

eScan Anti-Virus v11 VS Quick Heal AntiVirus Pro 2011

Why do we need an Anti-Virus?

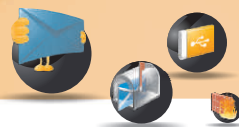
An Anti-Virus is considered to be one of the most important applications that your PC should have. It's a well known fact that the Internet is plagued with all kinds of malware; computer programs written to infect or even take control of unprotected PCs. An Anti-Virus on the other hand is designed to thwart such malicious programs from infecting your PC.

With the ever increasing number of security threats, organizations and individuals find the need to secure their personal details from identity thieves at far more alarming rate than it was a few years ago. In this day and age where broadband services have become a necessity, personal information can easily be hacked into in a matter of minutes. This can include anything from debit/credit card details, passwords for your personal accounts, bank details etc. That's the main reason why eScan Anti-Virus v11 also features a firewall. Apart from keeping potential hackers at bay the firewall also acts as a barrier between the user and the Web, where it only allows legitimate and known data packets to pass through to your computer.

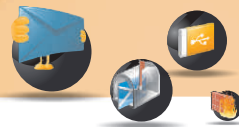
Spam is another major concern that has plagued the Internet. With a large number of unsolicited emails targeted towards mail servers, receiving emails using clients as Outlook, Thunderbird or even The Bat can be extremely time consuming. Moreover, unnecessary usage of bandwidth slows down other applications from accessing the Internet. To help prevent this, eScan Anti-Virus comes built with an Anti-Spam module. To enhance the overall functionality the module makes use of a feature called NILP (Non Intrusive Learning Pattern) that not only uses the Bayesian Filtering module but also works on the principles of Artificial Intelligence (AI) which is capable of categorizing emails as either spam or ham. Other advanced options include RBL (Real-time Blackhole List) and SURBL (Spam URL Realtime Blacklist). The RBL module basically checks the IP address of the senders against various RBL sites. So if the sender is found blacklisted on any of the RBL sites the mail will be automatically blocked from being downloaded. However the SURBLs main function is to check the URLs in the message body of an email. So if the URL is listed on the SURBL site the email is immediately blocked from being downloaded.

To help protect your digital identity eScan Anti-Virus provides a much needed secure environment in comparison to other Anti-Virus products. This would include the certification level reached by well known testing bodies such as AV-Comparatives, VirusBulletin and ICSA Labs. However another aspect that also needs to be taken into consideration is the number of false positives detected by the application. Therefore, just having a higher detection rate is never enough but being able to differentiate between malware (known/unknown) and genuine OS files is of utmost importance.

The first half of this document provides a brief explanation of the features that are overlooked by our competitor but are made available in eScan AV v11. The second half displays the effectiveness of the protection offered by both security companies – eScan and Quick Heal.



Product Name	eScan Anti-Virus v11	Quick Heal AntiVirus Pro 2010 (v11)
Manufacturer / Developer	MicroWorld	Quick Heal
VB 100% Certified	✓	✓
Unique Technology	MicroWorld Winsock Layer	DNAScan Technology/ Native Boot Scan
Proactive Security	✓	✓
Real-Time AV Scanning	✓	✓
Spyware, KeyLogger, Rootkit Blocker	✓	✓
Real-Time File Monitor	✓ (Intelligent and Faster)	✓
On-Demand Scan	✓ (with Cache Technology)	Not Documented
Anti-Spam	✓ (NILP, RBL, SURBL)	X
Firewall (Inbound & Outbound)	✓	✓
Anti-Phishing	✓	X
Malware URL Filter	✓	✓
History / Reports	✓	✓
Web based Help	✓	X
Asset Management	✓	X
Network Monitoring tool	✓	X
Update Rollback	✓	Not Documented
Hotfix Rollback	✓	Not Documented
Auto download / Update Software Version	✓	Not Documented
Auto Backup / Restore	✓	✓
Remote Support Application	✓	X
Virtual Keyboard	✓	X
Entertainment/Gaming /Silent mode	✓	✓
Files and Folders Protection	✓	X
Creating / Burning Bootable Rescue CD	✓ (Windows Based)	✓ (Windows Based)
Automatic Patching of Windows® Operating System Vulnerabilities	✓	X
Laptop / Battery / Power saving Mode for Schedule Scan	✓	X
Advanced Self-Protection Feature	✓	✓
Real-Time E-mail Scan	✓	✓
Password Protection	✓	✓
Heuristic Scanning	✓	✓
Registration / Activation: (via Web / SMS / E-mail / FAX)	✓	(Not Documented for SMS / FAX)
Real-Time Web Page Scan	✓	✓



Enhanced Spam Management

Non Intrusive Learning Pattern (NILP): Unlike most of our competitor's eScan AV comes featured with NILP technology (Non Intrusive Learning Pattern) that not only uses the Bayesian Filtering module but also works on the principles of Artificial Intelligence (AI). This drastically prevents junk email from reaching your inbox. In addition to this, NILP also uses a behavioral pattern that is capable of categorizing emails as either spam or ham.

Realtime Blackhole List (RBL): The RBL module basically checks the IP address of the senders against various RBL sites. So if the sender is found blacklisted on any of the RBL sites the mail will be automatically blocked from being downloaded.

Spam URL Realtime Blacklist (SURBL): The functionality of this is almost the same as that of RBL. However the SURBLs main function is to check the URLs in the message body of an email. So if the URL is listed on the SURBL site the mail is immediately blocked from being downloaded.

On-Demand Scan (with cache-technology)

eScan features cache technology that creates a record or Whitelist of all files that are scanned on the first run. This ensures faster scan speeds and lower usage of system resources every subsequent runs. Only new or modified files are examined by the scanner.

Update/Hotfix rollback

At the start of every update eScan v11 makes a backup of the current database. So if the event the application downloads an update/hotfix that's corrupt it automatically rolls back to its previous stable database. However to keep user interactivity at its bare minimum the roll back process has been automated and doesn't require the user to intervene.

Web Based Help

An aspect that is also well taken care of is the eScan Wiki which is just a click away on our home page. The eScan Wiki is a comprehensive coverage of all our products. Here users can find product related information, tips as well solution based content that help resolve specific product related issues.

Network Monitoring Tool

In addition to the Firewall, eScan Anti-Virus also features a network monitoring tool that provides a detailed overview of the applications connected to the Internet. Generation of reports is also made available that gives you a detailed summary of the overall data transferred either monthly or weekly. In addition to this, users can also view the top ten applications for the day or you could simply specify the dates that need to be looked into.

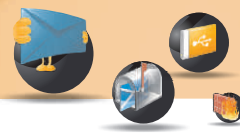
eScan Remote Support

Unlike our competitors eScan comes bundled with a special feature called eScan Remote Support. This module basically allows our support team to remotely connect and troubleshoot eScan related issues. The USP of this feature is that it allows most problems to be resolved remotely without having any support technician sent across. So as a user, you save a lot on time as the waiting period is almost negligible.

However, do keep in mind that this feature doesn't allow you – the user – to connect to our support department but will require you to call our support department and provide the Unique ID and Password that is generated. For security reasons the password is designed to change each time the eScan Remote Support is invoked.

Virtual Keyboard

User privacy is of our highest concern – reason why eScan 11 features a virtual keyboard. The implementation of a virtual keyboard allows users to enter confidential information such as banking passwords, credit/debit card details without any fear of your online identity being stolen. So even if your system is compromised by an unknown keylogger/spyware, the username and password that is entered during login remains protected.



Auto download/update of Product

There are a few security companies that don't include product patches or fixes within their updates. Therefore as a user you will need to manually download and install the required patch or fix. This sort of method is actually a concern as most users have the tendency to overlook or even disable such notifications – leaving your security product unpatched and vulnerable to security threats.

We at MicroWorld understand the importance of product patches. We therefore include them in the hourly updates that we provided. So if there is a patch available on our server, the built-in updater for eScan downloads and installs the required patch/fix without the need of user interactivity.

File and Folder Protection

There are a number of ways in which data can be lost – the first would include corruption of files in the event of a virus attack, the second would be the deletion of a particular file or folder which could happen knowingly or unknowingly. To prevent data loss, eScan comes with a special feature called 'Folder Protection'. Once a folder is specified the module prevents any further modifications from being made. This safeguards important data from corruption in the event of an infection. In addition to this the module also prevents deletion, creation and modification of files and folders.

Automatic Installation of Windows Critical Security Patches

A salient feature that our product implements is the vulnerability patching of the Windows Operating System. OS Vulnerabilities are the first cause of concern as most hackers scan for loopholes that allow them to bypass already implemented security settings. The implementation of OS patching in eScan v11 allows the application to directly connect to Microsoft's website and download only critical security patches for the Windows OS. This whole process is automated and doesn't require user intervention. So as a user you can be rest assured that your OS stays patched and secured from critical Windows related security vulnerabilities.

Restore Windows Default Settings

Users can eliminate modifications made to their desktop and background settings in the event of a virus attack. This is made possible by accessing the Restore Windows Default Settings via the Tools menu. Once activated, eScan automatically performs a virus check and then sets the system variables to their default values.

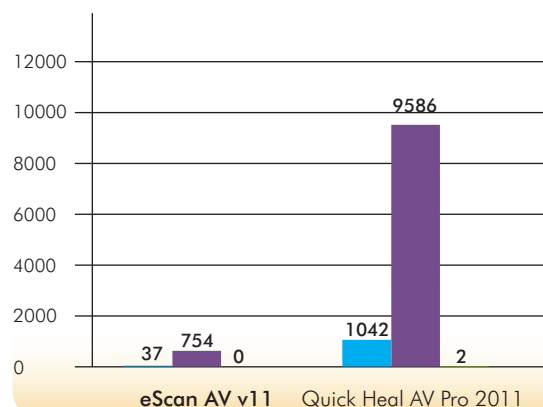
Laptop Battery Power Saving Mode

eScan AV v11 now features a built-in Battery mode wherein it prevents its own system intensive processes such as scheduled scan from running whenever the laptops power saver mode is detected – thereby increasing the overall runtime of the laptop. This feature is totally automated and requires no user intervention

Missed Samples (On-Demand scan test)

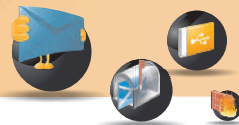
The graph below is a representation of the number of virus samples overlooked by the Anti-Virus engine. The exact number of virus samples tested are unknown but are well over a few hundred thousand. So missing even 0.1% translates to almost over one thousand of malicious files skipped during the test.

As shown eScan has a relatively lower score of missed samples than that of our competitor – Quick Heal. We haven't included WildList virus scores as both security suites scored a full 100% in detection and removal.



Source: VB100 (December 2010)

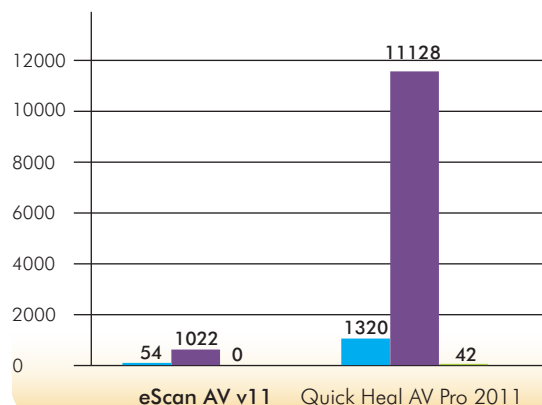
Worms & Bots Trojans Polymorphic Viruses



Missed Samples (On-access test)

The on-access scan test defines the programs real time protection capabilities, which is probably the most important feature that an Anti-Virus should have.

The following graph shows the number of virus samples missed by both eScan and Quick Heal during the on-access test conducted by Virus Bulletin. Here again the graph speaks about the performance of both the products.

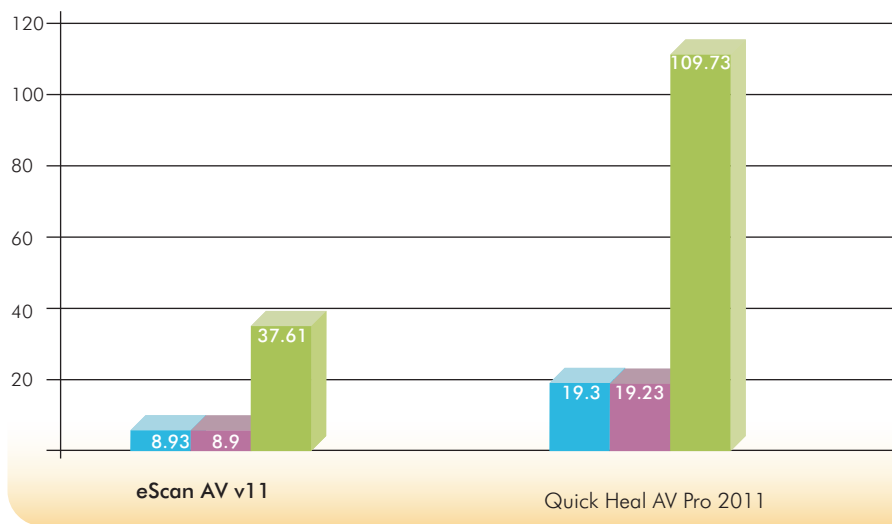


Source: VB100 (December 2010)

Worms & Bots Trojans Polymorphic Viruses

Memory & CPU Load (%)

The load that an antivirus engine puts on a system is crucial as it defines the overall response rate of a system. As most of us might have noted over the years that a high CPU usage by any scanner tend to slow down other processes that are in queue. Therefore limiting the number of CPU clicks (by the AV engine) is an important factor without compromising on the performance of the scanner. The chart below shows the percentage of Memory and CPU utilized when Idle and during file access by eScan and Quick Heal.



Vb100 (December 2010)

Idle Heavy File access CPU Load-Heavy file access