



eScan Internet Security Suite v11 VS Kaspersky Internet Security 2011

Why do we need Internet Security?

In this day and age data theft is by far a major concern – be it for organizations or even individuals. Now the question that needs to be answered here is, 'What do we understand by data theft?', 'Is it limited to organizations or does it trickle down to end users/consumers too?'. The answer is simple – data that is of importance to you is also mighty important to snoopers. It could be your school/college project or even specific files and folders. However for organizations, securing every bit is done on a much larger scale. Here it could be anything from financial accounts to intricate details of customers/employees. This is where endpoint protection plays a vital role.

But what do we mean by '**Endpoint Protection**'? In computing terms, Endpoint basically refers to ports to which USB and FireWire based devices connect. Therefore, having these ports left open is a concern as there are high chances of data theft. At eScan we understand the needs of not only our enterprise users but also end users who require protection not only from Malware but also from data theft. Not only can users lock down all endpoints but it also prevents malicious programs from executing as and when a pendrive is inserted.

Moreover with a large number of people logging into Networking Websites, malware writers are beginning to target sites such as Facebook, Twitter, Orkut (to name a few). For instance, 'My 1st St@tus' scam affected thousands of users on Facebook. However such applications don't just get added to your profile but are generally granted access by the user himself. Once allowed, the application can not only acquire profile details but can also post messages on your behalf. It not only ends there, the application then spreads across the network through all who are linked to your profile. While this particular application doesn't infect the PC there are many other who direct you to malicious websites that could be home to Trojans and various other malware. To prevent such rogue instances from taking place eScan comes built with a URL filtering module that prevents web pages from getting redirected to malicious websites or URLs.

In addition to this, personal information can include anything from debit/credit card details, passwords for your personal accounts, bank details etc. To help protect your digital identity eScan ISS provides a much needed secure environment in comparison to other Security Suites. This would include certification levels 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 ISS v11. The second half displays the effectiveness of the protection offered by both security companies – eScan and Kaspersky Lab.

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

Am sure that most if not 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 to this the module also prevents deletion, creation and modification of files and folders.

Endpoint Security

To prevent data theft, eScan ISS v11 features Endpoint Security that allows blocking of all USB and FireWire ports. This ensures a higher level of privacy and security since the chances of data theft is minimized to a great extent. That apart – Administrators or users can also choose to enable 'Read Only' mode which basically allows users to only read content from USB drives. Other features include – disabling AutoPlay, Password protection and Whitelisting specific USB drives.

Application Control

Another aspect of Endpoint Security is the Application Control feature. This added feature allows you to block applications from running on your PC. It includes pre-defined computer games, instant messengers, video/music players and P2P applications. In addition to this users can also add applications that need blocking.

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 ISS 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

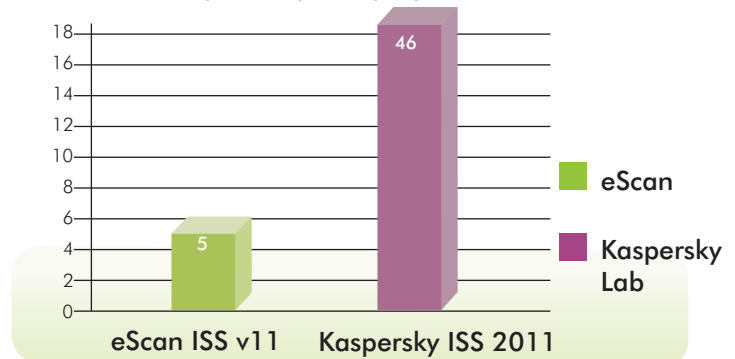


False Positive measurement of AV product (On-Demand Scan)

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.



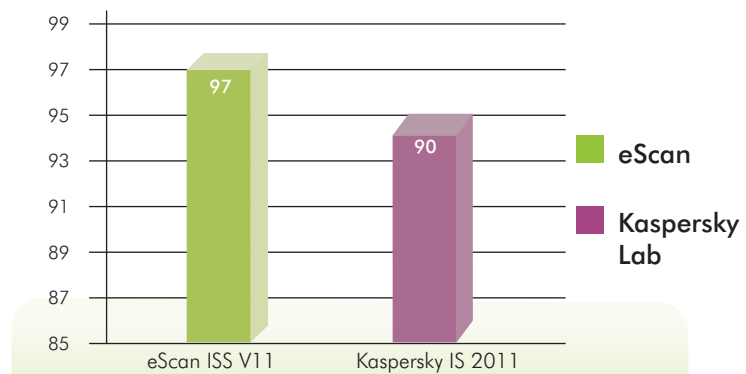
Source: AV-Comparatives.org (August 2010)

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.

PC Mark Score



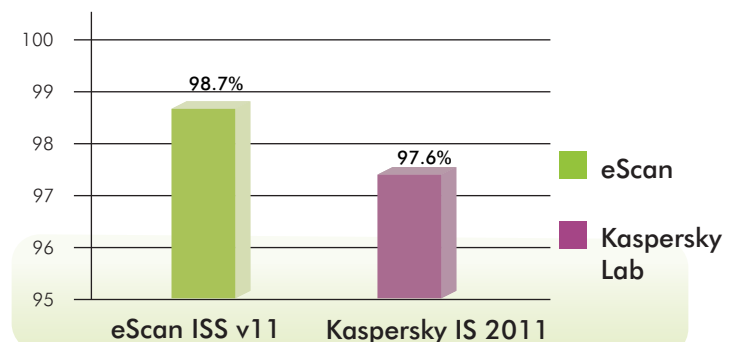
Source: AV-Comparatives.org (December 2010)

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.

Potentially Unwanted Applications



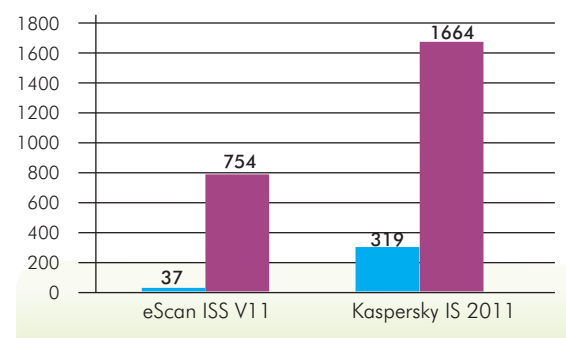
Source: AV-Comparatives.org (December 2010)



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.



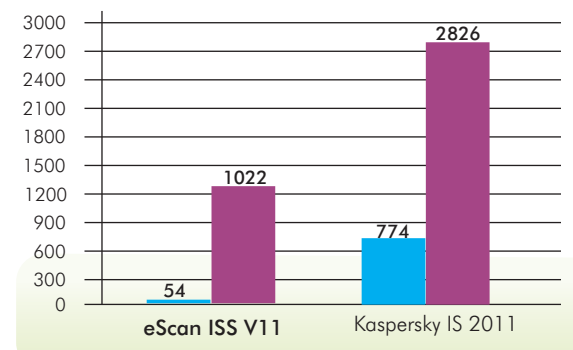
Source: VB 100 (December 2010)

■ 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 have.

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 products.



Source: VB 100 (December 2010)

■ Worms & Bots ■ Trojans