PASSMARK® SOFTWARE

Fast and Effective Endpoint Security for Business 2012

Comparative Analysis

August 2012

Document: Fast and Effective Endpoint Security for Business – Comparative Analysis
Authors: M. Baquiran, D. Wren
Company: PassMark Software
Date: 6 August 2012
Edition: 1
File: Fast and Effective Endpoint Security for Business 2012 - Ed1.docx

Table of Contents

Revision History

Rev	Revision History	Date
Edition 1	First edition of the document. Performance charts and comparative reviews added.	6 August 2012

References

Ref #	Document	Author	Date
1	AV Comparatives - Summary Report 2011 Current Edition: December 2011 The information in the most recent version of this report by AV Comparatives was used to determine the effectiveness of reviewed business security solutions.	AV Comparatives	22 Dec 2011
2	AV Comparatives - On-Demand Comparatives Current Edition: March 2012, Last Revision: 10 April 2012 The information from the most recent version of this report by AV Comparatives was used to determine the effectiveness of reviewed business security solutions.	AV Comparatives	10 April 2012
3	AV Comparatives – Retrospective/ProActive Test Current Edition: Aug 2011, Last Revision: 15 November 2011 Information from Retrospective/ProActive Test reports by AV Comparatives was used in determining the effectiveness of reviewed business security solutions.	AV Comparatives	15 Nov 2011
4	VB100 Test Results Overall test results obtained by VB100 were used in determining the effectiveness of reviewed business security solutions.	Virus Bulletin	18 Jul 2012
5	Network Traffic Monitor v2.01 A tool used to monitor the amount of inbound and outbound network traffic for the Update Size metric.	Nico Cuppen Software	-

Introduction

Endpoint protection is no longer an optional security measure for businesses. In this technology driven age, every business is now susceptible to the damages caused by malware (ranging from productivity loss to confidential and financial data theft), and endpoints have become the most vulnerable and targeted point of attack.

While there have been improvements in network security in recent years through better adoption and understanding of firewalls and intrusion prevention, endpoints have become particularly prone to security breaches. This is largely due to the fact that they have become more exposed -- not only are people working increasingly from laptops outside of the office, but the prevalence of web-based applications (in the form of Web 2.0) have brought about a greater level of interaction with external websites than ever before. As such, the endpoint has become the weakest link in an enterprises' overall security strategy, and a successful attack at the endpoint may not only reveal the data stored there but also provide the key to gain unauthorized access to the rest of the network.

There are a large number of solutions available from vendors, and the challenge for businesses is to now determine which security solution is the most effective at mitigating the threat of malware, while minimizing implementation cost and impact to existing business functions and workflow.

This report presents a comparative analysis on the performance, effectiveness and usability of seven security solutions from some of the world's most respected security vendors. In this report, PassMark Software evaluated the following business security products:

- ESET Endpoint Security
- Kaspersky Endpoint Security
- McAfee Total Protection for Endpoint
- Microsoft System Center 2012 Endpoint Protection
- Symantec Endpoint Protection 12.1
- Sophos Endpoint Protection 10.0
- Trend Micro OfficeScan 10.6

Ratings and Summary

Passmark Software has given each security product a rating which reflects its overall performance, ease of use, design, features and level of excellence in that category. Categories represent major functions or feature sets common to the sphere of business security. These ratings represent PassMark Software's subjective views and experiences in installing, configuring and use of business security products to manage endpoints.

The following table summarizes ratings in all categories for all products evaluated:

	ESET	Kaspersky	McAfee	Microsoft	Sophos	Symantec	Trend Micro
Overall Rating	4.5	4	4.5	2	4.5	4	4.5
Installation & Configuration	4.5	4	3	1	3	4	4.5
Migration	4	4	4.5	1	4	4.5	4
Policy Defaults & Policy Management	4.5	4.5	3.5	3	4	4.5	2
Client Installation	4	4	3	1	4.5	4.5	4
Interface Design	4	4.5	3	4	4	4	3
Client & Remote Management	4.5	4	4	2	3	4	4.5
Updates	4	4	2	1	4	4.5	4
Effectiveness	4.5	4.5	4.5	4	4.5	4	4.5
Performance	5	3	4	3.5	2	3	4

Rating Categories

The table below describes the criteria and factors which were considered for each business security solution in each category to determine a rating. Evaluation categories were determined prior to testing and were chosen as a set of expected features or functions which define business security products.

Category	Category Description
Overall Rating	The rating for this category is calculated as an average of all other ratings, with all categories carrying equal weight.
Installation & Configuration	This category evaluates the speed and relative ease of the installation and configuration process of server components, including the quality and accuracy of documentation, the ability to install pre-requisites and the level of installer integration.
Migration	This category rates the relative ease and simplicity of product migration from previous vendor solutions or third-party software solutions. Extra consideration is given to vendors who have documented the migration process well.
Default Policies & Policy Management	This category considers whether the policies created by default during product installation 'make sense' from a management perspective, taking into account whether different default choices are available. It also covers ease of use, flexibility and granularity of policy management.
Client Installation	This category evaluates the simplicity and ease of client installation, taking into account the speed of deployment and the level of impact of installation on endpoint users.
Interface Design	This category rates the design of the server console's user interface for responsiveness, intuitiveness, consistency and functionality.
Client Management & Remote Management	This category assesses the flexibility and functionality of client management from the server console, taking into account the level of automation in executing tasks, report viewing, organization and creation of groups, the depth of configuration options available to administrators, and the level of support provided for administrators to access the management console from a remote terminal.
Updates	This category rates the level of configuration required to enable the management server to update a central repository, as well as the ease of deployment to and the timeliness of retrieval by endpoint machines.
Effectiveness	This category rates the anti-malware effectiveness of a security product based on information from recently published material at reputable, third-party testing sites. The sources we have used for this category are VB100 and AV Comparatives.
Performance	This category assigns an overall rating based on a security product's performance over seventeen performance benchmark tests conducted by PassMark Software.

Star Rating Description

The table below explains the general significance of ratings relative to product performance, usability and functionality.

Star Rating	Rating Description
--	**Unsupported** – This category was not supported by the business security solution. Support was not documented in product guides, the online knowledgebase or help files.
★	**Very Poor** – The security solution offered very limited performance in this category. Products with this rating had sparse or inaccurate documentation, extremely poor usability, or technical issues which severely hampered product stability, usability and functionality.
★★	**Poor** – The security solution had inadequate or basic performance in this category, as a result of poor usability or functionality. Some products with this rating had bugs which hampered product performance in this category.
★★★	**Average** – The security solution had adequate performance in this category with some room for improvement.
★★★★	**Good** – The security solution provides good performance in this category area with useful features and good documentation.
★★★★★	**Exceptional** – The security solution provides outstanding performance in a category area, with unique, thoughtful or well-designed features that streamline usability or functionality and excellent documentation.

Task Description

PassMark Software has conducted performance benchmark testing and subjective comparative analysis on the overall ease of use, speed and effectiveness on seven (7) business security software products.

Hardware Environments

The following hardware platforms were used in conducting our comparative analysis and performance tests, and are intended to represent a typical server and business deployment:

Server Machine Specification

The following machine ran a virtual machine in which the server components of the security software were installed:

Operating System:	Windows 7 x64
CPU:	AMD Phenom II x4 940 (Quad Core)
Motherboard:	Gigabyte GA-MA790XT-UD4P
RAM:	4 x 4GB PC3-10600 1333MHz DDR3 Memory (16GB in total)
HDD:	Western Digital Caviar Green WD10EADS 1TB Serial ATA-II

Virtual Machine Specification

Operating System:	Windows Server 2008 R2 64-bit (for Daily Network Traffic test) Windows Server 2003 R2 SP2 32-bit (for all other performance tests)
RAM:	1-2 GB (depending on the product's requirements)

Client Machine Specification

Operating System:	Windows 7 Ultimate x64
CPU:	Intel Core i7 920 @ 2.67GHz
Video Card:	nVidia GeForce 8800 GT
RAM:	6 GB
HDD:	500 GB

Products and Versions Tested

Product Name	Server Component and Version	Client Component and Version
ESET Endpoint Security	Remote Administrator: v5.0.119.0 ERA Maintenance Tool: v5.0.119.0	ESET Endpoint Security: v5.0.2122.1
Kaspersky Endpoint Security	Kaspersky Security Center: v9.2.69	Kaspersky Endpoint Security: v8.1.0.646
McAfee Total Protection for Endpoint	ePolicy Orchestrator: v4.6.0	VirusScan Enterprise + AntiSpyware Enterprise: v8.8 SIteAdvisor Enterprise Plus: v3.0.0 Host Intrusion Prevention: v8.0.0
Microsoft System Center 2012 Endpoint Protection	Microsoft System Center 2012: 2.2.903.0	Antimalware Client 3.0.8410.0
Symantec Endpoint Protection	Endpoint Protection Manager: v12.1.1000.157 RU1	Symantec Endpoint Protection: v12.1.1000.157 RU1
Sophos Endpoint Protection Advanced Edition *Note: All performance metrics except for **Daily Network Traffic** were tested on the Enterprise Edition. Since this version is no longer supported by Sophos, the remainder of the review was conducted on the Advanced Edition.*	Sophos Enterprise Console: v5.1.0.1839	Sophos Endpoint Security and Control: v10.0
Trend Micro OfficeScan 10.6	Trend Micro OfficeScan Server: v10.6 Build 1062	Trend Micro OfficeScan client: v10.6.1062

Performance Benchmark Results

The following performance categories have been selected as 'real-life' metrics which may impact heavily on endpoint system performance and responsiveness. These benchmarks allow the comparison of the level of impact that business security software products may have on endpoint machines. Products with good performance will have less impact on business activities, workflow and productivity.

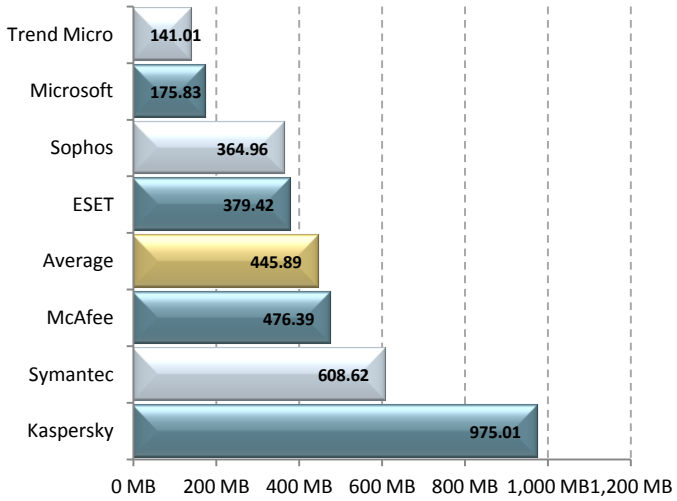
A more detailed description of the methodology used can be found in **Appendix A – Performance Methodology**.

Client Install Size

Protect endpoints without filling up disk space

Newer versions of products often have increased disk space requirements, ensuring disk space remains critical for endpoint systems. Endpoint clients with a larger installation footprint may be consuming more disk space than necessary.

This metric measures the total additional disk space consumed by the endpoint client after installation and a manual update. Our final result is measured in megabytes (MB).

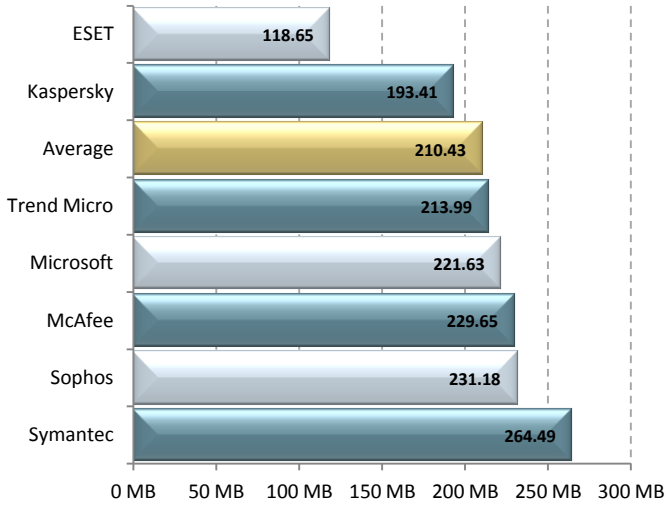


Client Memory usage During System Idle

Have more system resources to perform tasks

Extensive memory (or physical RAM) usage by security products have significant impact on endpoint system performance and cause more reliance on hard disk drives, which have slower read and write speeds than RAM. Business security products which use more memory will visibly slow performance on affected endpoints.

This metric measures the total additional memory usage by the endpoint machine during a period of system idle where an endpoint security product has been installed. Our final result is measured in megabytes (MB), and calculated from an average of forty (40) samples.

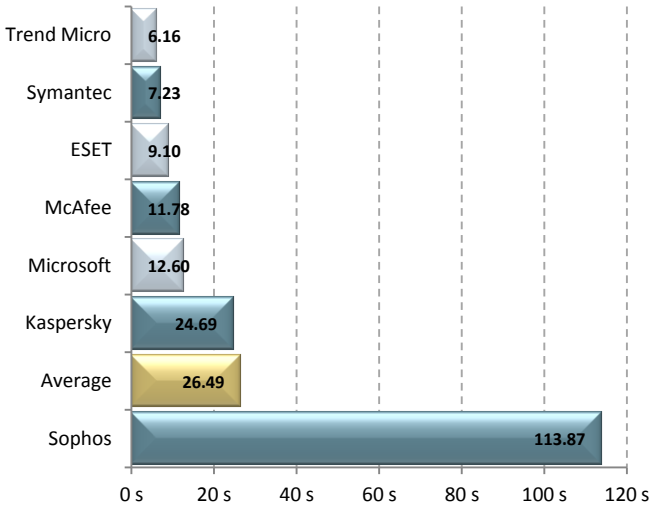


On Access Scan Time

Perform everyday tasks faster

On Access scanners are constantly monitoring a system for suspicious behavior. They are activated any time a program interacts with resources in memory or over the network. The performance of frequently carried out tasks can be impacted significantly by the overhead required to scan these tasks.

This metric measures the total additional time taken to browse a set of websites and open and close a set of MS Office documents, where an endpoint security product has been installed. Our final result is measured in seconds (s), and calculated from an average of five (5) samples.

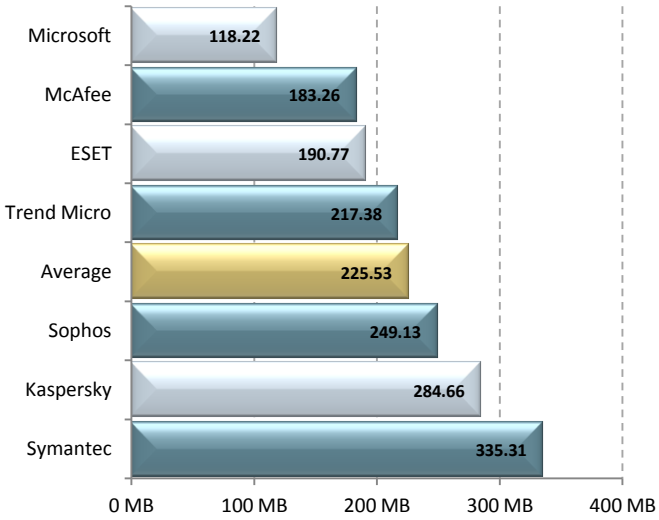


Memory Usage During On Access Scan

Have more system resources when performing everyday tasks

As above, On Access scanners can affect a systems performance during everyday tasks. Products with On Access scanners that use more memory may affect a systems ability to multitask and slow down memory intensive operations.

This metric measures the additional memory usage during the running of a script that automatically browses the internet, and open and close a set of MS Office documents, where an endpoint security product has been installed.

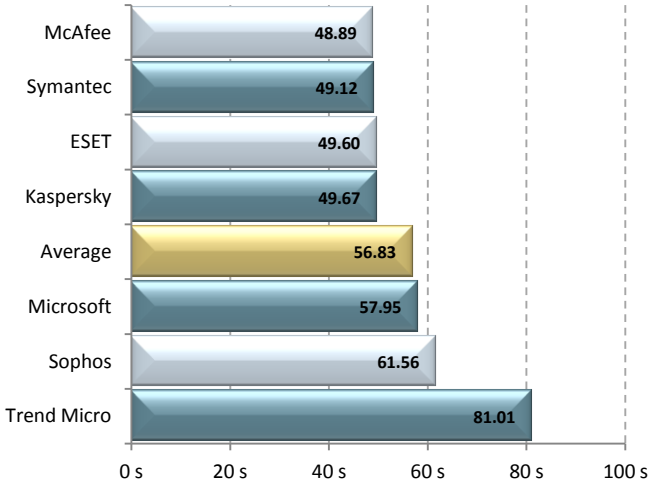


File copy time for small files

Copy your documents more quickly

Transferring files between devices and drives is a common activity undertaken by endpoint users. File copy times may be negatively affected by poor performance of business security products functionality, such as file scanning or heuristics.

This metric measures the total time taken to copy a set of small files between directories, where an endpoint security product has been installed. Our final result is measured in seconds (s), and calculated from an average of five (5) samples.

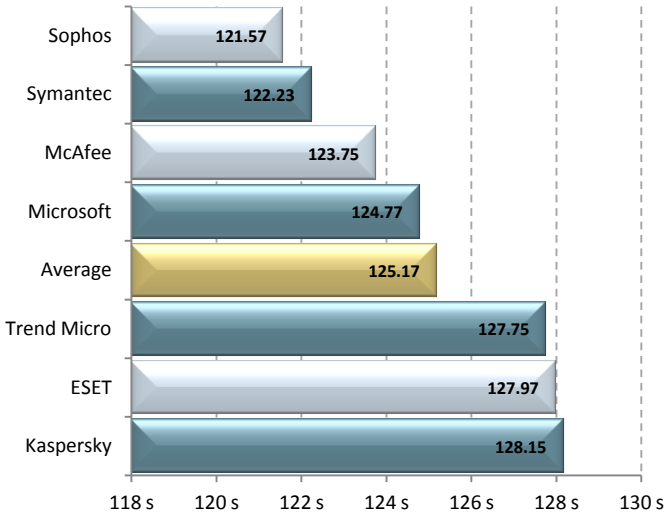


File copy time for large files

Copy your media files more quickly

Copying large files between directories may similarly be affected by poor performance of anti-malware functionality in business security products.

This metric measures the total time taken to copy a set of large files between directories, where an endpoint security product has been installed. Our final result is measured in seconds (s), and calculated from an average of five (5) samples. Our final result is measured in megabytes (MB), and calculated from an average of forty (40) samples taken over a period of 2 minutes.

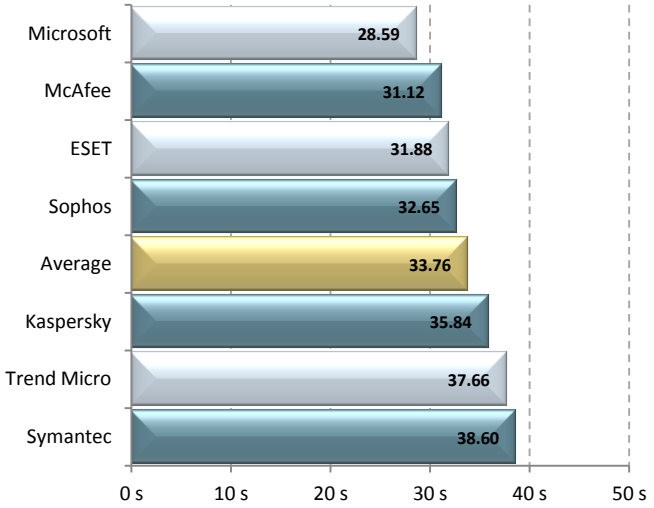


Boot Time

Spend less time waiting for your computer to start

Many business software suites create start up tasks and processes, causing machine boot times to take significantly longer. End users can do little but wait for their machine to become responsive. Better performing products will have less of an impact on boot time.

This metric measures the time taken to boot the machine where an endpoint security product has been installed. Our final result is measured in seconds (s) and calculated from an average of five (5) samples.

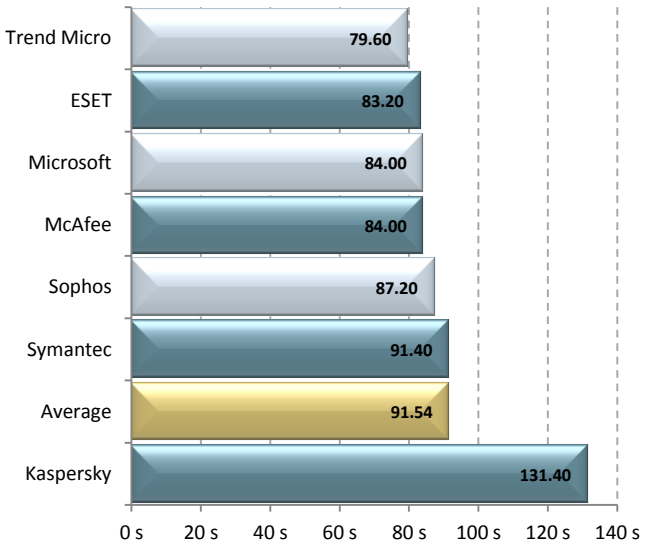


Machine restart time

Reduce the time needed to restart your computer

Extra system resources consumed by processes and services created by security software may delay shut down time and the restart cycle of endpoint machines.

This metric measures the time taken to restart the machine where an endpoint security product has been installed. Our final result is measured in seconds (s) and calculated from an average of five (5) samples.

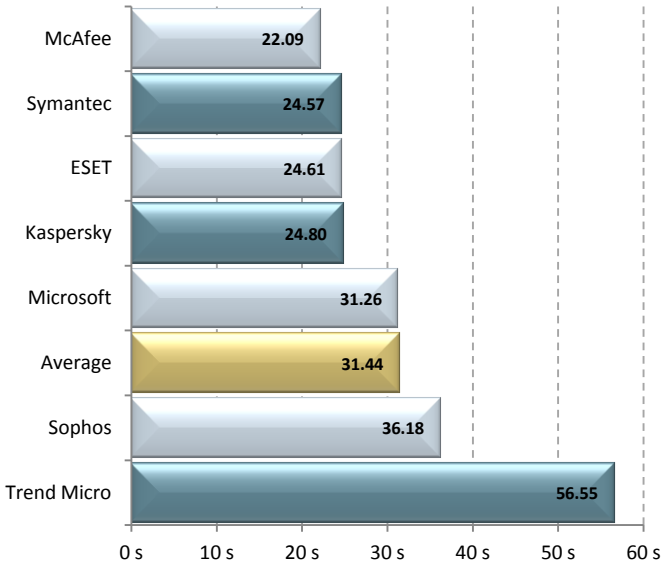


File Copy, Move, & Delete

Copy, move, and delete files more quickly

Security products need to monitor system activity every time a file is moved, copied, or deleted. The time required to carry out these tasks can be greatly increased by poorly performing security products.

This metric measures the total time taken to copy, move and delete a set of files of various formats between directories, where an endpoint security product has been installed. Our final result is measured in seconds (s) and calculated from an average of five (5) samples.

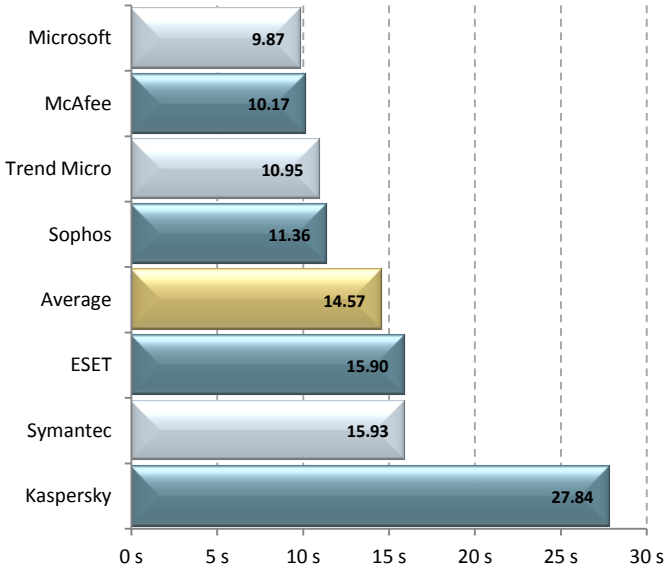


Network Throughput

Quickly download and transfer files across the network

Files are often transferred, accessed, and downloaded across networks, but not without inspection from installed security software. Download speeds can be significantly decreased by poorly performing security products.

This metric measures the total time taken to download a sample set of binary files from another location in the network. Our final result is measuredin seconds (s) and calculated as an average of five (5) samples.

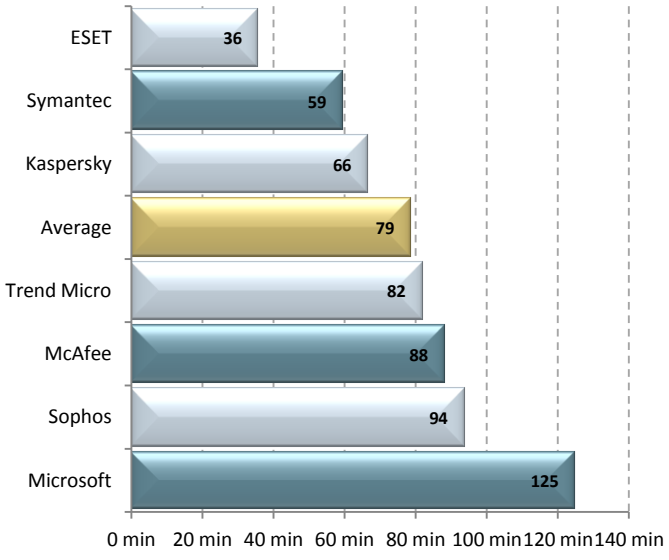


Full System Scan

Quickly determine the health of your system

Running a full system on-demand scan on an endpoint is necessary in order to thoroughly check hard drives and running programs for security threats. Ideally, it is performed on endpoints periodically (e.g. once per week) and is typically a rather lengthy task. Products with poorly performing scanning algorithms can inconveniently and unnecessarily increase the scan time.

This metric measures the total time taken to run a full system scan on an endpoint. The scan is carried out three (3) times. Our final result was taken as an average of both the initial scan time and the average subsequent scan time.

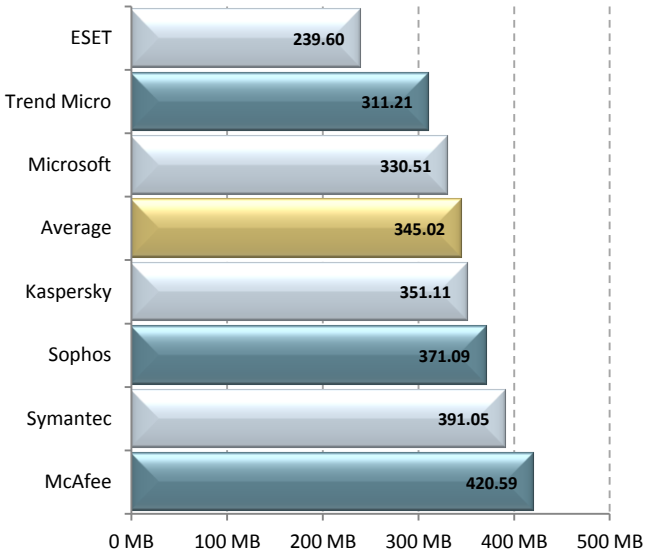


Memory Usage during Full System Scan

Reduce memory usage when carrying out a full system scan

Full system scans can be resource demanding and long in duration, thus memory usage should be minimized so that other tasks and processes may still function without system performance being slowed significantly.

This metric measures the additional memory usage during the running of full system scan on an endpoint. Our final result is measured in megabytes (MB) of data, and is taken as an average of forty (40) samples taken over 40 minutes.

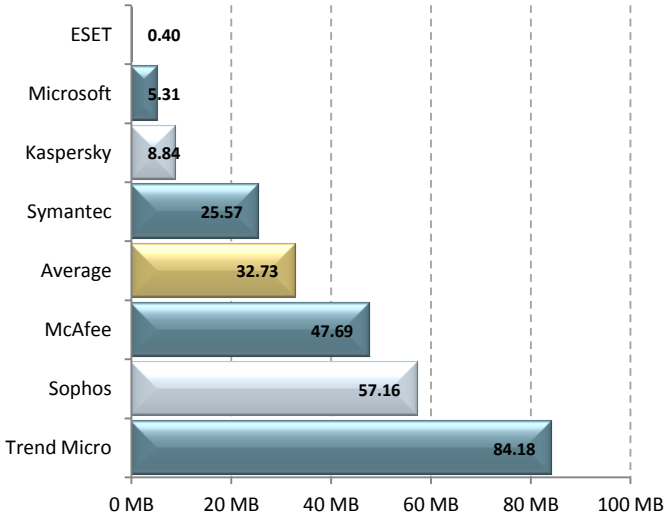


Daily network traffic

Minimize impact on the corporate network

All security solutions require the latest signatures and engine updates in order to provide managed networks the best possible protection against malware. However, not all security software is equal, with some products performing incremental updates and others downloading much more.

This metric measures the total daily inbound and outbound traffic as a result of security software engine and signature updates to the repository on the server machine. Our final result is measured in megabytes (MB) and is calculated as an average of fifteen (15) days of data.

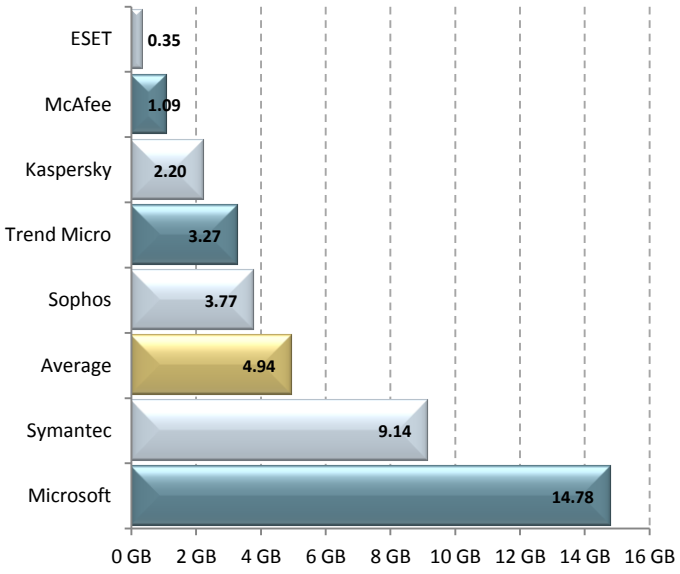


Management Server Installation Size

Reduce server disk usage on your management server

Ensuring the health and performance of the management server machine is essential for properly maintaining and monitoring dependent endpoint systems. Management server software disk space usage should be minimized in order to allow room for database collections and logging, important updates such as virus signature definitions, as well as other programs and files required by the server.

This metric measures the total additional disk space consumed by the management server software (including the management console) after installation and a manual update. Our final result is measured in gigabytes (GB).



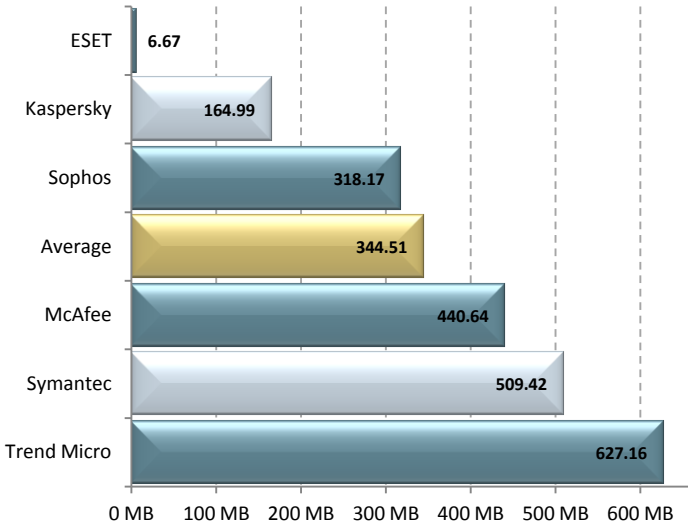
Server Memory Usage during System Idle

Have more system resources for your server to maintain and monitor endpoints

Extensive memory (or physical RAM) usage by management servers during idle can have significant impact on the security of dependent endpoints. Servers need to have enough resources available for receiving and responding to virus alerts, carrying out scheduled tasks, as well as monitoring and maintaining the health of endpoints across the network.

This metric measures the total additional memory usage by the server machine during a period of system idle where an endpoint security server product has been installed. Our final result is measured in megabytes (MB) and calculated from an average of forty (40) samples.

Note: Microsoft System Centre was omitted from this comparison as it did not support the test environment.



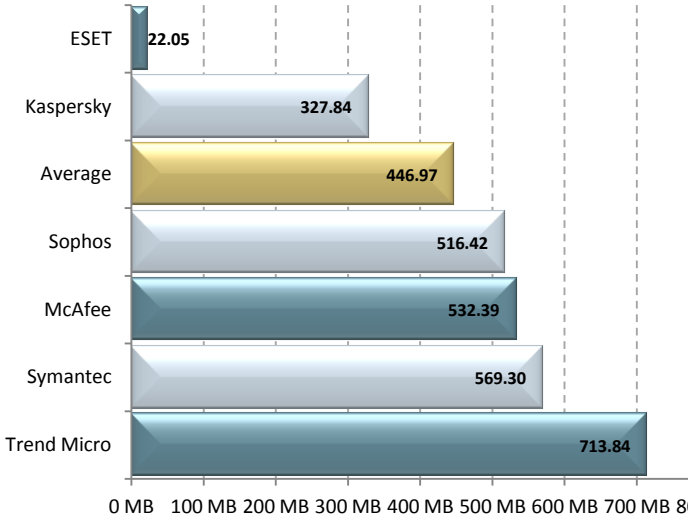
Server Memory Usage During On Deman Scan

Scan on your entire system faster

Running an on-demand scan on endpoints via the server is frequently performed in order to check for security threats in hard drives and programs across the network. Management Servers that require more resources per endpoint will not be capable of handling as many endpoints and may require additional servers to help handle the load.

This metric measures the total additional memory usage by the server when carrying out an on demand scan on an endpoint. Our final result is measured in megabytes (MB) and calculated from an average of forty (40) samples.

Note: Microsoft System Centre was omitted from this comparison as it did not support the test environment.



ESET Endpoint Security

Review Summary

Overall Rating	★★★★½
Installation & Configuration	★★★★½
Migration	★★★★
Default Policies & Policy Management	★★★★½
Client Installation	★★★★
Interface Design	★★★★
Client Management & Remote Management	★★★★½
Updates	★★★★
Effectiveness	★★★★½
Performance	★★★★★

- **Pros**
- Very little system impact on endpoint and server machines (fastest, best overall performance)
- Initial Setup and configuration took only a few minutes
- Low traffic overhead for updates
- Policy , client, and role Management is flexible and granular
- Organized and efficient interface design
- **Cons**
- Update repository is not setup automatically
- Web interface serves as a dashboard only

Installation and Configuration 4.5/5

Installing ESET Remote Administrator Server and Console was an extremely quick and easy process. The setup of ESET Remote Administrator (ERA) installs two separate components, the ERA Server (ERAS) and Console (ERAC). Quite impressively, the setup of both took us only a few minutes in total to complete. The installation wizard requires little input from the user, and all necessary components are automatically installed, including the built-in Microsoft Access database. Password setup, update parameters and other security options can be set post installation, and no additional configuration or restart is required to launch the console.

For testing, we installed ERAC to the same server machine as ERAS, so that the console connected to the server automatically. Otherwise, the console can be conveniently installed to a different machine, for e.g. the administrator's PC, in which case it is required to enter the ERA Server name or IP address during advanced setup of the console.

Support for platforms and pre-requisites is widespread, in which ERAS and ERAC support Windows 2000 and higher on 32-bit, and Windows XP and higher on 64-bit. Other than the built-in database, SQL, MySQL and Oracle are also supported.

Documentation is clear, with relevant and logically ordered headings. Network diagrams are given to help illustrate basic and more elaborate enterprise environments. In addition to a basic installation, advanced installations where multiple servers are required and cluster mode installation are also covered.

Migration from Previous Solutions 4/5

ERA 5.0 supports migration from previous versions (4.x, 3.x), which is performed simply by installing the current version over the previous version. However, migration over versions 1.x and 2.x requires migration to 3.x or 4.x first, and then migration to 5.0 can be performed.

The steps involved in migrating to ERA 5.0 are similar to that of performing a clean install of ERAC and ERAS. Database migration is optional, and a backup is created by default incase a rollback is required. This saves administrators having to run the backup themselves, which we saw was necessary for other products. Clients can be upgraded automatically from some versions, although policies are not automatically migrated. They can however, from Version 4.2 and after, be

manually and exported and imported to create a new policy.

Documentation in the ERA user guide is sufficient and covers basic information, although would benefit from having a dedicated section on migration, as related information was interspersed within the ERA Installation section. ESET provides a "Rip and Replace" service for US & Canada customers which is applicable to ERA v2.0 and higher and a range of competing solutions.

Default Policies & Policy Management 4.5/5

The ERA Policy Manager and Configuration Editor are highly efficient tools for viewing and setting policies. Policy variables are arranged in tree form, making them easy to locate and configure, and can be marked and/or reverted to default settings individually. A product filter allows administrators to switch quickly between policies, and a handy text search allows for quick location of items.

Default policies are created on installation and are set reasonably, with server updates being regular, prompting for computer restarts being turned on, cleaning levels set to medium, and more advanced options turned off. Some values are set to 0 to indicate that default settings will be used, although this default value is not displayed in the Editor.

There is only one default server and client policy, but new policies can be based on and merged from existing policies, and existing policies can be imported and exported.

Client Installation 4/5

Screenshot 1: ESET Endpoint Security (Client)

Client Installation of ESET Endpoint Security (EES) is easy and intuitive via remote push, so that any technically inclined user should have no trouble finding their way around the process without needing to refer to the documentation. Once initiated, the client module took us only a few minutes to install on the endpoint machine, and no machine restart was required for functional protection.

To perform a remote push task, the administrator must first create an installation package by importing the .msi file of the endpoint solution. In the Package Manager, installation packages are organized neatly by platform and package type, product info is displayed, xml configuration files can be imported, and created packages can be saved for later use. ERA also supports creation deployment of custom installation packages from non-ESET applications if it is available as an .msi file.

Running a quick search task displays computers on the network (Windows network, IP Address, and Active Directory searches are supported), and a push installation can be performed simply by right clicking the endpoint and selecting the appropriate task. The push installation wizard links to a list of endpoint requirements in the help file, such as TCP/IP protocol, simple file sharing disabled, and remove registry service enabled, most of which would already be satisfied on a typical enterprise endpoint machine. To bypass these requirements, a direct installation can be performed, which is more suitable for small computer networks. A tip in the ERAC clients tab advises that clients will connect automatically and be visible in the ERA Console simply by configuring Remote Administration window in the client's setup.

For larger computer networks, client deployment can be performed with Active Directory Synchronization, or by creating custom groups. Both of these methods are documented clearly and in detail.

Interface Design 4/5

The ERA Console uses a traditional Windows interface, which looks professional, neat, and feels responsive. What it lacks in fancy and flashy graphics, it makes up for in consistency and being quick and intuitive to navigate. Main areas of the console are quickly accessible from the tabs (Clients, Event Log, Scan Log, Tasks, Reports, etc.) which span the bottom of the UI. There are 10 different log categories, which might have been better organized as a single tab with a category filter perhaps, or have an option to hide certain tabs. Most tabs share a standard layout, with a left side menu with display filtering options and the right side showing status information and log entries. Important data such as errors, warnings, and importance level are viewable at a glance. At

times the interface may feel quite compact, but this also means that less is hidden.

The ERA web dashboard uses an AJAX based interface that is customizable and aesthetically pleasing. Windows can be reorganized, and graphs are tastefully colored with pastel gradients fills.

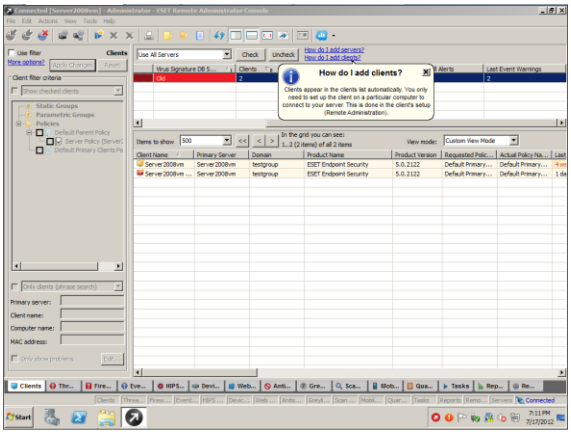
The EES interface is simple but well laid out and organized. Icons are colorful and suitable. 6 main tabs in the left-hand menu include Protection Status, Computer Scan, Update, Setup, Tools, and Help and support, making actions and information easily accessible.

Client Management & Remote Management 4.5/5

The ERA Console offers complete functionality via remote management, and can be connected to the ERA Server with minimal effort (e.g. using IP, server name). There is no license limit on the number of ERA Consoles and Servers installed on a network, which is convenient for larger enterprise setups that may require multiple servers and administrators.

The User Manager allows for creating and defining ERAC users with little effort. Permissions include configuration and execution of Group Management, Policy Management, Remote Install, On-Demand Scan Task, Update, and Run Scheduled Task, among many others.

On-demand scans, client configuration tasks, updates, and quarantine tasks can be administered using the ERA Console. Tasks can be easily created and configured, applied to target workstations via a right-click, and scheduled to run immediately or at a later time. Reporting is highly customizable and covers an extensive list of criteria (e.g. Clients Report, Scans Report, Quarantine Report, Server Database Load). Report templates can be saved, imported, exported, previewed, scheduled and targeted to a specific folder or the server database. In addition to the server console, the web dashboard provides a convenient means of remote monitoring. New dashboard templates can be created and configured, imported and exported from both the web dashboard and the server console.



Screenshot 2: ESET Remote Administrator Console (Server)

Updates 4/5

Setting up the ERA server updates requires a username and password given by ESET. The remaining default settings are reasonable, with the update server being set to automatic, and updates being checked for every 60 minutes. It is not made clear how often or under what circumstances clients check for updates based on the scheduler.

Creating an "update mirror" is an optional configuration, in which client workstations download updates from the ERA Server via the local network as opposed to downloading updates directly from the internet to save on bandwidth. It would be ideal if enabling the update repository was created automatically by default, as was the case with other products we tested.

Effectiveness 4.5/5

The most recent AV-Comparatives Summary Report, dated December 2011, ESET was placed as one of the 5 Top Rated Products of 2011, out of 20 products tested, awarded to products that achieved a "very high standard" in all tests. In their latest File Detection Test Report, AV Comparatives assigned the highest grade (ADVANCED+) to ESET NOD32 in their most recent On-Demand and Retrospective tests, dated August 2011. In the On-Demand File Detection of Malicious Software test, ESET achieved total detection rate of 97.6%, ranking 9th out of 15 products, and 2nd out of 18 products in the False Positives test, returning "very few FPs".

Overall, ESET products have had a total of 74 successes with only three misses since their inclusion in VB100 testing, giving them a success rate of 96%.

Kaspersky Endpoint Security

Review Summary

Overall Rating	★★★★
Installation & Configuration	★★★★
Migration	★★★★
Default Policies & Policy Management	★★★★½
Client Installation	★★★★
Interface Design	★★★★½
Client Management & Remote Management	★★★★
Updates	★★★★
Effectiveness	★★★★½
Performance	★★★

- **Pros**
- Initial configuration was quick and easy
- Wizard-based configuration eases administrators into management
- Relatively low traffic overhead for updates
- Policy and Client management is flexible
- One-click reporting with custom template creation
- **Cons**
- Performance is only average (large client installation size, slow On-Access scanning)
- Documentation is thorough but could be organized better

Installation and Configuration 4/5

Installing Kaspersky Security Centre (KSC) 9.2 was straightforward and quick, with the setup Wizard installing both the Administration Server and Console components in less than 5 minutes. Setup is completed in one major stage, and necessary prerequisites, including MS SQL Express, Microsoft .NET Framework 2.0, Windows Installer 3.1 and Microsoft Data Access Components 2.8 automatically if required. We conducted installation on a machine that only required MS SQL Express to be installed, so setup may have otherwise taken much longer, requiring restarts after installing Microsoft components.

Once the setup Wizard completes, the Quick Start Wizard appears, prompting for the Administrator to enter product activation details, which can be conveniently done later. Once complete, the product updates and no further restart is required to begin using the Administration Console. Like the setup Wizard, the Quick Start Wizard is transparent; informing the Administrator of every action it is taking, for e.g. creating default tasks and policies, and showing filenames as they are being downloaded during the update. The update took a while to complete (more than 20 minutes), but could be finished in the background by clicking 'Next'.

Documentation is split into four separate .pdf documents, an Administrator, Getting Started, Implementation, and User Guides. This makes it somewhat difficult to locate required information, and confusing as there is a significant amount of content overlap as well as cross-referencing between documents.

Migration from Previous Solutions 4/5

Upgrading from Kaspersky Administrator Kit (KAK) 8.0 to KSC 9.0 is documented clearly in 8 relatively simple steps, including creating a backup using the provided *klbackup* utility, installing KSC 9.0, and deploying an upgrade to migrate clients. The process does not require uninstalling KSC 9.0 or the client anti-virus separately, and all Administration Server data and settings are carried over when installed on the same computer where the previous version of Administration Server was installed.

Migrating to KSC 9.0 from previous versions of KAK 8.0 is not mentioned in the same document, but is not impossible as there are instructions available for migrating to KAK 8.0 from version 6 or higher in separate documentation. Thus migration from earlier versions may involve two major steps, i.e. migration to KAK 8.0 and then to KSC 9.0.

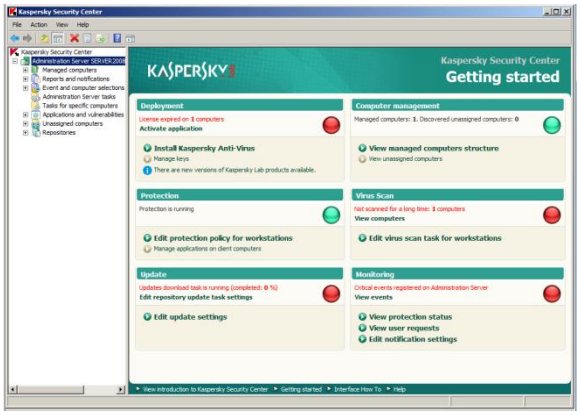
When deploying client software, administrators are given the option to automatically remove incompatible third-party security software.

Default Policies & Policy Management 4.5/5

On installation, KSC creates a single default policy for Kaspersky Endpoint Security (KES) 8.0. Default policy settings were reasonable, with all basic Anti-Virus features being enabled at the recommended medium security level. Separate policies for KSC Administration Server and KSC Network Agent can be created easily in a few clicks using the default settings in the New Policy Wizard.

Policy configuration options are extensive, covering all necessary basics, as well as more advanced areas, including defining of events types, grouping rules, and rights to protected resources (e.g. System files, Services). One useful feature is enabling a particular (stricter) policy to activate automatically at the onset of a 'Virus outbreak' event, in which a user-defined number of detected viruses has been exceeded within a specified time period. Policy behaviour is thoroughly documented, covering hierarchical inheritance and ambiguous scenarios (e.g. when a policy is deleted all settings are retained until manually altered).

A conversion wizard can be used for making policies of earlier versions of Kaspersky Lab applications usable with more current versions. This is useful for policies that were not automatically upgraded during migration, for example, because they were imported later from another Administration Server.



Screenshot 3: Kaspersky Administration Kit 9.2 (Server)

Client Installation 4/5

Client deployment is made simple using the Remote Installation Wizard, which follows the Quick Start Wizard. We were able to complete the process of deploying a single client was completed within five minutes. During deployment, the console displayed a progress bar and status text, which is reassuring to watch, but like most products the endpoint installation continued in the background after the task had 'completed' on the server side.

The documentation outlines installation options and instructions clearly in steps, with some steps being simplified and explained in later sections. While this means that the instructions are in-depth, it would be convenient if hyperlinks to relevant sections in the document were given to avoid the reader having to search for them.

As part of Kaspersky Endpoint Security Suite, we installed KES 8.0 to the endpoint, but similar to ESET's product, the deployment process is applicable not just to a range of Kaspersky Security products, but also to some non-Kaspersky applications as well. Another useful feature is the automatic installation of applications to new computers when they are added to an administration group.

Besides remote deployment, client installation is also possible by first creating a Stand-Alone package using KSC, which can then be sent via email, placed in a shared folder or on a web server. These packages can then be installed locally on an endpoint, which makes this method more suitable for smaller networks.

Instructions on configuring a connection between a locally installed client and the Administration Server were found separately in the Implementation Guide under Local Installation of Applications. This process involves the installation of a couple of additional components (Network agent, and control plug-in), which would be more convenient if done automatically using a wizard, or if these components can be added to a custom created install package.

Interface Design 4.5/5

Being built on Microsoft Management Console, the KSC interface looks uncluttered and well organized. A directory tree in the left pane provides a means of quick navigation, and window layout is visually consistent within categories, and related windows are well linked.

The server dashboard shows a colorful summary of Deployment, Computer management, Protection, Virus Scan, Update, and Monitoring statuses, with links for further details. The dashboard could perhaps benefit from having a representative icon for each category. Reports display 3-d like bar charts and pie charts, and red and green traffic lights are used to indicate a Critical and OK status respectively,

among other color conventions. The client interface is aesthetically pleasing, appropriately sized and simple, having two main tabs, Protection and Control and Settings.

Client Management & Remote Management 4/5

As with ESET's product, the KSC Administration Console can be installed on a separate computer to the Administration Server for remote management. While online documentation indicates that KSC supports configuration of permissions (e.g. access privileges, remote installation, editing of hierarchy settings) for different roles, we could not find any obvious way to do this from the management console.

One-click group creation makes it easy to create complex structures for larger networks. Group creation can also be automated by importing existing structures in Active Directory, Microsoft Windows Domains and Workgroups, or from a text file.

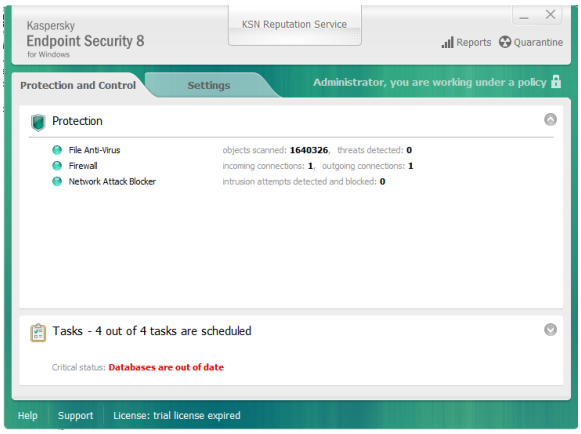
A wide range of filters can be applied when searching for managed computers, including domain, IP range, application, status, and application. Unmanaged computers are automatically discovered in the Windows network, Active Directory, specified subnets, or can be manually searched for using NetBIOS name, DNS name, IP, or IP range. Discovered computers are then listed in the directory tree, as they would be in Windows Explorer. Unassigned computers can be automatically assigned to administration groups by defining rules. As mentioned above, applications (in our case KES 8.0 and KSC 9.0) can be selected to be automatically installed on client computers in a group.

Under reports and notifications, 16 default reports (Error, Protection status, Deployment and Viruses reports to name a few) templates covering main areas of concern are generated upon viewing. Additional templates can be created and date ranges, presentation, and automated delivery can be configured. Like ESET's product, there is a web-based console to monitor server and client activities. According to online support, this component was only recently made commercially available (since 14 June 2012), so it was not included in the package that we tested in May 2012.

Updates 4/5

By default, an Update task is scheduled to run clients whenever updates are downloaded to the repository. Server Update default settings are set to check for updates from Kaspersky's Update server every hour, which is reasonable.

As with strict policy application, an update task can be configured to execute On "Virus Outbreak". While updates were highly configurable and flexible, it would have been useful to also have updates as being defined by policies.



Screenshot 4: Kaspersky Endpoint Security8 (Client)

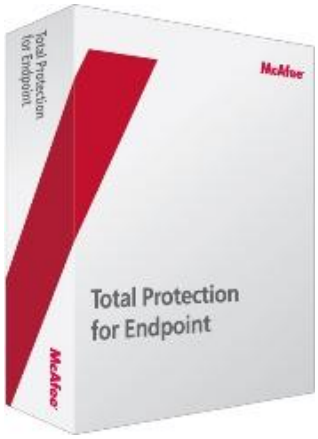
Effectiveness 4.5/5

In their latest Summary Report dated December 2011, AV Comparatives awarded Kaspersky an ADVANCED+ grade for all tests, including the Retrospective, and Removal tests. Kaspersky Anti-Virus was thus hailed as "Product of the Year" for 2011, placing it first overall out of 20 products.

In their most recent File-Detection Test Report, Kaspersky excelled in On- Demand Detection of Malicious Software, achieving a Total Detection rate of 99.3%, placing them 3rd out of 20 competitors. In the False positives test, they placed 5th out of 20, with "few FP's".

Kaspersky passed the VB100 test 71 times and failed 23 times, resulting in a 75% success rate.

McAfee Total Protection for Endpoint



Review Summary

Overall Rating	4.5
Installation & Configuration	3
Migration	4.5
Default Policies & Policy Management	2.5
Client Installation	3
Interface Design	3
Client Management & Remote Management	4
Updates	2
Effectiveness	4.5
Performance	4

- **Pros**
- Management console uses only a web-based console, which is sometimes difficult to navigate
- Low system impact (2nd best performance out of 7 products tested)
- **Cons**
- Documentation is thorough but could be organized better
- Configuration options are generally limited or hidden

Installation and Configuration 3/5

The installation of McAfee ePolicy Orchestrator (ePO) 4.6.0 was a much longer process than that of ESET and Kaspersky's products, taking around 30 minutes to complete. The process was not particularly smooth, requiring that setup be restarted after required prerequisites were installed. In addition, we ran into an error specific to Windows Server 2008 R2. We were at least provided with an error code, and McAfee having thorough online documentation meant that a quick search online gave us a solution which required changing a specific registry value.

Most software prerequisites are installed automatically (SQL Server 2005 Express, unless a Supported SQL Server is already installed, C++ Redistributables). .NET Framework 2.0 or later is required if installing SQL Server 2005 Express, but is not installed automatically and requires that Setup be cancelled and an appropriate package is acquired and installed manually.

Detailed step-by-step installation instructions can be found online in the ePolicy Orchestratior 4.6.0 Software Installation Guide. The documentation is well formatted and ordered, with appropriate indentation and labelling, and defined typographical conventions and icons that help make the document more readable.

Migration from Previous Solutions 3.5/5

Upgrading ePO is outlined in the ePO 4.6.0 Installation Guide, available online. It advises in the section summary that ePO version 4.6.0 can be migrated to from version 4.0 Patch 8, version 4.5 Patch 3, or an earlier version of 4.6.

The migration process is relatively straightforward and does not require uninstalling previous software versions. Backing up of the SQL database can be done either manually, or using the McAfee provided DBBAK utility. For different components (Orchestrator Server, Orchestrator Cluster Server, Remote Agent Handlers), a corresponding upgrade wizard is provided.

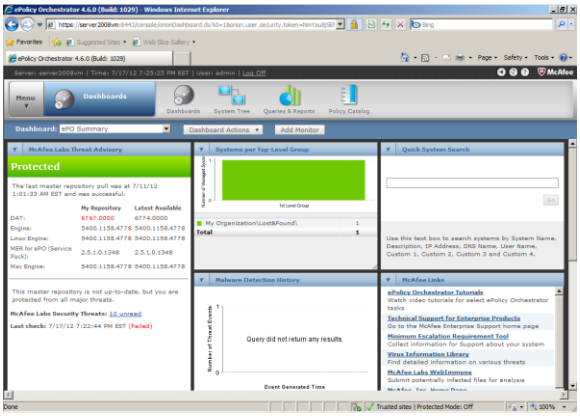
McAfee also provides separate knowledgebase articles detailing supported, unsupported products, and various backup procedures, which are comprehensive but sometimes redundant. Despite this, documentation is generally clear and easy to follow.

Policy Migration for some component versions (e.g. VSE 8.7i to 8.8) of ePO policies is supported using the ePolicy Orchestrator Migration Tool.

Default Policies & Policy Management 2.5/5

Upon installing ePO, several default policies are created, including 3 policies for McAfee Agent labeled "McAfee Default", having one for each category, General, Repository, and Troubleshooting. Similarly, there are another 3 policies labeled "My Default" and a "Large Organization Default" policy. The policy catalog displays policies by product and category. "McAfee Default" and "My Default" policies were provided for VirusScan Enterprise (VSE) 8.8 for 11 different categories. We found these categories to be quite specific (e.g. On-Access General Policies, On-Access High-Risk Processes Policies, Buffer Overflow Protection Policies and On Delivery Email Scan Policies). We feel that this could have been organized better for simpler management, for example it is probably not necessary to have 4 different On-Access policies, which could have been combined as one.

Policies can be edited, renamed, duplicated, deleted, exported, and shared easily, except for McAfee Default policies, which can only be duplicated. New policies can also be created and configured in a few clicks, but the web console makes this feel a bit slow and cumbersome. Policies were sufficient for protection, with all alerts and basic features being enabled.

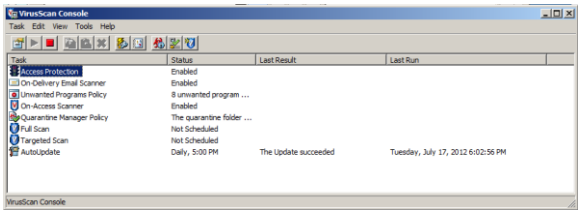


Screenshot 5: McAfee ePolicy Orchestrator (Server)

Client Installation 3/5

To prepare client software components for deployment, it is required to first install a set of zip files for the required software as extensions to ePO, as well as check them in to the Main Repository, so that the software can be deployed, managed, and integrated with ePO. It would be easier if only one of these tasks, i.e. checking in or installing as an extension, was required (for e.g. if checking in the software also automatically installed it as an extension).

The deployment process can be conducted by following a Guided Configuration. This involves 5 steps, Software Selection, System selection, Policy Configuration, Software Updating, and Software Deployment. System selection can be done either manually, or by Active Directory Synchronization. The system selection task was difficult to use, requiring domain login credentials before enumerating the list, and creating an empty list several times. It would be clearer if the target systems were selected or searched for first, and then credentials were required, as most other products have done.



Screenshot 6: McAfee VirusScan Enterprise 8.8 (Client)

We found that while the Guided Configuration indicated success, this was not necessarily the case. For e.g. if the target endpoint login details were incorrect, the deployment appears to continue and only displays an error when the task status is checked.

In the VSE 8.8 documentation, a standalone installation as well as a table of command-line parameters to configure installation is given, although there is no clear indication of whether it is possible to manage the endpoint from ePO after running these local installation methods.

Interface Design 3/5

McAfee uses an AJAX based web console which looks fancy but feels clunky and slow to respond at times. Shades of blue and grey for buttons, graphics, and text make the interface look consistent and professional, but somewhat cold. Icons are used to illustrate tabs, although some are a bit too vague and abstract to be helpful, for e.g. a screen with a ribbon marker is used for to illustrate the Policy Assignment Rules tab.

A drop down main menu and some shortcuts (Dashboards, System Tree, Queries & Reports, and Policy Catalog) make up the navigation bar along the top. The drop down menu is not really ideal, having menus within menus. Naming and terminology sounds sophisticated but is sometimes confusing and not immediately obvious. There are several dashboard templates to view summarized information, including Audit, Thread Events, Product

Deployment, Trends, and an ePO Summary. Client software components, including VirusScan Enterprise and McAfee agent, are functionally well designed but look plain and outdated.

Client Management & Remote Management 4/5

Administration is performed from a web-based console, so management can be performed remotely from anywhere on the network. Role based management is possible, in which user accounts can be created and configured and permission sets can be applied to users to allow or deny access to specific areas of management.

Creating and scheduling client tasks can be performed fairly easily in the Client Task Catalog window, although the range of deployable tasks is quite limited. The client antivirus component (VSE 8.8) has only two tasks listed in the client task catalog, On Demand Scan, and Restore from Quarantine, probably because functionality is split amongst several products. Tasks can be first created and configured, and then assigned, or added as an assigned task for a node (or group) in the system tree. From the system tree, endpoints can be left-clicked to view details (System Properties, installed products, threat events) or right-clicked to have a task executed on them.

In the Queries & Reports window, pie charts and statistics are generated for different queries (e.g. Malware Detection History, Failed Product Deployment in the Last 24 Hours), and reports can be manually created by dragging, dropping, and editing widgets from the toolbox (Image, Query Table, and Text). Report Properties can also be edited, and saved as .pdf files. Having a customizable presentation is nice, but some administrators may find that they prefer reports to be generated automatically.

Updates 2/5

In the Server Task Catalog, updating the master repository is enabled to be carried out daily at 1 a.m., which is much less frequent than other products (which scheduled this every hour). This task checks available updates for all products that have been checked into the Master Repository. Specific products can be updated by initiating a "Schedule Pull" or "Pull Now" task.

Updates are configured by editing the McAfee Agent Update policy, although options are limited. In the McAfee Agent Update Repository policy, there is an option to "Automatically allow clients to access newly-added repositories", which is disabled by default.

There is very little support for configuring updates for the client antivirus component (VSE 8.8). One option is to "Disable default AutoUpdate task schedule", which is unchecked by default. However, according to online support, this is a one way process and can't be reversed once checked. The only other option we could find was to apply a password to the VirusScan AutoUpdate feature. Perhaps there should be a separate AutoUpdate policy that features a more complete range of options.

Effectiveness 3.5/5

McAfee achieved relatively good ratings in the latest AV Comparatives Summary Report, dated December 2011. They were awarded an ADVANCED+ and STANDARD rating in the Aug 2011 On-Demand and Nov 2011 Removal test respectively. McAfee received a GOLD award for having the lowest false positives for 2011.

In the latest File-Detection Test Report, dated March 2012, McAfee obtained a Total Detection Rate of 98.6% in the AV Comparatives On-Demand Detection of Malicious Software Test, placing them 5th out of 20 competitors.

In previous VB100 tests, McAfee has achieved a total of 51 passes and 24 fails (a 68% success rate), with the most recent failure being a WildList miss in 2010.

Review Summary

Overall Rating	★★
Installation & Configuration	★
Migration	★
Default Policies & Policy Management	★½
Client Installation	★
Interface Design	★★★★
Client Management & Remote Management	★★
Updates	★
Effectiveness	★★★★
Performance	★★★½

- **Pros**
- Interface is elegant and familiar
- SCCM is used for a wide range of purposes
- Performance is fairly good
- **Cons**
- Provided and online documentation is scarce and very poorly organized
- Installation is very difficult, requiring many prerequisites and hotfixes
- Most administration tasks are not intuitive and convoluted to carry out

Installation and Configuration 1/5

Microsoft's solution (SCEP 2012) is the most complex and intricate of the products tested, taking no less than 5 hours to complete (not including troubleshooting). Endpoint Protection is part of the System Center 2012 environment, which in turn, comprises of 7 components: Orchestrator, Virtual Machine Manager, App Controller, Operations Manager, Configuration Manager, Service Manager and Data Protection Manager. Microsoft attempts to simplify this by providing a "Unified Installer" utility for the SC2012 environment but the fragmented component-based design inevitably leads to difficult troubleshooting due to the many points of failure.

Inconveniently, System Center 2012 does not support Windows Server 2003, so we had to instead perform installation on Windows Server 2008 (R2). There are strict integration requirements with many other Microsoft packages such as SQL Server, SQL Server Reporting Services, varying versions of the .NET Frameworks, Analysis Management Objects, PowerShell, Windows Update Services and Active Directory. This means that, unlike some of the other products tested which provided built-in update services or internal databases (that came preconfigured and customized to suit their needs), SC2012 required finicky configuration of each external service it utilizes. While this design may have been aimed to "slot in" to a Microsoft dominant enterprise Intranet environment (that would already have these Microsoft services well configured and fine-tuned), the benefits are curtailed by the strict version prerequisites of each component. One jarring example is that SCSM 2012 requires SQL Server 2008 SP2 or SQL Server 2008 R2, but it does not support SQL Server 2012, and would require a rollback of your SQL Server to accommodate.

Microsoft's solution had the largest number of software pre-requisites. Furthermore, the installers did not come with any of the pre-requisites, and required all components to be individually sourced online (there was no page of links), separately downloaded and manually installed. Documentation was largely provided through Microsoft TechNet. Information was scattered and not well-linked, with related topics hard to find. Some steps were missing and often ambiguous. The documentation in general was difficult to follow, requiring more elaborate guides that were informally provided in the Microsoft forums or blogs.

Migration 1/5

There have been several vastly different (and incompatible) enterprise security offerings from Microsoft.

Microsoft's earlier solution, Forefront Client Security (supported from 2007 to 2010) runs on a custom version of Microsoft Operations Manager 2005, while the new Endpoint Protection 2012 is part of the System Center 2012 platform. Being completely different beasts, there is officially no direct upgrade path from this solution.

A migration between these two would require manually documenting the settings for all policies you want to preserve, before unapproving all the FCS installation packages via WSUS (Windows Server Update Service) and effectively uninstalling them from all clients, and then proceeding with a clean installation of the System Center 2012 platform. This "completely from scratch" approach is obviously costly and the most cumbersome migration process of all products tested.

The more recent offering of Forefront Endpoint Protection 2010 (supported from 2010 to 2012) was a part of SCCM 2007, but it does not integrate with SCCM 2012. As such, to upgrade to the latest offering (Endpoint Protection 2012), you must upgrade the System Center platform. Due to the number of different components that make up the SC2012 platform, each component needs to be evaluated individually for eligibility and compatibility with existing components. Needless to say, this is not a simple task and a complete upgrade can take days of preparation in a large network.

Each component has an elaborate upgrade path. Simpler installations will be able to utilize the upgrade wizards, but multiple-server scenarios will require more effort. In the case of the Operations Manager, the latter is catered for with an "Upgrade Helper Management Pack" which will help discover the servers and agent-managed computers in the SCOM management group, in addition to monitoring the upgrade progress. Some of the components support "in-place" upgrades, such as Operations Manager and Configuration Manager, but as in the case of the latter, they may be limited to Distribution Points only.

Default Policies & Policy Management 1.5/5

A default installation of SCEP 2012 comes with 25 template policies that can be imported and deployed. These are well selected and range from "Default", "High Security", "Std Desktop" to "Performance optimized".

Most products have several options to manage client groups from within security solution, but Microsoft Forefront Client Security relies solely on the use of existing Windows server infrastructure to manage endpoints, such as through Group Policy Management (GPM) and the Active Directory domain. Endpoint machines must be organized into groups or Organizational Units (OU) within the Active Directory Domain before Forefront Client Security policies can be deployed and enforced.

Forefront Client Security policy management appears somewhat basic, with limited options for security management. The apparent lack of granular control is surprising given the product's complexity and intended large-scale corporate audience. Deployed policies do not come into enforcement until the Group Policy refresh takes place, which may take hours. Administrators can manually force an update by issuing a command through the command prompt on endpoint machines, but Forefront Client Security does not provide this functionality.

Client Installation 1/5

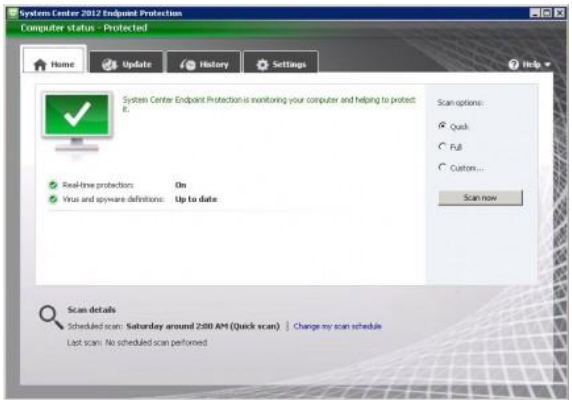
Once the System Center 2012 environment is properly setup, the SCEP client can be deployed via the Default Client Setting for Endpoint Protection. This setting enables or disables all SCEP clients on the managed machines.

Once again, the disadvantages of a solution which relied on so many different components became evident during our deployment. There was no centralized logging system so error messages were scattered and difficult to correlate from one module to another. Often, many modules are involved, and it was difficult to determine the cause or even investigate the symptom of the problem resulting in very difficult troubleshooting, not to mention the lack of clear documentation.

Interface Design 4/5

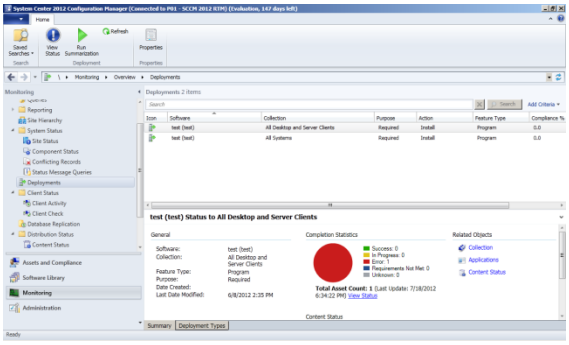
The SCEP client interface is almost identical to Forefront Endpoint Protection 2010. It is appropriately simple and readable, with features grouped under four tabs. Its consistency with the

Windows 7 look-and-feel and integration with Windows Action Center makes it one of the more approachable and familiar to use.



Screenshot 7: Microsoft Endpoint Protection 2012 Client

The server-side interface is a part of System Center 2012 Configuration Manager which uses an elegant and sophisticated layout. Users of other recent Microsoft products (such as Office 2010) will be comfortable and familiar with navigation devices such as the ribbon bar. The integration of the security features amidst other System Center features makes it a little harder to filter out unrelated details if your primary focus is on protection. However it can be useful when using SCCM to monitor other aspects of a network.



Screenshot 8: Microsoft System Center 2012 Configuration Manager (Server)

Client Management & Remote Management 2/5

Configuration Manager "clients" can be installed and deployed on multiple machines, so remote management is possible. The terminology is somewhat misleading, but deploying a "Configuration Manager client", as Microsoft calls it, is equivalent to installing another server manager console. However, given the complexity of System Center, this is not always practical, e.g. there are bound to be difficulties installing the SCCM "client" to the target machine. We found this to be ultimately restricting compared to the other remote management features offered by competing solutions.

Updates 1/5

Unfortunately, there were no update policies created by default. We had to manually configure Configuration Manager Software Updates to deliver definitions to clients using the less-than-intuitive and generic "Automatic Deployment Rules" which is used for all other deployments in System Center 2012.

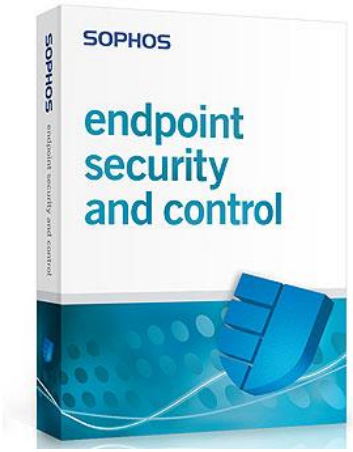
This involved the use of a complicated procedure (documented as 25 steps in TechNet), with many irrelevant features needing to be bypassed or worked around, such as the need to construct a "Property Filter" and "Search Criteria" by modifying a SQL-like query and running through a selection of windows and check boxes, simply to specify that we want definition updates and not updates for the "Bing Search Bar" or other Microsoft products. This is doubly confusing when the Product filter needed to be selected turns out to be "Forefront Endpoint Protection 2010" which is the name of the predecessor solution, and there is no choice for the current "Endpoint Protection 2012". This naming mistake (or design oversight) is also part of the official 2012 documentation so one presumes Microsoft has no intention to fix or change this in the near future.

Effectiveness 4/5

Microsoft achieved ADVANCED ratings in the 2011 On-Demand, Retrospective, and Removal tests in the latest AV Comparatives Summary Report, dated December 2011. However, in the latest File Detection Test Report, Microsoft came last out of 20 products in the On-Demand Detection of Malicious Software Test, obtaining a total detection rate of 93.1%. This also meant that, on the other hand, Microsoft came first in the False Positives tests, detection zero FP's.

In the VB100 tests, Microsoft Forefront has passed in all 16 tests it was entered in. Overall, Microsoft has obtained a total of 27 successes and only 2 fails, giving them a success rate of 93%.

Sophos Endpoint Protection 10



Review Summary

Overall Rating	3.5
Installation & Configuration	3
Migration	4
Default Policies & Policy Management	4
Client Installation	3.5
Interface Design	4
Client Management & Remote Management	3
Updates	4
Effectiveness	3.5
Performance	2

- **Pros**
- Documentation is very clear and in-depth
- Interface is familiar and intuitive to use
- Migration is fairly automated
- **Cons**
- Performance is only average (large client installation size, slow On-Access scanning
- No web console for monitoring and/or management

Installation and Configuration 3/5

Installing Sophos Enterprise Console Advanced is fairly straightforward, but requires some prerequisite Microsoft software (SQL Server 2008 Express unless SQL Server 2005 Express or later is already installed, .NET Framework 3.5 SP1 or later, and Microsoft Message Queuing) which are installed automatically during setup. System property checking for the above prerequisites performed automatically by the installer was helpful prior to setup, and wasted no time in having to restart the installer (which was not the case for McAfee's product). Setup and configuration was clear, although required fields were not correctly marked, instead providing an error when clicking 'Next'.

Due to all the required prerequisites, setup was lengthy and required restarts in between prerequisite installation stages. Using the default settings, the entire setup process took us around half an hour to complete, including a mandatory restart before opening the Console.

Documentation is in-depth, well organized and logically ordered. The installation process is described over 20 main topics that can be thought of as setup stages, including console server preparation and installation, server configuration, creation of policies, preparation and protection of endpoint machines, and post installation steps.

Migration from Previous Solutions 4/5

The Sophos Endpoint Protection upgrade process is complex but thoroughly documented, with extensive details on user account requirements and security policies. There are potential complications in the process with maintaining software subscriptions and updating policies from previous version. In spite of this, the documentation provides a systematic approach to handling these obstacles.

Unfortunately, supported versions to migrate from are not listed in the documentation. Instead, the enterprise console installer of the newer version provides advice on whether or not migration from the currently installed version is possible after checking if system requirements are satisfied.

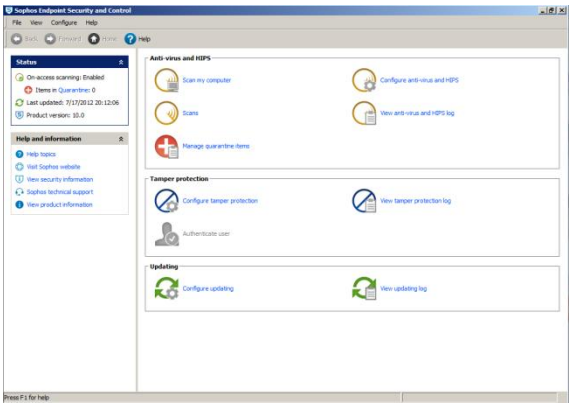
On the client side, upgrades to Sophos Endpoint Security and Control 10.0 are possible only from versions 9.0, 9.5 and 9.7. Upgrades are also possible from Sophos Anti-Virus 7 and Sophos Client Firewall 1.5. Endpoint computers can be upgraded gradually (allowing you to evaluate new versions before

upgrading all computers) or completely in one step. The latter process can be performed simply by configuring the Software Subscriptions window, allowing the Console to download updates that will then be used to upgrade the endpoint software automatically. Another convenient migration feature is that the Sophos client Installer also removes third-party software automatically.

Default Policies & Policy Management 4/5

Default policies are created on installation for all policy categories, which includes Updating, Anti-virus and HIPS, Firewall, NAC, Application control, Data control, Device control, Tamper Protection, Patch, and Web control. Policies can be managed from the left window when viewing Endpoints, and are helpfully organized in a tree. Policy configuration options are sufficient, covering most important areas. Some policy categories only contained a few variables (e.g. toggle tamper protection) and could have been merged with another category.

By default, there is no scheduled scan set in the Anti-virus and HIPS policy. Creating a scheduled scan is simple, although the default settings schedule the scan for every weekday at 9am, which would be inconvenient for users.



Screenshot 9: Sophos Endpoint Security and Control (Client)

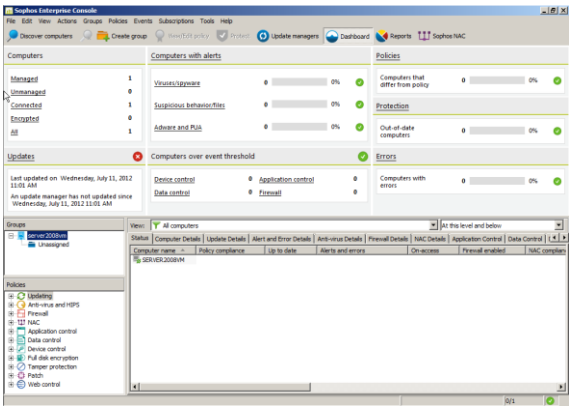
Client Installation 3.5/5

Like most other products we tested, main methods of endpoint discovery are covered, including Windows Network, IP/Subnet and Active Directory.

Before client deployment can be performed, the required software must first be downloaded from the management console by entering the credentials provided by Sophos, and connecting to the vendor's server. When we tried to download the required software, the vendor's server was initially unresponsive and required a few attempts to connect to.

The documentation outlines some specific requirements that must be met before deployment (e.g. the Remote Registry service must be started), but most of these would be satisfied on a typical workstation. The remaining deployment process takes only a few steps using the Protect Computers Wizard. Additional product components can be checked for inclusion in the deployment, and an option is given to automatically remove third-party security software, although this feature requires some manual configuration and a local restart.

Interface Design 4/5



Screenshot 10: Sophos Enterprise Console (Server)

The Sophos Enterprise Console interface is both functional and aesthetically pleasing, despite using more adventurous colors such as pink, purple and orange. Graphics are simple, but modern and stylish.

The dashboard can be toggled on or off, in which it takes up the top half of the main screen. The Endpoints/Update managers button allows for quick switching between Endpoints and Update managers windows, although we found that when switching between the two views, the button changes size, which throws off the navigation bar by a bit.

The client software launches an unnecessarily large window that shows a lot of empty white space, although this can be resized. The layout (particularly the navigation bar and left-hand menu) and icons are very reminiscent of Windows Explorer in XP, which makes it feel familiar but a little outdated for most.

Client Management & Remote Management 3/5

Role-based access to the administrator console can be used to assign Windows users and groups to

specific roles. An example of this, given in the documentation, is a help desk engineer who can perform updates but not configure policies. There are 4 preconfigured roles, System Administrator, Administrator, Helpdesk, and Guest. Roles can be edited created and defined by the System Administrator.

Client management can be performed in the endpoints tab, which displays a list of managed and unmanaged computers, with separate tabs for Status, Computer details, and each policy category.

Group structures can be created in one click, and configured after creation. Active directory containers can also be imported and used as a group structure. Alternatively, groups can be synchronized with Active Directory containers.

The Report Manager creates comprehensive and highly configurable reports using the Report wizard. Similar to other products, the report can also be scheduled for creation and automatic emailing.

Updates 4/5

The default updating policy has the client check the manager server every 10 minutes for newly downloaded updates, which is probably more frequent than necessary (most products we reviewed had this feature set to 4 hours, or had a feature to trigger updates when they are available).

Sophos Update Manager enables automatic updating from either a Sophos server or a server on your network, and distributes the downloaded security software to a suitable location for installation on endpoints, which will then update automatically when configured to do so. In more complex networks, additional update managers can be installed to a remote location, allowing for updates from one office location to be distributed to other office locations which have limited or slow external Internet connection.

Sophos subscriptions can be added and configured to download specific versions for different platforms. The settings offer a useful option for enabling automatic upgrading of software when it is no longer supported by Sophos.

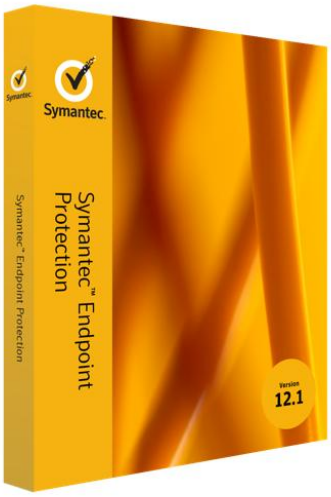
Effectiveness 3.5/5

Sophos were given average ratings in the latest AV Comparatives Summary Report, dated December 2011, being awarded an ADVANCED, STANDARD, and STANDARD score in the On-Demand, Retrospective, and Removal 2011 tests respectively.

In the latest AV Comparatives File-Detection Test Report, Sophos ranked 4th out of 20 products in the On-Demand Detection of Malicious Software Test, achieving a total detection rate of 98.9%. However, they ranked 9th out of 20 in the False Positives Test, with around a fair number of false positives.

In the VB100 tests, Sophos has achieved a total of 61 passes and 18 fails, giving them a success rate of 77%.

Symantec Endpoint Protection 12.1



Review Summary

Overall Rating	★★★★
Installation & Configuration	★★★★
Migration	★★★★½
Default Policies & Policy Management	★★★★½
Client Installation	★★★★½
Interface Design	★★★★
Client Management & Remote Management	★★★★
Updates	★★★★½
Effectiveness	★★★★
Performance	★★★

- **Pros**
- Web console (in addition to the desktop console) allows for remote monitoring and management
- Migration is highly automated and well documented
- Interface looks pleasant and is intuitive to use
- **Cons**
- Performance is only average (High memory usage, installation size and boot time on client)

Installation and Configuration 4/5

Installing the Symantec Endpoint Protection 12.1 management server and console is very straightforward. The wizard-based setup provides brief explanations of key features and minimal input is needed from the user, with only a few fields being marked as required. Setup progress through 3 stages (Installation, Server Configuration, and Product Migration) is shown, and administrators are advised when a particular step (e.g. database creation and initialization) may take some time.

Once the Installation wizard completes, the Management Server Configuration Wizard automatically starts, offering options for a default or custom configuration type, using a disaster recovery file, and an email address for notifications and reports etc. The default setup process was not long, taking us around 10 minutes to complete. Unlike other products we reviewed, setup was entirely standalone, and was thus smoother and integrated, not requiring any external installer packages to be run.

Support for different platforms (Windows 8, XP, Server 2003, Server 2008 and more) and database systems are well covered. By default, the SEP embedded database is included in installation, with support for up to 5,000 clients. For larger networks with up to 50,000 clients, Microsoft SQL Server (2000 SP4 or later, 2005 SP2 or later, 2008) is supported and can be installed prior to setup, but there are specific configuration requirements to follow. SEP also offers support for both Mac (OSX 10.5/10.6 and OSX Server 10.5/10.6) and Windows clients.

The documentation explains the entire setup process in 11 simple steps, with hyperlinks to related sections within the document where necessary.

Migration from Previous Solutions 4.5/5

Symantec provides a well designed migration path, involving minimal steps compared to other reviewed products. Backing up of the database is made simple with the included one-click backup tool. Migration of both the management server and endpoint clients is wizard based, uninstallation of previous versions does not require any extra steps, and all legacy settings are detected and maintained.

Migration is possible from the a wide range of Symantec endpoint products, including Symantec AntiVirus Corporate Edition 9.x and 10.x, SEP SBE 12.0, and SEP 11.x. Clients can be upgraded in a

number of ways, including an AutoUpgrade (an Automatic Upgrade Wizard), configuring LIveUpdate settings to permit product updates, and a local installation. As we saw with other reviewed products, the Client Deployment Wizard provides an option for automatically uninstalling existing security software.

Documentation is relevant and well presented, frequently using tables to compare and summarize information, for e.g. a feature map between 11.x and 12.1 clients shows improvements from previous versions. Symantec also offers migration assistance through their Endpoint Security service.

Default Policies & Policy Management 4.5/5

During installation, default policies are created for each category, Virus and Spyware Protection, Firewall, Intrusion Prevention, Application and Device Control, LiveUpdate, and Exceptions. By default, three different Virus and Spyware policies are defined (Balanced, High Security, and High Performance), and one policy is defined for each remaining category, with the balanced policy appropriately being used by default.

Antivirus policy settings are conveniently split into two sections, Windows Settings and Mac Settings, although there are naturally less than half the options under Mac Settings than there are under Windows Settings.

Policies management is intuitive, and configuration is fairly granular. Policies can be edited, deleted, assigned to specific groups, replaced, copied, pasted, exported and imported quite easily. A list of policy components helps organize objects used for defining policies (e.g. Scheduled Scan Templates, Management Server Lists, and Network Adaptors).

Client Installation 4.5/5

Remote deployment is very straightforward using the Client Deployment Wizard, which explains options and provides links for further help at each step. Installation options include Web link and email, Remote push, and Save package, in which the endpoint is automatically linked to the management server. Another option is to install the software as an unmanaged client, which must be managed separately, and may be useful for computers which are not always connected to the local network. It would be useful if there was a way to configure the management server to discover unmanaged clients so that they can be potentially changed to managed clients.

Like Kaspersky's product, the Management Console shows the deployment status using a progress bar in real time, which is reassuring for the administrator, although the response from the client side took longer than the completion confirmation from the console, which was the case for most products. Completing client installation requires a restart which can be executed from the management server at any convenient time. The entire process was short, taking less than 5 minutes.

Screenshot 12: Symantec Endpoint Protection (Client)

Interface Design 4/5

The SEP Manager interface is well designed, being visually welcoming and intuitive to use. Colors are appropriate to the company's logo, using mainly yellow and blue. A navigation bar on the left contains nicely sized and illustrated buttons that link to main areas (Home, Monitors, Reports, Policies, Clients, and Admin). Fitting color conventions are used, with green denoting good/up-to-date, red denoting that Attention is required/out-of-date. The ThreatCon security Response box shows a spectrum that ranges from green to read, to indicate normal to extreme threat levels. However, when we tested this product In Windows Server 2003, charts and graphics in the main pane did not appear, leaving a white space in place of them. There was no indication of whether we required a particular plugin for example, to render these graphics. We also found that the management console was sometimes slow to start up and login to.

The web console is almost identical to the console, in both function and layout, with some colors being slightly different. While this is not the case for the web-console, font type and size in the Manager console was slightly inconsistent.

The client user interface looks clean, and professional, although appears to have been simplified since the previous versions, perhaps indicating a focus on lightness and performance.

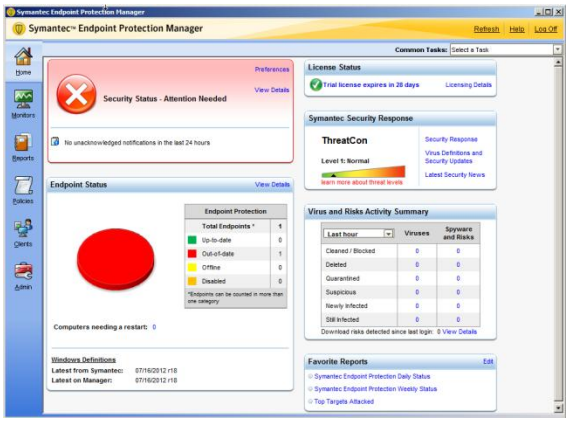
Client Management & Remote Management 4/5

Since the web console shares the same functionality as the management console, remote management from anywhere on the network is possible, sparing administrators the need to install the management console software on additional workstations.

Role based administration is well supported, where 3 default administrators can be created (System Administrator, Administrator, and Limited Administrator). System Administrators have full access and permissions, as do Administrators, but only within a single domain. Limited Administrators configuration is flexible, configurable rights within a wide range of areas (View reports, Manage groups, Remotely run commands, Site rights, Manage installation packages, Manage policies).

Group structures can be easily created by entering at least a name, and Active Directory structures can be imported and synchronized. Location specific policies and settings, as well as policy inheritance can be applied to groups.

Tasks can be easily carried out by right clicking target endpoints and selecting the appropriate action. While these functions cover basic actions, including Scan and Update Content, some are unique to the software's (e.g. Enable Auto-Protect, Enable Download Insight). Unlike most products we reviewed, there is no way to create a scheduled or conditional task.



Screenshot 11: Symantec Manager Console (Server)

Updates 4.5/5

Updates are controlled by Symantec's LiveUpdate utility. Server settings are configured to use both the management server and the default Symantec LiveUpdate server to provide updates for clients. Enabling both is not really necessary and may waste internet bandwidth. Unlike most products, there was no parameter for the frequency of server update checks. Clients are by default scheduled to check for updates every 4 hours, with a retry time of 2 hours. There is a useful download randomization option to reduce the load on the server (or on the internet connection).

In the LiveUpdate content policy editor, security definitions and signatures can be included or excluded in updates, or specific revisions can be chosen. One interesting feature is the use of a Group Update Provider, in which a client that downloads content from the management server passes this content on to other clients.

We found SEPM's update options to be more sophisticated and extensive than most products without being too difficult to configure and understand.

Effectiveness 4/5

Symantec achieved solid ratings in the latest AV Comparatives Summary Report dated December 2011, being awarded an ADVANCED rating in the Aug 2011 On-Demand Test, and ADVANCED+ rating in the Nov 2011 Removal Test.

In the VB100 tests, Symantec has performed respectably, having achieved 57 passes and 8 fails, giving it a success rate of 88%. They have not failed the test since August 2009, having been tested successfully every year since then.

Trend Micro OfficeScan 10.6

Review Summary

Overall Rating	3.5
Installation & Configuration	3.5
Migration	4
Default Policies & Policy Management	2
Client Installation	4
Interface Design	3
Client Management & Remote Management	3.5
Updates	4
Effectiveness	3.5
Performance	4

- **Pros**
- Light weight product (low client installation size)
- Documentation is thorough in covering complex scenarios, especially on migration and client installation
- **Cons**
- Configuration is generally limited and settings are sometimes difficult to find
- Very high file copy time on endpoints
- Very high network usage

Installation and Configuration 3.5/5

Setup was fairly easy, taking less than 15 minutes to complete, although configuration requires a bit more attention compared to other products. During setup, the administrator is prompted to enter in Activation Codes for three services, Antivirus, Damage Cleanup Services which is optional, and Web Reputation and Anti-spyware. Trend Micro had emailed us 4 different activation codes for different product components that did not match the service names, which was a bit confusing, but we eventually resolved to use the main OfficeScan code for all three services.

We kept all the default settings, so Apache Web Server 2.0 was installed as the IIS web server option was grayed out, although this can be enabled by first enabling the IIS web server in Windows settings

There are two main client configurations that can be set during installation, a smart scan and conventional scan. The default installation uses a smart scan configuration for clients, but this can be changed afterwards.

The installation guide covers considerations for more complex setups, such as using an IIS web server for IPV6 support, and firewall positioning within the network. Diagrams are used to illustrate a basic as well as multiple site network configurations.

Upon starting the web console, we had some difficulty logging in as Active-X would not install. Using the given error number, we found a solution online which required manually running a regsvr32 command on specific trend micro .dll and .ocx files, which was inconvenient. During later use, we ran into problems with the console informing us that some the OfficeScan master service has stopped, which happened intermittently. We suspect that the installation may not have run correctly, or required further configuration.

Documentation is extensive, provides useful links within the document, and is well formatted, using a table to outline font conventions to assist the reader. A glossary table outlines basic terminology, some of which are specific to OfficeScan, which is useful for administrators who are just starting out. It is also a nice change to see terminology organized as clearly and simply as possible, as product-specific naming and wording can quickly become a confusing mess, as we have seen for other products.

Migration 4/5

OfficeScan 10.6 supports upgrades from OfficeScan 8.0 SP1 and OfficeScan 10.x. Migration is documented in acute detail in the Installation and Upgrade Guide. A 4 step process is outlined for backing up the database and configuration files before upgrading, which is a bit more complicated than other products we reviewed, requiring stopping the Office Master Service and backing up a list of files manually.

Upgrading the server can be performed either locally or manually. There are 4 main upgrade options to choose from. Two of these options involve upgrading the server by installing 10.6 over the previous version. Once the server component is upgraded, connected Clients are upgraded to OfficeScan 10.6 gradually (for larger networks), or automatically, depending on whether or not automatic update was disabled prior to the server upgrade.

Clients can also be upgraded from 10.x and 8.0 SP1 to 10.6 by moving them to an OfficeScan 10.6 server, in which case specific actions must be taken depending on the popularity of either client configuration amongst the clients. The last upgrade method involves upgrading the update agents.

While it is good to have a range of options to choose from, some migration methods are a bit convoluted and require careful attention to detail which may be overwhelming for less experienced administrators.

Default Policies & Policy Management2/5

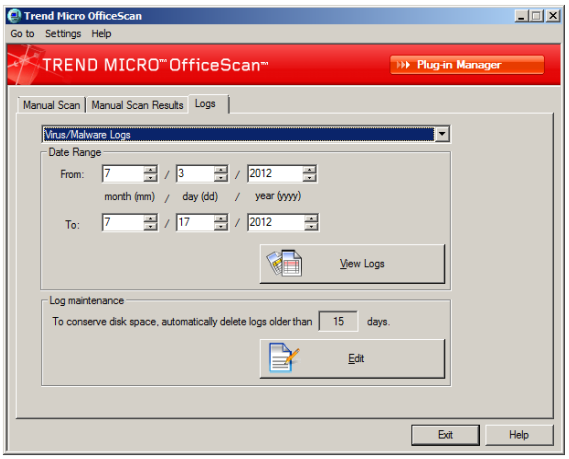
Policy/Settings management is somewhat confusing and not particularly intuitive. Client settings are configured in the client management area, where the Settings tab opens a menu linking to Scan Settings, Web Reputation Settings, Update Agent Settings, Device Control Settings, and so on. Settings can also be imported and exported, although it was not clear as to whether or not they could be applied to specific groups. Most settings only show options to either “Apply to All Clients” or “Apply to Future Domains Only”. Security settings were generally set to low (out of low, medium and high) for internal clients and medium for external clients (those which are not connected to the OfficeScan server), which is fair. We feel that these ‘settings’ could have been better organized and managed as policies.

While this was not possible for most client management settings, Firewall policies (of which there were 5 already defined) could be created, managed, and assigned to specific profiles or groups. Despite the emphasis on firewall management, the default firewall policy is set to the lowest security level.

Client Installation 4/5

Client Installation Methods are outlined thoroughly in the Administrator’s Guide. A helpful table summarizes each installation method (of which there are 8) outlining several deployment considerations, such as whether it is suitable for mass deployment, bandwidth consumption level, and whether it requires user intervention.

Client Installation methods include a web install (instructions and a link to the installer are sent to endpoint users via email), a client package deployment (through Active Directory or Microsoft SMS), and remote installation. Computers can be searched for by name or conduct an Advanced Search (by IP range, Platform, platform, architecture, and domain). We conducted a remote installation, which was quick and easy, taking only a few minutes.



Screenshot 6: Trend Micro OfficeScan (Client)

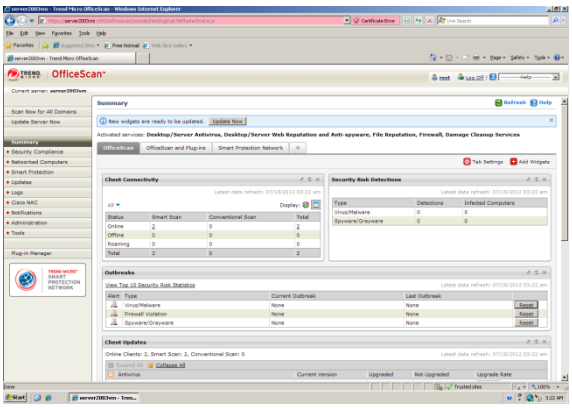
Interface Design 3/5

Like McAfee’s product, the management console interface is web-based and thus feels a bit slow and unresponsive at times. The layout is neat and well composed, with a navigation bar on the left linking to main areas including Networked Computers, Updates, Logs and Tools.

While the interface is well laid out, it could benefit from a more interesting color scheme. Some fancier graphics, including pie charts and maps displayed in the Smart Protection Network widgets, were animated, allowed for user interaction, and thus required Adobe flash. As with ESET’s web

dashboard, widgets can be added to the dashboard, shuffled around and resized. The map widgets were amusing, highlighting countries in red and displaying a score for threat sources and threatened users as the cursor hovers over them.

The client software launches a relatively small window. The interface is quite simple and looks bland and outdated. As with the web console, the client interface would benefit visually from more use of color.



Screenshot 7: Trend Micro OfficeScan (Server)

Client Management & Remote Management 3.5/5

Clients are managed via a web console, so it can easily be accessed from anywhere on the network. Role based administration is supported, providing two built-in role types (Administrator and Guest) to select from, although there seemed to be no other options for defining custom roles, despite options for importing and exporting roles.

A dashboard on the main summary page displays important information on Client Connectivity, Security Risk Detections, Outbreaks, and Client Updates. One nice feature was that when we ran a server update, update progress was displayed for individual endpoint software components.

Client details and statuses are displayed efficiently in the Client management tab. Client tree view can be changed to Update view, Antivirus view, Firewall view, among others, showing important information for each client. Client groups can be created, either using Active Directory, DNS domain, or administrator defined Custom client groups, although setting this up was confusing.

Like Kaspersky, virus outbreak parameters can be specified (in detections per hour), and when triggered will send a notification to the administrator. Client user notifications can be reworded, although not much more can be configured (e.g. if and under what circumstances they appear). A security compliance report can be sent via email at scheduled times, although there is no immediate way to preview the report. Client task coverage is only basic; a Scan Now, Client Uninstallation, and Spyware/Grayware Restore task can be performed on selected clients, but there is no obvious way to schedule them.

Updates 4/5

Updates for the OfficeScan server are by default carried out hourly, applying to all networked computer components (Antivirus, Anti-spyware, Damage Cleanup Services, Firewall and Behavior Monitoring Components). These components and features within them can be excluded from the update. Current version and last update status for each is shown clearly in a table on the dashboard.

Clients can be configured to use an Event-triggered and/or Schedule-based update. By default, schedule-based updating is set to weekly, every Sunday. However, we think that it would make more sense to instead have event-triggered updating enabled for when the OfficeScan server has downloaded a new component. A one-click manual update can also be carried out on both the server and client components.

Effectiveness 3.5/5

Trend Micro performed well in the latest AV Comparatives Summary Report, obtaining an ADVANCED rating for the Removal Test and an ADVANCED+ rating in the 2011 On-Demand Test. In the March 2012 File Detection Test Report however, Trend Micro ranked 3rd last out of 20 competitors, with a Total Detection Rate of 95.6% for the On-Demand Detection of Malicious Software Test. They also ranked 2nd last out of 20 in the False Positives tests, returning "very many FP's".

Trend Micro has had limited testing in the VB100 results. It has been entered only 27 times, passing 16 times, giving them a success rate of 59%. The last test occurred in April 2008, where they failed with 3 WildList misses and 2 false positives.

Disclaimer and Disclosure

This report covers selected Enterprise Security products that were available at the time of testing. Version numbers of software reviewed within this document are provided in the "Product Versions Tested" section of this report. With the exception of the performance test results and product effectiveness which are quantitative measures, the product reviews herein represent PassMark Software's subjective opinions and experiences in installing, configuring or operating each product. The metrics included in this report were selected by ESET LLC, and the production of this report was funded by ESET LLC.

Disclaimer of Liability

While every effort has been made to ensure that the information presented in this report is accurate, PassMark Software Pty Ltd assumes no responsibility for errors, omissions, or out-of-date information and shall not be liable in any manner whatsoever for direct, indirect, incidental, consequential, or punitive damages resulting from the availability of, use of, access of, or inability to use this information.

Disclosure

Trademarks

All trademarks are the property of their respective owners.

Contact Details

PassMark Software Pty Ltd
Suite 202, Level 2
35 Buckingham St.
Surry Hills, 2010
Sydney, Australia
Phone + 61 (2) 9690 0444
Fax + 61 (2) 9690 0445
Web www.passmark.com

Appendix A – Performance Methodology

Client Image Creation

After installation of the client image, the following Windows services/features were disabled to minimize the impact of Windows background activity and ensure the consistency of test results:

- **Windows SuperFetch** – Disabled for all tests. Re-enabled to allow boot time optimization functionality, and for boot and restart time tests.
- **Microsoft Search Indexer** – Disabled for all tests.
- **Windows Sidebar** – Disabled for all tests.
- **Windows Defender** – Disabled for all tests.
- **Windows Updates** – Initially, Windows updates will be installed. Prior to baseline tests, Windows Updates will be disabled and remain for the duration of testing.

After installation of each security product on the endpoint machine, variability of client activity has been limited by disabling client product updates and automatic or scheduled scans.

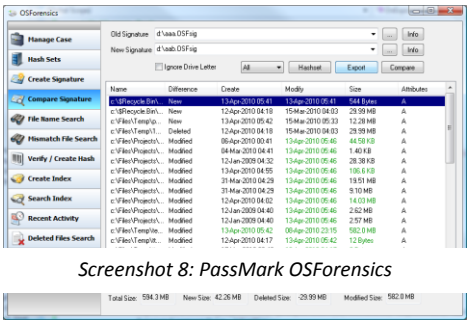
Adobe Flash Player, Microsoft Word, Microsoft PowerPoint, and Microsoft Excel will also be installed on endpoint machines prior to testing, in order to facilitate **the On Access Scan Time** tests.

Install size (Endpoint & Server)

Description This metric measured the total additional disk space consumed by the endpoint client and the management server components after installation.

Test Tool(s) **OSForensics (formerly OSCheck)**
By: PassMark Software

OSForensics can be used to capture and compare signatures of disks, folders and files. File comparisons can be made between two signatures to determine newly created files, modified or deleted files.



Screenshot 8: PassMark OSForensics

Methodology

- OSForensics was used to take an initial disk signature prior to each installation to establish a baseline value.
- The client component of the security product was installed on the endpoint machine.
- Where possible, the package was installed via the network, i.e. deployed from the server component through the network to the client machine. Deploying through the network more adequately reflects a user's 'real' installation experience.
- Where applicable, PassMark has selected default options during client installation.
- After installation, PassMark will initiate a manual update for the client software and then restart the endpoint machine to clear away temporary files.
- After the manual update and machine restart, a second disk signature was taken.
- Disk signatures were compared using OSForensics to discover the size and amount of files added or modified during client installation.
- The above steps were also applied to the server machine, but with the management server software being installed instead.

Result The final result was calculated as the total size of additional files and changes in modified files (files that were larger) after client installation, manual update and machine restart.

Boot time (Endpoint)

Description This metric measured the time taken to boot the machine, where an endpoint security product was

installed.

Test Tool(s) **xbootmgr and xperf**
by: Microsoft

These tools are available from the Windows Performance Toolkit version 4.6 (as part of the Microsoft Windows 7 SDK, obtainable from the Microsoft Website). Xbootmgr was used to optimize the boot process, as well as to benchmark the time taken to boot the machine. Xperf was used to parse the detailed boot traces outputted by xbootmgr.

Methodology

- Network connections were disabled prior to and during this test to ensure consistent results and minimize network interference.
- The Windows service SuperFetch will be enabled prior to testing, in order for boot optimization to function correctly. This process is disabled for the rest of testing to minimize background activity.
- Prior to boot time testing, xbootmgr was used to perform boot time optimization using the command "*xbootmgr.exe -trace boot –prepSystem*". Optimization ensures consistent results.
- After boot optimization, the benchmark test was conducted using the command "*xbootmgr.exe -trace boot -numruns 5*".
- The xbootmgr command boots the system five times in succession, taking detailed boot traces for each boot cycle.
- xperf was used to parse the boot traces and obtain the BootTimeViaPostBoot value. This value reflects the amount of time it takes the system to complete all (and only) system startup processes.

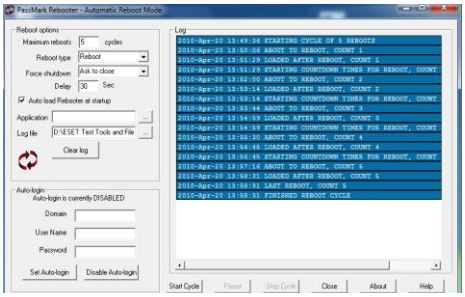
Result Our final result is measured in seconds (s) and calculated from an average of five (5) samples.

Machine Restart Time (Client)

Description This metric measured the time taken for the machine complete the entire restart cycle. We measured the time taken from the execution of a "Restart" command from within the operating system, through shutdown and system startup, to when the operating system becomes responsive to user interaction.

Test Tool(s) **Rebooter**
by: PassMark Software

A test utility developed by PassMark software which measured the time taken to complete a restart cycle starting from the operating system. Rebooted can be downloaded from our website at: http://www.passmark.com/products/rebooter.htm



Screenshot 9: PassMark Rebooter

Method

- Network connections were disabled prior to and during this test to ensure consistency and minimize network interference.
- Prior to this test, we executed the boot time test. Prior to the boot time test, xbootmgr.exe was used to perform boot time optimization to ensure consistent results. The effects of optimization were in effect during the Restart Time test. SuperFetch was also enabled for this test and for boot optimization to function correctly.
- Rebooter was used to restart the machine from the operating system and measure the time taken to complete each restart cycle.
- The machine was restarted five times to obtain five test results.

Result Our final result was measured in seconds (s) and calculated from an average of five (5) samples.

File Copy Performance – Large Set of Small Files (Endpoint)

Description This metric will measure the time taken to copy a large set of small files between directories on the endpoint machine.

Test Tool **CommandTimer**
by: PassMark Software

A command line utility developed by PassMark software which measures and logs the time taken to perform a task in a command prompt.

Method

- At the start of each test cycle, the machine will be left to idle for five minutes to minimize the impact of startup or background processes.
- CommandTimer will measure the amount of time taken to copy a large set of small files to another directory on a local drive using the xcopy command.
- This test will be performed five times with a machine restart between each cycle.

Test File(s) A file set 659 MB in size, with over 821 files.

This file set is intended to represent a large set of small files found on an average user PC. It includes a range of file formats such as Windows system files (DLL, EXE, CPL, UCE, etc), image files (GIF, JPG, PNG), movie files (AVI, WM, RM), music files (MP3), Office documents (PPT, PPTX, DOCX, DOC, XLS) and PDFs.

Result The final result is calculated as an average of five test results.

File Copy Performance – Small Set of Large Files (Endpoint)

Description This metric will measure the time taken to copy a small set of large files between directories on the endpoint machine.

Test Tool **CommandTimer**
by: PassMark Software

A command line utility developed by PassMark software which measures and logs the time taken to perform a task in a command prompt.

Method

- At the start of each test cycle, the machine will be left to idle for five minutes to minimize the impact of startup or background processes.
- CommandTimer will measure the amount of time taken to copy a small set of large files to another directory on a local drive using the xcopy command.
- This test will be performed five times with a machine restart between each cycle.

Test File(s) A file set roughly 2.5GB in size, with over 11 files.

This file set is intended to represent a small set of large files found on an average user PC. It includes a range of file formats such as data files (DAT), large image files (BMP, JPG), document files (PDF, TXT), large archive files (ZIP) and installation executable files (EXE).

Result The final result is calculated as an average of five test results.

File Copy, Move and Delete (Endpoint)

Description This metric will measure the time taken to copy, move, and delete samples of files in various formats.

Test Tool **CommandTimer**

A command line utility developed by PassMark software which measures and logs the time taken to perform a task in a command prompt.

Method

- At the start of each test cycle, the machine will be left to idle for five minutes to minimize the impact of startup or background processes.
- CommandTimer will measure the total amount of time taken to copy, move, and delete each file in the file set.
- This test will be performed five times with a machine restart between each cycle.

Test File(s) A file set 725 MB in size, made up of 812 files.

This file set is intended to represent a large set of small files found on an average user PC. The file set consists of documents (26%), media files (54%), and PE files (i.e. system files) (20%).

Result The final result is calculated as an average of five test results.

Network Throughput (Endpoint)

Description This metric will measure the time taken to download a sample set of binary files of various sizes and types over a 100MB/s network connection.

Test Tool **CommandTimer**
by: PassMark Software

A command line utility developed by PassMark software which measures and logs the time taken to perform a task in a command prompt.

GNU Wget

A GNU command line utility which sends a HTTP request and downloads the response to disk.

Method

- The files will be hosted on a server machine running Windows Server 2008 and IIS 7.
- At the start of each test cycle, the machine will be left to idle for five minutes to minimize the impact of startup or background processes.
- CommandTimer will measure the amount of time taken to download the sample set.
- This test will be performed five times with a machine restart between each cycle.

Test File(s) A file set roughly 527MB in size, over 484 files.

This file set consists of two file categories: media files (74%) and documents (26%).

Result The final result is calculated as an average of five test results.

Memory Usage during Idle (Endpoint & Server)

Description This metric measured the total additional memory use consumed by the endpoint machine during a period of system idle where an endpoint security product has been installed.

Test Tool(s) **SysinfoAvg**
by: PassMark Software

A command-line utility developed by PassMark software which retrieved and logged memory commit charge values (e.g. Total commit charge, Peak commit charge, etc) from Windows.

Methodology

- Prior to testing, the endpoint machine was left idle for five minutes to minimize the impact of startup or background processes.
- SysinfoAvg is configured to retrieve and log the system memory commit charge every 15 seconds for five minutes, for a total of 20 samples per test.
- This test will be run on the first and fifth test cycle, for a total of two runs and 40 test samples.

Result The final result was measured in megabytes (MB) and calculated as an average of 40 samples. This average was subtracted from the baseline to obtain the total amount of additional memory consumed by the security solution.

Full System Scan Time (Endpoint)

Description This metric will measure the average total time taken to run a full system scan on an endpoint machine where an endpoint security product has been installed.

Test Tool **Stopwatch (or scan logs were applicable)**

Method

- Prior to testing, the endpoint machine was left idle for five minutes to minimize the impact of startup or background processes.
- A full system scan is initiated via the endpoint software's interface and SysinfoAvg is started immediately.
- The scan is timed either manually with a stopwatch, or the time is taken from a reliable record of the scan by the endpoint software.
- The test is run 3 times in total.

Result The final result was measured in minutes (min) and is calculated as a weighted average, in which the subsequent scans collectively have the same weighting as the initial scan.

Memory Usage during Full System Scan (Endpoint)

Description This metric will measure the total additional memory use consumed by the endpoint machine during a full system scan where and endpoint security product has been installed.

Test Tool **SysinfoAvg**
by: PassMark Software

A command-line utility developed by PassMark software which retrieved and logged memory commit charge values (e.g. Total commit charge, Peak commit charge, etc) from Windows.

Method

- Prior to testing, the endpoint machine was left idle for five minutes to minimize the impact of startup or background processes.
- SysinfoAvg is configured to retrieve and log the system memory commit charge every 15 seconds for five minutes, for a total of 20 samples per test.
- A full system scan is initiated via the endpoint software's interface and SysinfoAvg is started immediately.
- This test will be run on the first and fifth test cycle, for a total of two runs and 40 test samples.

Result The final result was measured in megabytes (MB) and calculated as an average of 40 samples. This average was subtracted from the baseline to obtain the total amount of additional memory consumed by the security solution.

On Access Scan Time (Endpoint)

Description This metric will measure the average additional time taken to run a script that automatically browses a set of websites in IE and accesses three MS Office documents.

Test Tool

CommandTimer
by: PassMark Software

A command line utility developed by PassMark software which measures and logs the time taken to perform a task in a command prompt.

AppTimer
by: PassMark Software

An application developed by PassMark software used for automatically opening and closing an application and measuring the startup time.

Method

- Prior to testing, the endpoint machine was left idle for five minutes to minimize the impact of startup or background processes.
- CommandTimer will measure the total amount of time taken to browse the set of popular websites, and then open and close each document three times.
- This test will be performed five times with a machine restart between each cycle.

Test File(s) A file set 659 MB in size, over 821 files.

The website set consists of the front page of 106 high traffic websites (e.g. shopping, social, news, finance and reference websites). The set of MS office documents consists of a Word document (~10MB), a PowerPoint document (~1MB), and an excel document (~1MB).

Result The final result was measured in seconds (sec) and is calculated as an average of five test results.

Memory Usage during On Access Scan (Endpoint)

Description This metric will measure the total additional memory use consumed by the endpoint machine during an On Access scan where an endpoint security product has been installed. (See On Access Scan Time)

Test Tool

SysinfoAvg
by: PassMark Software

A command-line utility developed by PassMark software which retrieved and logged memory commit charge values (e.g. Total commit charge, Peak commit charge, etc) from Windows.

Method

- Prior to testing, the endpoint machine was left idle for five minutes to minimize the impact of startup or background processes.
- SysinfoAvg is configured to retrieve and log the system memory commit charge every 15 seconds for five minutes, for a total of 20 samples per test.
- The On Access Scan script is run and SysinfoAvg is started immediately.
- This test will be run on the first and second test cycle, for a total of two runs and 40 test samples.

Result The final result was measured in megabytes (MB) and calculated as an average of 40 samples. This average was subtracted from the baseline to obtain the total amount of additional memory consumed by the security solution.

Memory Usage during On-Demand Scan Task (Server)

Description This metric will measure the total additional memory use consumed by the server machine during the period in which On-Demand Scan Task is being run on an endpoint client.

Test Tool **SysinfoAvg**
by: PassMark Software

A command-line utility developed by PassMark software which retrieved and logged memory commit charge values (e.g. Total commit charge, Peak commit charge, etc) from Windows.

Method

- Prior to testing, the endpoint machine was left idle for five minutes to minimize the impact of startup or background processes.
- SysinfoAvg is configured to retrieve and log the system memory commit charge every 3 seconds for two minutes (40 samples).
- This test is run once, giving a total of 40 samples. If the task finishes before 40 samples have been taken, the test will be rerun in order to obtain the remaining samples.

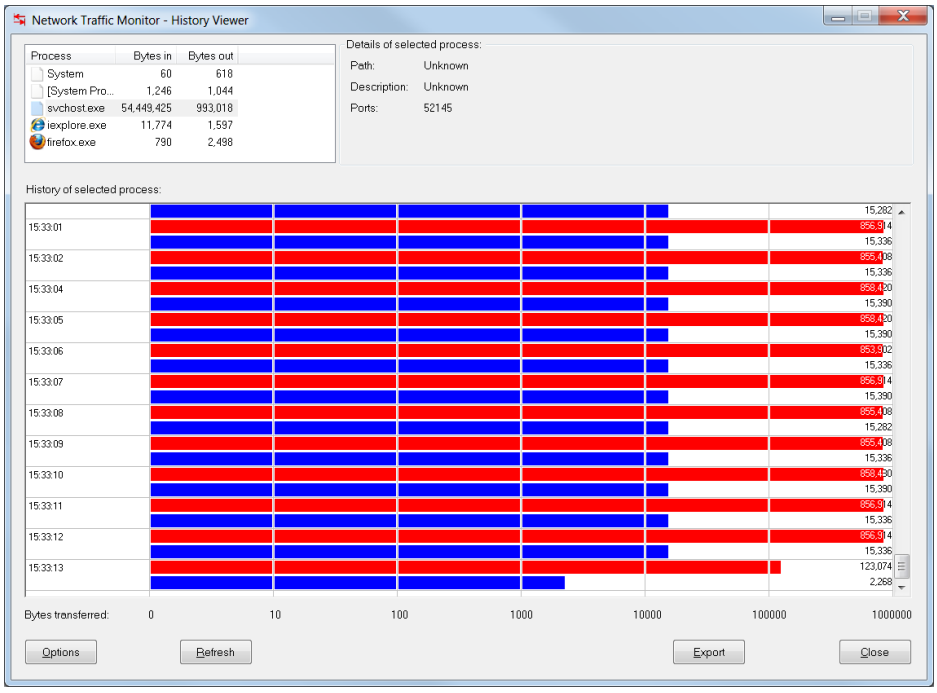
Result The final result was measured in megabytes (MB) and calculated as an average of 40 samples. This average was subtracted from the baseline to obtain the total amount of additional memory consumed by the security solution.

Daily Network Traffic (Server)

Description This metric measures the size and frequency of updates required by a security product.

Test Tools **Network Traffic Monitor**

We investigated NetLimiter and discovered its ability to monitor bandwidth was restricted to product pre-defined processes only (e.g. iexplorer.exe). We now propose to use Network Traffic Monitor to monitor network traffic for services and processes.



Method

- This test will be run in parallel to other performance testing.
- All server modules are installed in separate virtual machines on a single host machine. The single host machine will require a large amount of RAM and HDD space to support this.
- Process(es) used by each security product to update, poll or monitor for updates will be identified.
- Network activity for relevant process(es) will be logged until the end of the project or one

month (30 days), whichever comes first.

Result Update Size: The final result is calculated as the total amount of data downloaded by the product over 30 days.
Update Frequency: The network activity log is analyzed and the download frequency described (e.g. polling every hour, scheduled download every day, etc) over 30 days.

Issues Microsoft Forefront required WSUS to be synchronized in order to access updates.