# Anti-Virus Comparative

**AV comparatives**

# Performance Test

Impact of Anti-Virus Software on System Performance

**Microsoft Forefront Endpoint Protection (Release Candidate)**

Language: English
November 2010
Last Revision: 13th December 2010

**www.av-comparatives.org**

## Introduction

We want to make clear that the results in this report are intended to give only an indication of the impact on system performance (mainly by the real-time/on-access components) of the various Anti-Virus products in these specific tests. Users are encouraged to try out the software on their own PCs and form an opinion based on their own observations.

## Tested product

The following product, which was provided in mid-November, was evaluated (with <u>default</u> settings) in this test:

**Microsoft Forefront Endpoint Protection (RC)**[1]

The following activities/tests were performed:

- File copying
- Archiving / Unarchiving
- Encoding / Transcoding
- Installing / Uninstalling applications
- Launching applications
- Downloading files
- PC Mark Vantage Professional Testing Suite

## Test methods

The tests were performed on an Intel Core 2 Duo E8300 machine with 2GB of RAM and SATAII hard disks. The performance tests were first done on a clean Microsoft Windows 7 Professional (32 Bit) system and then with the installed Anti-Virus software (with default settings).

The hard disk was defragmented before starting the various tests, and care was taken to minimize other factors that could influence the measurements and/or comparability of the systems (network, temperature, etc.). Optimizing processes/fingerprinting used by the products were also considered – this means that the results represent the impact on a system which has already been used by the user for a while. The tests were repeated several times (with and without fingerprinting) in order to get mean values and filter out measurement errors. After each run the workstation was defragmented and rebooted.

---

[1] Release candidate was provided by Microsoft, tested without server

We simulated various file operations that a computer user would execute: copying[2] different types of clean files from one place to another, archiving and unarchiving files, encoding and transcoding[3] audio and video files, converting DVD-Files to IPOD format, downloading files from Internet, launching applications, etc. We make use of windows automation software to replicate the activities and measure the times.We also used a third-party industry recognized performance testing suite (PC Mark Vantage Professional Edition) to measure the system impact during real-world product usage.

Readers are invited to evaluate the various products themselves, to see how they impact on their systems (such as software conflicts and/or user preferences, as well as different system configurations that may lead to varying results).

Anti-Virus products need to load on systems at an early stage to provide security from the very beginning – this load has some impact on the time needed for a system to start up. Measuring boot times accurately is challenging. The most significant issue is to define exactly when the system is fully started, as many operating environments may continue to perform start-up activities for some time after the system appears responsive to the user. It is also important to consider when the protection provided by the security solution being tested is fully active, as this could be a useful measure of boot completion as far as the security solution is concerned. Some Anti-Virus products are loading their services very late (even minutes later) at boot (users may notice that after some time that the system loaded, the system gets very slow for some moments), so the system looks like loading very fast, but it just loads its services later and makes the system also insecure/vulnerable. As we do not want to support such activities, we still do not measure boot times.

To support our concerns, we tested if the products are loading their protection modules before e.g. malware in Autostart is executed. **Microsoft Forefront Endpoint Protection successfully** blocked the malware before its execution after system start-up (by loading itself at an early stage).

---

[2]  We used 3GB data of various file categories (pictures, movies, music, various MS Office documents, PDF files, applications/executables, Windows 7 system files, archives, etc.).

[3]  Converting MP3 files to WAV, MP3 to WMA, AVI to MPG and MPG to AVI, as well as IPOD format

## Test results

These specific test results show the impact on system performance that Anti-Virus products have, compared to the other tested Anti-Virus products. The reported data just give an indication and are not necessarily applicable in all circumstances, as too many factors can play an additional part. As we noticed that delivering percentages gets easily misinterpreted/misused, we grouped the results in four categories, as the impact within those categories can be considered almost equal, also considering error measurements. The categories were defined by the testers, based on what would be felt/noticed from user's perspective (e.g. "slow" means that the user would notice and label the added slowdown as too high, also compared to the impact of other security products). Under Windows 7 the performance impact is smaller than e.g. on XP. Due that, we use new categories to reflect better the differences under this operating system.

### File copying

We copied a set of different file types which are widespread at home and office workstations form one physical hard disk to another physical hard disk.

| +0% to +10% | very fast |
| +10% to +30% | fast |
| +30% to +60% | mediocre |
| over +60% | slow |

|  | On first run | On subsequent runs (with fingerprinting, if available) |
|---|---|---|
| **Microsoft FEP** | fast | fast |

## Archiving and unarchiving

Archives are commonly used for file storage, and the impact of Anti-Virus software on the time taken to create new archives or to unarchive files from existing archives may be of interest for most users.

We archived a set of different file types which are widespread at home and office workstations form one physical hard disk to another physical hard disk and unzipped them after this again on a third physical hard disk.

The results below already consider the fingerprinting/optimization technologies of the Anti-Virus products, as most users usually make archives of files they have on their disk.

| | |
|---|---|
| +0% to +10% | very fast |
| +10% to +20% | fast |
| +20% to +30% | mediocre |
| over +30% | slow |

| Microsoft FEP | very fast |
|---|---|

## Encoding/transcoding

Music files are often stored and converted on home systems, and converting such files takes system resources. Due that, many home users may be interested to know if their Anti-Virus products imposes a slowdown while converting multimedia files from one format to another.

We encoded and transcoded some multimedia files with FFmpeg, and for the IPOD conversion we used HandBrakeCLI. The impact during FFmpeg and IPOD converting was almost the same.

| | |
|---|---|
| +0 to +5% | very fast |
| +5 to +10% | fast |
| +10 to +25% | mediocre |
| over +25% | slow |

| Microsoft FEP | very fast |
|---|---|

## Installing/uninstalling applications

We installed several programs (like Visual C++, .NET Framework, etc.) with MSI installers, and then uninstalled them and measured how long it took. We did not consider fingerprinting, because usually an application is only installed once.

| | |
|---|---|
| +0% to +10% | very fast |
| +10% to +25% | fast |
| +25% to +50% | mediocre |
| over +50% | slow |

| | |
|---|---|
| **Microsoft FEP** | very fast |

## Launching applications

Office document files and PDF files are very common. We opened some large document files in Microsoft Office (and closed it) and some large PDF files in Adobe Acrobat Reader (and closed it). Before each opening, the workstation was rebooted. The time taken for the viewer or editor application to open and a document to be displayed was measured.

Although we list the results for the first opening and the subsequent openings, we consider the subsequent openings more important, as normally this operation is done several times by users, and optimization features of the Anti-Virus products take place, minimizing their impact on the systems.

| | |
|---|---|
| +0% to +25% | very fast |
| +25% to +75% | fast |
| +75% to +150% | mediocre |
| over +150% | slow |

| | Open Word | | Open PDF | |
|---|---|---|---|---|
| | **On first run** | **On subsequent runs (with fingerprinting, if available)** | **On first run** | **On subsequent runs (with fingerprinting, if available)** |
| **Microsoft FEP** | fast | **very fast** | very fast | **very fast** |

Some optimization features may not take place in some products (or not reduce enough the impact), as documents and PDF files are common infection targets and therefore are anyway scanned when opened. Nevertheless, the fingerprinting would take place in on-demand scans.

## Downloading files from the Internet

Files are commonly downloaded from the internet. To avoid external influences, we used an in-house Apache web server (wget) connected with 1GB LAN and measured the download time. We tested using various large files/archives.

+0% to +25%        very fast
+25% to +50%       fast
+50% to +100%      mediocre
over +100%         slow

| Microsoft FEP | very fast |
|---|---|

## PC Mark Tests

In order to provide an industry-recognized performance test, we used the PC Mark Vantage Profession-al Edition[4] 1.0.2 testing suite of FutureMark. Users using PC Mark Vantage should take care to mini-mize all external factors which could affect the testing suite and follow strictly at least the considera-tions/suggestions documented inside the PC Mark manual, in order to get consistent and valid/useful results. Furthermore, the tests should be repeated several times to verify them.

*"The six Consumer Scenario suites are based on a collection of actual real-world end user applications, and reflect the system performance a typical user would expect running those applications. Each test suite contains a subset of the following tests as applicable: data encryption, decryption, compression and decompression, GPU and CPU image manipulation, image import, video playback, editing and trans-coding, audio playback and transcoding, GPU and CPU game tests, game data loading, web page render-ing, mail operations, media player operations, contacts search, text editing and applicable HDD tests. Each Consumer Scenario test suite generates a unique, fully comparable performance score for that series of tests. A comprehensive, overall PCMark score is generated by running the PCMark Suite. And the HDD Suite produces its own fully comparable performance score."[5]*

|                  | PC Mark score | Points |
|------------------|:-------------:|:------:|
| *without AV*     | *3843[6]*     | -      |
| **Microsoft FEP**| **3433**      | **89** |

We are not showing the scores for the subtests "Memories", "TV and Movies", "Gaming" and "HDD", because the difference was minimal to a system with no AV product.

|                | PC Mark Music score |
|----------------|:-------------------:|
| *without AV*   | *4497*              |
| Microsoft FEP  | 4209                |

|                | PC Mark Communications score |
|----------------|:----------------------------:|
| *without AV*   | *4323*                       |
| Microsoft FEP  | 4053                         |

|                | PC Mark Productivity score |
|----------------|:--------------------------:|
| *without AV*   | *3211*                     |
| Microsoft FEP  | 2537                       |

---

[4] For more information, see http://www.futuremark.com/benchmarks/pcmarkvantage/introduction/
[5] http://www.futuremark.com/pressroom/companypdfs/PCMark_Vantage_Reviewer%27s_Guide_v1.1_(PDF)
[6] Baseline system: Intel Core 2 Duo E8300 machine with 2GB of RAM

## Summarized results

Users should weight the various subtests according to their needs. We applied a scoring system in order to sum up the various results.

| | File copying (mean value) | Archiving / unarchiving | Encoding / transcoding | Installing / uninstalling | Download | Launching applications | PC Mark | **TOTAL** |
|---|---|---|---|---|---|---|---|---|
| **Microsoft FEP** | fast (10) | very fast (15) | very fast (15) | very fast (15) | very fast (15) | very fast (15) | 89 | **174** |

In our rating system this would be awarded with Advanced+.

## Copyright and Disclaimer