

R245: eScan Virus Control Edition (no profanity scanning)

0000

R335: eScan Pro Edition (includes profanity scanning)

Whenever I hear about someone's PC being infected by a new virus, I tend to blame service providers, from the point of view that most viruses these days come via the Internet and are on your system via email

before you realise it's time to fire up the

virus scanner. But then I remember

that not everyone has their own Unix

mailserver, as we do, and I suppose it's

a lot easier for us to implement security

on our server than it is for an ISP

with thousands of users.

If your ISP can't, or won't, filter your email for nasties, you have to do it yourself. Virus writers are constantly finding "new and improved" ways of getting their offspring into computers, so applications that detect viruses have to stay one step ahead.

The explosive growth in email use has meant that it is easier than ever to pick up a virus – innocently clicking on an attachment could wipe out your data before you know it. Now an Indian company, MicroWorld Software Services, has come out with eScan, a product that protects your system from viruses in a completely new way.

Most anti-virus programs will only detect a virus after it is on your system, so if an email attachment contains a virus, your anti-virus software will only warn you when you try to open the attachment. eScan scans incoming data before it reaches the application that will be activated by it.

Data reaching Internet-aware applications is routed through a layer called the WinSock layer. eScan creates its own layer, MWL (MicroWorld WinSock Layer), between the WinSock layer and your PC. By doing this, data passes through the MWL before reaching the application that uses it. eScan can, therefore, detect a virus or other malicious content before it reaches the application.

eScan also uses heuristic and reference analysis to protect your PC. Heuristic analysis can find viruses that are not yet included in the eScan virus database by comparing similarities to other viruses within files, while reference analysis generates checksums for files that are analysed and compares these sums with the results of the next analysis, making it easier to see which files might have been modified by a virus.

As with most virus programs, you can define what actions to perform once a virus is detected. You can delete or quarantine the file, remove the virus, stop scanning, or just log the event. You can also scan shared network drives.

A feature that is really useful is eScan's content analyser. It can check for specific phrases in incoming email and attachments, and it contains a list of known viruses and worms. If it finds a virus or unwanted content, you have the choice of being notified, or you can set it to delete or quarantine the suspect file automatically. You can also specify your own file names or extensions, making it easier to avoid new Trojan types of files (assuming, of course, that you stay up to date with what's happening in the virus world).

eScan is also able to send an email to the sender of a virus or unwanted content, notifying him of the problem and the program can be set to update via the Internet automatically. Although I was a bit disappointed with the quality of the manual, eScan is surprisingly good at what it does.

