

eScan Anti-Virus v11 **VS** Kaspersky Anti-Virus 2011

Why do we need an Anti-Virus?

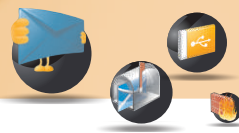
An Anti-Virus is considered to be one of the most important applications that your PC should have. It's a well known fact that the Internet is plagued with all kinds of malware; computer programs written to infect or even take control of unprotected PCs. An antivirus on the other hand is designed to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

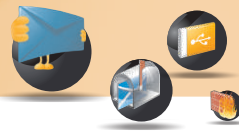
Spam is another major concern that has plagued the Internet. With a large number of unsolicited emails targeted towards mail servers, receiving emails using clients as Outlook, Thunderbird or even The Bat can be extremely time consuming. Moreover, unnecessary usage of bandwidth slows down other applications 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 Kaspersky Lab.



Product Name	eScan Anti-Virus v11	Kaspersky Anti-Virus 2011
Manufacturer/Developer	MicroWorld	Kaspersky
VB 100% Certified	✓	✓
Unique Technology	MicroWorld Winsock Layer	System Watcher
Proactive Security	✓	✓
Real-Time AV Scanning	✓	✓
Spyware, KeyLogger, Rootkit Blocker	✓	✓
Real-Time File Monitor (Intelligent and Faster)	✓	✓
On-Demand Scan	✓	✓ (iChecker and iSwift)
Anti-Spam (NILP, RBL, SURBL)	✓	✓
Firewall (Inbound & Outbound)	✓	X
Malware URL Filter	✓	X
History/ Reports	✓	✓
Web based Help	✓	X
Vulnerability detection	X	X
Asset Management	✓	X
Network Monitoring tool	✓	X
Update Rollback	✓	✓
Hotfix Rollback	✓	Not Documented
Auto download / update software version	✓	✓
Auto Backup / Restore	✓	Not Documented
Online Backup	X	X
Remote Support Application	✓	X
Virtual Keyboard	✓	✓
Entertainment/Gaming /Silent mode	✓	✓
Files and Folders Protection	✓	X
Creating/Burning Bootable Rescue CD	✓ Windows Based	✓ Linux Based
Automatic Patching of Windows® Operating System Vulnerabilities	✓	X
Laptop/Battery /Power saving mode for schedule scan	✓	✓
Advanced Self-Protection Feature	✓	✓
Real-Time email Scan	✓	✓
Password protection	✓	✓
Heuristic Scanning	✓	✓
Registration/Activation: (via Web/SMS/eMail/FAX)	✓	✓ Not Documented
Real-Time web page scan	X	✓
Grid-based Web Access/Timing	X	X
Personalized Dash Board	X	X
Instant Messenger Encryption	X	✓
Pulse/Push Updates	X	X



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.

File and Folder Protection

We are all are paranoid about losing important data. However 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 the module also prevents deletion and creation of files within specified 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.

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.

Dual layer firewall protection (Network / Application layer)

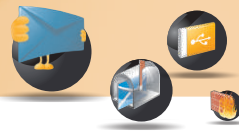
When it comes to standalone Anti-Virus programs most security companies overlook the most important aspect – the Firewall. Having a Firewall installed prevents unauthorized users, such as Hackers, from accessing confidential or private data over a network. Having said that, the Firewall implemented by eScan is not only limited to our Security Suite but trickles down to the Anti-Virus that we provide. As mentioned, it comes unchanged and is designed to monitor both incoming and outgoing traffic thereby providing a higher level of security. It comes with a predefined set of rules that monitors (protocol specific) both network traffic and applications that require Internet connection. In addition, advance users can fine tune the firewall by adding their own set of rules and also permit/deny applications from accessing the Internet or network.

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.

Auto-backup/restore

The auto backup/restore feature of eScan is probably the most striking feature that our product has. The basic functionality of this is to create backups of critical files that correspond to the Windows OS. So in the event of an infection the auto backup and restore kicks in and restores critical OS related files that cannot be disinfected. This whole process is automated and requires no user intervention.



Malware URL Filter

With social networking on the rise, malware writers are using sites such as Facebook and Twitter as a platform to infect PCs. This is achieved either by appearing as a legitimate social networking application or it could spread via spoofed links that make their way to your Inbox. To help prevent this, eScan 11 features a malware URL filter that prevents access to infected sites.

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.

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 email will be automatically blocked from being downloaded.

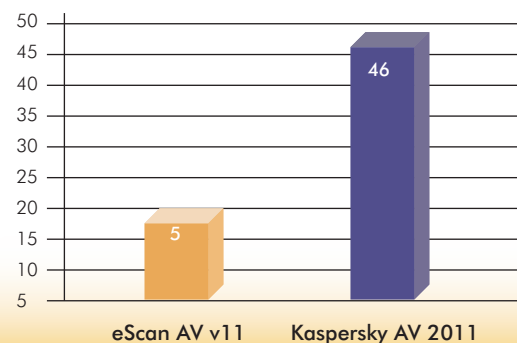
Spam URL Realtime Blacklist (SURBL): The functionality of this is almost the same as that of RBL. However the SURBLs main function is to check the URLs in the message body of an email. So if the URL is listed on the SURBL site the email is immediately blocked from being downloaded.

False Positive measurement of AV product (On-Demand Scan)

AV-Comparatives is an Austrian Non-Profit-Organization, who provide independent Anti-Virus software tests free to the public. It is not only important to measure the products detection capabilities but the overall reliability of the product is of utmost importance. The goal of conducting a False Positive test is to help users differentiate between a good product from a far more superior product.

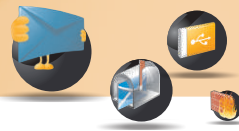
Before proceeding with the tests both programs were updated with the latest signatures. The test conducted shows the overwhelming FP's detected by Kaspersky as compared to eScan. A decent 46 FP's were detected in comparison to just 5 FP's by eScan.

The following chart displays the number of false positives reported by both programs.



Source: AV-Comparatives.org (August 2010)

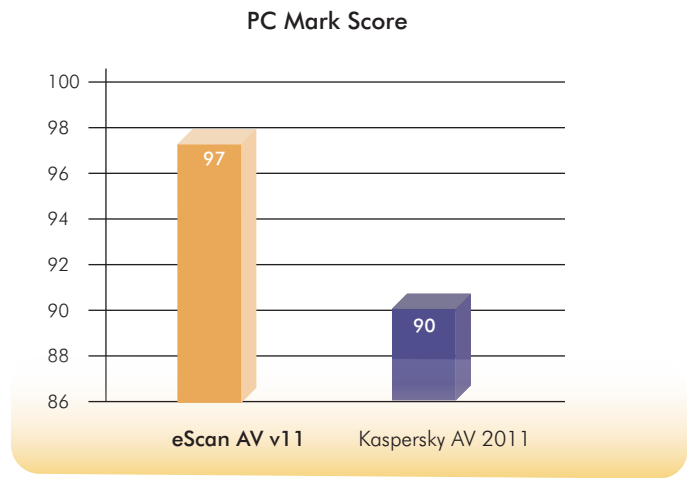
■ eScan ■ Kaspersky



Performance Test

The tests were conducted by AV-Comparatives on an Intel Core 2 Duo E8300 PC with 2GB of RAM and SATAII hard disks. The performance tests were first carried on a clean Microsoft Windows 7 Professional (32-bit) system and then with the installed Anti-Virus software.

The chart shown below is a summarized score of various tests conducted by AV-Comparatives. Tests include file copying, archiving/unarchiving, encoding/transcoding, installing/uninstalling. In addition to this, tests that were also taken into consideration were file download speed and application launch speed. These tests basically give a brief overview of the affects on system performance by individual Anti-Virus products



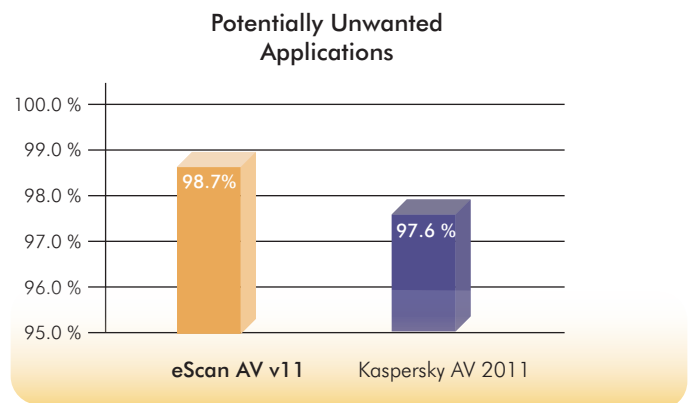
Source: AV-Comparatives.org (December 2010)

eScan Kaspersky

PUAs: Detection Rate

PUAs or Potentially Unwanted Applications can be directly linked to spyware, adware, dialers or even misleading applications. They can come across as legitimate programs repackaged and distributed via the Internet. So what you feel is legitimate in fact comes packed with a Trojan or Root Kit that bury themselves deep within the System, oblivious to the Virus scanner.

The following test shows the overall performance of the Virus scanner to detect PUAs and rogue software. The test set used by AV-Comparatives include a total of 82036 samples.



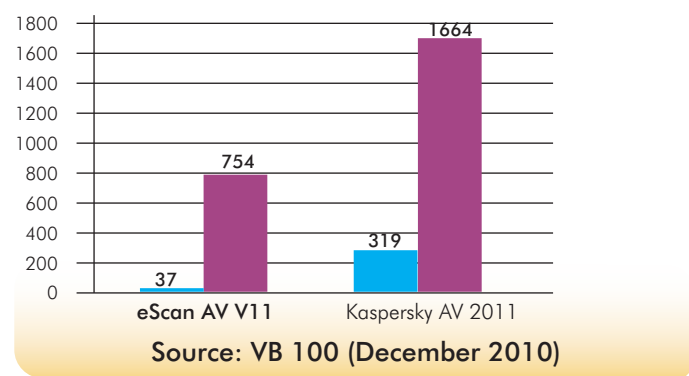
Source: AV-Comparatives.org (December 2010)

eScan Kaspersky AV 2011

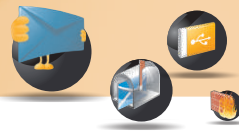
Missed Samples (On-Demand scan test)

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 – Kaspersky. We haven't included the WildList and Polymorphic virus scores as both security suites scored a full 100% in detection and removal.



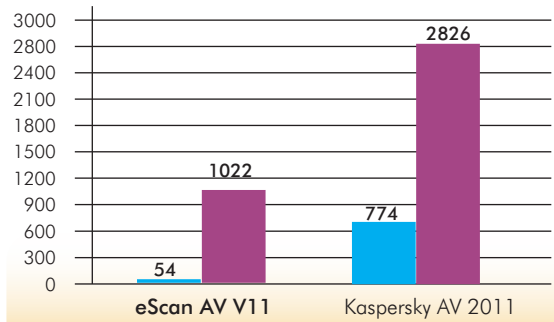
Worms & Bots Trojans



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 hone.

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



Source: VB 100 (December 2010)

■ Worms & Bots ■ Trojans