PASSMARK® SOFTWARE

# Fast and Effective Endpoint Security for Business

## Comparative Analysis

**June 2010**


**Document:** Fast and Effective Endpoint Security for Business – Comparative Analysis
**Authors:** K. Lai, D. Wren
**Company:** PassMark Software
**Date:** 15 June 2010
**Edition:** Edition 1
**File:** Fast and Effective Security for Business - Ed1 June 2010.docx

# Table of Contents

# Revision History

| Rev | Revision History | Date |
|---|---|---|
| Edition 1 | First edition of the document.<br>Performance charts and comparative reviews added. | 15 Jun 2010 |
| | | |
| | | |

# References

| Ref # | Document | Author | Date |
|---|---|---|---|
| 1 | AV Comparatives - Summary Report 2009<br>Current Edition: December 2009<br>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 | 24 Dec 2009 |
| 2 | AV Comparatives - On-Demand Comparatives<br>Current Edition: Report Number 25, February 2010<br>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 | 17 Mar 2010 |
| 3 | AV Comparatives – Retrospective/ProActive Test<br>Current Edition: Report Number 26, May 2010<br>Information from Retrospective/ProActive Test reports by AV Comparatives was used in determining the effectiveness of reviewed business security solutions. | AV Comparatives | 5 Jun 2010 |
| 4 | VB100 Test Results<br>Current results: Windows Server 2008 R2, June 2010<br>Overall test results obtained by VB100 were used in determining the effectiveness of reviewed business security solutions. | Virus Bulletin | Jun 2010 |
| 5 | Network Traffic Monitor v2.01<br>A tool used to monitor the amount of inbound and outbound network traffic for the Update Size metric. | Nico Cuppen Software | - |

# Introduction

The importance of effective security for businesses cannot be understated, with malware damage and costs to businesses escalating every year[1]. The nature of the threat landscape has become more sophisticated, with malware events not only causing lost productivity and reputation for affected businesses but a staggering potential for losses from theft of data and other security breaches[2] from more targeted attacks.

In response, businesses have been placing their confidence in a wide range of security solutions to meet their needs. With the large amount of software available from many vendors, the challenge for businesses now becomes determining 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 largest security vendors. In this report, PassMark Software has evaluated the following business security products:

- ESET Smart Security 4 Business Edition
- Kaspersky Business Space Security
- McAfee Total Protection for Endpoint
- Microsoft Forefront Client Security
- Symantec Endpoint Protection
- Sophos Endpoint Security and Data Protection
- Trend Micro Worry-Free Business Security: Standard Edition

[1] A 2007 survey conducted by 'Computer Economics Inc' estimates that worldwide, malware costs businesses over US$13B each year.

[2] The Fifth Annual "Cost of a Data Breach" report by Ponemon Institute, Jan 2010, puts the average price of data breach at US$204 per compromised record.

# 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 | 4.5 | 3 | 1 | 4.5 | 4.5 | 4.5 |
| Migration | 4.5 | 5 | 2 | 1 | 5 | 4.5 | 5 |
| Default Policies | 4.5 | 4 | 4.5 | 2 | 4.5 | 4.5 | 4 |
| Client Installation | 4 | 5 | 3 | 1 | 3 | 3 | 4.5 |
| Interface Design | 4 | 5 | 4.5 | 2.5 | 1.5 | 4.5 | 2.5 |
| Client & Policy Management | 5 | 4 | 5 | 1.5 | 3 | 4 | 3 |
| Remote Management | 4.5 | 5 | 4.5 | -- | 4 | 4.5 | 4 |
| Updates | 4 | 2.5 | 4 | 2 | 1.5 | 5 | 4.5 |
| Common Use Cases | 5 | 5 | 3 | 2 | 4.5 | 4.5 | 3 |
| Effectiveness | 5 | 4.5 | 4.5 | 4 | 4.5 | 5 | 2 |
| Performance | 4.5 | 4 | 2.5 | 2 | 3 | 4 | 2 |

## 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 | 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. |
| 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 & Policy Management | This category assesses the flexibility and granularity of policy management from the server console, taking into account the level of automation in setting up groups and the depth of configuration options available to administrators. |
| Remote Management | This category examines how much support is 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. |
| Common Use Cases | This category examines the relative ease of use and handling for three common management use cases by each security product. These scenarios are: conducting an 'on-demand' scan of selected endpoints; creating and viewing a malware report 'on-demand'; and creating, assigning and deploying a new policy. |
| 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 ten 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 on which the server components of the security software were installed:

**Operating System:** Windows Server 2003 32-bit
**CPU:** Intel Xeon CPU @ 3.4GHz
**Motherboard:** Hewlett-Packard 08B4h Motherboard
**RAM:** 4GB ECC RAM
**HDD:** Western Digital Raptor 74GB 10,000RPM

### Virtual Machine Specification

**Operating System:** Windows Server 2003 32-bit
**RAM:** 1-2 GB (depending on the product's requirements)

### Client Machine Specification

**Operating System:** Windows 7 Ultimate x64
**CPU:** Intel Core i7 720 @ 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 Smart Security 4 Business Edition | Remote Administrator Console: v4.0.122.0 | Smart Security 4 Business Edition: v4.2.40 |
| Kaspersky Business Space Security | Administration Kit: v8.0.2090 | Kaspersky Anti-virus 6.0: v6.0.4.1424 |
| McAfee Total Protection for Endpoint | ePolicy Orchestrator: v4.5 | McAfee Agent: v4.5.0.1270 |
| Microsoft Forefront Client Security | Forefront Client Security Console: v1.1.1710.90 | Forefront Client Security: v1.5.1981.0 |
| Symantec Endpoint Protection | Endpoint Protection Manager: v11.0.600.550 | Symantec Endpoint Protection: v11.0.6000.550 |
| Sophos Endpoint Security and Data Protection | Enterprise Console: v4.0.0.2362 | Endpoint Security and Control: v9.05 |
| Trend Micro Worry-Free Business Security: Standard Edition | Worry-Free Business Security: v6.0 SP2 build 3025 | Client/Server Security Agent: v16.0.3052 |

# 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.

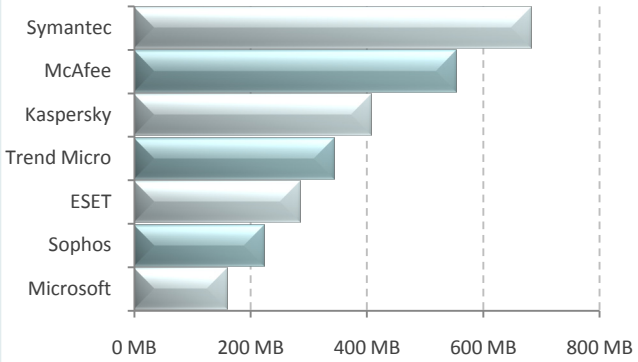
More detailed description of the methodology used can be found in **Appendix A – Performance Methodology**.

## 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).*

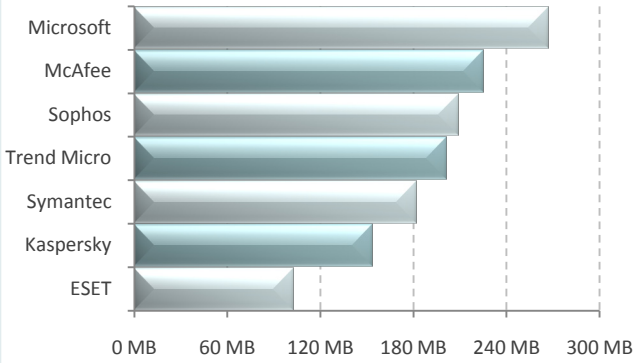



## Memory usage commit charge

***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 use consumed 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 40 samples.*

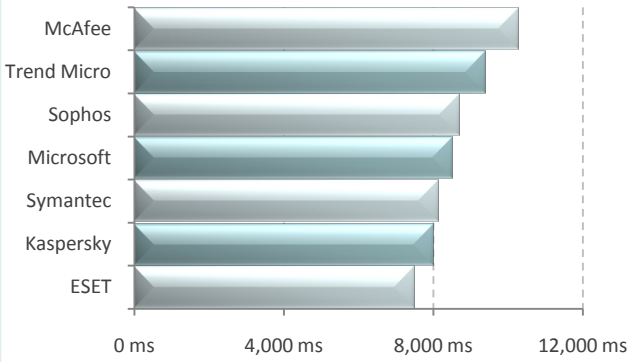



## Word document launch time

***Spend less time waiting for documents to launch***

Security products may hinder launch times of applications and documents as a result of poorly performing anti-malware functionality, such as real-time file scanning or behavioural heuristics. Slow endpoint system response times can bring about avoidable issues for productivity.

*The metric measures the total time taken to launch a large Microsoft Word 2007 document with a system restart prior to application launch. Our final result is measured in milliseconds (ms), and calculated from an average of five (5) samples.*

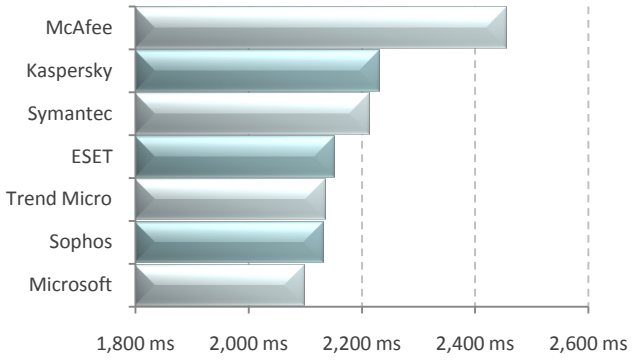


## Word document restart time

***Restart your applications without the wait***

Restarting applications is a common task for endpoint users, who may quickly close or switch between documents and applications as they conduct work tasks. The amount of time taken by applications to restart is a visible measure of system responsiveness for endpoint users.

*This metric measures the total time taken to re-open a large, mixed media Microsoft Word 2007 document, where an endpoint security product has been installed. Our final result is measured in milliseconds (ms), and calculated from an average of ten (10) samples.*

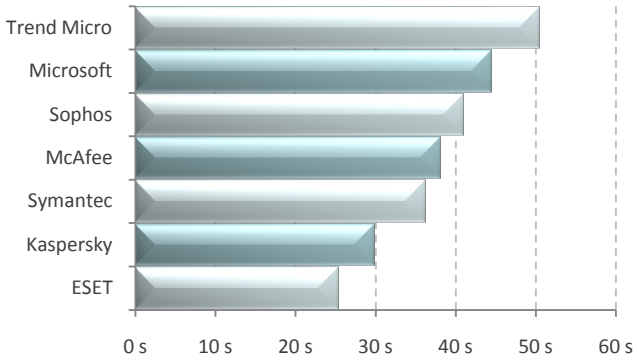



## File copy time for small files

***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.*

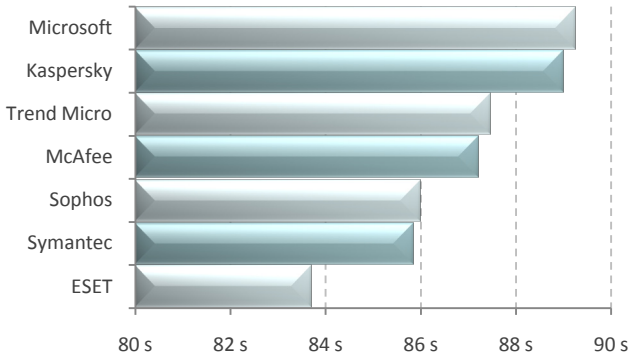



## File copy time for large files

***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.*

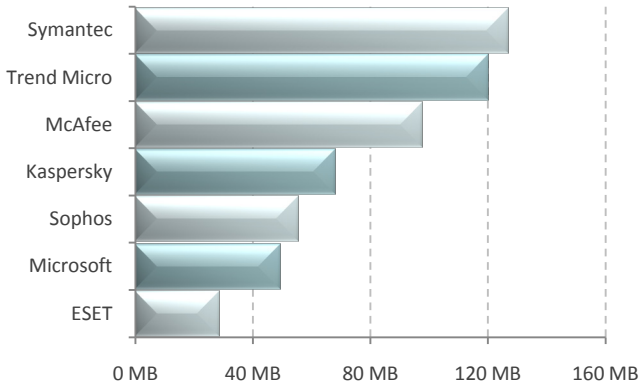



## Client Signature Database Size

***Reduce the footprint of endpoint solutions***

The size of the anti-malware signature database on endpoint machines gives an indication of a product's footprint on the local disk drive.

*This metric measures the total size of anti-malware signature files on the endpoint machine after a manual update. Our final result is measured in megabytes.*

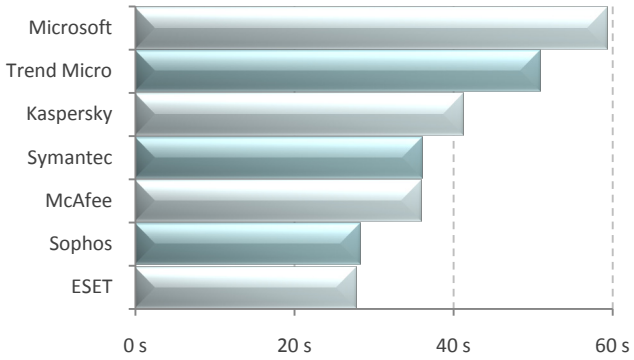


## Boot time

***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.*

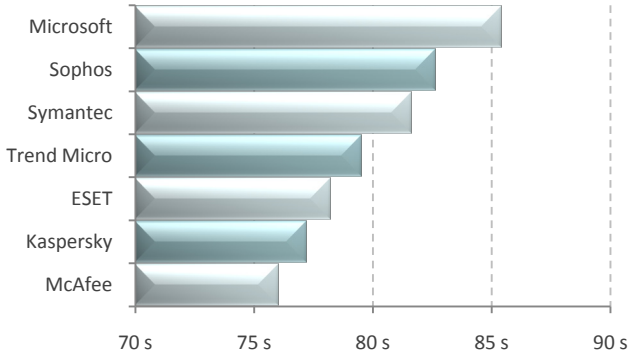



## Machine restart time

***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.*

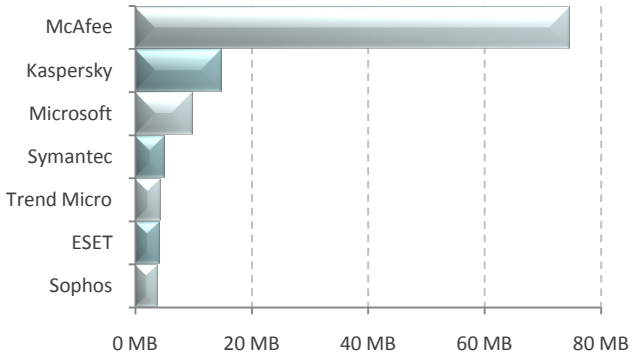



## Daily network traffic

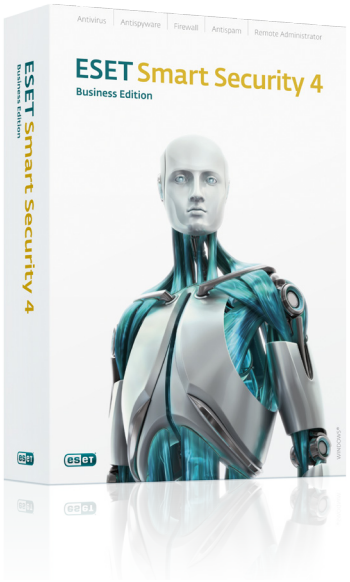
***Minimize impact on the coporate network***

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 and is calculated as an average of sixteen (16) days of data.*



# ESET Smart Security Business Edition




## Review Summary

| | |
|---|---|
| **Overall Rating** | 4.5 |
| Installation & Configuration | 4 |
| Migration | 4.5 |
| Default Policies | 4.5 |
| Client Installation | 4 |
| Interface Design | 4 |
| Client & Policy Management | 5 |
| Remote Management | 4.5 |
| Updates | 4 |
| Common Use Cases | 5 |
| Effectiveness | 5 |
| Performance | 4.5 |

- Very little system impact on endpoint machines. Fastest, best overall performance.
- Low traffic overhead for updates (3-4MB per day on average)
- Flexibly manage older versions and variants of ESET client solutions from a single, compatible console.
- Endpoints can be automatically sorted into parametric groups as they join the network.
- Signature updates are transportable.
- Mirror server is not automatically created during a typical installation.
- Remote Administrator Console interface is functional, rather than aesthetically appealing.

## Installation and Configuration 4/5

Installing ESET Remote Administrator Server and Console, the management components of ESET Smart Security 4 Business Edition, was a relatively fast and streamlined process. It took approximately an hour to complete the installation, updates and basic configuration of management components.

The typical Administrator Server installation required very little input from the user, seamlessly installing all needed components including the embedded Access JET database. ESET Remote Administrator Server also supports other databases such as SQL Server, Oracle and MySQL, and can automate the creation of an empty database for use where an “Advanced” installation is selected. During installation, administrators can set security passwords but this step is entirely optional and passwords may be configured at a later stage. After installing the Remote Administrator Server, installing the Remote Administrator Console took under ten minutes to install.

The ESET Smart Security Business Edition Basic Setup guide was extremely user-focused. The guide gave step-by-step instructions for users from purchase and download to installation and configuration, and even included estimated times for completion of each phase. The guide also provided useful tips for less technical users. ESET also provides a comprehensive User Guide which documents custom installations and more advanced product functionality.

## Migration from Previous Solutions 4.5/5

The removal of third party software prior to ESET client deployment can be performed through the ESET Remote Administrator Console via a push installation. Administrators will first need to download the relevant third party removal tool from a list of links provided by ESET, before creating a custom package for push installation.

Some versions of ESET clients are automatically upgraded by the Remote Administrator. In all cases, the Remote Administrator Console can manage most different types and versions of ESET security software, making it unnecessary to remove or upgrade existing ESET client software.

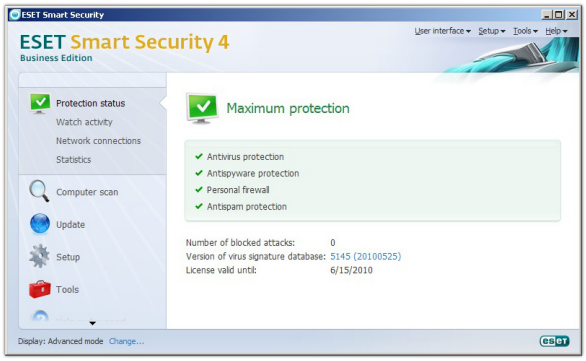
Upgrading to a new version of ESET Remote Administrator is easy. Administrators can simply install the latest version of Remote Administrator and the existing database and settings will be automatically migrated. For businesses with specific upgrade or migration needs, ESET also provides a “Rip and Replace” service for North American customers.

## Default Policies 4.5/5

Default policies are created during the Remote Administrator installation and generally provide a good balance for most deployments.

The Basic Setup guide gives some starting points to assist in moving away from default settings, such as the disabling of nonessential notifications for endpoint machines.

## Client Install 4/5




*Screenshot 1: ESET Smart Security 4 Business Edition (Client)*

The Basic Setup guide provides a checklist of items to confirm prior to installation. In our case, the only configuration change needed to start remote installation was the enabling of the Remote Registry service on the endpoint machine.

After pre-requisites are met, administrators can browse to the Remote Install tab and create an ESET Security Products installation package. Package creation is reasonably fast, taking around five minutes to configure and create by the management server. Once correctly set up, a single package can be used to remotely install to both 32-bit and 64-bit endpoint systems.

Administrators can also use Remote Administrator to flexibly deploy any custom install package, even non-ESET applications, as long as the installer is a .msi file.

Target systems can be discovered via NetBIOS, IP search or through existing Active Directory infrastructure. Once initiated, the client module took roughly ten minutes to install and update on the endpoint machine. No machine restart was required for functional protection.

For larger deployments, client installation can be performed through Windows Group Policy Management. This procedure is well-documented in the User Guide.

## Interface Design 4/5

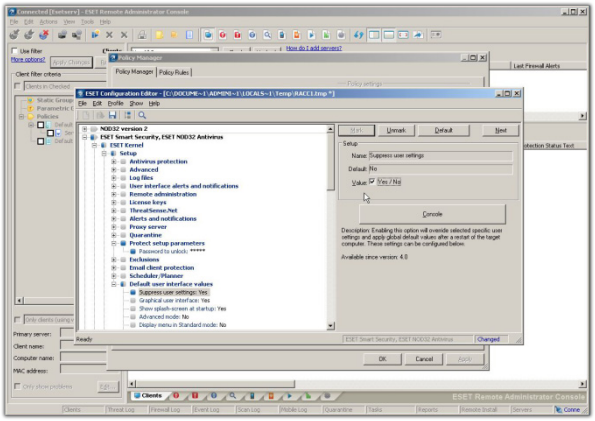
The Remote Administrator console is designed to appear similar in format to many familiar Windows applications. Unfortunately, this means the console interface is a bit bland and grey, with an emphasis on functionality rather than aesthetics.

Major functions can be accessed from categories of tabs or from the large menu buttons across the top of the interface. Navigating from the interface was extremely responsive, taking a fraction of a second to navigate between windows and menus.

An endpoint status dashboard can be viewed from the Clients tab, with conditionally formatted panels providing a quick indication about warnings, errors or alerts for each endpoint machine.

## Client and Policy Management 5/5

Endpoint machines can be arranged into groups manually or dynamically added to user-defined parametric groups when certain conditions are met. Parametric groups are extremely powerful, automatically assigning policies to clients as they connect to servers, or for filtering and reporting under certain conditions. Businesses with existing group infrastructure, such as Active Directory, can also make use of the Policy Rules Wizard to create user-defined rules and automate the mapping of policies to existing groups and objects.



*Screenshot 2: ESET Remote Administrator Console (Server)*

The propagation of policy changes is not immediate, but clients will update and enforce policies on the next connection to the server. Should an administrator need to revert to default policies, they can simply click on the “Default” button from the policy manager.

The Remote Administrator console is highly compatible with most variants and legacy versions of ESET security products, all of which can be managed

simultaneously from a single platform. The flexibility of the Remote Administrator Console caters well to scenarios where client upgrades may not be possible.

All policies can be imported or exported in an XML format for backup or duplication purposes.

## Remote Management 4.5/5

Where installed on a terminal, the Remote Administrator Console (RAC) allows for fully functional remote management of server modules. No additional configuration from the management server is required for remote access. If the default settings are selected for the management server installation, accessing the management server will not require a password. ESET strongly recommends that users set a secure password in their installation guides.

## Updates 4/5

Basic server configuration included the setup of the mirror server from which endpoint machines will retrieve signature updates. While the process was simple, well-documented and requiring only a few minutes, other products we tested automated the creation of an update repository during the installation process.

Administrators are initially required to enter their username and password details in order to access the ESET Update Servers. These details are remembered by the management server for future repository updates.

All signature files downloaded by ESET Smart Security are transportable and able to be manually moved between machines where required. This feature is advantageous for administrators managing machines on isolated networks.

## Effectiveness 5/5

AV Comparatives awarded ESET NOD32 Antivirus (v4.0.474.0) the **ADVANCED+** rank in their latest On-Demand Comparative, citing very few false positives and a total detection rate of 97.7%.

The most recent Summary Report (2009) from AV Comparatives noted that ESET has high detection rates, a very good heuristics engine and low system impact. Overall, this report awarded the ESET engine third place out of 16 products.

Impressively, ESET is the only security vendor to have an unbroken record of **ADVANCED+** rankings in the Retrospective/Proactive Test from AV Comparatives. ESET has been awarded a total of 13 **ADVANCED+** rankings since AV Comparatives began testing in February 2004, which is the maximum amount of ratings possible out of 13 reports and the most highly awarded vendor in this category.

Overall, ESET products have had a total of 62 successes with only three misses since their inclusion in VB100 testing. Its flagship product was tested since May 1998 and has the most consecutive awards in VB100 testing, with the highest success rate of **97%**.

## Common Use Cases 5/5

| Task | Ease of Use | Details |
|---|---|---|
| Conducting an 'on-demand' scan of selected endpoints | **Simple** | The on-demand scan is one of several preset tasks in the Remote Administrator Console. It can be accessed from the Clients tab by selecting New Task. |
| Creating and viewing a malware report 'on-demand' | **Simple** | Malware reports are accessed from under the Reports tab, and can be customized with filters for target clients or threats. By default, an HTML report is generated. |
| Creating, assigning and deploying a new policy | **Simple** | The Policy Rules wizard walks administrators through policy creation. This can be accessed by right-clicking on the Policies heading. |

# Kaspersky Business Space Security


## Review Summary

| | |
|---|---|
| **Overall Rating** | 4 |
| Installation & Configuration | 3.5 |
| Migration | 4.5 |
| Default Policies | 4 |
| Client Installation | 4.5 |
| Interface Design | 4.5 |
| Policy Management | 4 |
| Remote Management | 4.5 |
| Updates | 2.5 |
| Common Use Cases | 5 |
| Effectiveness | 4.5 |
| Performance | 4 |

- Low system impact on endpoint machines, relatively good performance.
- Relatively high amounts of traffic generated by server repository updates.
- User-focused interface provides good feedback for task status and progression.
- Mobile policies offer flexible management based on endpoint status.
- Initial server repository update may be slow to perform.
- Relatively time-consuming to deploy clients across the network.

## Installation and Configuration 3.5/5

The typical installation, configuration and update process for management components of Kaspersky Business Space Security took roughly two to three hours. Within a few screens of initiating the Administration Kit installer, it detected that Microsoft .NET Framework 2.0 was not installed and prompted to install it as a pre-requisite. Agreeing to install the missing component launched the .NET Framework installer and closed the Kaspersky Administration Kit wizard. After installing .NET, the Administration Kit installer needed to be manually restarted for the installation process to continue.

The installation process proceeded without any issue after this minor disruption. Though it is not integrated into the installer, the Administration Kit installer wizard successfully initiated the installation of SQL Server 2005 Express Edition with default settings.

The Quick Start wizard appears straight after installation, prompting for a key file to enable product evaluation. The wizard created default tasks and policies before initiating the update process for the Administration server.

Kaspersky offers four technical guides documenting the installation and use of Business Space Security. The content in the guides lacked definition with some content duplicated across guides. The need to cross-reference between guides occasionally made it challenging to locate information on a specific topic. Generally, we found that the Quick Start guide was concise, but oversimplified the process in some areas.

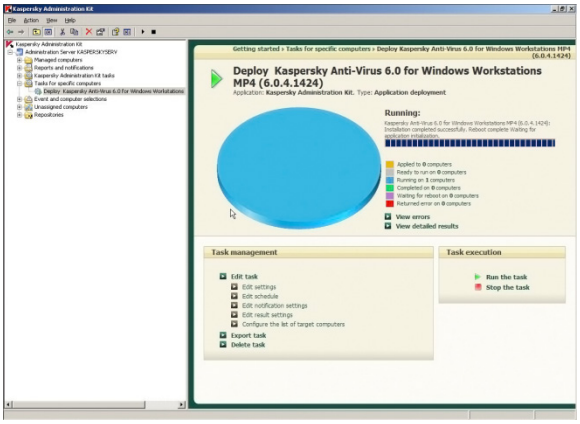
## Migration from Previous Solutions 4.5/5

Migration from version 6 or higher to the current version of the Administration Kit is reasonably simple compared to some products. Administrators need to back up the existing database using the provided utility from Kaspersky, and all previous settings and data from the previous version will be migrated on installation. In this case, the installation will simply upgrade the Administration Kit component without the need to uninstall.

Client software migration is also simple, with existing versions or variants of Kaspersky client products automatically uninstalled during client installation. Administrators can choose to automatically remove third party security or other incompatible software prior to installing the Kaspersky client using the Deployment Wizard.

## Default Policies 4/5

Two default policies profiles are created by the Quick Start wizard after installation, one for Windows Servers and the other for Windows Workstations. The default policies cater well to each of the needs of both machine roles, with balanced security settings and pre-defined alert levels for types of events.




*Screenshot 3: Kaspersky Administration Kit (Server)*

## Client Install 4/5

The deployment wizard appears after the Quick Start wizard, making it simple to get started deploying the client software for even the least prepared individual.

Out of all tested products, Kaspersky provided the best administrator feedback for the client installation process. The Administration Kit displayed the status of installation in 'real time', with a pie chart showing the status of endpoints and a progress bar. A few minutes later, it was discovered that the reporting mechanism may not be entirely accurate, as the status of the task took 25 minutes to move from the "Waiting for Application Initialization" to the "Completed" status, despite client deployment appearing fully functional on the endpoint machine. Regardless of this potential flaw, it was a welcome change to have feedback about client progress.

The deployment wizard also provided the flexibility to add non-Kaspersky applications for deployment, and options for background installation and automated machine restarts where required. The installation of the Kaspersky client took approximately fifteen minutes and required the endpoint machine to be restarted to finalize the installation.

## Interface Design 4.5/5

The Administration Kit interface is relatively intuitive, with a directory tree on the left –providing access to major areas of functionality and a display pane which closely resembles a web-interface with organized sections of information.

The dashboard is displayed after logging into the Administration Kit. The overall health status of the network is indicated by red, amber and green traffic symbols over several security categories. More specific information about the status of individual endpoints can be retrieved as a report. Reports are flexible and able to be generated quickly, making use of pie and bar charts to increase readability.

The progress and status of deployed tasks is well presented, and generally appears to update in real-time. At the conclusion of tasks, status is clearly marked with a large tick or cross symbol.

## Client and Policy Management 4/5

The Administration Kit provides some options for partially automating policy management, for example, policies can be configured to automatically activate upon a "Virus Outbreak". Unfortunately, these policies will need to be manually reverted back to original policies by administrators when more secure settings are no longer required.

Protection policies for Windows workstations can be delegated the "Mobile Policy" status. These policy settings will be enforced when any computer affected by the policy is disconnected from the server.

Generally, policies are propagated instantly to the client. Administrators can also view the results and status of policy enforcement by viewing a policy's properties. Polices can be duplicated, imported or exported to a file in KLP format.

## Remote Management 4.5/5

The Kaspersky Administration Kit console can connect remotely to any Kaspersky Management Servers on the network. Once connected, the console provides full functionality in managing endpoints and policy.

The console appears to be a customized version of the Microsoft Management Console, offering server connection/disconnection functionality which is unique to Kaspersky Administration Kit.

## Updates 2.5/5

Initially downloading updates to the Server Repository took more than two hours. Fortunately, administrators are able to proceed through installation while downloading server updates in the background.


*Screenshot 4: Kaspersky Anti-Virus 6.0 (Client)*

The Kaspersky client solution took approximately 20 minutes to update and, somewhat perplexingly, opted to download the updates from the Kaspersky update servers by default instead of the up-to-date management server repository. Further investigation revealed that the creation of an update task was required for clients to retrieve update from the central repository.

## Effectiveness 4.5/5

The most recent On-Demand Comparative from AV Comparatives awarded Kaspersky Anti-virus (v9.0.0.736) the **ADVANCED+** rank, noting a low number of false positives and a total detection rate of 97.1%.

The latest Summary Report (2009) from AV Comparatives noted that Kaspersky had very good heuristics, good detection rates and many protection features, awarding the engine second place out of 16 products.

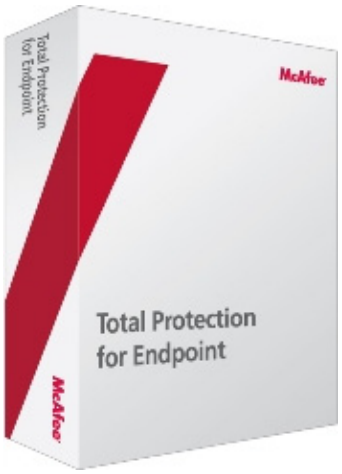
Kaspersky Anti-virus further attained an **ADVANCED+** ranking in the June 2010 Retrospective/ProActive Test report. Since February 2004, Kaspersky has attained a total of seven **ADVANCED+** ratings, making it the second most awarded vendor in this category.

Kaspersky has passed the VB100 test 54 times and missed 18 times, resulting in a **75%** success rate for all products entered. The most recent failure was by Kaspersky Antivirus in April 2010 due to a missed In-the-Wild virus.

## Common Use Cases 5/5

| Task | Ease of Use | Details |
|---|---|---|
| Conducting an 'on-demand' scan of selected endpoints | **Simple** | A Virus Scan group task is automatically created by the Quick Start wizard for use in on-demand scanning. This task is accessible from under Managed Computers heading. |
| Creating and viewing a malware report 'on-demand' | **Simple** | Malware reports are accessible from under the Reports and Notifications heading. Reports can be generate "on-the-fly" and viewed from the Administration Kit. |
| Creating, assigning and deploying a new policy | **Simple** | The New Policy wizard walks administrators through policy creation. This can be accessed by right-clicking on the Policies heading. |

# McAfee Total Protection for Endpoint




## Review Summary

| | |
|---|---|
| Overall Rating | 3.5 |
| Installation & Configuration | 3 |
| Migration | 2 |
| Default Policies | 3.5 |
| Client Installation | 3 |
| Interface Design | 3.5 |
| Policy Management | 5 |
| Remote Management | 4.5 |
| Updates | 4 |
| Common Use Cases | 3 |
| Effectiveness | 3.5 |
| Performance | 2.5 |

- Moderate system impact on endpoint machines with average performance.
- Highest amount of traffic generated by update client out of all tested products.
- Initial server task and policy configuration is not straightforward and requires patience or experience.
- A powerful and granular policy management solution intended for use by large enterprises and more experienced administrators.

## Installation and Configuration 3.5/5

The total time needed to perform installation, updating and the basic configuration of the McAfee Total Protection for Endpoint and ePolicy Orchestrator was approximately two hours. Generally, the installation proceeded well and without much hassle, with the most time consuming aspect proving to be task and policy configuration prior to client deployment.

Conveniently, the ePolicy Orchestrator installer did not require a key to install the evaluation version of the software. The default installation automated the installation of Microsoft SQL 2005 Express including its pre-requisites, MSXML Parser, Microsoft .NET Framework and MS Visual C++ 2005. All component installations were integrated and executed in order as part of the McAfee ePolicy Orchestrator installer. This component of installation was a bit slow, taking over half an hour to complete.

At the conclusion of installation, administrators can opt to launch ePolicy Orchestrator immediately from the final prompt. We observed that the initial launch of ePolicy Orchestrator from this prompt appeared to crash the web application. Closing and restarting the browser instance manually fixed the issue.

The Evaluation Guide provided accurate, step-by-step instructions interspersed with technical notes. Conversely, the Quick Overview Guide appeared to be a high level marketing document rather than the expected “Quick Start” guide.

## Migration from Previous Solutions 2/5

The procedure to upgrade or migrate to the latest version of ePolicy Orchestrator is not documented anywhere in official guides or in the McAfee Corporate Knowledgebase.

The ePolicy Orchestrator product guide included a few sentences about server tasks which appear to be used in migrating historical data (such as Host IPS Policy Migration, Event Migration), but provided no further information on the migration process.

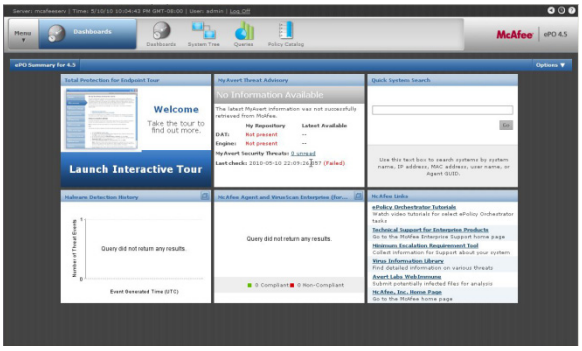
On the client-side, McAfee VirusScan Enterprise will check for and attempt to remove existing third party security software on client machines by invoking software removal through Windows. McAfee VirusScan will also automatically remove older versions and types of McAfee client solutions prior to installation. While this migration functionality is well-documented in the Evaluation guide, it is not referred to or explained during the client deployment process via ePolicy Orchestrator.

## Default Policies 3.5/5

Some default policies created on installation are on the more restrictive side of the security spectrum. Until they are changed, these restrictive policies may impact some business functions and endpoint users.

Fortunately, the Evaluation Guide suggests some reasonable policy changes which can be made to improve default policies, such as making the default e-mail policy less restrictive by turning off the e-mail port blocking rule for e-mail servers.

Other policies required further configuration to ensure balanced security, such as adding a password to secure the client console from tampering.




*Screenshot 5: McAfee ePolicy Orchestrator (Server)*

## Client Install 3/5

Setting up the ePolicy Orchestrator to deploy McAfee client software to endpoint machines is initially complex, especially for administrators who are unfamiliar with ePolicy Orchestrator. However, after the procedure has been correctly set up, the process becomes more or less automated for unmanaged machines.

Unmanaged endpoints must first be organized into groups in the system tree. Administrators may opt to perform this task manually at first, or configure criteria-based filtering to automatically sort discovered endpoints into groups.

The administrator must then create a custom product deployment task which specifies products to be deployed to endpoints. This task will be executed by the McAfee Agent after it is deployed to endpoints and commences policy enforcement. With the exception of Microsoft Forefront, this is the only product that requires additional tasks or policies to be created in order to install a client product. The task then needs to be applied via policy to selected groups or endpoints.

The deployment of McAfee Agent and the subsequent installation of modules took roughly fifteen minutes to install and update.

## Interface Design 3.5/5

Overall, the ePolicy Orchestrator web interface is polished and well-designed. The product is ideal for international use, as the administrator may select from one of ten language choices from the ePolicy Orchestrator login page without needing to download additional components. After logon, administrators are presented with a dashboard showing network status using charts and quick links to relevant security categories. The dashboard can be customized according to preferences using premade monitors, or through user-defined database queries.

The user interface is relatively responsive and stable for a web interface, pausing for a mere second or two while navigating between categories. In contrast, the help files for ePolicy Orchestrator appeared somewhat slow to browse or search through.

Major functions can be accessed from the menu button on the top left, with each category item represented by an easily recognized, unique icon.

## Client and Policy Management 5/5

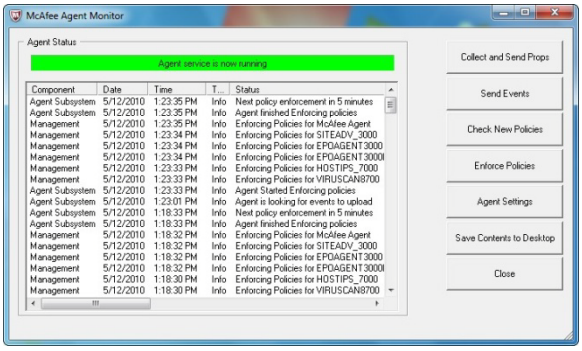
While initial policy and task configuration may prove daunting for less experienced administrators, McAfee Total Protection for Endpoint is able to automate client sorting and policy mapping after correct configuration.

ePolicy Orchestrator is able to sort discovered endpoints into groups and subgroups in the system tree using an algorithm. This algorithm is based on criteria such as the IP address range and tags defined by users. Policies control is granular, with administrators able to control security behavior to a fine level using a myriad of settings for each component. Compared to other reviewed products, the depth of control over components is impressive and likely to be more suitable for experienced administrators managing larger deployments.

A feature that is unique to ePolicy Orchestrator is its ability to open “issues” as a response to virus security, monitoring or other events. Issues can then be manually or automatically assigned to different remote users, who manage the issue by opening, re-assigning or closing tickets.

## Remote Management 4.5/5

ePolicy Orchestrator is easy to access remotely from any terminal via the web interface. All management functionality is available from the web interface without additional configuration from the browser or ActiveX downloads.




*Screenshot 6: McAfee Agent Monitor (Client)*

Accessing the management server remotely is smooth and responsive, with the interface able to navigate between functions or retrieve data relatively quickly.

## Updates 4/5

Repository and client updates are simple to configure and manage from ePolicy Orchestrator.

The "Update Master Repository" task is created during the installation of ePolicy Orchestrator, which schedules the download of repository updates daily by default. The client task "Update Client Protection" is also set up during installation and checks for downloads once a day with randomization in place to minimize network impact. While these default settings make a reasonable amount of sense for very large deployments, administrators managing smaller deployments should seriously consider configuring more frequent updates to ensure comprehensive protection.

The initial update of the McAfee client software from the ePolicy Orchestrator server was conducted manually from the client machine. The process was quick, taking roughly three minutes to complete.

Systems which are temporarily disconnected from the network are still able to run their update tasks, but retrieve updates from the McAfee Update Server rather than the ePolicy Orchestrator Server.

## Effectiveness 3.5/5

The most recent On-Demand Comparative from AV Comparatives awarded McAfee AntiVirus (v14.0.306) the **ADVANCED** rank, noting a high number of false positives but a total detection rate of 98.9%.

The latest Summary Report (2009) from AV Comparatives reiterates these findings, noting very high malware detection rates but unfortunately a high number of false positives.

The latest Retroactive/ProActive Test awarded McAfee Antivirus with a **STANDARD** ranking. To date, McAfee has been awarded the **ADVANCED+** rating two times since February 2004.

McAfee has passed the VB100 test 48 times and missed 21 times, attaining an overall **70%** success rate. In three of these tests, McAfee has entered two products and placed #6 out of 7 reviewed products in this report.

## Common Use Cases 3/5

| Task | Ease of Use | Details |
|---|---|---|
| Conducting an 'on-demand' scan of selected endpoints | **Moderate** | Administrators can edit the default On-Demand Scan task to scan all endpoints, or endpoints with certain criteria. The schedule must be set to "Run immediately", and there isn't much feedback on the status of the task. After the scan task has been issued, administrators may wish to change this task back to default settings. |
| Creating and viewing a malware report 'on-demand' | **Moderate** | Reports are run from Queries, there are several dozen default queries which may be edited or run. Reports are generated and viewed from ePolicy Orchestrator. |
| Creating, assigning and deploying a new policy | **Moderate** | Policies can be created from the Policy Catalog or through the System Tree. The depth of configuration makes selecting desired configuration settings and assigning a policy somewhat complex. |

# Microsoft Forefront Client Security


## Review Summary

| | |
|---|---|
| **Overall Rating** | 2 |
| Installation & Configuration | 1 |
| Migration | 1 |
| Default Policies | 2 |
| Client Installation | 1 |
| Interface Design | 2.5 |
| Policy Management | 1.5 |
| Remote Management | -- |
| Updates | 2 |
| Common Use Cases | 2 |
| Effectiveness | 4 |
| Performance | 2 |

- Relatively high system impact on endpoint machines, below average performance.
- Relatively high amounts of traffic generated by server updates.
- Convoluted installation, configuration and client deployment may challenge even experienced administrators.
- Troubleshooting is time-consuming as a result of independent error logging by each component.
- Limited ability to perform on-demand tasks from the Management Server.

## Installation and Configuration 1/5

A typical, single-server installation of Microsoft Forefront Client Security took more than a day to complete. The installation was challenging and convoluted, with a successful installation relying upon deep knowledge of and experience with a variety of Windows server components. Overall, installing and configuring Microsoft Forefront was the least user-friendly experience of all software reviewed.

As an exception to the relatively neat and self-contained installers from other security vendors, the Microsoft Forefront installer came in two parts with the main installer provided on an ISO image, which needed to be transferred to a CD prior to installation. The product update to Forefront SP1 was provided as a separate executable.

Microsoft Forefront did not install any pre-requisites, instead requiring all necessary components to be researched, separately downloaded and installed in advance. Microsoft Forefront had the largest number of pre-requisites necessary for installation, some of which required other pre-requisites to be downloaded and installed.

It appeared to be possible to install Forefront without necessary Windows components (such as the Windows Server Update Services), resulting in a partially functional installation.

Documentation for Forefront was provided online from Microsoft TechNet. Documentation was average and, at worst, unhelpful. Occasionally, support articles would omit important steps or details in the installation and configuration process.

## Migration from Previous Solutions 1/5

No documentation was provided from Microsoft TechNet in regards to migration from older versions of Forefront, or from third party security solutions. Some documentation is available describing the removal of an existing installation, or the migration process between different operating systems or server topologies.

The limited, migration procedures which are documented appear awkward, comprising of many steps of manual configuration or application removal in a strict order, depending on your current topology or configuration. Some steps required the performing of low level system tasks, such as manually observing or altering values in system registry.

## Default Policies 2/5

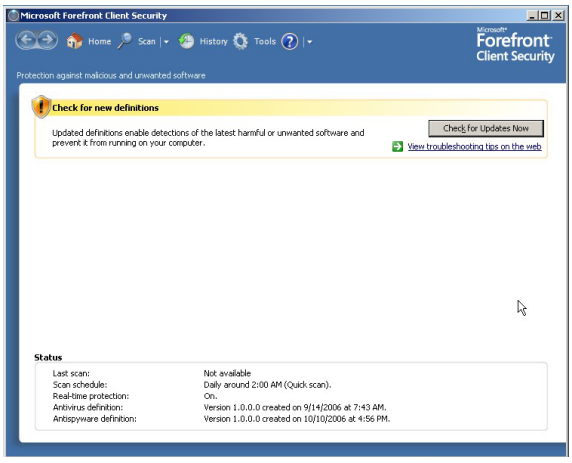
Default policies are not automatically generated by the installation of Microsoft Forefront Client Security.

A policy with default settings needs to be created by navigating to the Policy Management tab and selecting "New" under Policy. If deployed, the default policy provides endpoint machines with real-time malware protection, and scheduled vulnerability and malware scans.

## Client Installation 1/5

Forefront Client Security supports remote deployment to clients via several independent Windows components and services. Administrators are required to create and deploy policies to initiate the installation of the client solution. Some of the components involved in client installation, configuration and updating include the WSUS (Windows Server Update Services) or SMS (System Management Server), the GPMC (Group Policy Management Console), GPO (Group Policy Objects) and the MOM (Microsoft Operations Manager).

The disadvantages of a deployment process which relies on so many different components became evident during our testing. Error reporting lacked integration and clarity, with each component making use of an independent error logging system and output location. Any single issue with client deployment may involve a number of different modules; documentation for which was scattered over different areas of the Microsoft TechNet Library.



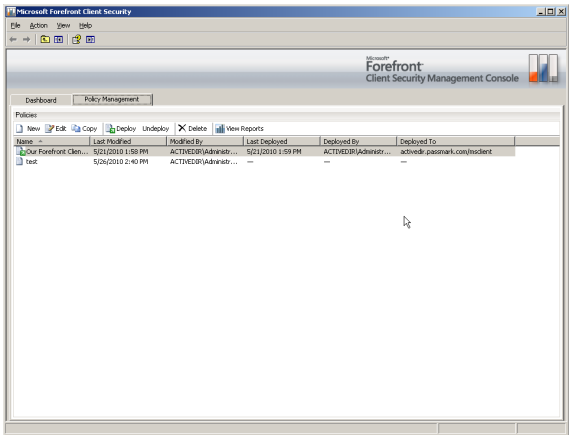

*Screenshot 7: Microsoft Forefront Client Security (Client)*

The installation procedure may be more familiar for an administrator who is extremely experienced with Windows modules involved, but some of the "common components" have special rules and exceptions which would seem to defeat the purpose of such a design. For example, servers with an existing MOM infrastructure cannot use the existing infrastructure for Forefront but instead will need to obtain a customized version of MOM for this purpose.

## Interface Design 2.5/5

The interface for the Microsoft Client Security console lacks many functions seen in other security solutions, and appears to be very minimalistic. The simplicity of the console does not assist administrators in managing the underlying complexity of components.

The interface uses the Microsoft Management Console framework, with two tabs enabling access to the Dashboard and Policy Management in the display pane. The dashboard provides links to Summary Reports and a list of issues affecting endpoints.




*Screenshot 8: Microsoft Forefront Security Console (Server)*

## Client and Policy Management 1.5/5

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.

## Remote Management 0/5

Microsoft Forefront Client Security does not appear to support Remote Management. If remote management is supported, it has not been documented in Forefront Client Security help files or the TechNet Library. Other products in the Microsoft Forefront range such as Forefront Threat Management Gateway document support remote management.

It's possible that Microsoft documentation authors assumed that administrators would make use of existing remote desktop infrastructure to remotely access their Forefront Client Security server. While most modern servers will already have Remote Desktop services implemented for other purposes, the Microsoft TechNet library should at least document the possibility of using it for remote management.

## Updates 2/5

In order to delegate the management server as a central repository for scheduled Forefront Client Security updates, the Windows Server Update Services (WSUS) component must be installed. However, since client synchronization is staggered across the network, it is difficult to predict when specific clients will update with the latest definitions and upgrades. For this reason, the distribution of virus definition updates and scan engine updates to client machines is difficult to perform on-demand from the management server.

The client component of Forefront Client Security has a button which users can click to manually "Update now". However, clicking on this button provides no functional response. This issue was resolved by manually downloading the first update from Microsoft Update. As the first update forms part of the deployment process, this is a further troubling issue caused by Microsoft Forefront's reliance on independent components.

## Effectiveness 4/5

The most recent On-Demand Comparative from AV Comparatives awarded Microsoft Business Essentials (v1.0.1611.0) the **ADVANCED** rank, noting very few false positives and a total detection rate of 96.3%.

The latest Summary Report (2009) from AV Comparatives notes that Microsoft has high proactive detection rates and good removal capabilities.

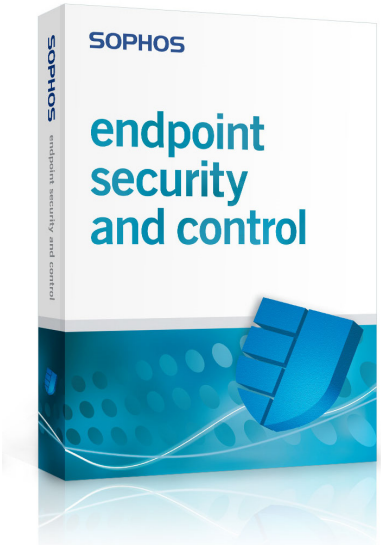
The latest Retroactive/ProActive Test report gives Microsoft Business Essentials the **ADVANCED+** rating. To date, Microsoft has received three **ADVANCED+** awards, making it the third most awarded vendor in our testing overall.

Microsoft's score in VB100 testing including all their products is 17 successes and two misses giving them an **89%** success rate, though it entered one test with two products. Out of all reviewed products, Microsoft has achieved second place in VB100 testing.

## Common Use Cases 3/5

| Task | Ease of Use | Details |
|---|---|---|
| Conducting an 'on-demand' scan of selected endpoints | **Moderate** | Administrators can click the "Scan Now" button to conduct an on-demand scan. Only two options are provided for targets, either all managed computers are scanned or a single target computer is scanned. Administrators can, however, choose between Quick and Full scans. |
| Creating and viewing a malware report 'on-demand' | **Simple** | Administrators can create and view a malware report from the dashboard which provides a list of report links. The reports are generated in HTML by default. |
| Creating, assigning and deploying a new policy | **Complex** | Creating, assigning and deploying a new policy can be accomplished from the "Policy Management" tab. Enforcement of the policy may or may not occur at the scheduled interval, administrators may need to refer to logs to ensure policy has deployed correctly. |

# Sophos Endpoint Security and Data Protection




## Review Summary

| | |
|---|---|
| Overall Rating | ★★★ |
| Installation & Configuration | ★★★½ |
| Migration | ★★★★★ |
| Default Policies | ★★★½ |
| Client Installation | ★★★ |
| Interface Design | ★½ |
| Policy Management | ★★★ |
| Remote Management | ★★★★ |
| Updates | ★½ |
| Common Use Cases | ★★★½ |
| Effectiveness | ★★★½ |
| Performance | ★★★ |

- Moderate system impact on endpoint machines. Good performance in some areas, poor performance in others.
- Migration process from legacy variants and third party solutions is well-documented and straightforward.
- Updating the server repository can be problematic.
- Some default policies are visibly restrictive, and may disrupt business functions if not changed.
- Technical documentation is organized into nine separate technical guides.

## Installation and Configuration 3.5/5

A 'complete' server installation of the management components in Sophos Endpoint Security and Data Protection took roughly two to three hours to complete. While the installation itself was straightforward, updating the server repository took a significant amount of time due to unexplained timeouts from the Sophos update server.

After file extraction, the Enterprise Console installer detected that the Microsoft .NET Framework was missing and prompted for its installation as a pre-requisite. Clicking "Yes" activated the Microsoft installer for .NET Framework while the Enterprise Console installer paused in the background. This was also the case for the MS XML and SQL Server Setup, with the Enterprise Console installer guiding the installation process by initiating necessary installers. At the conclusion of installation, Enterprise Console required us to log out of Windows to complete the process.

Sophos provides nine separate technical guides documenting the installation and use of Endpoint Security and Data Protection. While the advanced guides were useful and comprehensive, the sheer number of guides made referencing information beyond the brevity of instructions in the Quick Startup Guide clumsy and difficult.

## Migration from Previous Solutions 5/5

The migration process is very straightforward and well-documented. Sophos offers two guides which document the upgrade process; the Quick Upgrade Guide describes the upgrade procedure from a single-server scenario while the Advanced Guide covers more complex implementations.

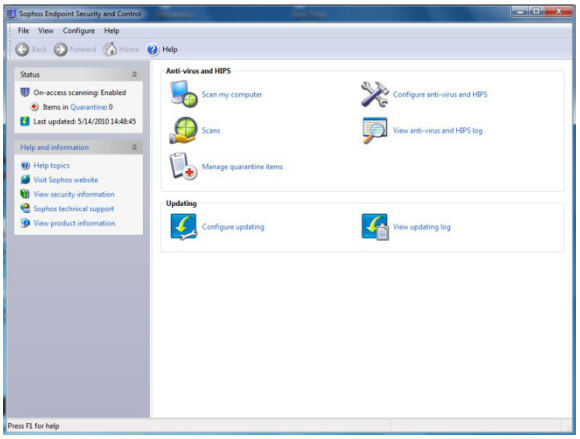
In a typical installation, Sophos recommends backing up database components prior to migrating from a supported variant of Sophos. Installation packages for different components requiring upgrades can be downloaded and activated much like a clean installation. All previous settings, computer groups and policies will be detected by the installation wizard and remain unchanged in the new installation.

Where selected during client deployment, the Sophos Endpoint Security can automate the removal third party security software where it is discovered on endpoints. By default, the client solution uses a standard removal tool, but a non-standard removal tool is also provided which supports the removal of more third party software than the standard tool. The non-standard tool requires user configuration prior to use. The removal process is documented in the Third Party Security Software Removal Guide.

## Default Policies 3.5/5

Where the firewall component is installed on target machines, the default settings are visibly restrictive with a heavy impact on network connectivity for endpoints. Default firewall policies block all non-essential connections, which include most inbound and outbound connections. Thankfully, Sophos advises administrators about the restrictiveness of the firewall policy in the Advanced Startup Guide.

Otherwise, default policies make sense and provide reasonable protection for most managed networks. Some of the more specialized security management and compliance features are disabled by default, such as data control, device control and application control.



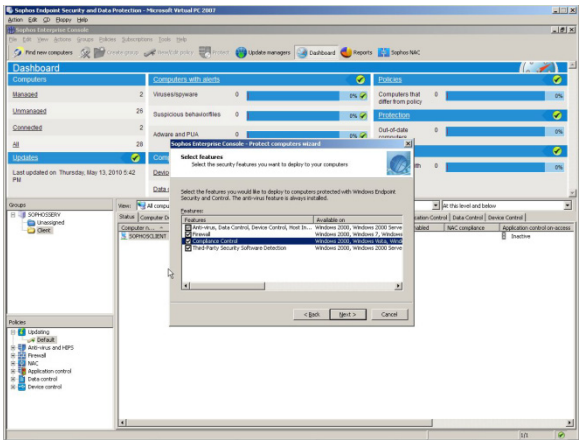

*Screenshot 9: Sophos Endpoint Security and Control (Client)*

## Client Install 3/5

Our client installation experience was indicative of the problems associated with providing nine separate technical guides for users. After referencing the Quick Start Guide, we initially attempted to deploy the client via network installation. Client installation failed twice without a resulting error message and we referred to the Troubleshooting Guide without much luck. Finally, referring to the Advanced Startup Guide revealed that enabling the Remote Registry service on the endpoint machine was required to deploy over the network. Unfortunately, this pre-requisite was not mentioned in the Quick Start Guide, which is likely to be the first place administrators will look.

The Protect Computers wizard guided us through the rest of the installation process, giving a choice of components to install on target endpoints. The installation over the network was fast, taking less than five minutes for a silent installation. After installation, the client automatically updated without manual intervention, after which the server indicated that the endpoint required a restart for updates to become effective.

## Interface Design 3.5/5




*Screenshot 10: Sophos Enterprise Console (Server)*

The Enterprise Console appears to have been designed with practicality in mind. The dashboard is a consistent element of the interface, enabling the administrator to monitor network health regardless of the task being performed. The height of the dashboard can be adjusted where required.

The layout of the interface is straightforward. By default, administrators can check the status of security components of individual computers below the dashboard, or switch this view by clicking “Update Managers” to show software subscriptions. Group structure and policies are accessible to the left, arranged into tree directories.

Despite the available mechanisms for monitoring, there appeared to be no obvious way to check the status of on-demand scanning.

## Client and Policy Management 3/5

Client and policy management using Sophos Endpoint Security was easy to learn but ultimately lacked the depth of policy automation or location-based that some security products offered.

The only automated group management feature offered by the Enterprise Console was the Download Security Software wizard. When executed, this wizard could import and replicate existing domain infrastructure, automatically placing discovered computers into groups. Otherwise, administrators can find new computers via Active Directory, network or IP range.

Without importing existing Active Directory structure, there is currently no method to automate the filtering of discovered endpoints into groups

with defined policies. Unassigned computers need be manually dragged and dropped into groups.

## Remote Management 4/5

Remotely managing the Sophos server required some additional configuration through the existing Enterprise Console on the management server. The administrator needs to enable remote access on an account by adding it to the correct administrative groups.

After this, administrators should select a "custom" installation of the Management Console at the terminal from which they wish to remotely access the Sophos server. If the account is configured correctly with database access, the remote version of the Enterprise Console should have remote access to all management features.

## Updates 1.5/5

The initial update of the server repository as part of installation was problematic.

The Download Security software wizard dialog popped up after the initial launch of the Enterprise Console, prompting us to enter the key and password provided by Sophos to access the download server. Initially, the wizard was unable to connect to the Sophos update server after repeated attempts citing server timeouts. Based on feedback in the Sophos forum, we attempted to repair the Update Manager component using the installer which appeared to resolve the issue.

The initial update to the server repository was quite large, taking over an hour and 200MB of bandwidth.

At some point, the Download Security software prompt had reported an ambiguous error that it was unable to retrieve the update. The error message suggested that users wait for the next automatic download to complete the download. After closing the error message, the "Run the Download Security Software Wizard" item had vanished from the Actions menu and there appeared to be no way to manually retry the update.

Conversely, client updates were automatically downloaded after client installation and applied without issue.

## Effectiveness 3.5/5

The most recent On-Demand Comparative from AV Comparatives awarded Sophos Antivirus (v9.03) the **ADVANCED** rank, noting few false positives and total detection rate of 93.7%.

The latest Summary Report (2009) from AV Comparatives noted that Sophos had relatively good detection rates. We believe that, compared to other products, a detection rate of 93.7% is relatively low and mean that roughly one in twenty viruses may not be detected.

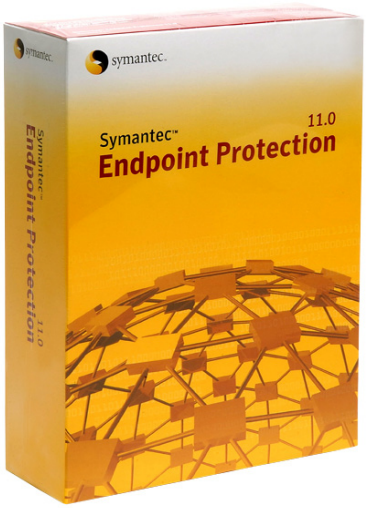
The Retroactive/ProActive Test in June 2010 awarded Sophos Anti-Virus with an **ADVANCED** rating. Sophos has not achieved an ADVANCED+ rating in this category to date.

Sophos has passed the VB100 test 52 times and missed 16 times, attaining an overall **77%** success rate. Since the first test in January 1998, Sophos has only entered one product into VB100 testing.

## Common Use Cases 3.5/5

| Task | Ease of Use | Details |
|---|---|---|
| Conducting an 'on-demand' scan of selected endpoints | **Moderate** | Administrators can right-click on target endpoints or groups to initiate a full system scan. The console provides no immediate feedback on performing this action. No choices on the depth of scanning. |
| Creating and viewing a malware report 'on-demand' on-demand | **Simple** | Clicking on the Reports action opens the Report Manager. To create a report on-demand, users can choose a report and select "Run" |
| Creating, assigning and deploying a new policy | **Simple** | Create a new policy by right-clicking on a security category and choosing "New". Double-click the new policy to activate the Policy Wizard and select new settings. |

# Symantec Endpoint Protection




## Review Summary

| | |
|---|---|
| **Overall Summary** | 4.0 |
| Installation & Configuration | 3.5 |
| Migration | 3.5 |
| Default Policies | 3.5 |
| Client Installation | 3.0 |
| Interface Design | 3.5 |
| Policy Management | 4.0 |
| Remote Management | 4.5 |
| Updates | 5.0 |
| Common Use Cases | 4.5 |
| Effectiveness | 5.0 |
| Performance | 4.0 |

- Below average system impact on endpoint machines.
- Moderate amounts of traffic generated by server repository updates.
- Malware detection rates were very highly rated by third party testing firms.
- Flexible policy management and deployment of endpoint clients and locations.
- Retrieving and distributing signature updates to endpoints is easy to setup.
- Manager Console user interface is somewhat sluggish.
- No support is provided for migrating from third party products.

## Installation and Configuration 3.5/5

Installing and configuring the management components of Symantec Endpoint Protection took roughly two hours from start to finish. The Symantec Endpoint Protection Manager installer required the server to have the IIS World Wide Web Publishing Service (WS3SVC) enabled, which was added as a Server Role from Windows Server Management.

We then manually restarted the Endpoint Protection Manager installer, and it guided us through the rest of the process without issue. Symantec Endpoint Protection did not even require the entering of a registration key to complete the installation. After installation, the Management Server Configuration Wizard created and set up an embedded database via an integrated installer.

After basic installation, administrators may choose to run the Migration and Deployment wizard or proceed directly to the Manager Console.

Overall, the documentation for the installation procedure was well-written, providing accurate step-by-step instructions regarding user options in each phase of installation, along with recommendations for typical installations.

## Migration from Previous Solutions 3.5/5

Migration from other versions or variants of Symantec products is reasonably well supported. Some of this is documented on the Symantec support website in high-level through FAQs and online presentations. The website gives administrators quick access to information about migration product paths, server “before and after” hierarchy snapshots, post and pre-migration tasks and some information about pricing.

A low level walkthrough of the migration process for the server is available in the Installation Guide. For compatible variants of older Symantec server software, the installation will detect the existing and export all existing settings during the installation of the new product version. It is not necessary to remove existing server components in this situation. Once the server has been upgraded, the server will automatically upgrade the endpoint machines using the AutoUpgrade function.

For organizations using an older version of Symantec Antivirus, existing groups and policies can be migrated using the Migration and Deployment wizard.

Unfortunately, no documentation or support is available for upgrading from third party products.

## Default Policies 3.5/5

Most protection features are enabled by default policies. Default protection of endpoints is balanced and intended to be 'silent' for endpoint users, for example, quarantined items on client machines will be repaired and restored where possible.

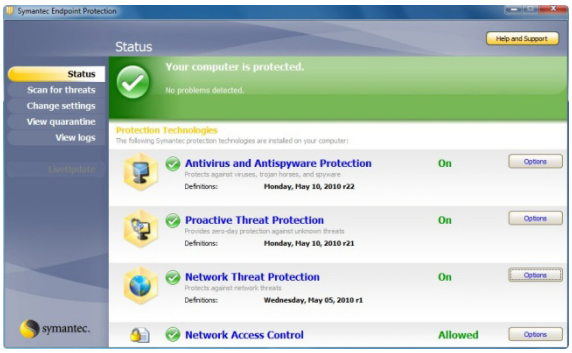
Default firewall policies are not overtly restrictive, with endpoint users able to access the internet and internal network as usual. The only policy areas where default policies are not created on installation is for Application and Device Control and Centralized Exceptions.

Administrators can choose from three preset policy profiles for Antivirus and Antispyware protection: balanced protection, high-performance protection or high-security protection. Balanced protection is enabled by default.

For new policies to be deployed to endpoint machines, the administrator must wait for the next network 'refresh' cycle, which pushes new policies to endpoints. We discovered that the default auto-refresh setting in Console Manager is set to "Never" by default. Until an administrator changes this default setting, new policies will not be downloaded and enforced on endpoint machines.

## Client Install 3/5

The Migration and Deployment wizard can create an installation package to deploy across the network, giving administrators a choice between either an 'unattended' or a silent installation.




*Screenshot 11: Symantec Endpoint Protection (Client)*

The names used for these two network deployment options can be confusing. When an 'unattended' installation is selected, the client software installer is visible on the endpoint machine, showing installation progress before prompting the endpoint user to restart the machine. Conversely, a silent installation progresses in the background with no restart prompt or end-user input required.

It takes under three minutes to create the installation package prior to deployment. After package creation, the Push Deployment Wizard allows discovery of unmanaged endpoints through NetBIOS, existing group structures such as Active Directory, IP address or host name. Unmanaged computers can also be discovered through the Manager Console by IP address or host name.

Some instability was encountered during the deployment of the client to the endpoint machine, where the remote deployment application (ClientRemote.exe) quietly crashed without providing any feedback to the administrator via the Troubleshooter log. This issue was resolved by restarting the management server.

Once deployed, the client package took roughly four minutes, requiring a machine restart to finalize the installation.

## Interface Design 3.5/5

The Symantec Endpoint Protection console is let down by its sluggishness and slow response times. Generally, it is slow to navigate around the interface, taking a few seconds to retrieve data or to move between categories and perform tasks. The initial load of a category is always the slowest, with subsequent accesses improving responsiveness. We believe that, despite appearing to be a Windows application, one possible explanation for the Manager Console's poor data retrieval speed is that it is using somewhat slower web technologies.

The tab categories are succinct and task headings are descriptive or task-based, making it relatively intuitive to perform common administrative tasks. A summarized dashboard is visible from the Home tab, or administrators can look under the Monitors tab for pie charts about specific items.

As a minor issue, the task wizards, while helpful in streamlining migration, client deployment and backups, are not accessible from the Manager Console directly.

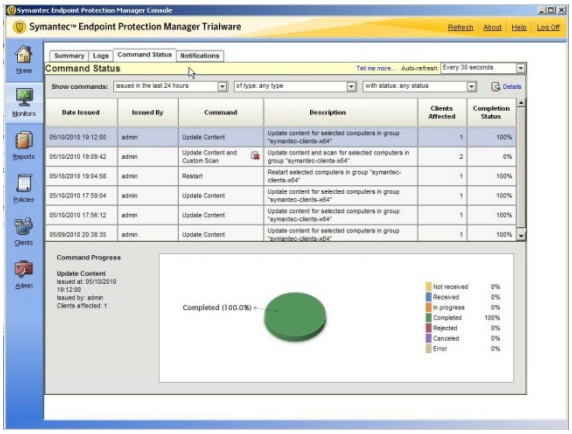
## Client and Policy Management 4/5

The Manager Console provides relatively granular policy management options for endpoint machines and locations. Shared policies are standard and are able to be applied to any group or physical location. Conversely, non-shared policies are more specialized and apply only to a group when it is in a specific location.

Groups can be imported from existing organizational structures, such as LDAP or an Active Directory

server. Otherwise groups must be manually added to the client tree prior to client installation.

Symantec Endpoint Protection Manager Console gives administrators flexibility between push or pull modes for policy deployment. Different modes can be set for different locations. This feature is great for allowing administrators to adapt the deployment of policies to network conditions and the size of deployment.




*Screenshot 12: Symantec Manager Console (Server)*

## Remote Management 4.5/5

The management server can be remotely accessed using the Symantec Protection Manager Web Access interface. With the correct login and password, access to the management server remotely requires no additional configuration of user accounts or installation of browser components.

The Web Access remote console is fully functional and looks identical to the Manager Console on the management server. Similar to the Manager Console, navigating between categories and headings is somewhat slow.

## Updates 5/5

Downloading and distributing updates to clients is effortless in Endpoint Protection, requiring little setup.

The management server is designated as the central repository during installation and clients retrieve updates from the management server by default. In some cases, the default setting is ideal and requires no further configuration from the administrator. For larger deployments, administrators can designate other servers as Group Update Providers which act as an intermediary in retrieving updates from the management server to distribute to nodes.

Updating the Symantec client solution from the management server was fast compared to other solutions.

## Effectiveness 5/5

The most recent On-Demand Comparative from AV Comparatives awarded Norton Antivirus (v17.5.0.127) the **ADVANCED+** rank, noting few false positives and a total detection rate of 98.6%.

The latest Summary Report (2009) from AV Comparatives noted that Symantec had very high detection rates, low system impact and was easy to use. In this report, Symantec were awarded first place out of 16 products.

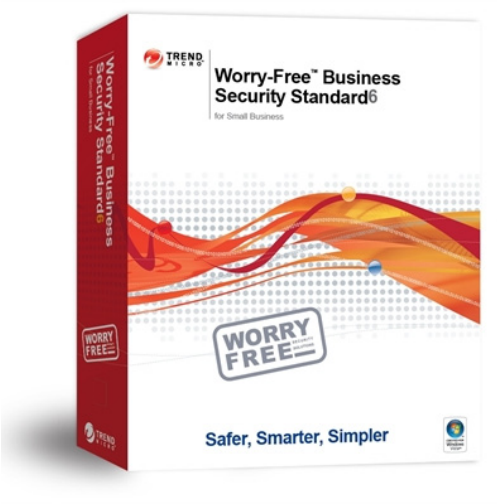
The Retroactive/ProActive Test in June 2010 awarded Norton Anti-Virus with an **ADVANCED** rating. To date, Symantec has not yet received an ADVANCED+ rating in this category.

Overall, Symantec has passed the VB100 test 54 times and missed seven times. With an **88%** success rate, Symantec has the third best overall rate of success in VB100 testing.

## Common Use Cases 4/5

| Task | Ease of Use | Details |
|---|---|---|
| Conducting an 'on-demand' scan of selected endpoints | **Simple** | From the Clients tab, right-click on the group or target computer and activate "Run Command on Group > Scan". Manager Console offers three scan options: Active, full or custom. Command process can be viewed from Command Status. |
| Creating and viewing a malware report 'on-demand' | **Moderate** | From the Reports tab, administrators can select the type of report and the period of time for reporting. Reports are generated in HTML format by default, and take some time to generate on-demand. |
| Creating, assigning and deploying a new policy | **Simple** | From the Policies tab, choose the relevant security category and right-click to "Add" a new policy. The new policy can then be assigned to a location or group. |

# Trend Micro Worry Free Business Security




## Review Summary

| | |
|---|---|
| Overall Summary | 3.5 |
| Installation & Configuration | 3.5 |
| Migration | 4.5 |
| Default Policies | 4 |
| Client Installation | 3.5 |
| Interface Design | 2.5 |
| Policy Management | 3 |
| Remote Management | 4 |
| Updates | 4.5 |
| Common Use Cases | 3 |
| Effectiveness | 2 |
| Performance | 2 |

- Relatively high system impact on endpoint machines, below average performance.
- Relatively low amounts of traffic generated by server repository updates.
- Migration from previous solutions is well supported.
- Somewhat simplistic client and policy management which may be better suited for smaller organizations.
- Outbreak defense manages possible virus outbreaks on a network without intervention.
- Graphical glitches detract from an otherwise streamline interface.

## Installation and Configuration 3.5/5

A typical "evaluation version" Installation of Trend Micro Worry-Free Business Security management components took roughly two hours to complete.

While the installation progressed without issue, the installer required a moderate amount of input from the user about items which could be either excluded from the installation process or moved to the configuration phase, for example, prompting the user about conducting a pre-scan of the machine before installation and asking about the user's professional industry on the telemetric prompt screen. One or two installation screens lacked detail, for instance, the "Select Components" prompt asked that components be selected for installation, but provided no explanation about the functionality of components.

The Worry-Free Business Security installer automatically installed the .NET framework and Apache Web Server as an integrated part of the main installation. The evaluation version of Worry-Free also did not require a license key to be entered in order to proceed with installation.

While Trend Micro does not provide a "Quick Start" guide, the Installation Guide has all the information required, with step by step guides for all types of installations.

## Migration from Previous Solutions 4.5/5

The migration process is reasonably well supported by Trend Micro Worry Free Business Security.

Only some older versions of Trend Micro business security products are supported for upgrade to Worry-Free Business Security. For supported product variants, upgrading is as simple as running the standard installation and identifying the existing Security Server when prompted.

Client-side migration is supported for most variants of Trend Micro products as well as most third party antivirus products. Where a Trend Micro product is detected by the client deployment, endpoints will be upgraded to the Trend Micro Client/Server Security Agent. Existing third party antivirus software will be removed by Worry-Free Business Security prior to replacement with the Trend Micro client.

## Default Policies 4/5

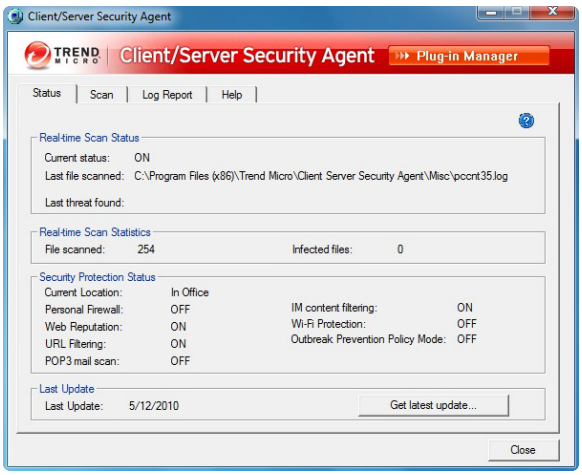
Worry-Free Business Security comes with default policies which are well balanced for standard usage. Depending on whether a typical installation was selected or an upgrade was implemented, default policies may vary slightly.

The default setting of policy options for security components differ depending on a group's business role or physical location, for example, desktop groups will have Behavior Monitoring enabled while Server groups will have this protection disabled.

The firewall and POP3 Mail Scanning is disabled by default. Where enabled, the Firewall comes with default settings which take into account common scenarios encountered by endpoint users, such as the need to access the web.

## Client Install 3.5/5

Deployment of the Client/Server Security Agent through the network to endpoints was relatively easy, but documentation for the process wasn't entirely accurate which made it more challenging to troubleshoot. The Administrator's Guide mentions the need to enable the Remote Registry Service on Windows Vista clients prior to proceeding, but we discovered that it was also necessary to enable this service manually on Windows 7 machines.




*Screenshot 13: Trend Micro Client/Server Security Agent (Client)*

Target machines are first manually added from the Installation from Security Settings. Endpoint machines can be discovered through NetBIOS, Active Directory or by searching for a computer name. Our deployment through the network took under five minutes to complete. Worry-Free Business Security has a number of methods of client deployment, making it reasonably flexible to an organization's needs. Automated deployment methods include agent installation for unprotected computers that log onto the domain using a Login script created by Worry-Free Business Security. Other methods rely on the participation of end users, for example, by instructing users to download and install the Agent package from the Worry-Free Business Security internal site created during setup or from an e-mail link.

## Interface Design 2.5/5

As a web interface, the Trend Micro Worry-Free Business Security console has a streamlined "webpage-like" feel. Unfortunately, we experienced graphical glitches while interacting with some elements of the console, which detracted from its otherwise slick and responsive design. The worst example of this was when we attempted to configure Security Settings; after clicking on a few items, the interface was littered with broken navigation tabs and drop-down graphics.

Another disadvantage of the Worry-Free Business Security web interface was the requirement to install an ActiveX control named "AtxEnc" from Trend Micro before the console could be accessed. The requirement to install this ActiveX control isn't documented explicitly by Trend Micro, though it is mentioned that the Web Console uses ActiveX as an internet technology.

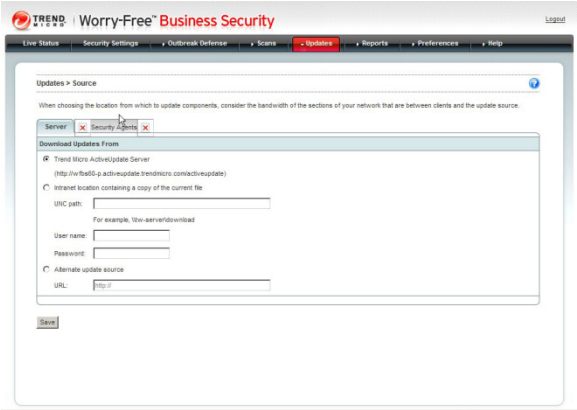
Management functionality is intuitively accessible from the toolbar above the display pane, with categories dropping down to reveal more specific options. The "Live Status" dashboard is shown as the main page from logon and displays network status for systems and threats. Dashboard status isn't in real-time, but administrators are free to manually refresh the dashboard if they require information on-demand.

## Client and Policy Management 3.5/5

Worry-Free Business Security has a reasonable depth of security configuration options, but is let down by 'group only' policy assignments, the inability to import existing node infrastructure and the lack of capacity to automate sorting of endpoints into relevant groups.

However, Worry-Free Business Security does have a unique client management feature called 'Outbreak Defense'. Outbreak Defense acts as an automated response to a world-wide virus outbreak detected by Trend Micro. Where an outbreak occurs, Worry-Free Business Security takes pre-emptive measures to prevent the network from being infected by the specific malware threat. Preventative steps may include raising security by blocking shared file and

folder access, blocking ports, denying write access or assessing endpoint clients for vulnerabilities.




*Screenshot 14: Trend Micro Worry-Free Business Security (Server)*

Each security component in Worry-Free Business Security has a large amount of configuration options available. There is also some policy flexibility in the form of "Out of Office" policies for the Web Reputation and TrendSecure modules. Where configured correctly, different policies will be enforced for these modules where endpoints have been disconnected from the server.

## Remote Management 3.5/5

Remotely accessing the Worry-Free Business Security server is simple. The management server can be remotely accessed using the web interface with no further configuration required from the management server. The interface performs moderately well across the network, with all functionality enabled and reasonably fast response times between categories and functions.

As previously noted, an ActiveX add-on is required to access the web console. The need to install this ActiveX control for access needs to be better documented. No other security solution which we evaluated required an additional browser installation for access.

## Updates 4.5/5

Updating Worry-Free Business Security is simple. Installing the management software configures the server to check and download updates from the Trend Micro ActiveUpdate Server every hour, and to act as a central repository for retrieval of updates by endpoints.

Updating clients the first time after installation is similarly simple. By default, a Client/Server Agent automatically updates virus definitions on installation, prior to the first launch. This ensures that a client is fully protected from the first launch.

The Worry-Free Business Security Console also enables administrators to synchronize clients to the latest update, or rollback a patch by one version on-demand.

## Effectiveness 2/5

The most recent On-Demand Comparative from AV Comparatives awarded Trend Micro Antivirus (v17.50.1366.0) the **TESTED** rank, noting a great number of false positives and a total detection rate of 90.7%. This total detection rate was the lowest compared to all other evaluated vendors and products.

The latest Summary Report (2009) from AV Comparatives did not include results for any Trend Micro products.

The Retroactive/ProActive Test in June 2010 awarded Sophos Anti-Virus with a **STANDARD** rating. Since the introduction of this test in February 2004, Sophos has not yet achieved an ADVANCED+ rating in this category.

Trend Micro has passed the VB100 test 16 times and missed 11 times, attaining an overall **59%** success rate. Trend Micro failed the last three tests they participated in and since April 2008, have withdrawn their products from participation in VB100 tests.

## Common Use Cases 3/5

| Task | Ease of Use | Details |
|---|---|---|
| Executing an on-demand scan for endpoints | **Simple** | On-demand scans can be conducted by clicking on the Scan category and selecting a Manual Scan. While administrators can only select groups of computers to scan, they can choose from a range of scanning options and actions. |
| Creating and viewing a malware report 'on-demand' | **Moderate** | A one-time report can be generated from the Reports menu item. Unfortunately, reports can only be generated in the PDF format. |
| Creating, assigning and deploying a new policy | **Moderate** | Editing existing policy for a group proves to be much simpler than Creating, assigning and deploying a new policy. |

# 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.

## 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

The production of this report was funded by ESET LLC.

## Trademarks



# 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.

**Microsoft Word** will also be installed on endpoint machines prior to testing, in order to facilitate the Word Document Launch Time test

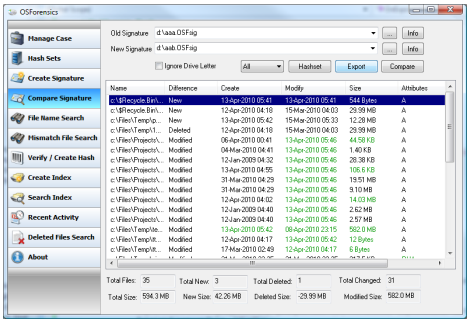
## Install size (Endpoint)

**Description** This metric measured the total additional disk space consumed by the endpoint client component after installation via the network.

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

New version of software currently being developed by PassMark Software. Currently publically available as OSCheck at the PassMark Website: http://www.passmark.com/products/oscheck.htm

OSCheck is 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 15: 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.

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

## Memory usage commit charge (Endpoint)

**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.

## Word document launch and restart time (Endpoint)

**Description** This metric measured the total time taken to open or re-open a large, mixed media Microsoft Word 2007 document, where an endpoint security product has been installed.

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

A test utility developed by PassMark software which measured and logged the time taken to launch an application in Windows. AppTimer can be downloaded from:
http://www.passmark.com/products/apptimer.htm

**Methodology**

- AppTimer was configured to launch a 'large' word document.
- We have defined 'large' as a mixed media Word document roughly 980 KB in size.
- The document was in *.docx format and was launched in Microsoft Word 2007 (v1.2.0.4518.1014).
- At the start of each test cycle, the machine was left idle for five minutes to minimize the impact of startup or background processes.
- After five minutes, AppTimer was used to launch and close the word document three times.
- The test was performed over five cycles with a machine restart between each cycle to limit possible caching behavior by the Windows operating system. Three test results were obtained per cycle, for a total of 15 test results.
- Out of fifteen results:
  - Five results represent the time taken to launch the word document **after restarting the machine**. These results tend to be slower because Windows has not yet cached the application/document being launched. Out of fifteen results, these are the 1st, 4th, 7th, 10th and 13th results; and
  - Ten results represent the time taken to launch the word document **by restarting the application without restarting the machine**. Out of fifteen results, these are the 2nd, 3rd, 5th, 6th, 8th, 9th, 11th, 12th, 14th and 15th results.

**Test File(s)** One 980 KB Microsoft Office Word Document in DOCX format.

**Result** Our final results were measured in milliseconds (ms), and calculated from an average of ten (10) samples. This test provides results for two separate metrics:

- **Word document launch time:** The final result is calculated as an average of five results (out of fifteen), specifically the 1st, 4th, 7th, 10th and 13th results.
- **Word document restart time:** The final result is calculated as an average of ten results (out of fifteen), specifically the 2nd, 3rd, 5th, 6th, 8th, 9th, 11th, 12th, 14th and 15th results.

## File copy time for small files (Endpoint)

**Description** This metric measured the total time taken to copy a set of small files between directories, where an endpoint security product was installed.

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

A command line utility developed by PassMark Software which measured and logged the time taken to perform a task in a command prompt.

**Methodology**

- At the start of each test cycle, the machine was left idle for five minutes to minimize the impact of startup or background processes.
- CommandTimer measured 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 was performed five times with a machine restart between each cycle.

**Test File(s)** A file set containing 821 files totaling roughly 659 MB.

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

## File copy time for large files (Endpoint)

**Description** This metric measured the total time taken to copy a set of large files between directories, where an endpoint security product was installed.

**Test Tool** **CommandTimer**
by: PassMark Software

A command line utility developed by PassMark Software which measured and logged the time taken to perform a task in a command prompt.

**Methodology**

- At the start of each test cycle, the machine was left idle for five minutes to minimize the impact of startup or background processes.
- CommandTimer measured 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 was performed five times with a machine restart between each cycle.

**Test File(s)** A file set containing 11 files totaling roughly 2.5GB in size.

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

## 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.

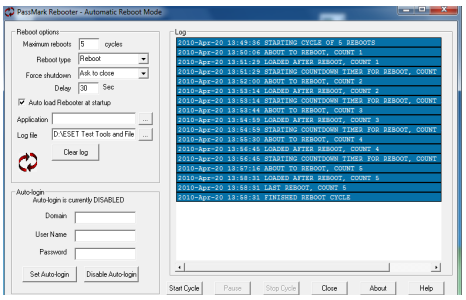
**Result** Our final result is measured in seconds (s) and calculated from an average of five (5) samples.

## 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 16: 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.