

May 2006

Evaluating Client-Server SMB Solutions

Trend Micro Client Server Messaging Solution for SMB
Symantec Client Security for Groupware
McAfee Active Defense 8.0



Comparative Test

Executive Summary	3
Introduction and Objectives	4
Description of Products	5
Test Environment – Summary	6
Test Methodology	7
Test Scenarios	8
Test Results	9
Conclusion	20
Appendices	
• Appendix A – Test Environment – Detailed.	18
• Appendix B – Test Procedures.	24
• Appendix C – Trend Micro Real-world Outbreak.	27



West Coast Labs, William Knox House, Britannic Way, Llandarcy, Swansea, SA10 6EL, UK.
Tel : +44 1792 324000, Fax : +44 1792 324001. www.westcoastlabs.org

Executive Summary

This test report describes a comparative assessment of three SMB-focused solutions from leading anti-virus vendors: McAfee, Symantec, and Trend Micro. An insight is provided into each solution's ease-of-use and its ability to assess, prevent, protect, and cleanup following virus outbreaks, with potentially little or no IT intervention.

In the context of these specific tests, Trend Micro's solution proved to have an advantage over the other solutions, as its features seemed to be tailored for businesses with little or no IT staff.

It is the only solution that has built-in automatic capabilities to monitor and prevent propagation of a new virus before a signature file is available, and to identify computers that have a system vulnerability that can be exploited by this new threat. Given that most small and mid-size businesses don't have 24/7 IT security staff, this automatic protection capability should help to ensure business uptime within such organizations.

Introduction and Objectives

When it comes to protecting small and mid-sized businesses, not all security products operate in the same way. In this report, West Coast Labs had the privilege of analysing and evaluating leading malware security vendors - McAfee, Symantec, and Trend Micro – through a series of balanced and carefully managed test methodologies, specifically designed not to favour one particular technology over another.

This test is a comparison of these solutions:

- Trend Micro - Client Server Messaging Security for SMB 3.0
- Symantec - Client Security 3.0 for Groupware
- McAfee - Active AV Defense 8.0i

Each solution's features and functionality were assessed in the context of its response to a malware outbreak, how much involvement was potentially needed from IT staff, and how much time and effort was potentially required to restore a computer / network to its original operational state following an outbreak.

Objectives

The primary objectives of these tests were to evaluate and validate the top-tier content security management players and their client-server products for the SMB environment, criteria was assessed within these specific areas:

- Usability in the areas of installation, management, and intuitiveness
- Ability to detect and defend against known and unknown future malware threats
- Clean and repair network clients, with little or no IT intervention.
- Assess and identify computers vulnerable to specific malware attack

Description of Products

McAfee Active AV Defense 8.0i...as stated by McAfee

“...The most complete anti-virus solution available, designed to meet the needs of growing businesses with limited resources. McAfee® Active Virus Defense SMB Edition With the new McAfee® ProtectionPilot™ easy to use management console, delivers virus detection and cleaning for desktops and servers, plus protection at the Internet gateway”.

<http://www.mcafee.com/>

Symantec Client Security 3.0 for Groupware...as stated by Symantec

“...Client Security 3.0 with Groupware Protection protects business from viruses, spyware, hackers, and spam. Symantec AntiVirus™ automatically detects and removes malicious code, while Symantec™ Mail Security filters unwanted email. Centralized management and automatic updates make it easy to defend businesses against both known and emerging threats”.

<http://www.symantec.com/>

Trend Client Server Messaging Security for SMB 3.0...as stated by Trend Micro

“...Worry-Free Antivirus, Anti-Spam and Personal Firewall solution for SMB which protects PCs, Windows servers, and Microsoft™ Exchange servers against viruses, spam and hackers in an all-in-one integrated defense. Trend Micro Client Server Messaging Security for SMB dramatically simplifies security management for businesses who demand a worry-free approach”.

<http://www.trendmicro.com/>

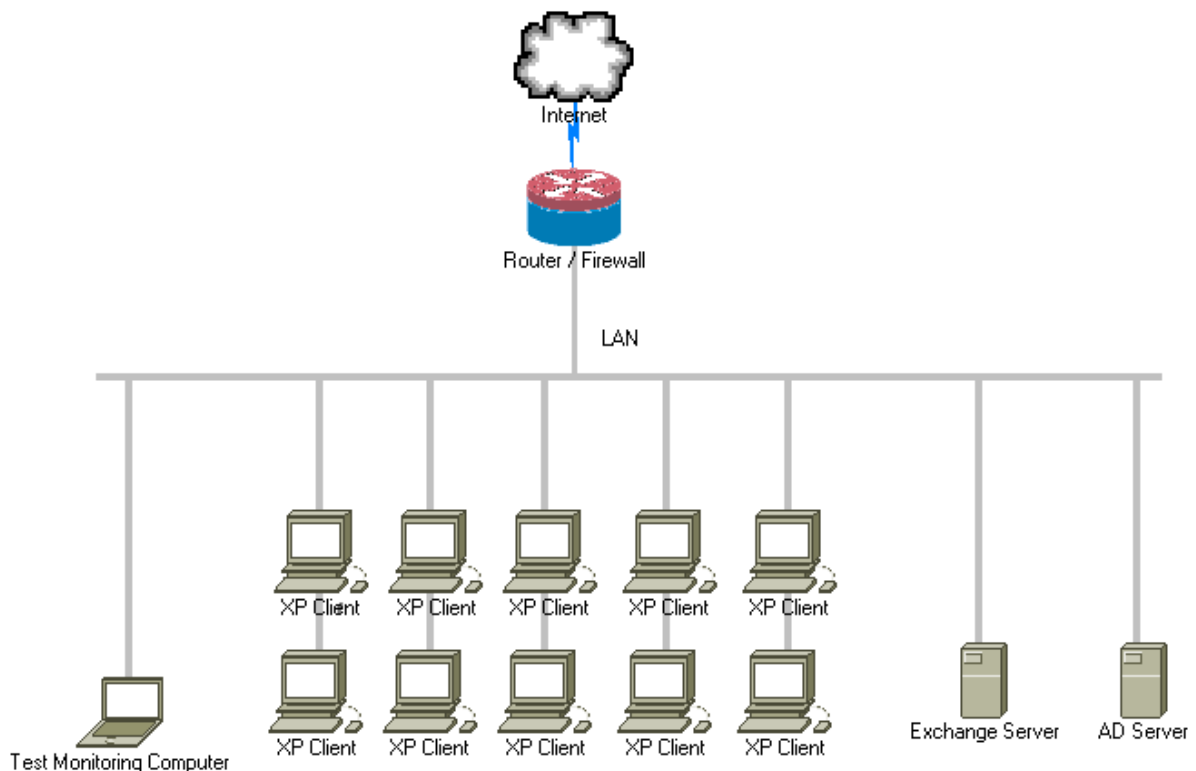
NOTE: It is important to note that whilst each product has been developed for use in an SMB environment, each also has different technical features and functionalities.

Test Environment - Summary

The test environment – designed to mirror a real-world SMB network – comprised:

- 10 client machines with Microsoft Windows XP Professional installed,
- 1 server with Microsoft Windows Server 2003 installed and primarily configured as an Active Directory Domain Controller,
- 1 server with Microsoft Small Business Server 2003 installed and primarily configured as a Microsoft Exchange email gateway,
- An Internet connection, accessed via a router / firewall,
- A West Coast Labs test monitoring and data recording computer.

The following network diagram is a simplified representation of the test environment:



NOTE: For further details regarding the test environment and network configuration, please refer to Appendix A of this report.

Test Methodology

Tests were carried out at West Coast Labs' test facilities in an emulated real-world SMB environment. Scenario-based tasks were executed in relation to each solution's usability, detection, prevention, remediation, and assessment capabilities.

Each task was repeated and observed in exactly the same manner and environmental conditions for each solution under test.

West Coast Labs quantified ease-of-use testing in terms of intuitiveness (time and complexity) of installation, management / administration and automation versus manual steps to perform basic functions such as, remediation, and executing preventive measures on the network. Analysis of other features such as aesthetics and layout were not part of these tests.

While malware detection using signature techniques are among the most popular methods employed today, 'zero-day' protection or stopping the infection within the first day of an outbreak prior to the availability of a signature has been a challenge. Therefore, in addition to known malware samples, West Coast Labs also tested a set of unknown malware samples to evaluate each solution's response prior to virus signature availability.

Test Scenarios

1. Usability

Usability was analysed by quantifying the number of installation media and installation steps involved during a primarily default installation of each solution under test, combined with basic management tasks required to get each solution operational.

2. Vulnerability Assessment

A vulnerability assessment to evaluate malware-related patch levels was initiated across the entire test network using the in-built functionality of each vendor solution, where such functionality existed in the native product without the purchase of add-on solutions. The 'Windows Update' tool was used to assess vulnerabilities in the absence of a specific product feature in this area. The time duration and efforts involved were recorded as measurable outcomes.

3. Malware Outbreak – 'Set A' / 'Set B' – Known Threats

'Set A' and 'Set B' malware were introduced to the test network to validate out-of-the-box detection / remediation capabilities against known samples. West Coast Labs had previously – as part of this project - determined that virus signatures or heuristics detection were available for these samples in each of the products under test.

4. Malware Outbreak – 'Set C' - Unknown Threats

'Set C' malware was introduced to the test network to validate out-of-the-box detection / remediation capabilities against unknown samples. West Coast Labs had previously determined that virus signatures or heuristics detection were not available for these samples in each of the products under test. This scenario – including all synchronized times and events – was carried out in line with the simulated zero day malware outbreak scenario described in the 'Appendix B – Test Procedures' section of this report.

NOTE: The actual samples in sets A, B and C are detailed in Appendix A of this report.

Test Results

(# = Total Number)

Installation Media /Programs

These tests assessed the media type and the number of separate programs needed to completely install each solution.

	McAfee	Symantec	Trend Micro
Media Type:	Internet Download	CD / Internet Download	CD / Internet Download
# Install Programs:	3	2	1

Default Installation Activities.

These tests quantified the primarily default installation activities – the steps involved to completely install each solution – in terms of the number of screens the person installing each solution saw, the number of manual actions / interventions required to install each solution, extra activities, such as externally connecting to the Internet to fulfil licensing requirements and the restarting of all computers following an install. These data span the installation of the management console, the Exchange module and the client set-up, including product updates.

<u>Management Console / Exchange Module</u>	McAfee	Symantec	Trend Micro
# User Screens:	41	63	21
# User Actions:	62	85	33
# External Licensing:	0	9	0

<u>Client</u>	McAfee + 8.0i Client	Symantec	Trend Micro
User Screens:	5	5	6
User Actions:	15	14	12
Restart Required:	Yes	No	No

Test Results

Management Consoles

These tests quantified the number of separate management consoles needed to completely administer each solution and also provided the vendor assigned name of each console.

	McAfee	Symantec	Trend Micro
# Separate Consoles:	2	2	1
Console Description:	ProtectionPilot / GroupShield	System Center / Mail Security	Security Dashboard

Test Results

Vulnerability Assessment

These tests quantified time, as well as the tasks involved in performing a vulnerability assessment on all computers in the test network.

Trend Micro was the only solution with an integrated, centrally operated vulnerability assessment tool, therefore when testing the McAfee and Symantec solutions, West Coast Labs had to download and leverage the 'Windows Update' tool to manually assess the vulnerability level of each computer. The process involved connecting to the Microsoft website and checking for patch updates. The total time in minutes and the total user actions involved relate to the entire network of 12 computers and is broken down, as follows:

- 2 minutes for 'Windows Update' to assess the patch requirements of each computer,
- 1 minute to physically travel between computers,
- 2 user actions per computer; connecting / selecting options.

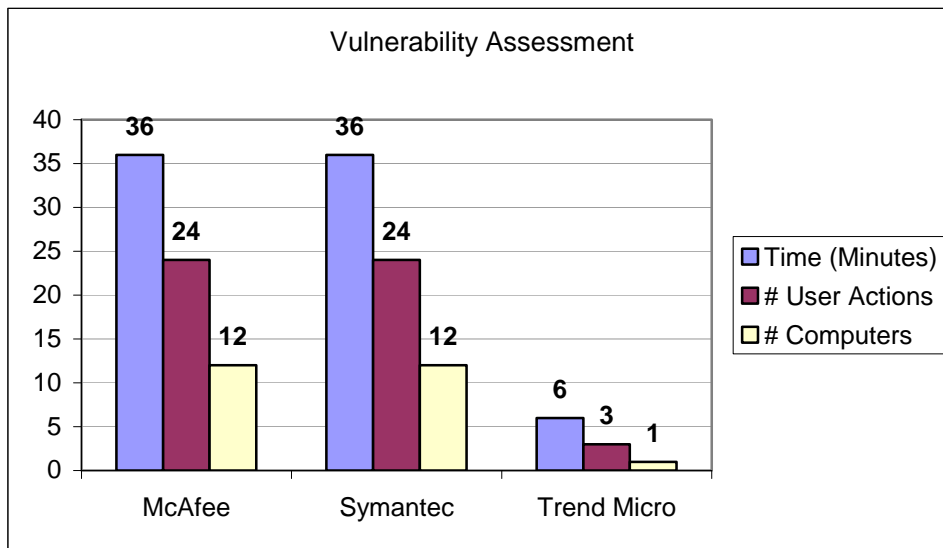
The metrics will vary, depending upon the number, physical location and specification of machines on a network and the performance of Internet-related infrastructure. In addition, the availability of remote control software and the physical speed and understanding of the system administrator will also impact the results. For example, in a network with 120 computers it could conceivably take 10 times longer to complete this process; alternatively, in a network of six computers it could take half the time to complete.

West Coast Labs expect that the results obtained using the vulnerability assessment tool in the Trend Micro product, to be relatively the same – in terms of time and effort - in any sized SMB network. The client agents perform the assessment under centralized administrative control, therefore as network size increases, total time taken should not increase exponentially.

NOTE: The same standard naming convention and number of operating system vulnerabilities were found, when using both the Trend Micro solution and the 'Windows Update' tool.

Test Results

	McAfee	Symantec	Trend Micro
# Time (Minutes):	36 (3 minutes per computer)	36 (3 minutes per computer)	6 (6 minutes, all computers)
# User Actions:	24	24	3
# Computers - requiring manual user intervention	12 (12 separate computers assessed)	12 (12 separate computers assessed)	1 (12 separate computers assessed)



Test Results

Total Network Scan Time – Malware-free Network

These test results assessed the length of time in hours, minutes and seconds (HH:MM:SS) that it took to perform a scan for malware, across the entire test network, using the default scan settings of each product. Each solution had previously been updated via the Internet and the test network was malware-free. The data are broken down into server and client categories. The server figure is the average value of three separate scans on both the Active Directory and the Exchange server, combined. The client figure is the average value of ten separate scans on the ten separate Windows XP client computers in the test network.

	McAfee	Symantec	Trend Micro
# Server:	00:12:36 (HH:MM:SS)	00:10:12 (HH:MM:SS)	00:06:50 (HH:MM:SS)
# Client:	00:04:09 (HH:MM:SS)	00:06:04 (HH:MM:SS)	00:02:55 (HH:MM:SS)

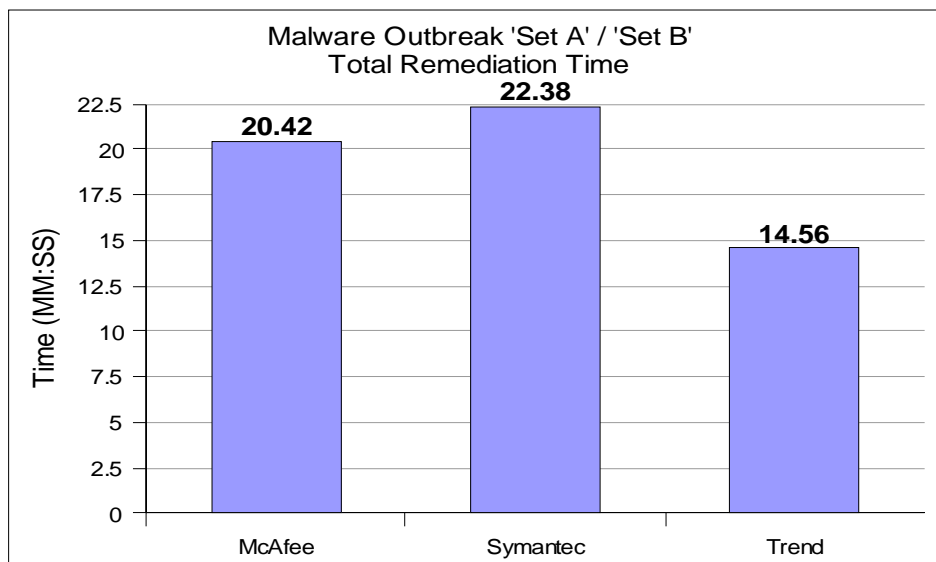
Test Results

Malware Outbreak ‘Set A’ / ‘Set B’ – Known Threats

These tests assessed the effects of introducing known Malware samples – ‘Set A’ and ‘Set B’ – to the test network and recorded the amount of time in hours, minutes and seconds (HH:MM:SS) that it reportedly took to completely scan and clean the entire network.

All three vendors successfully detected these samples after vendor updates were applied. Manual verification of complete malware removal was beyond the scope of this test phase and was fully and separately assessed in the context of the ‘Simulated Zero Day Malware Outbreak – ‘Set C’ - Unknown Threats’ test, described later in this report. The total reported scan / clean times for the known samples are shown below in tabulated and graphical format.

	McAfee	Symantec	Trend Micro
Scan & Clean Time (Reported):	00:20:42 (HH:MM:SS)	00:22:38 (HH:MM:SS)	00:14:56 (HH:MM:SS)



Test Results

Simulated Zero Day Malware Outbreak – ‘Set C’ - Unknown Threats

These tests assessed the effects of introducing the unknown ‘Set C’ malware samples to the test network – each solution did not have virus signatures available for these samples at the point of infection, nevertheless virus signatures were subsequently made available and each solution’s total scanning / cleaning capabilities were then assessed – all tests were carried out in line with the times and events specified in the simulated zero day malware outbreak scenario, located in the ‘Appendix B – Test Procedures’ section of this report and designed to mirror a potential real-world situation.

The results show that on both the McAfee and Symantec installed instances of the test network all twelve computers became contaminated with the ‘Set C’ malware by the time virus signatures were available, in line with this specific scenario.

However, the Trend Micro solution’s in-built Outbreak Prevention Policy (OPP), an XML based file was automatically issued after three computers had been contaminated – this arbitrary number was used for the purpose of evaluating Trend Micro’s automatic protection / containment capabilities following an infection – and before virus signatures were available.

The OPP successfully and automatically prevented further network propagation of the malware, protecting the remaining nine computers. The OPP was issued from a Trend Micro internal update server and distributed to the entire SMB test network automatically via the Security Dashboard component.

The purpose of the OPP is to prevent and contain a malware outbreak well in advance of traditional virus signatures / definitions being available, it works by blocking ports, file attachments, content filtering and preventing services on networked computers with identified vulnerabilities that are in line with the infection characteristics of any particular malware threat. One alternative in non Trend Micro environments is a manual lock down, which may be more difficult for non-specialist personnel to research and implement.

Test Results

After virus signatures / definitions for the 'Set C' samples were available, downloaded and applied to all three solutions, a full network scan was performed. All solutions reported the successful detection and removal of malicious content for the 'Set C' samples and the total reported scan / clean times were recorded in hours, minutes and seconds (HH:MM:SS), as shown in the table below.

	McAfee	Symantec	Trend Micro
Reported Network Scan / Clean Time:	00:10:23 (HH:MM:SS)	00:12:16 (HH:MM:SS)	00:10:04 (HH:MM:SS)

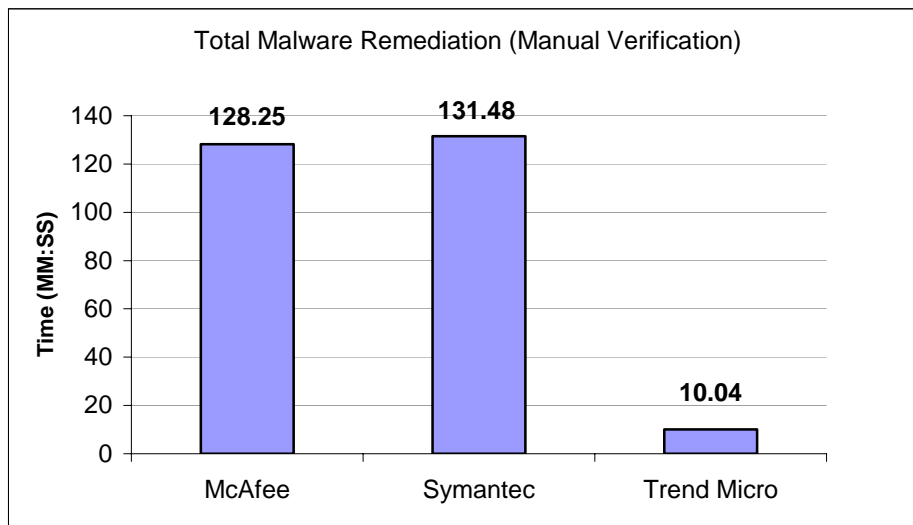
West Coast Labs then manually verified that all remnants of the 'Set C' samples had been fully removed – and not simply rendered harmless at the point of detection – from all computers on the test network.

This task involved determining the infection characteristics of each sample by performing research on each of the vendor's websites, identifying Internet sources for additional study through search engines and further manual analysis of registry entries, processes and files on machines infected with the 'Set C' samples. The overall time taken to accomplish this task was approximately 60 minutes; conceivably, this time period would increase substantially if non-specialist personnel attempted similar research.

Once the infection characteristics were identified, West Coast Labs examined each machine on the test network – for McAfee, Symantec and Trend Micro installed instances – and determined that although the McAfee and Symantec solutions did inoculate the network following a vendor update, they did not remove all remnants – registry entries remained – however, the Trend Micro product did not have any registry entries, files or processes remaining, the malware had been completely cleaned and all traces removed. The following tabulated and graphical data clearly show the results and calculations involved.

Test Results

	McAfee	Symantec	Trend Micro
Reported Network Scan / Clean Time:	00:10:23 (HH:MM:SS)	00:12:16 (HH:MM:SS)	00:10:04 (HH:MM:SS)
Research Time (Determining the infection characteristics of the 'Set C' samples):	60 Minutes		0 Minutes (Not included in the calculation, as West Coast Labs had previously verified that the Trend Micro solution had completely removed all traces of this specific malware)
Manual Removal Time:	48 Minutes 12 (computers) x 4 (minutes to physically travel to each computer and manually remove the 'Set C' malware remnants).		
Reported Secondary Re-scan / Clean Time (To confirm removal):	00:10:02 (HH:MM:SS)	00:11:32 (HH:MM:SS)	
Total Clean Time (Actual / Verified):	02:08:25 (HH:MM:SS)	02:11:48 (HH:MM:SS)	00:10:04 (HH:MM:SS)



Test Results.

Simulated Zero Day Malware Outbreak – ‘Set C’ - Unknown Threats

This test was only carried out on the Trend Micro product given that neither the McAfee nor the Symantec solutions currently contain a pre-signature file protection capability.

This test assessed Trend Micro’s Automatic Threat protection (OPP) capabilities when applied to an entire network, before the availability of virus signatures and prior to the unknown ‘Set C’ malware samples infecting the network. West Coast Labs ensured that Automatic Threat protection was operational and then attempted to introduce the unknown ‘Set C’ samples to the test network, recording the results.

The results proved that following the automatic deployment of an OPP, the test network was automatically protected against the ‘Set C’ samples before the availability of traditional virus signatures – a unique ability compared with the default versions of the McAfee and Symantec products under test – this ensured that the ‘Set C’ samples were unable to infect any computers or propagate on the test network.

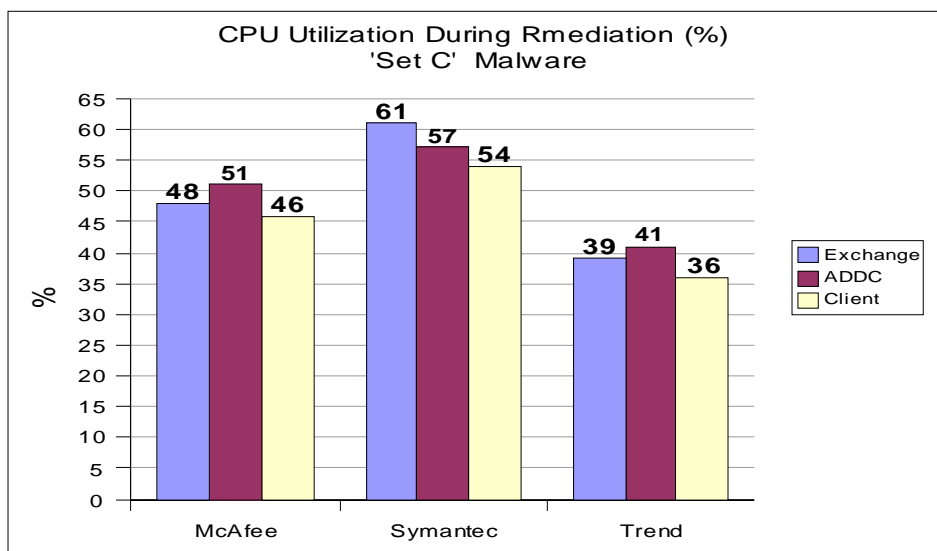
	McAfee	Symantec	Trend Micro
Pre-signature File Protection Available:	No	No	Yes

Test Results

Average CPU Utilization during Scan / Clean Time (%)

These tests recorded the average CPU utilization in percent for the complete duration of the reported scan / clean time for the initial 'Set C' malware outbreak; data was taken from in-built performance tools on the Exchange server, Active Directory server and the ten Windows XP client computers.

	McAfee	Symantec	Trend Micro
Exchange Server (Average):	48	61	39
Active Directory Server (Average):	51	57	41
Windows XP Client (Average):	46	54	36



NOTE: All CPU data was obtained from a single metric - as opposed to an average CPU usage value across a number of scans - and although the time and environment are the same for all solutions under test, background processes may be different and have some impact on the data. This data is not conclusive evidence that the Trend Micro solution has a consistent CPU performance advantage. All time / duration data detailed within this report relate to a specific test environment and where appropriate, specific malware samples including the associated number of network / computer infections present at a specific point in time - additional background processes, different malware samples and an alternative test environment may impact such data - therefore, these data should not be taken as conclusive evidence that Trend Micro has consistently faster scanning / cleaning technologies.

Conclusion

On the basis of the test results and assessed in the context of the specific test scenarios and technologies tested in this report, it was evident that the Trend Micro product had an advantage. The product was well designed for ease-of-deployment – with an unchanged, default install providing a high level of protection - general ease-of-use was facilitated through the intuitive, user-friendly web-based management interface. From this centralized interface, administrators were able to:

- Get an overview of the security status of the entire network at a glance,
- See what actions had been taken to combat a malware threat,
- Remotely manage, configure and enforce security settings across all networked computers.

The automatic threat prevention, protection and remediation capabilities were extremely effective and required zero user intervention.

The test results highlight the value of Trend Micro's vulnerability assessment functionality and Outbreak Prevention Policy (OPP) technology, which combine with minimal user intervention to produce a highly effective threat protection product; a computer network can quickly and accurately be assessed for vulnerabilities, locked down and immunized against new malware outbreaks in advance of more traditional virus solutions, while not requiring specialist IT security skills.

IMPORTANT NOTE: In the interest of impartiality, West Coast Labs – through previous and on-going evaluation - recognize that all three products have advantageous functionality in different areas. The test objectives defined within this report did not require the complete assessment of all individual product functionality across all three products under test. Accordingly, organizations may need to further assess these products individually, based on specific business requirements, scenarios and environmental conditions, while also considering any available in-house / outsourced security skill sets.

Appendices

Appendix A - Test Environment - Detailed

Hardware

<u>Qty.</u>	<u>Node Type</u>	<u>CPU</u>	<u>RAM</u>	<u>HDD</u>	<u>Network</u>
11	Client	3.0 GHz	1 GB	40 GB	Gigabit
2	Server	3.06 GHz	1 GB	40 GB	Gigabit

Core Software

<u>Qty.</u>	<u>Operating System</u>
10	Microsoft Windows XP Professional SP1
1	Microsoft Small Business Server 2003
1	Microsoft Windows Server 2003
1	Microsoft Office 2000
1	West Coast Labs Customized Linux

Infrastructure

<u>Qty.</u>	<u>Description</u>
1	24 Port 10 / 100 / 1000 LAN Switch
1	Cisco 800 Series Router (Firewall)
1	Broadband Internet Connection

Malware Samples

<u>Set</u>	<u>Name</u>
A	W97M/markhap.A
	W32/Bagle-EF
B	W23/Sober.X
C	WORM_RBOT.DLC
	WORM_RBOT.CQN
	WORM_COMBRA.P

Appendices

Test Evaluation and Reporting Toolkit

West Coast Labs used a custom set of testing and metric recording software, based on established open-source and commercial products, toolkit components were activated on client and server devices and the resulting test data was captured on a separate computer, enabling further detailed analysis.

Test Network Configuration

The following machines were defined and manually set-up by West Coast Labs in an isolated LAN configuration and designed to mirror a real world SMB environment:

<u>Qty.</u>	<u>Operating System</u>	<u>HDD Partition</u>		<u>Key Components</u>
10	Windows XP Professional SP1	19.53 GB C: System	17.71 GB D: Image	Outlook / Word
1	Small Business Server 2003	19.53 GB C: System	17.71 GB D: Image	Exchange
1	Windows Server 2003	19.53 GB C: System	17.71 GB D: Image	AD / DNS / IIS
1	West Coast Labs Customized Linux	N / A		Test / Metric Tools

Each operating system within the test network was installed on the 'C: System' partition and then an exact copy (snapshot image) of this partition was compressed, password-protected and copied to the 'D: Image' partition. Each snapshot image was tested by re-writing it to the 'C: System' partition, ensuring that each operating system environment was reproducible and functioning correctly as specified in the test methodology / scenario. Network time synchronization software for all client / server devices was installed and activated, then reset to the original value prior to each testing phase, ensuring time synergy, as specified in the test methodology / scenario. The following table contains further details on the configuration of the test network:

Appendices

<u>Computer Name</u>	<u>Node Type</u>	<u>User</u>	<u>IP Address</u>
T130	Client	T130	10.10.10.130 / 24
T131	Client	T131	10.10.10.131 / 24
T132	Client	T132	10.10.10.132 / 24
T133	Client	T133	10.10.10.133 / 24
T134	Client	T134	10.10.10.134 / 24
T135	Client	T135	10.10.10.135 / 24
T136	Client	T136	10.10.10.136 / 24
T137	Client	T137	10.10.10.137 / 24
T138	Client	T138	10.10.10.138 / 24
T139	Client	T139	10.10.10.139 / 24
T140	Server	Administrator	10.10.10.140 / 24
T141	Server	Administrator	10.10.10.141 / 24
Linux	Client / Server	Root	10.10.10.142 / 24

Each computer was attached to the network using the 24 port LAN switch and an Internet gateway was provided by the Cisco 800 Series router / firewall device. This device was assigned an internal IP address of 10.10.10.254 / 24 and the appropriate firewall rules were configured to ensure complete isolation from the Internet and all other internal test networks, as appropriate to the test methodology / scenario.

Appendices

Appendix B - Test Procedures

West Coast Labs defined and applied these test procedures and recorded all resulting data:

- Subsequent to the test network set-up, configuration and testing, malware 'Set A' was introduced to the test environment and allowed to propagate for a set period of time via file and network based techniques, in line with standard SMB user activities, including, email, web-browsing and file sharing. All test machines were infected at this point. All network / session data generated during this process was captured and recorded via a pre-configured analyzer toolset resident on the customized Linux machine.
- The test network was then re-imaged and returned to the exact original state (without any malware present), subsequent to that process, malware 'Set B' was introduced to the test environment and allowed to propagate for a set period of time via file and network based techniques, in line with standard SMB user activities, including, email, web-browsing and file sharing. All test machines were infected at this point. All network / session data generated during this process was captured and recorded via a pre-configured analyzer toolset resident on the customized Linux machine.
- The test network was again re-imaged and returned to the exact original state (without any malware present), subsequent to that process, malware 'Set C' was introduced to the test environment and allowed to propagate for a set period of time via file and network based techniques, in line with standard SMB user activities, including, email, web-browsing and file sharing. Three test machines were initially infected at this point. All network / session data generated during this process was captured and recorded via a pre-configured analyzer toolset resident on the customized Linux machine.
- Each set of malware (A, B and C) was then re-introduced at separate time intervals to a re-imaged instance of the test network, ensuring that the malware infection data was reproducible in line with the test scenario. An appropriate data replay tool was used, facilitating time and data synergy for comparative testing purposes.

-
- Each vendor solution was installed at a separate time interval on a clean, malware-free instance of the test network and all user intervention activities were recorded, based on a default set-up of the core components; defined as management console, Exchange agent and client software.
 - The test network was installed with each vendor solution at separate points in time, then infected with each set of malware (A, B and C) at separate points in time – using the appropriate data replay tool and aligning with the test scenario described within this report – all malware sets were introduced both with and without vendor product updates applied, enabling West Coast Labs to assess the virus signature database of each product, specifically ensuring that malware ‘Set C’ signatures were not present within each product at the time of installation. In addition, West Coast Labs made certain that the malware ‘Set C’ signatures were available for each product following an Internet update.
 - An internal update server was set-up on the Active Directory Domain Controller for West Coast Labs to emulate, assess and validate the automatic Outbreak Prevention Policy of the Trend Micro solution in line with the test scenario / methodology.
 - A simulated zero-day outbreak – the ‘Set C’ malware samples - and at this time virus signatures were not available from any of the three vendors with products under test. The ‘Set C’ samples were chosen to test unknown malware. West Coast Labs had previously – as part of this project - determined that virus signatures or heuristics detection were unavailable for these samples in each of the products under test. The following details further describe the test scenario structure:

Zero-day - 09:00 hrs: A previously undetected collection of worms - ‘Set C’ - was released into the wild, actively spreading and infecting vulnerable computers.

Zero-day - 09:20 hrs: The SMB-mirrored test network was infected with ‘Set C’ resulting in the initial contamination of three machines out of a possible twelve nodes.

Zero-day – 09:21 hrs: Trend Micro issued Automatic Threat protection (OPP), prior to virus signatures being available for the ‘Set C’ threats.

Zero-day - 10:00 hrs: New virus signatures for ‘Set C’ were released by all vendors (McAfee, Symantec and Trend Micro) and were available for download via the Internet. These updates were applied to all vendor solutions at this point.

NOTE: In real-world conditions, virus signature availability may vary, based on the threat complexity, type and vendor involved. The one-hour time period between the release of the ‘Set C’ malware and the availability of a mitigating signature – in addition to being realistic – was specified in this scenario to ensure that the same baseline comparison was possible between all vendor solutions and to permit testing of the Outbreak Prevention Policy (OPP) in real-world conditions.

From 09:00 hrs to 10:00 hrs: normal SMB computer operations were continuing, including, email, web browsing and file sharing activities.

During this process, each of the vendor solutions were assessed for known threat prevention, protection and remediation capabilities in addition to administration usability.

It was a further requirement to record the total time taken to research and subsequently fully remove the ‘Set C’ worm samples from all infected machines – this was in the event of a product not being able to completely clean the worm and / or any remnants, after a vendor update had been applied – and to note the manual processes involved. The research path followed is described in the ‘Test Results’ section of this report under the ‘Zero-day Malware Outbreak – Total Malware Remediation (Manual Verification)’ test heading.

NOTE: Vendors may provide a malware removal tool after a new virus signature has been released, in this instance, the use of a removal tool was not deemed the most appropriate response as West Coast Labs were testing under a real-world zero-day outbreak scenario. A manual method was therefore used for removal.

Appendices

Appendix C – Trend Micro Real-world Outbreak

To support the test results and scenarios shown within this report, Trend Micro describe a real-world outbreak, detailing the background events and how they responded to the specific incident:

On October 5th, 2005 the world was hit with an email worm, WORM_SOBER.AC. This worm propagated via email messages. It used an in-built SMTP engine to send a copy of itself as an attachment to target email addresses. It gathered the said addresses from files with certain extensions on an infected system. Most of the files with the said extensions were related to the Web pages visited by an affected user. The worm gathered these types of files under the assumption that visited Web pages might contain text strings referring to email addresses.

To prevent the spread of this worm, Trend Micro delivered Outbreak Prevention Policy 186 that directed Trend Micro products to:

1. Block incoming email with .ZIP attachments (This prevents the entry of all incoming email brought about by infection of WORM_SOBER.AC on external systems)
2. Delete malware dropped files

To remove the damage caused by this worm, Trend Micro delivered Damage Cleanup Template 661.04 directing Trend Micro products to:

1. Terminate the malware program
2. Delete the dropped files and folder
3. Remove the malware registry entry

NOTE: West Coast Labs were not required to verify the specific details of the above account, as part of the test process. However, the description of these events and the subsequent prevention, remediation and removal processes mirror the test results contained in this report.

Revision History

Issue	Description of Changes	Date Issued
1.0	Trend Micro Client Server Messaging Solution for SMB	05/10/06



West Coast Labs, William Knox House, Britannic Way, Llandarcy, Swansea, SA10 6EL, UK.

Tel : +44 1792 324000, Fax : +44 1792 324001. www.westcoastlabs.org