

eScan Personal Edition

This scans all incoming data before it reaches the application

Viruses are finding newer and creepier ways of getting into computers and making our lives hell. So applications that block them also have to get smarter. There is no denying that e-mail is the most common medium for the spread of viruses these days. eScan Personal Edition not only protects your system from viruses, but also follows a different technique to do so. It servers. So, if an e-mail attachment contains a virus then your anti-virus will warn you when you actually try to open the attachment.

eScan is available for different versions of DOS, and Windows 9x/ME/NT/2000. It's pretty straightforward to install and creates an eScan monitor icon in your taskbar, which constantly runs in the background looking for viruses. All configuration settings can be accessed from this icon. Apart from the normal detection method, it follows two more methods called Heuristic and Reference analysis.

scans all incoming data before it reaches the applications it's meant for. Let's first understand how it achieves this.

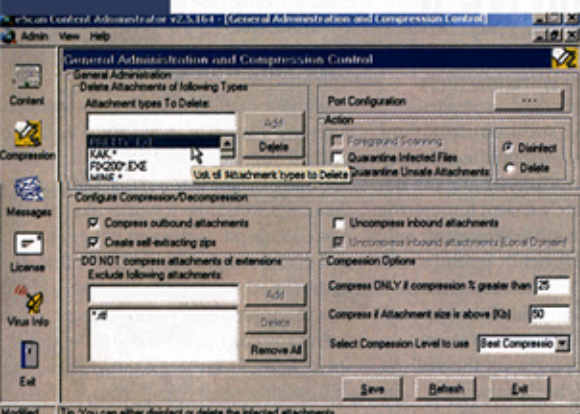
All data reaching applications like Outlook Express ICQ or IE passes through the WinSock layer, which is located at the transport layer of the OSI (Open Systems Interconnect) reference model. eScan creates its own layer, MWL (Microworld WinSock Layer), between the WinSock layer and your PC. This way all data passes through the MWL before reaching the application it's meant for. eScan can therefore detect viruses or malicious content before it reaches the application. Most anti-virus programs, on the other hand, detect a virus after it has entered the application, unless they route your e-mail through their scanning, or just log the event. You can scan network drives, provided they're shared. As with most anti-virus packages, this one too allows you to schedule scans.

Content Analyzer

The interesting part about eScan is its content analyzer. This can check for specific phrases in your incoming mail content and also scan attachments. It also has a list of files, which are known to be viruses such as KAK.*, and Love*.VBS. eScan will prompt you with a message the moment it finds a virus or unwanted content. You can also set it to automatically delete or quarantine such attachments. You can also specify your own file names or extensions for it to look out for. Another useful feature in eScan is that you can choose to automatically compress all outgoing mail attachments. This is useful as it saves both time and bandwidth. If you are not sure whether the recipient will be able to uncompress your attachments, then you can also send self-extracting zip files. For smaller files, however, this can actually increase the size of your attachment because the self-extracting program also needs space.

To see eScan's MWL in action we did a couple of interesting tests. We first set up a filter in Outlook Express to look for the word 'PCQ' in all incoming e-mail and move that mail to a specified folder. We then went to eScan's Content Analyzer and configured it to do the same thing, meaning look for the word 'PCQ' in all incoming e-mail. Here, if the word was found, we configured it to quarantine that mail. Finally, we sent a mail filled with lots of text with the word PCQ hidden deep inside. The result was quite interesting. As soon as we tried to receive the message in Outlook Express, eScan prompted us with the message that the mail contains the protected word 'PCQ' and is being quarantined. This happened much before the Outlook Express filchouse Network then you just have to specify the network path where the latest definition files are available. This could be useful because you only have to download the updates on one computer on the network and the others can pick it up from there. eScan can also be scheduled to automatically download the updates. Overall a very useful package, considering the functionality it provides.

Sachin Makhija at PCQ Labs



Modified Tip: You can either distract or delete the infected attachments.

eScan has a list of files that are known to be viruses, and scans your e-mail for attachments with these names

The Heuristic analysis lets you find viruses that are not yet included in the eScan virus database. The Reference analysis generates checksums for files that are analyzed and compares these sums with the results of the next analysis. This helps it detect viruses that may not have been discovered yet, and have made changes to your files. It also allows you to specify the objects to include while scanning, for example, compressed files, program files, all files, or the file types you specify.

eScan's other functionality is similar to any other ordinary virus scanner. You can specify certain actions to perform once a virus is detected. You can delete or quarantine the file, remove the virus, stop your ter got its turn. eScan also sends back a mail to the sender who's sent a virus or unwanted content.

Like other anti-virus programs, eScan also has an update utility called the eScan updater, which runs in the background and can easily be accessed from your system tray. It lets you download the updates using HTTP, FTP or your network. If you access the Net through a proxy server then you can also specify its address. If you