internal Virus Outbreak	YES	YES	YES
Spyware Infection	YES	YES	YES
Security Incidents			
Viruses	YES	YES	YES
Spyware	YES	YES	YES
Spam	YES	NO	YES
Network Viruses	YES	NO	NO
Virus Detection Distribution			
Major Threats and Targets			
Computers with Viruses	YES	YES	YES
Prevalent Viruses	YES	YES	NO
Prevalent Spyware	YES	YES	NO
Infected Computers	YES	YES	YES
Names of Infected Files	YES	YES	YES
Report Format			
PDF	YES	YES	NO
DOC	YES	YES	YES
XLS	YES	YES	YES
CVS	YES	YES	YES
XML	NO	NO	NO
TIFF	NO	NO	NO
Exportable	YES	YES	NO
Duration			
Daily	YES	YES	YES
Weekly	YES	YES	YES
Bi-Weekly	NO	YES	YES
Monthly	YES	YES	YES
Report Content			
Antivirus	YES	YES	YES
Outbreak Defense	YES	YES	YES
Anti-spyware	YES	YES	YES
Anti-spam	YES	NO	YES
Web Reputation	YES	NO	NO

Trend Micro™ WFBS Comparative Testing Report

Appendix F: Component Comparison (Cont)

Behavior Monitoring	YES	NO	NO
Content Filtering	YES	NO	NO
Network Virus	YES	NO	NO
Application and Device Control	NO	YES	NO
Computer Status	YES	YES	YES
Network Threat Protection	YES	YES	YES
Events block by Firewall	YES	YES	YES
Email Security	YES	NO	YES
Duplicate Computers	YES	YES	YES
Computer Profiles	YES	YES	YES
Detection History	YES	YES	YES
Most Vulnerable computers	YES	YES	YES
Update			
Multiple update sources	YES	YES	NO
Update Schedule Policy	NO	YES	NO
Update Content Policy	NO	YES	NO

N.B. Trend Micro has removed the keylogging encryption function in post-5.0 versions of Worry-Free™ Business Security Standard and Advanced.

Trend Micro™ WFBS Comparative Testing 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 Worry-Free™ Business Security Advanced Comparison Test	20 th February 2009

westcoast labs

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.

Facilities also in Hong Kong, Singapore and Sydney

E info@westcoast.com

W www.westcoastlabs.com