Virtual desktop malware defence

A Web Threat Protection Test Of Anti-Malware Products Running In Virtual Desktop Environments (Sponsored by Symantec)

Dennis Technology Labs, 28/04/2011
www.DennisTechnologyLabs.com

This test aims to compare the effectiveness of the most recent releases of anti-malware products designed to run in virtual desktop environments. The list of products includes solutions from McAfee, Symantec and Trend Micro (see below).

The test is based on the following assumptions. The virtual systems are intended for use by office workers who are granted unrestricted access to the web. There are no inline security products deployed, such as network IPS devices or other gateway-style protection measures.

A total of three products were exposed to genuine internet threats that real customers could have encountered during the test period. Crucially, this exposure was carried out in a realistic way, reflecting a customer's experience as closely as possible. For example, each test system visited genuinely infected websites and downloaded files exactly as an average user would.

Products are awarded marks for detecting real threats and providing adequate protection. Points are deducted for failing to protect the system.

Executive summary

Products tested
McAfee MOVE AntiVirus with Host Intrusion Prevention for Desktop and SiteAdvisor Enterprise (**MOVE**)

Symantec Endpoint Protection 12, Amber pre-release (**SEP**)

Trend Micro OfficeScan 10.5 with Intrusion Defense Firewall and VDI plug-in (**OS**)

In the following charts and tables the product groups have been abbreviated to MOVE, SEP *and* OS *respectively.*
For specific product configurations please see Appendix E: Product versions *on page 21.*

- **Vendors recommend installing 'VDI-aware' endpoint clients**

1. The three vendors involved in this test have different approaches to protecting virtualized desktops that have unfettered access to the web. However, they all recommend using relatively standard desktop products rather than moving all of the malware protection mechanisms away from the client and into the virtual infrastructure. The Symantec Endpoint Protection client and the Trend Micro OfficeScan installation are VDI-aware, rather than fully embedded into the virtual infrastructure.

- **On-demand scanning played no part in protecting these systems**

2. While on-demand scanning is no doubt useful in certain circumstances, in this web threat test it played no significant part. Almost all detections and protections took place before files were copied to the targets' hard disk. At no time did an on-demand scan fix an infected system.

Version 1.1 [Changes: Corrected version number of Trend Micro OfficeScan to 10.5.]

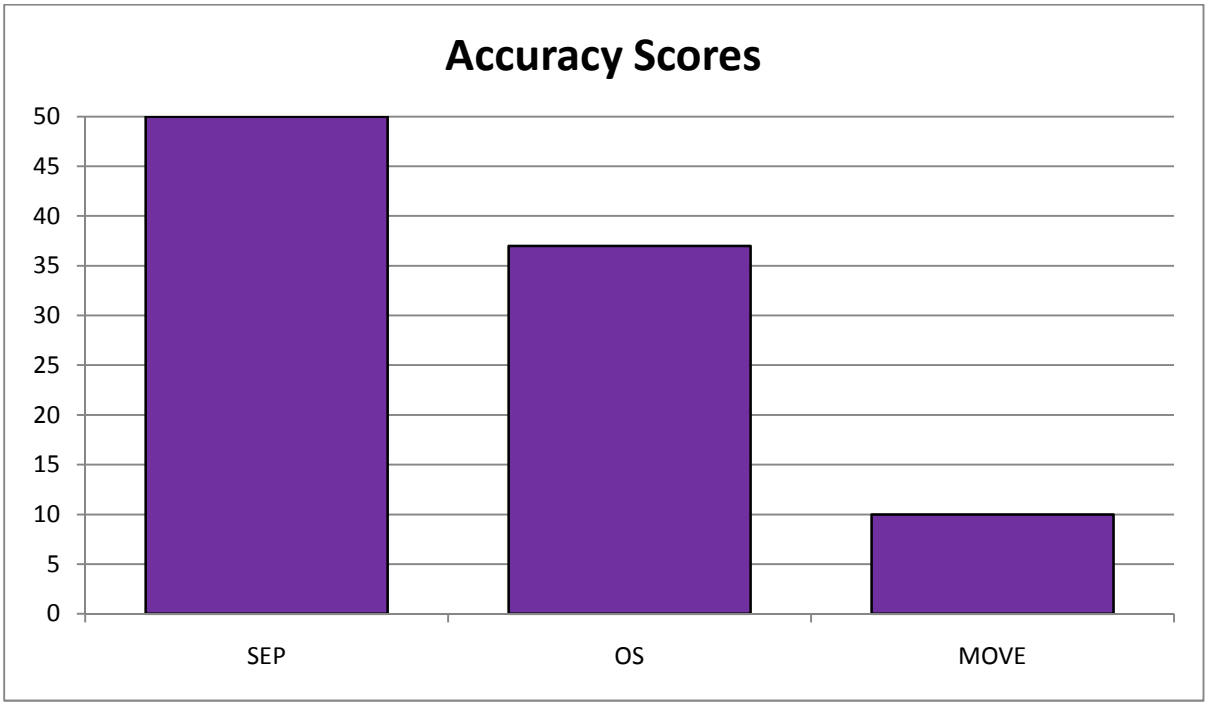
Simon Edwards, Dennis Technology Labs

CONTENTS

1. Overall Accuracy

Each product has been scored for accuracy. We have awarded two points for defending against a threat, one for neutralizing it and removed two points every time a product allowed the system to be compromised.

The reason behind this score weighting is to give credit to products that deny malware an opportunity to tamper with the system and to penalize those that allow malware to damage it.



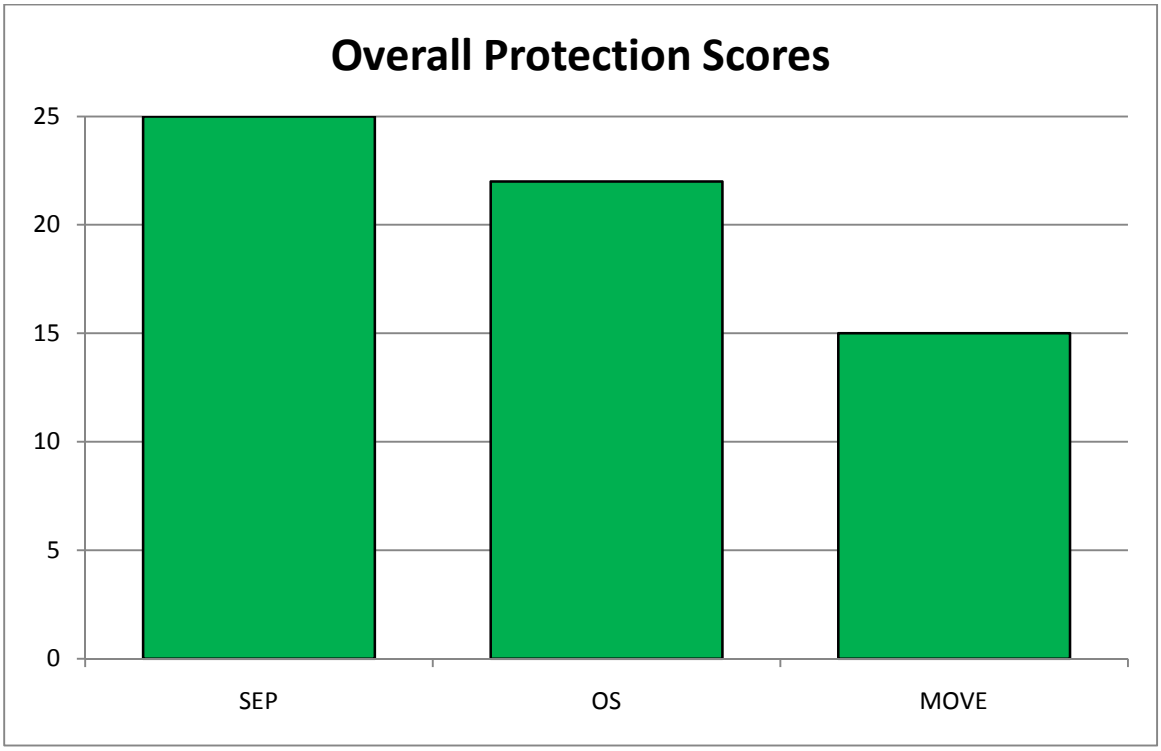
Symantec Endpoint Security scored top marks for preventing threats because it defended every threat. Trend Micro OfficeScan defended most of the threats and neutralized one. McAfee MOVE's score is low because it was compromised ten times out of 25 exposures.

ACCURACY SCORES

PRODUCT	DEFENDED	NEUTRALIZED	COMPROMISED	ACCURACY
SEP	25	0	0	50
OS	21	1	3	37
MOVE	15	0	10	10

2. Overall Protection

The following illustrates the general level of protection provided by each of the security products, combining the defended and neutralized incidents into an overall figure. This figure is not weighted with an arbitrary scoring system as it was in **1. Overall accuracy**.



All of the products protected against at least 60 per cent of the web-based threats.

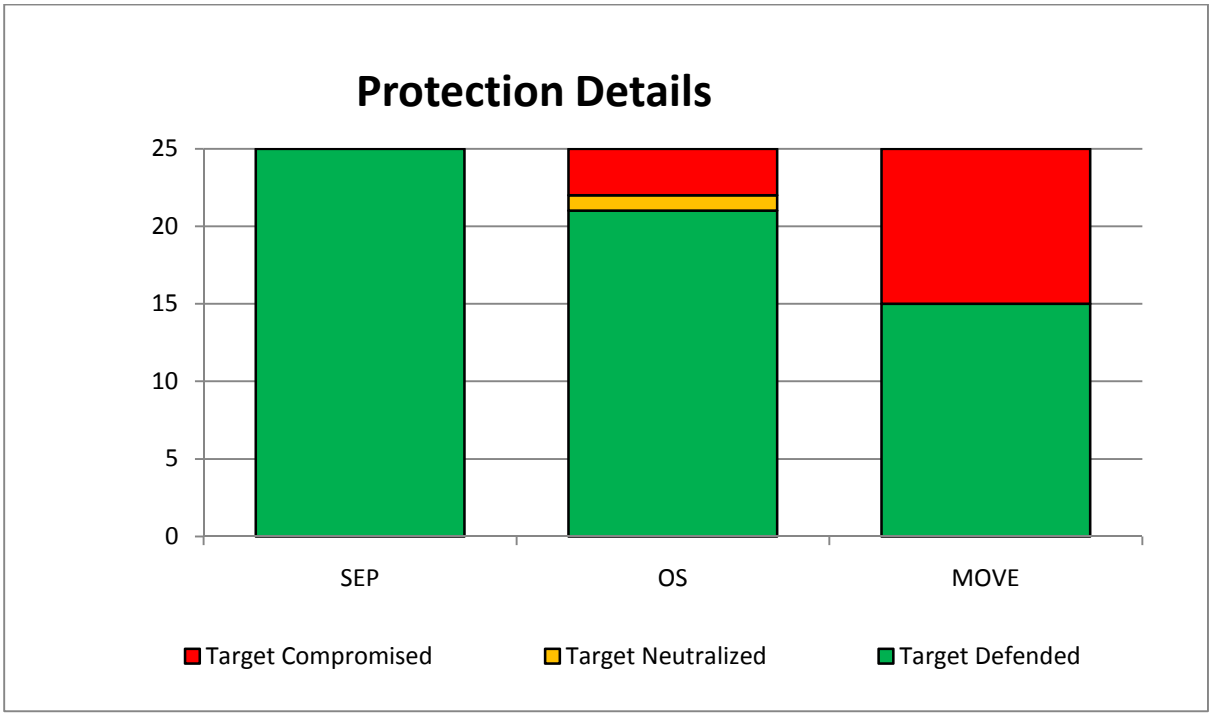
OVERALL PROTECTION SCORES

PRODUCT	COMBINED PROTECTION SCORE	PERCENTAGE
SEP	25	100 per cent
OS	22	88 per cent
MOVE	15	60 per cent

(Average: 83 per cent)

3. PROTECTION DETAILS

The security products provided different levels of protection. When a product **defended** against a threat, it prevented the malware from gaining a foothold on the target system. A threat might have been able to infect the system and, in some cases, the product **neutralized** it later. When it couldn't, the system was **compromised**.



In most cases a running threat meant a compromise. In one incident OfficeScan neutralized running malware.

PROTECTION DETAILS

PRODUCT	DEFENDED	NEUTRALIZED	COMPROMISED
SEP	25	0	0
OS	21	1	3
MOVE	15	0	10

4. FALSE POSITIVES

4.1 False positive levels

A security product needs to be able to protect the system from threats, while allowing legitimate software to work properly. When legitimate software is misclassified a false positive is generated. We split the results into two main groups because the products all took one of two approaches when attempting to protect the system from the legitimate programs. They either warned that the software was suspicious or took the more decisive step of blocking it.

Blocking a legitimate application is more serious than issuing a warning because it directly hampers the user. Warnings may be of variable strength, sometimes simply asking if the legitimate application should be allowed to access the internet.

In this test not one of the security products generated a false positive of any kind. Nevertheless, we have included our standard false positive testing methodology and marking system for completeness.

4.4 Distribution of impact categories

Products that scored highest were the most accurate when handling the legitimate applications used in the test. The best score possible is 25, while the worst would be -125 (assuming that all applications were classified as Very High Impact and were blocked). In fact the distribution of applications in the impact categories was not restricted only to Very High Impact. The table below shows the true distribution:

FALSE POSITIVE CATEGORY FREQUENCY

Impact category	Number of instances
Very High Impact	2
High Impact	10
Medium Impact	12
Low Impact	1
Very Low Impact	0

For more information on false positive testing please see **6.9 False positives** on page 12.

5. THE TESTS

5.1 The threats

Providing a realistic user experience was important in order to illustrate what really happens when a user encounters a threat on the internet. For example, in these tests web-based malware was accessed by visiting an original, infected website using a web browser, and not downloaded from a CD or internal test website.

All target systems were fully exposed to the threats. This means that malicious files were run and allowed to perform as they were designed, subject to checks by the installed security software. A minimum time period of five minutes was provided to allow the malware an opportunity to act.

5.2 Test rounds

Tests were conducted in rounds. Each round recorded the exposure of every product to a specific threat. For example, in 'round one' each of the products was exposed to the same malicious website.

At the end of each round the test systems were completely reset to remove any possible trace of malware before the next test began.

5.3 Monitoring

Close logging of the target systems was necessary to gauge the relative successes of the malware and the anti-malware software. This included recording activity such as network traffic, the creation of files and processes and changes made to important files.

5.4 Levels of protection

The products displayed different levels of protection. Sometimes a product would prevent a threat from executing, or at least making any significant changes to the target system. In other cases a threat might be able to perform some tasks on the target, after which the security product would intervene and remove some or all of the malware.

Finally, a threat may be able to bypass the security product and carry out its malicious tasks unhindered. It may even be able to disable the security software. Occasionally Windows' own protection system might handle a threat, while the anti-virus program can ignore it. Another outcome is that the malware may crash for various reasons. The different levels of protection provided by each product were recorded following analysis of the log files.

5.5 Types of protection

Symantec Endpoint Protection and Trend Micro OfficeScan provide two main types of protection: real-time and on-demand. Real-time protection monitors the system constantly in an attempt to prevent a threat from gaining access. On-demand protection is essentially a 'virus scan' that is run by the user at an arbitrary time.

McAfee MOVE is a different type of product. Designed specifically for improving system performance in virtual desktop environments, it uses an additional product called McAfee VirusScan Enterprise for Offline Virtual Images (OVI) to scan infected systems. We did not install this additional software so, when a McAfee-protected virtual desktop was infected, we did not run an offline scan.

The test results note each product's behavior when a threat is introduced and afterwards. The real-time protection mechanism was monitored throughout the test, while an on-demand scan was run towards the end of each test to measure how safe either the SEP or OS products determined the system to be.

6. TEST DETAILS

6.1 The targets

To create a fair testing environment, each product was installed on a clean Windows XP Professional target system. The operating system was updated with Windows XP Service Pack 3 (SP3), although no later patches or updates were applied. The high prevalence of internet threats that rely on Internet Explorer 7, and other vulnerable Windows components that have been updated since SP3 was released, suggest that there are many systems with this level of patching currently connected to the internet. We used this level of patching to remain as realistic as possible. Windows Automatic Updates was disabled.

A selection of legitimate but old software was pre-installed on the target systems. These posed security risks, as they contained known vulnerabilities. They include out of date versions of Adobe Flash Player and Adobe Reader.

A different security product was then installed on each system. Each product's update mechanism was used to download the latest version with the most recent definitions and other elements. Due to the dynamic nature of the tests, which are carried out in real-time with live malicious websites, the products' update systems were allowed to run automatically and were also run manually before each test round was carried out. The products were also allowed to 'call home' should they be programmed to query databases in real-time. At any given time of testing, the very latest version of each program was used.

Each target system was a virtual desktop running on an HP ProLiant DL360 G5 server running VMware ESXi 4.1. Each virtual desktop was allocated 2GB RAM, one processor and up to 27GB disk space. The management tools required by the different products were deployed, including the management consoles for McAfee ePolicy Orchestrator (ePO) 4.5, Trend Micro OfficeScan Management Console and VMware vCenter. Symantec Endpoint Protection (Amber) was run as a stand-alone product without management tools.

6.2 Threat selection

The malicious web links (URLs) used in the tests were picked from lists generated by Dennis Technology Labs' own malicious site detection system, which uses popular search engine keywords submitted to Google. It analyses sites that are returned in the search results from a number of search engines and adds them to a database of malicious websites. In all cases, a control system (Verification Target System - VTS) was used to confirm that the URLs linked to actively malicious sites. Malicious URLs and files are not shared with any vendors during the testing process.

6.3 Test stages

There were three main stages in each individual test:

1. Introduction
2. Observation
3. Remediation

During the *Introduction* stage, the target system was exposed to a threat. Before the threat was introduced, a snapshot was taken of the system. This created a list of Registry entries and files on the hard disk. We used Regshot (see **Appendix D: Tools**) to take and compare system snapshots. The threat was then introduced.

Immediately after the system's exposure to the threat, the *Observation* stage is reached. During this time, which typically lasted at least 10 minutes, the tester monitored the system both visually and using a range of third-party tools. The tester reacted to pop-ups and other prompts according to the directives described below (**see 6.6 Observation and intervention**).

In the event that hostile activity to other internet users was observed, such as when spam was being sent by the target, this stage was cut short. The *Observation* stage concluded with another system snapshot. This 'exposed' snapshot was compared to the original 'clean' snapshot and a report generated. The system was then rebooted.

The *Remediation* stage is designed to test the products' ability to clean an infected system. If it defended against the threat in the *Observation* stage then there should be few (if any) legitimate alerts during this procedure. An on-demand scan was run on the target where possible, after which a 'scanned' snapshot was taken. This was compared to the original 'clean' snapshot and a report was generated. All log files, including the snapshot reports and the product's own log files, were recovered from the target. The target was then reset to a clean state, ready for the next test.

6.4 Threat introduction

Malicious websites were visited in real-time using Internet Explorer. This risky behavior was conducted using live internet connections. URLs were typed manually into Internet Explorer's address bar.

Web-hosted malware often changes over time. Visiting the same site over a short period of time can expose systems to what appear to be a range of threats (although it may be the same threat, slightly altered to avoid detection). In order to improve the chances that each target system received the same experience from a malicious web server, we used a web replay system. When the first target system visited a site, the page's content, including malicious code, was downloaded and stored. When each consecutive target system visited the site, it should have received the same content, with some provisos.

Many infected sites will only attack a particular IP address once, which makes it hard to test more than one product. We used an HTTP session replay system to counter this problem. It provides a close simulation of a live internet connection and allows each product to experience the same threat. Configurations were set to allow all products unfettered access to the internet.

6.5 Secondary downloads

Established malware may attempt to download further files (secondary downloads), which will also be cached by the proxy and re-served to other targets in some circumstances. These circumstances include cases where:

1. The download request is made using HTTP (e.g. http://badsite.example.com/...) and
2. The same filename is requested each time (e.g. badfile1.exe)

There are scenarios where target systems will receive different secondary downloads. These include cases where:

1. A different filename is requested each time (e.g. badfile2.exe; random357.exe) or
2. The same filename is requested over HTTP but the file has been modified on the web server. In this case even the original download may differ between target systems

6.6 Observation and intervention

Throughout each test, the target system was observed both manually and in real-time. This enabled the tester to take comprehensive notes about the system's perceived behavior, as well as to compare visual alerts with the products' log entries. At certain stages the tester was required to act as a regular user. To achieve consistency, the tester followed a policy for handling certain situations including dealing with pop-ups displayed by products or the operating system, system crashes, invitations by malware to perform tasks and so on.

This user behavior policy included the following directives:

1. Act naively. Allow the threat a good chance to introduce itself to the target by clicking OK to malicious prompts, for example.
2. Don't be too stubborn in retrying blocked downloads. If a product warns against visiting a site, don't take further measures to visit that site.
3. Where malware is downloaded as a Zip file, or similar, extract it to the Desktop then attempt to run it. If the archive is protected by a password, and that password is known to you (e.g. it was included in the body of the original malicious email), use it.
4. Always click the default option. This applies to security product pop-ups, operating system prompts (including Windows firewall) and malware invitations to act.
5. If there is no default option, wait. Give the prompt 20 seconds to choose a course of action automatically.
6. If no action is taken automatically, choose the first option. Where options are listed vertically, choose the top one. Where options are listed horizontally, choose the left-hand one.

6.7 Remediation

When a target is exposed to malware, the threat may have a number of opportunities to infect the system. The security product also has a number of chances to protect the target. The snapshots explained in **5.3 Test stages** provided information that was used to analyze a system's final state at the end of a test.

Before, during and after each test, a 'snapshot' of the target system was taken to provide information about what had changed during the exposure to malware. For example, comparing a snapshot taken before a malicious website was visited to one taken after might highlight new entries in the Registry and new files on the hard disk. Snapshots were also used to determine how effective a product was at removing a threat that had managed to establish itself on the target system. This analysis gives an indication as to the levels of protection that a product has provided.

These levels of protection have been recorded using three main terms: defended, neutralized, and compromised. A threat that was unable to gain a foothold on the target was *defended* against; one that was prevented from continuing its activities was *neutralized*; while a successful threat was considered to have *compromised* the target.

A defended incident occurs where no malicious activity is observed with the naked eye or third-party monitoring tools following the initial threat introduction. The snapshot report files are used to verify this happy state.

If a threat is observed to run actively on the system, but not beyond the point where an on-demand scan is run, it is considered to have been neutralized. Comparing the snapshot reports should show that malicious files were created and Registry entries were made after the introduction. However, as long as the 'scanned' snapshot report shows that either the files have been removed or the Registry entries have been deleted, the threat has been neutralized.

The target is compromised if malware is observed to run after the on-demand scan. In some cases a product will request a further scan to complete the removal. For this test we considered that secondary scans were acceptable, but further scan requests would be ignored. Even if no malware was observed, a compromise result was recorded if snapshot reports showed the existence of new, presumably malicious files on the hard disk, in conjunction with Registry entries designed to run at least one of these files when the system booted. An edited 'hosts' file or altered system file also counted as a compromise.

6.8 Automatic monitoring

Logs were generated using third-party applications, as well as by the security products themselves. Manual observation of the target system throughout its exposure to malware (and legitimate applications) provided more information about the security products' behavior. Monitoring was performed directly on the target system and on the network.

Client-side logging

A combination of Process Explorer, Process Monitor, TcpView and Wireshark were used to monitor the target systems. Regshot was used between each testing stage to record a system snapshot. A number of Dennis

Technology Labs-created scripts were also used to provide additional system information. Each product was able to generate some level of logging itself.

Process Explorer and TcpView were run throughout the tests, providing a visual cue to the tester about possible malicious activity on the system. In addition, Wireshark's real-time output, and the display from the web proxy (see Network logging, below), indicated specific network activity such as secondary downloads.

Process Monitor also provided valuable information to help reconstruct malicious incidents. Both Process Monitor and Wireshark were configured to save their logs automatically to a file. This reduced data loss when malware caused a target to crash or reboot.

In-built Windows commands such as 'systeminfo' and 'sc query' were used in custom scripts to provide additional snapshots of the running system's state.

Network logging

All target systems were connected to a live internet connection, which incorporated a transparent web proxy and network monitoring system. All traffic to and from the internet had to pass through this system. Further to that, all web traffic had to pass through the proxy as well. This allowed the tester to capture files containing the complete network traffic. It also provided a quick and easy view of web-based traffic, which was displayed to the tester in real-time.

The network monitor was a dual-homed Linux system running as a bridge and transparent router, passing all web traffic through a Squid proxy.

An HTTP replay system ensured that all target systems received the same malware as each other. It was configured to allow access to the internet so that products could download updates and communicate with any available 'in the cloud' servers.

6.9 False positives

A useful security product is able to block threats and allow useful program to install and run. The products were also tested to see how they would respond to legitimate applications.

The prevalence of each installation file is significant. If a product misclassified a common file then the situation would be more serious than if it failed to permit a less common one. That said, it is fair for users to expect that antimalware programs should not misclassify any legitimate software.

The files selected for the false positive testing were organized into five groups: Very High Impact, High Impact, Medium Impact, Low Impact and Very Low Impact. These categories were based on download numbers for the previous week, as reported by the specific download site used at the time of testing or as estimated by Dennis Technology Labs when that data was not available. The ranges for these categories are recorded in the table below:

CATEGORY	PREVALENCE
Very High Impact	>20,001 downloads
High Impact	>999 downloads
Medium Impact	>99 downloads
Low Impact	>24 downloads
Very Low Impact	<25 downloads

(Figures published by the download sites used, at the time of testing)

In the false positive accuracy tests a product scored one full point when it neither warned nor blocked the legitimate application. If it warned against running or installing it then it lost points. It lost twice as many points if it blocked the software.

The actual number of points (or fraction of a point) lost depended on how prevalent the file was. For example, if a security product blocked a Very High Impact program (such as the DivX installer, which Download.com once claimed was downloaded 69,465 times in the previous week) then it would lose five points. If it only warned against it then it would lose 2.5 points. If it blocked a much less common program, such as Wordsearch Solver (23 downloads in the previous week) then it would lose only 0.1 points. A warning would modify the product's score by just -0.05 points.

The score modifiers are as follows:

FIXED SCORING MODIFIERS

Blocked	Very High Impact	-5
	High Impact	-2
	Medium Impact	-1
	Low Impact	-0.5
	Very Low Impact	-0.1
Warning	Very High Impact	-2.5
	High Impact	-1
	Medium Impact	-0.5
	Low Impact	-0.25
	Very Low Impact	-0.05

The test included 25 legitimate applications. This means that the maximum possible score is 25 and the lowest possible score is -125 (assuming that all false positive candidates were very high impact files).

7. CONCLUSIONS

Technical approaches to virtual malware defense

The three vendors have different approaches to protecting virtualized desktops. According to our research[1] this is due to a combination of reasons, including individual development cycles; professional relationships between vendors of security software and developers of virtualization products; the protection features currently available to security vendors as provided by the virtualization businesses; and finally because different security vendors have different ideas on how they believe virtual systems (desktop or otherwise) should be protected.

The challenges that companies rolling out a virtual desktop infrastructure face, in terms of anti-virus protection, include balancing the protection of individual virtual systems against the system performance impact that comes with running multiple on-access and on-demand virus scanners on one piece of hardware.

Our test ran virtual desktop systems using VMware's ESXi hypervisor product. SEP is a regular endpoint client, as is Trend Micro's OfficeScan 10.5, albeit one with a plug-in that aims to improve performance by scheduling scans and updates to run serially. SEP has a randomization feature that is intended to accomplish similar performance benefits. McAfee MOVE offloads file-based anti-virus scanning from the virtual desktop. It requires other software to protect against web-based threats, threats running in memory and to perform on-demand scanning.

These products and their configurations were selected by the vendors themselves. Their brief was to recommend a solution for protecting virtual desktops that would be permitted full access to the web. McAfee added HIPS and SiteAdvisor Enterprise to its MOVE AntiVirus product, while Trend Micro elected to use OfficeScan instead of its Deep Security product. Symantec requested that we tested the MOVE and Deep Security products on their own, but McAfee and Trend Micro convinced us that these products were not the appropriate ones for the roles in which our test desktops would be used.

Where are the threats?

The threats used in this test were genuine, real-life threats that were infecting victims globally at the same time as we tested the products. In almost every case the threat was launched from a legitimate website that had been compromised by an attacker. This means that the old advice of, "keep away from the dark parts of the internet" is out of date. Similarly, blocking only 'bad' types of site using keyword-based filtering services or gateways will not prevent access to compromised sites that are innocent but infected.

The vast majority of the threats installed automatically when a user visited the infected webpage. This infection was usually invisible to a casual observer. In some cases the malware made itself known once installed, appearing as a fake security application or similar rogue utility. These rogue applications pretend to detect viruses on the system and harass the user into paying for a full license, which the program claims will allow it to remove the 'infections'. In reality the only infection is the fake anti-virus program itself.

All of the products were able to block at least some of the web threats before they were installed. This behavior was as a result of a combination of technologies: web reputation databases, intrusion prevention systems and on-access scanners. In none of the compromised incidents did a product detect and remove a success malicious installation at the manual scan phase.

[1] See Dennis Technology Labs' 2011 virtual desktop infrastructure anti-malware report.

APPENDIX A: TERMS

Compromised	Malware continues to run on an infected system, even after an on-demand scan.
Defended	Malware was prevented from running on, or making changes to, the target.
False Positive	A legitimate application was incorrectly classified as being malicious.
Introduction	Test stage where a target system is exposed to a threat.
Neutralized	Malware was able to run on the target, but was then removed by the security product.
Observation	Test stage during which malware may affect the target.
On-demand (protection)	Manual 'virus' scan, run by the user at an arbitrary time.
Prompt	Questions asked by software, including malware, security products and the operating system. With security products, prompts usually appear in the form of pop-up windows. Some prompts don't ask questions but provide alerts. When these appear and disappear without a user's interaction, they are called 'toasters'.
Real-time (protection)	The 'always-on' protection offered by many security products.
Remediation	Test stage that measures a product's abilities to remove any installed threat.
Round	Test series of multiple products, exposing each target to the same threat.
Snapshot	Record of a target's file system and Registry contents.
Target	Test system exposed to threats in order to monitor the behavior of security products.
Threat	A program or other measure designed to subvert a system.
Update	Code provided by a vendor to keep its software up to date. This includes virus definitions, engine updates and operating system patches.

APPENDIX B: LEGITIMATE SAMPLES

Incident	Product	Program type	Obtained via
1	GetRight	GetRight extends your file-downloading power by resuming broken downloads and accelerating them to make them faster and more flexible.	http://download.cnet.com/GetRight/3000-2071_4-10005533.html
2	FreeRAM XP Pro	Increase your system performance by cleaning the content of your RAM.	http://download.cnet.com/FreeRAM-XP-Pro/3000-2086_4-10070530.html
3	Revo Uninstaller	Uninstall unwanted and even broken applications accurately.	http://download.cnet.com/Revo-Uninstaller/3000-2096_4-10687648.html
4	Tweak UI	Enhance Windows with this free set of tools.	http://download.cnet.com/Tweak-UI/3000-2072_4-10002117.html
5	DriverMax	Extract and back up your Windows drivers and reinstall them easily after a new Windows setup.	http://download.cnet.com/DriverMax/3000-18513_4-10572602.html
6	Daemon Tools Pro	For loading virtual disk drives, Daemon Tools is the best-known app around.	http://download.cnet.com/Daemon-Tools-Pro/3000-2646_4-10744439.html?tag=main;productListing
7	Xnews	Try this NewsXpress-like newsreader.	http://download.cnet.com/Xnews/3000-2164_4-10026377.html
8	Ashampoo PowerUp 3	Learn how to configure and maintain Windows.	http://download.cnet.com/Ashampoo-PowerUp-3/3000-18512_4-10028404.html
9	PerfectDisk	Defragment disks, free up space, and optimize system performance.	http://download.cnet.com/PerfectDisk/3000-2094_4-10349543.html
10	Maxthon	Surf the Internet using a browser with various features.	http://download.cnet.com/Maxthon/3000-2356_4-10681895.html
11	Xplorer2 Lite	Manage, view, and search files in a tabbed, dual-pane mode.	http://download.cnet.com/Xplorer2-Lite/3000-2248_4-10407731.html
12	SyncBack Freeware	Back up, restore, or sync files to drives, servers, or removable media.	http://download.cnet.com/SyncBack-Freeware/3000-2242_4-10413802.html
13	BitZipper	View and open RAR, ZIP, 7Z, ISO and 43 other file types in batch mode.	http://download.cnet.com/BitZipper/3000-2250_4-10048965.html
14	Salaat Time	Calculate Muslim prayer time and Qiblah direction anywhere in the world.	http://download.cnet.com/Salaat-Time/3000-2135_4-10415729.html
15	SETI@home	Analyze data captured by a radio telescope and help find extraterrestrial life.	http://download.cnet.com/SETI-home/3000-2257_4-10029649.html
16	FontCreator	Create and modify TrueType font files.	http://download.cnet.com/FontCreator/3000-2316_4-10026325.html
17	Super Ad Blocker	Block all forms of advertising, including pop-ups, Flash ads, and banner ads.	http://download.cnet.com/Super-Ad-Blocker/3000-7786_4-10295147.html
18	Recover Files	Recover permanently deleted files from hard disks and removable media.	http://download.cnet.com/Recover-Files/3000-2094_4-10715455.html
19	WinDirStat	Scan your hard drive or local devices to get detailed statistics on disk usage.	http://download.cnet.com/WinDirStat/3000-2248_4-10614593.html

20	RadioSure	Listen to over 12000 online radio stations and record your favorite songs.	http://download.cnet.com/RadioSure/3000-2168_4-10911517.html
21	Fbackup	Make full and mirror backups.	http://download.cnet.com/FBackup/3000-2242_4-10907579.html
22	3D Realistic Fireplace Screen Saver	Feel the irresistible charm of a real wood fire on your Windows Desktop	http://download.cnet.com/3D-Realistic-Fireplace-Screen-Saver/3000-2257_4-10210081.html
23	Offline Explorer	Acquire Web and FTP sites for offline browsing.	http://download.cnet.com/Offline-Explorer/3000-2377_4-10024310.html
24	Anti Tracks	Erase your tracks, hide IP, lock files, and clean up your hard drive from junk and duplicate files.	http://download.cnet.com/Anti-Tracks/3000-2144_4-10277553.html
25	Secunia Personal Software Inspector	Scan your installed programs and categorize them by their security update status.	http://download.cnet.com/Secunia-Personal-Software-Inspector/3000-2162_4-10717855.html

APPENDIX C: THREAT REPORT

Code	Product	Code	Product	Code	Product
MOVE	McAfee MOVE AntiVirus with Host Intrusion Prevention for Desktop and SiteAdvisor Enterprise	SEP	Symantec Endpoint Protection 12, Amber pre-release	OS	Trend Micro OfficeScan 10.5 with Intrusion Defense Firewall and VDI plug-in

NOTE: The following table is a summary. The full report was provided to Symantec as an Excel spreadsheet, which includes the Notes referred to in some Threat Report entries.

In cases where the malware fails for any reason, the product is given the full benefit of the doubt and is classified as having Defended with full remediation.

		Introduction			Manual scan			Remediation			
Incident	Product	Alert	Effect	Threat Report	Alert	Effect	Threat Report	Complete?	Defended	Neutralized	Compromised
1	MOVE	Pop-up	Deleted	Generic FakeAlert	N/A	N/A	N/A	1	1		
1	OS	Pop-up	Cleaned	TROJ_PIDIEF.SMZB x2, FAKEAV.SM10 x2	None	None	None	1	1		
1	SEP	Toaster	Deleted	JAVA Script	None	None	None	1	1		
2	MOVE	None	None	None	N/A	N/A	N/A				1
2	OS	Pop-up	Blocked	djy.exe	None	None	None			1	
2	SEP	Toaster	Blocked	Fake AV	None	None	None	1	1		
3	MOVE	Pop-up	Access denied	Generic Dropper.va.gen.t	N/A	N/A	N/A				1
3	OS	Pop-up	Blocked	LowRiskFile Types in Win Registry	None	None	None				1
3	SEP	Toaster	blocked access to the IP	web attack	None	None	None	1	1		
4	MOVE	Pop-up	Deleted	Generic FakeAlert.ama	N/A	N/A	N/A	1	1		
4	OS	Browser	Blocked	JAVA_DLOADER.VI x8	None	None	None	1	1		
4	SEP	Toaster	Blocked	web attack exploit tool kit	None	None	None	1	1		
5	MOVE	None	None	None	N/A	N/A	N/A	1	1		
5	OS	Pop-up	Blocked	LowRiskFile Types in Win Registry	None	None	None				1
5	SEP	Toaster	blocked access to the IP	web attack	None	None	None	1	1		
6	MOVE	None	None	None	N/A	N/A	N/A				1

		Introduction			Manual scan			Remediation			
Incident	Product	Alert	Effect	Threat Report	Alert	Effect	Threat Report	Complete?	Defended	Neutralized	Compromised
6	OS	Pop-up	Blocked	sbp.exe	None	None	None	1	1		
6	SEP	Toaster	Blocked	web attack exploit tool kit	None	None	None	1	1		
7	MOVE	Pop-up	Deleted	FakeAlert-SecurityTool.bit	N/A	N/A	N/A	1	1		
7	OS	Browser	Blocked	JAVA_DLOADER.VI x8	None	None	None	1	1		
7	SEP	Toaster	Blocked	web attack	None	None	None	1	1		
8	MOVE	Pop-up	Deleted	FakeAlert-SecurityTool.ca; exe.exe	N/A	N/A	N/A	1	1		
8	OS	None	None	None	None	None	None	1	1		
8	SEP	Toaster	Blocked	Web attack	None	None	None	1	1		
9	MOVE	Browser	Blocked	videoskk.org	N/A	N/A	N/A	1	1		
9	OS	None	None	None	None	None	None	1	1		
9	SEP	None	None	None	None	None	None	1	1		
10	MOVE	Pop-up	Access denied	Generic Dropper.va.gen.t	N/A	N/A	N/A				1
10	OS	Pop-up	Cleaned	TROJ_PIDIEF.SMZB x2; TROJ_FAKEAL.LPS	None	None	None	1	1		
10	SEP	Toaster	Blocked	web attack	None	None	None	1	1		
11	MOVE	None	None	None	N/A	N/A	N/A	1	1		
11	OS	None	None	None	None	None	None	1	1		
11	SEP	Toaster	Blocked	Web Attack Blackhole Toolkit Website	None	None	None	1	1		
12	MOVE	None	None	None	N/A	N/A	N/A				1
12	OS	Pop-up	Blocked	tyr.exe	None	None	None	1	1		
12	SEP	Toaster	Blocked	Fake AV	None	None	None	1	1		
13	MOVE	None	None	None	N/A	N/A	N/A				1
13	OS	Pop-up	Blocked	htv.exe	None	None	None	1	1		
13	SEP	Toaster	Blocked	Fake AV	None	None	None	1	1		
14	MOVE	None	None	None	N/A	N/A	N/A				1
14	OS	Pop-up	Blocked	LowRiskFile Types in Win Registry	None	None	None				1
14	SEP	Toaster	Blocked	Web Attack Blackhole Toolkit Website	None	None	None	1	1		
15	MOVE	Pop-up	Access denied	W32/pinkslipbot.gen.ae	N/A	N/A	N/A	1	1		
15	OS	Pop-up	Quarantined	Mal_Qakcgf1	None	None	None	1	1		
15	SEP	Toaster	Blocked	HTTP Blackhole Activity x5	None	None	None	1	1		
16	MOVE	None	None	None	N/A	N/A	N/A	1	1		
16	OS	Pop-up	Cleaned	BKDR_ZLOB.SMGS	None	None	None	1	1		
16	SEP	Pop-up	Access denied	install.48728[1].exe	None	None	None	1	1		
17	MOVE	Pop-up	Access denied	FakeAlert-SpyPro.gen.a	N/A	N/A	N/A	1	1		
17	OS	Pop-up	Terminated	dvf.exe	None	None	None	1	1		

		Introduction			Manual scan			Remediation			
Incident	Product	Alert	Effect	Threat Report	Alert	Effect	Threat Report	Complete?	Defended	Neutralized	Compromised
17	SEP	Toaster	Blocked	Fake AV	None	None	None	1	1		
18	MOVE	Pop-up	Access denied	w32/Bamital.p	N/A	N/A	N/A	1	1		
18	OS	Pop-up	Quarantined	JAVA_DLOADER.VI x8	None	None	None	1	1		
18	SEP	Toaster	Blocked	Malicious JAVA activity	None	None	None	1	1		
19	MOVE	Pop-up	Access denied	FakeAlert-SecurityTool.bt!dam	N/A	N/A	N/A	1	1		
19	OS	None	None	None	None	None	None	1	1		
19	SEP	Toaster	Blocked	ExploitKit Variant Activity 3	None	None	None	1	1		
20	MOVE	Pop-up	Blocked	FakeAlert-SecurityTool.bt	N/A	N/A	N/A	1	1		
20	OS	Pop-up	Quarantined	JAVA_DLOADER.VI x8	None	None	None	1	1		
20	SEP	Toaster	Blocked	ExploitKit Variant Activity 3	None	None	None	1	1		
21	MOVE	None	None	None	N/A	N/A	N/A				1
21	OS	Pop-up	Cleaned	TROJ_PIDIEF.SMZB	None	None	None	1	1		
21	SEP	Toaster	Blocked	Malicious File Download	None	None	None	1	1		
22	MOVE	Pop-up	Access denied	Generic FakeAlert.ama	N/A	N/A	N/A	1	1		
22	OS	Pop-up	Blocked	JAVA_DLOADER.VI x8	None	None	None	1	1		
22	SEP	Toaster	Blocked	ExploitKit Variant Activity 3	None	None	None	1	1		
23	MOVE	None	None	None	N/A	N/A	N/A				1
23	OS	Pop-up	Terminated	pmx.exe	None	None	None	1	1		
23	SEP	Toaster	Blocked	Web Attack Blackhole Toolkit Website	None	None	None	1	1		
24	MOVE	Pop-up	Access denied	W32/pinkslipbot.gen.ae	N/A	N/A	N/A	1	1		
24	OS	Pop-up	Terminated	ZwCreateThread	None	None	None	1	1		
24	SEP	Toaster	Blocked	ExploitKit Variant Activity 2	None	None	None	1	1		
25	MOVE	None	None	None	N/A	N/A	N/A				1
25	OS	Pop-up	Quarantined	JAVA_DLOADER.VI x8	None	None	None	1	1		
25	SEP	Toaster	Blocked	ExploitKit Variant Activity 3	None	None	None	1	1		

APPENDIX D: TOOLS

Ebtables
http://ebtables.sourceforge.net
The ebtables program is a filtering tool for a bridging firewall. It can be used to force network traffic transparently through the Squid proxy.

Fiddler2
www.fiddlertool.com
A web traffic (HTTP/S) debugger used to capture sessions when visiting an infected site using a verification target system (VTS).

HTTPREPLAY
http://www.microsoft.com
A SOCKTRC plug-in enabling the analysis and replaying of HTTP traffic.

Process Explorer
http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx
Process Explorer shows information about which handles and DLLs processes have opened or loaded. It also provides a clear and real-time indication when new processes start and old ones stop.

Process Monitor
http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx
Process Monitor is a monitoring tool that shows real-time file system, Registry and process/thread activity.

Regshot
http://sourceforge.net/projects/regshot
Regshot is an open-source Registry comparison utility that takes a snapshot of the Registry and compares it with a second one.

Squid
www.squid-cache.org
Squid is a caching web proxy that supports HTTP, HTTPS, FTP and other protocols.

Tcpdump
www.tcpdump.org
Tcpdump is a packet capture utility that can create a copy of network traffic, including binaries.

TcpView
http://technet.microsoft.com/en-us/sysinternals/bb897437.aspx
TcpView displays network connections to and from the system in real-time.

Windows Command-Line Tools
Those used included 'systeminfo' and 'sc query'. The systeminfo command "enables an administrator to query for basic system configuration information". The sc command is "used for communicating with the NT Service Controller and services.

Wireshark
www.wireshark.org
Wireshark is a network protocol analyzer capable of storing network traffic, including binaries, for later analysis.

APPENDIX E: PRODUCT VERSIONS

Vendor	Main version (Build or engine)
McAfee	ePO 4.5 (5400.1158)
	MOVE AV Agent 1.6.0.1110
	Host Intrusion Prevention 8.00 (8.0.0.1741)
	Agent 4.5.0.1810
	SiteAdvisor Enterprise 3.0.0.561
Symantec	Endpoint Protection 12.1.399.4350
Trend Micro	OfficeScan Client 10.5.10.83 (9.205.1002)
	OfficeScan Server 10.5 (1083)
	OfficeScan Integrated Protection Server 2 (1325)

Products were updated at the start of the test (18/04/2011) and throughout, before each exposure. The final test was run on 27/04/2011.

Product configurations by vendor:

McAfee client

- Management for Optimized Virtual Environments (MOVE) AntiVirus
- Host Intrusion Prevention for Desktop
- SiteAdvisor Enterprise (MOVE)

Note: McAfee decided not to specify the on-demand product known as 'McAfee VirusScan Enterprise for Offline Virtual Images (OVI)' because, although that would be a relevant inclusion in the real-world, it would make no difference to any protection provided in this test.

Blocking is set to high-risk only. SiteAdvisor is set to block red sites.

Symantec client

- Symantec Endpoint Protection 12, Amber pre-release (SEP)

In this phase of testing the SEP product was installed as a stand-alone client and was run using default settings.

Trend Micro client

- OfficeScan 10.5
- Virtual Desktop Support
- Intrusion Defense Firewall

Web reputation is turned on. The default is off.