Computer Security - Antiviruses

In the previous chapter, we saw how to secure our computers and one of the points was installing and updating antivirus software. Without this software there is a high chance that your systems and networks will be hit and will suffer hacking attacks and also can be affected by the various viruses.

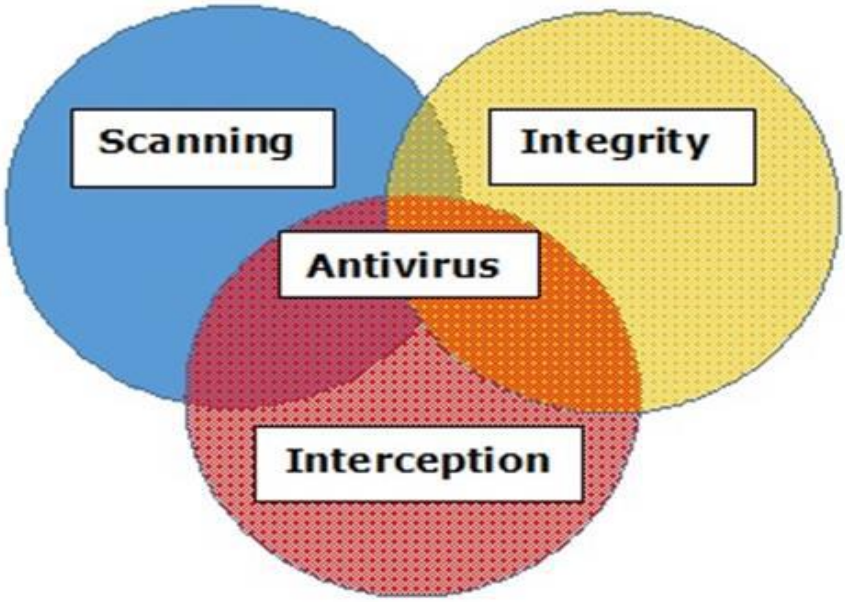
It is important that the antivirus scan engine and virus signatures to be updated regularly, we do this because if your system is hit by the latest malware it will be detected.

Basic Functions of Antivirus Engines

All antivirus engines have three components to function accordingly. It is important to have a look at these functions because it will help us for better manual cleaning of viruses in case we need.

- **Scanning** − When a new virus is detected in the cyberspace, antivirus producers start writing programs (updates) that scans for similar signature strings.
- **Integrity Checking** − This method generally checks for manipulated files in OS from the viruses.
- **Interception** − This method is used basically to detect Trojans and it checks the request made by the operating system for network access.

The following image shows the schema for an antivirus engines functionality.



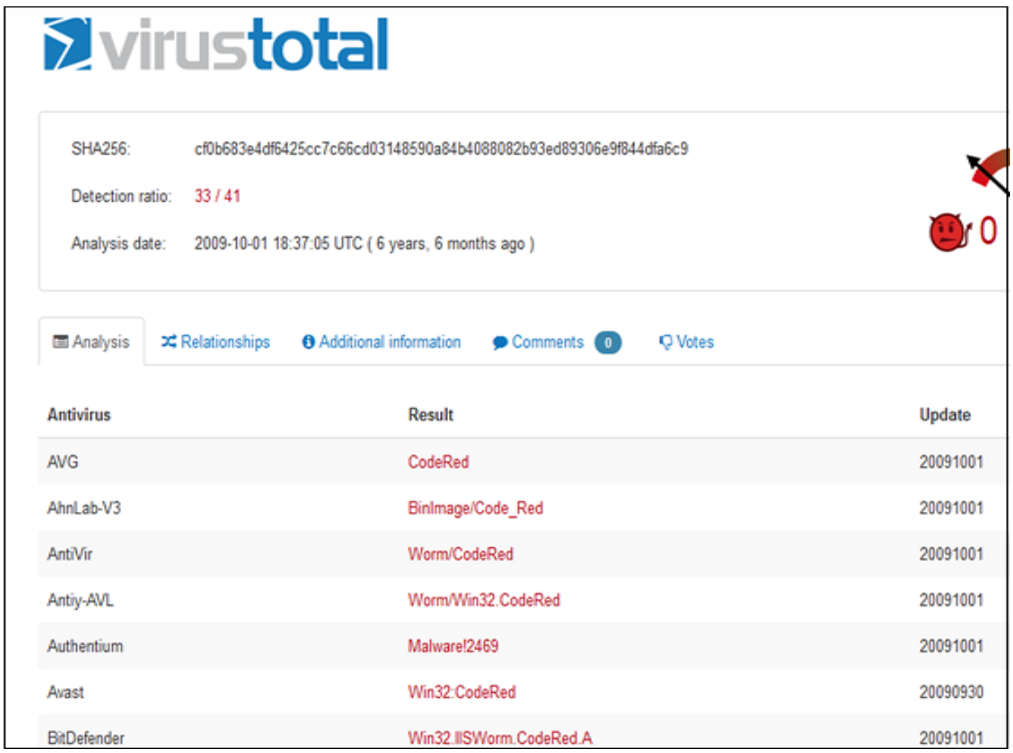
Online Virus Testing

If the system administrator does not have an antivirus installed or suspects a file that is infected. They would recommend to use the online testing antivirus engine which (according to me) is one of the best – https://virustotal.com/.

Q. Why this option?

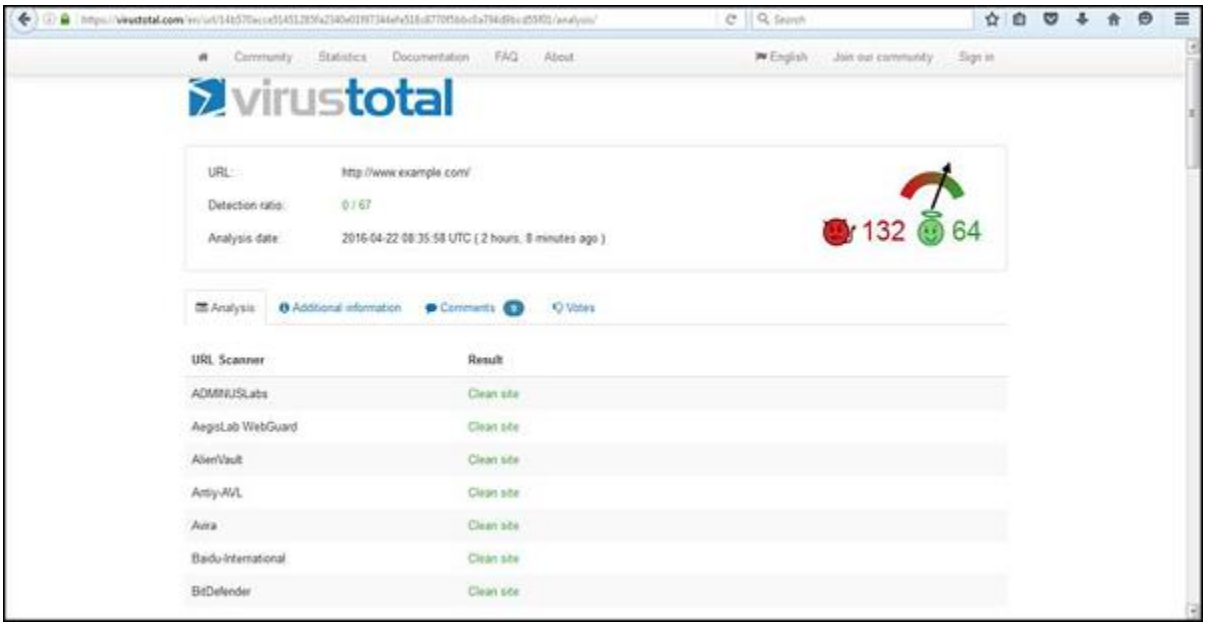
Ans. It is a free and independent service. It uses multiple antivirus engines (41 anti-virus engines), so its result will be showing for all the 41 engines. It updates the engines in real-time.

For further clarity, please see the following screenshot, wherein I uploaded a file with virus and the result is **33/41 (Detection Ratio)**, which means that it has virus and did not pass the class, so it should not be opened.



A good feature of this site is URL checking, before entering to a website you can enter the URL and it checks for you if the site has infection and can harm you.

I did a test with a URL and it came out to be clean and that too 100%, so I can visit it without my computer being infected.



Free Antivirus Software

As this tutorial is hands-on practice, I will show you where to get free antiviruses and where to download in case you don't have enough budget.

The free versions of anti-viruses have nearly identical malware detection scores to the paid versions produced by the same company, but the commercial antivirus makes a small difference in the performance of security and in our case we are system administrators and we want maximum protection in the work environment.

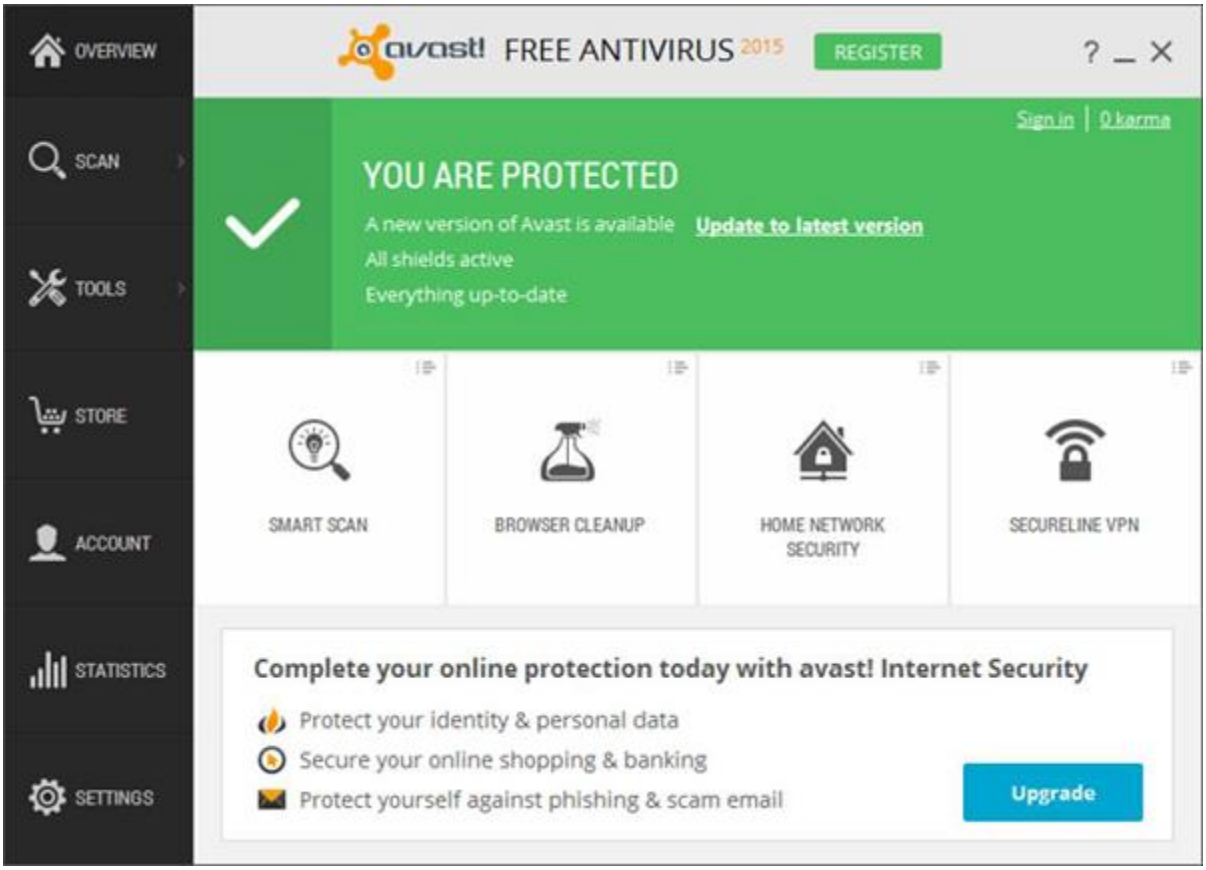
From the PCMagazine (http://in.pcmag.com/) you can get a review which are the best top rated free antiviruses at the moment. In the following URL you can check by yourself http://www.pcmag.com/article2/0,2817,2388652,00.asp

Let us understand in detail about some of these antivirus software −

Avast Antivirus

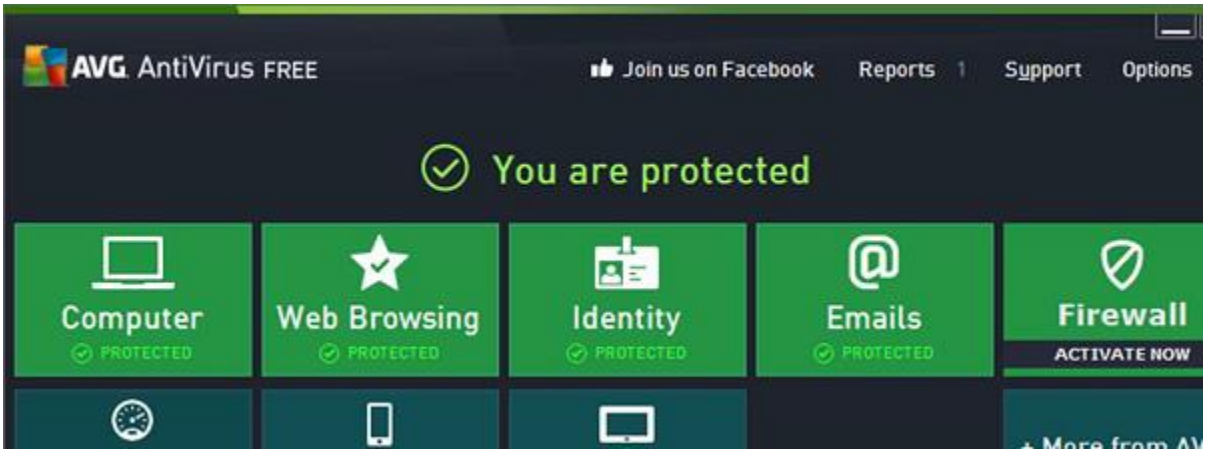
This antivirus has good scores in malware blocking and anti-phishing test scans, it can be downloaded from https://www.avast.com/en-eu/index

For server installation you need a commercial version.



AVG Antivirus

It can be downloaded from http://www.avg.com/us-en/free-antivirus-download. For server installation you need to purchase the commercial version.



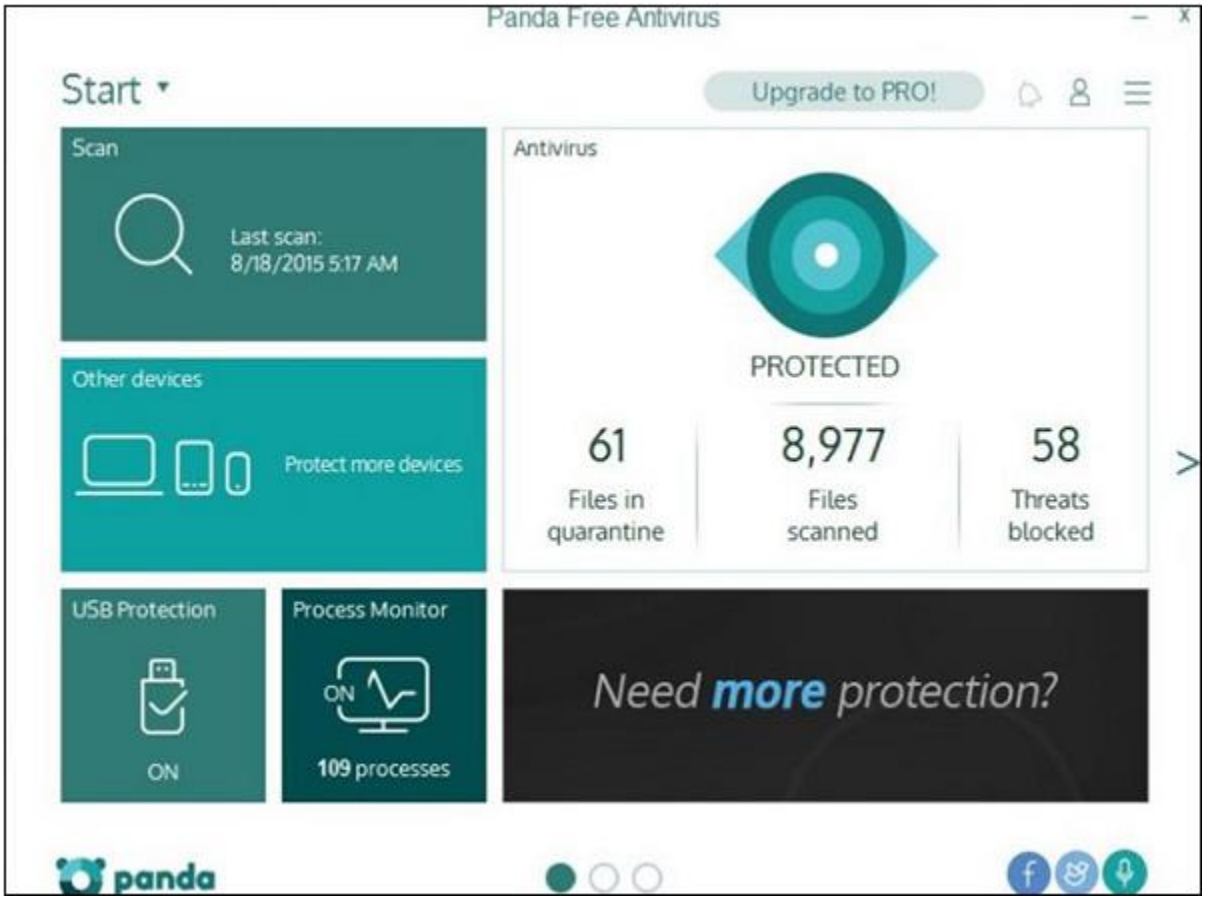
Panda Antivirus 2016

It can be downloaded from http://www.pandasecurity.com/usa/homeusers/downloads/

It has the following good features −

- Rescue Disk
- USB protection
- Process Monitor

For server installation you will need to purchase the commercial version.



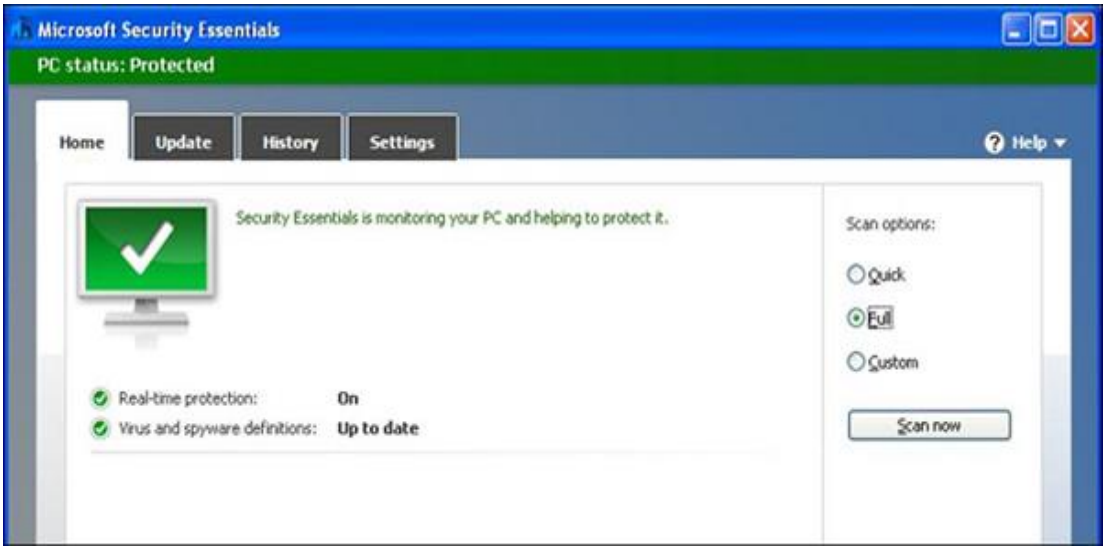
Bitdefender Antivirus

It can be downloaded from http://www.bitdefender.com/solutions/free.html A good feature in this antivirus is that it can work entirely in the background. No configuration setting. For server installation you need to buy the commercial version.

Microsoft Security Essentials

Even though it is not among the top-most free antiviruses owing to the Microsoft brand, it is worth a mention that Microsoft itself offers you a free antivirus which is called as Microsoft Security Essentials.

It can be downloaded from http://windows.microsoft.com/en-us/windows/security-essentials-download



Commercial Antivirus

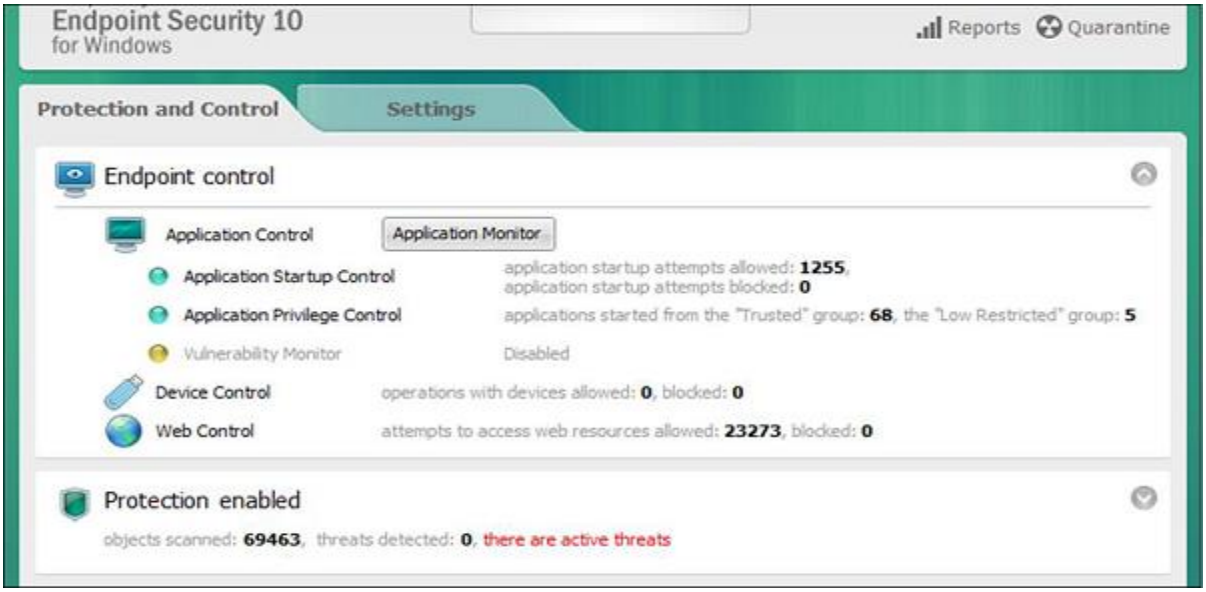
I should mention that all the producers of free antiviruses offers their commercial versions too. Based on PC magazine, the best commercial antiviruses are −

- Kaspersky Anti-Virus
- Bitdefender Antivirus Plus 2016
- McAfee AntiVirus Plus (2016)
- Webroot SecureAnywhere Antivirus (2015)

Please see the following link to check by yourself − http://www.pcmag.com/article2/0,2817,2372364,00.asp

Kaspersky Antivirus

It can be downloaded as a free trial from http://www.kaspersky.com/free-trials/anti-virus It has an excellent score in anti-phishing. It also gives a useful bonus in security tools like credit card protection in your computers.



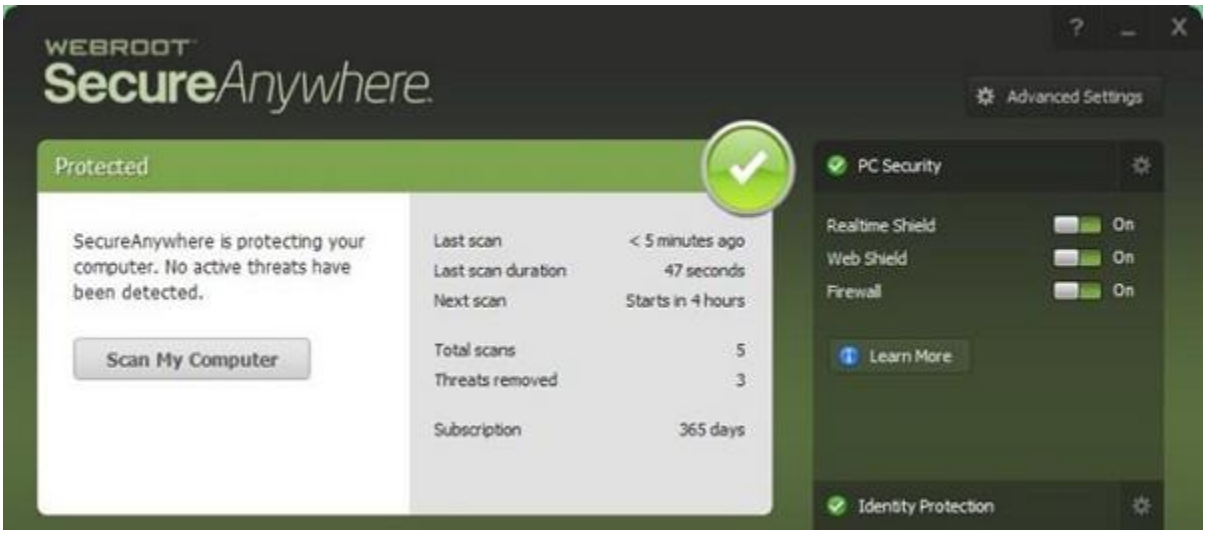
McAfee AntiVirus Plus

It can be downloaded as a free trial from – http://home.mcafee.com/downloads/OneClickTrial.aspx?culture=en-us

It protects all the operating systems like Windows, Mac OS, Android, and iOS devices. very good malicious URL blocking and anti-phishing.

Webroot SecureAnywhere Antivirus

It can be downloaded as a free trial from – http://www.webroot.com/us/en/home/products/av

Some of its prominent features are –

- Recover files encrypted by ransomware
- Uses tiny amount of disk space
- Very fast scan
- Handles unknown malware
- Includes firewall