



# virus

## BULLETIN

### VIRUS BULLETIN PRODUCT REVIEW: MICROWORLD ESCAN INTERNET SECURITY SUITE 10 – JANUARY 2009

*MicroWorld Technologies* was founded in 1994, and is incorporated in New Jersey with its development team based in India, and offices and partner companies worldwide. The firm specializes in security, providing a wide range of solutions and services on multiple platforms. Its best-known and flagship product range is the *eScan* range of security software.

*eScan* has been a regular entrant and pretty consistent performer in VB100 testing since 2003. In the course of five years of testing, the product has picked up 16 VB100 awards, with only a handful of false positives upsetting things on a few occasions in the last few years. Over this time, the product has evolved from providing an alternative front end to multi-engine scanning to the current complete Internet suite, with the *Kaspersky* detection engine at the core of the anti-malware protection. A slick new look accompanies the upgraded set of functions and protection features, and after putting it through its paces in the last VB100 comparative, we were keen to take a deeper look at what it had to offer.

#### WEB PRESENCE, INFORMATION AND SUPPORT

The main online home of *MicroWorld* is at [www.mwti.net](http://www.mwti.net), a simple, unflashy site with the tagline ‘We add confidence to computing’. The sober, pared-down nature of the home page is offset by a glossy, animated advertisement for the product under review this month, *eScan 10*, which is due for release very soon. The remainder of the page is simply rendered and information-packed. The left pane carries a comprehensive menu of the site’s offerings, with the product range highlighted and categorized by user type, product type and operating system. Also here are links to support, product purchasing, downloads, licensing and updates, as well as some company information. The central panel runs through the product range again, with links leading to detailed pages on each, and below this is a cluster of company news items and press releases. The right-hand pane is more support-oriented,

with a 24/7 toll-free US support number prominent, closely followed by a link to support forums. Below this, information is provided on the latest threats and product updates, and there is the option to sign up to a newsletter for those wanting to keep up to date with this kind of news.

The product section is very clear and thorough, with each market sector (home-user, small business and enterprise) treated to a thorough list of the available solutions with full details on the protection they provide. The range itself is pretty extensive, with support for a variety of *Windows* requirements – from the desktop suite under review here through enterprise versions with full management and reporting systems, to mail and web gateway solutions – while *Linux* users are similarly well catered for, the product list again running the gamut from the desktop to the gateway.

The download section sits behind a form requesting some personal information, such as your email address and which product you are interested in downloading, but this seemed not to work for us.

The support section suggests users contact the firm via email if possible, but also provides a chat system, with links to *MSN Messenger* or *Yahoo! Chat* for those that need them, as well as free telephone support for all users – an admirable provision for users in dire need. For those with less urgent issues, the forum section provides a reasonable collection of FAQs alongside the busy tech support area, where answers seem to be provided promptly and graciously.

More in-depth product information seemed a little hard to come by – with no search option obvious on the website, a rummage around eventually turned up manuals for the products, the links tucked away at the bottom of the details pages. The manuals seemed fairly thorough and clearly written, if a little short on colour and illustration, and organized more by function than task. Help within the product itself, we later found, had no local data but instead connected to the web, calling up the appropriate page of a wiki-based system – an interesting new direction for such



functionality. Sadly, as the product under test is still in the final stages of beta, no manual was available and much of the wiki remained unpopulated, so no assessment could be made of its quality and usefulness.

Returning to the main website, the virus information area presents a cursory malware encyclopaedia, not over-stocked with entries, but lucid and detailed on those covered. The company sections provide a selection of tidbits on the company's past and achievements, including its VB100 awards, as well as lists of events being attended by company representatives in the upcoming months, job vacancies, and more complete contact details for the various branches.

One of the most useful things to be found here is a free version of the on-demand scanner, *MWAV*. This neat little tool provides the full functionality of the on-demand part of the product, including cleaning, quarantining and updates, without the need for a full installation process. It can be run in conjunction with installed anti-virus without much further effort, providing a useful alternative to online scans and other such extra layers of security reassurance. Most of the company's other products also seem to be offered on a free trial basis for interested users.

## INSTALLATION AND CONFIGURATION

Moving off the web and into the lab, we took a second look at the new *ISS* product, having given it a quick run-through in the recent VB100 comparative. The set up process is pretty standard, going through the usual options and then taking about a minute or so to perform its copying and configuration processes before launching an immediate scan of vital areas, the system folders and registry. A reboot was then required to complete the installation, after which a popup declared *eScan* had provided 'The world's first real-time email and webscanner', while a swift and unobtrusive update of definitions etc. zipped along in the background. Beyond that, no further manual configuration seemed to be required – all firewall rules etc. are applied automatically at a default level with none of the customary requests for detailed technical information seen in many products these days, making *eScan* suitable for the most technophobic of users. With everything set up and safe, we fired up the main interface to explore what was on offer for those with more particular and exacting requirements.

The main interface is pleasantly straightforward, with a simple list of sections down one side and checkboxes in the main window to indicate the status of various modules. Some of the main options seem a little less vital than others: while the 'Protection' tab covers a seriously wide range of controls, 'Update' is perhaps less of a major issue, at it should mostly be automated, while one wouldn't expect to use the 'Product key' section more than once a

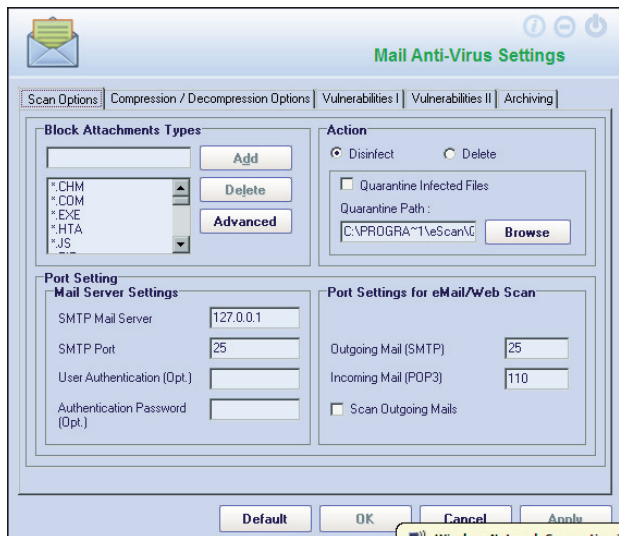


year – perhaps it disappears once a full licence is applied. Looking into the update tab, a huge range of configuration options are available beyond the usual basics of automatic/manual and frequency options. Update sources and connection protocols can be set, including local network updates, schedules can be fine-tuned to great depth, and a range of post-update activities, including mail notifications and customs execution of commands, are also available, providing enterprise-grade configurability to those who want it. The licence key tab, however, simply offered a dialog box to enter a licence key.

A quick glance through the remainder of the main tabs showed a pleasant continuity of design, with initial pages clear and simple, providing basic data on the module in question and buttons to access detailed configuration and reporting options. We looked through some of these in more depth, starting with the system protection tab.

## SYSTEM PROTECTION AND MALWARE DETECTION

The anti-malware components are controlled from the first two tabs, the first of which covers real-time monitoring and the second on-demand scanning. The on-demand tab provides a good list of default scan types, covering core areas such as memory, registry and system folders, the local file system, spyware and adware, USB drives and further custom options. A scheduling system allows simple set up of multiple types and depths of scan. Default settings tend towards the thorough, and the scanning speeds recorded in the recent VB100 test reflect this thoroughness, but there are plenty of options to exclude archives, areas, file types and so on, as well as prioritization options which can speed scans up or minimize system impact as required – such impacts were barely noticed, and on-access times in our earlier test



showed pretty decent overheads. Even running on a fairly low-powered test notebook, no slow down in operation was evident to the naked eye.

Detection, mainly provided by the *Kaspersky* engine with some enhancements of *MicroWorld's* own, is superb. The product, like many using the *Kaspersky* engine, has a pretty decent record in our VB100 testing. Undetected items are vanishingly rare, even in the more obscure test sets, and WildList misses almost unheard of, even when complex and difficult polymorphic viruses make their way onto the list. The recent addition of new, freshly updated sets of trojans into our test sets has shown up deficiencies in some products, but *eScan* has maintained an excellent standard, regularly catching more than 90 per cent of the samples with the standard scanner alone, putting it in the top handful of products in this regard. On the few recent occasions on which *eScan* has failed to achieve a VB100 award, it has been relatively minor false positive incidents that have let it down.

Of course, with the vast number of new malicious items being seen these days, simple signature-based detection is increasingly sidelined in favour of heuristics and other techniques. While the *Kaspersky* research lab has an excellent record of speed and throughput, keeping up with the flood at a remarkable pace, many products, including *Kaspersky's* own suites, have begun to introduce more advanced behavioural monitoring and HIPS systems into their suites. Although no such options are evident in *eScan*, the few items we managed to find that were not detected by the standard scanners were blocked instantly on attempting to execute by some more sophisticated heuristic or emulation techniques – a simple message is presented, warning that the files in question are suspicious, and the user is given the

option to allow them to run if trusted. Where the monitor has been protected with an administrator password, this password is required before such potentially unsavoury items are granted access to the system.

Anything not spotted by this protective layer would then come up against the firewall, which seems to operate well with sensible defaults and minimal interruption of the user with requests for permissions. Again, configurability is enormous, with the default 'limited filter' setting easily switched into a more interactive mode for those wishing to monitor events for themselves, and simple allow all/block all buttons permitting easy lockdown or opening up of the system. The advanced tabs offer all the expected configurability, laid out and controlled with admirable clarity and simplicity.

The mail malware filtering is similarly configurable. The mail scanner allows attachment file types, multi-extension files, and even files with specified strings in the name to be blocked automatically, introducing an element of content filtering and policy enforcement to the mix. It can be set to decompress and scan compressed attachments if required, and has a number of anti-exploit techniques including the blocking of HTML mails containing scripts. All are readily customizable.

All these areas offer in-depth logging, with the firewall particularly well provided for in this area – detailed summaries and reports can be generated on recent network activity and what filtering was applied, with a graph generator included. Current activity can also be monitored in real time using a TCP viewer utility included with the suite. This is a nifty little tool which provides details of all processes and connections passing through the firewall, and allows the user to kill any undesired processes.

The remainder of the 'Protection' section, while providing some protection from malware, also addresses a range of other security issues, and will thus be analysed in the next section.

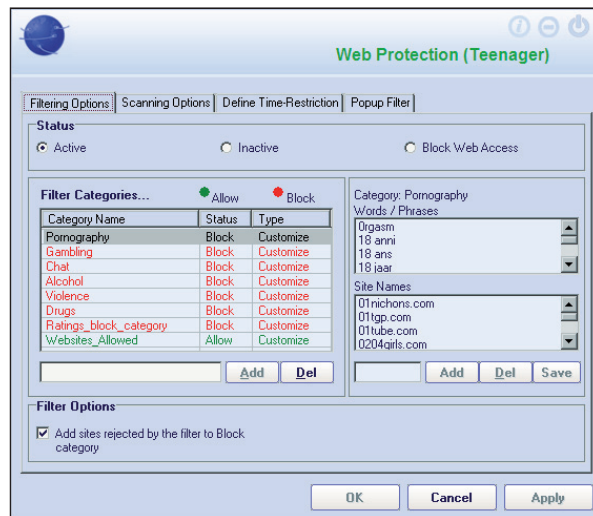
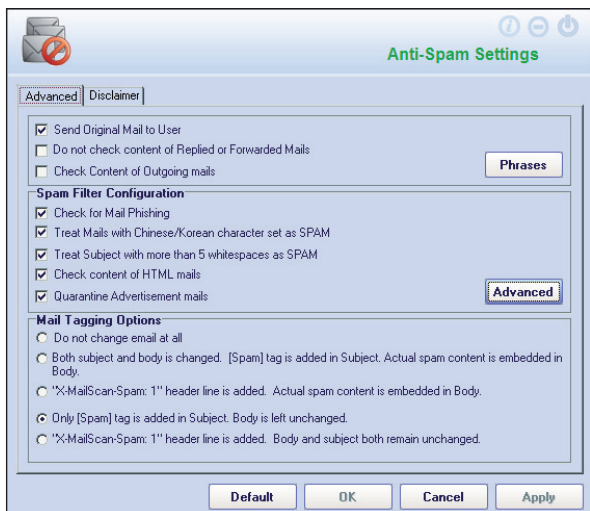


## OTHER FUNCTIONALITY

Without wanting to play down the main anti-malware and anti-hacking components of this suite, which are clearly of high quality and solidly implemented, they are fairly standard and to be expected in a security product. Much of the beauty of this latest iteration of *eScan* lies in the many extras to be found in the additional tabs and in advanced configuration controls of the main modules.

The anti-spam component has become another basic and expected part of any Internet security suite, and it is not omitted here. The filter, when fired up, checks out installed mail software including *Outlook* and *Thunderbird*, with many other tools supported, and boasts ‘Non Intrusive Learning Pattern’ checking. The controls and configuration are extremely clear and easy to navigate, and the advanced options splendid – there is an option (enabled by default) to classify all mails containing Chinese or Korean characters as spam, which would reduce my personal spam level by about 60% in a single blow. Further checkboxes activate the use of the SPF system, and connection to RBLs and SURBLs, with a customizable list of reputation data sources. An address whitelist is automatically populated with accepted mails within inboxes found on the system, and can be further expanded with ease. A further white/blacklisting system, based on words and phrases, is equally easy to configure, allowing specific terms to be barred or allowed with a few clicks.

We had neither the time nor resources to test the filtering performance properly, but a quick look at it over a few days’ worth of personal mails seemed to show a perfectly reasonable spam detection rate, with no false positives spotted. Even if the catch rate were to be at a bare minimum, the depth and simplicity of the user configuration options make this a remarkable and highly effective tool.



Moving on to the remainder of the modules under the main ‘Protection’ tab, the first on the list is labelled ‘Web Protection’. Having at first assumed this would be a component of the anti-virus protection (scanning web downloads as they came down), we were surprised to find that it is in fact a fully featured parental control system, with four levels of control. The control levels are intended for small children, two classes of teenagers and adults. The complex and in-depth control system allows access to sites to be blocked by category, name and keywords; defaults in the ‘Pornography’ section include ‘hot bottom’ and ‘legume’. A maximum permitted frequency of such shocking words is configurable for each user category. Specific content types can also be blocked, the filter using data from respected online safety agencies including *SafeSurf*. Time restrictions can also be configured to limit usage, and full logging of all violations is provided. A lengthy default whitelist of sites is provided, which is again highly configurable, and for the youngest category of users only these approved sites are accessible.

Next up is a section rather vaguely labelled ‘Endpoint Security’. This is an application control system, disabled by default, with a well-stocked list of applications split into categories including games, IM and P2P applications, and media players, with further user-defined options easily set up. The second part of this module, labelled ‘USB control’, manages connection of USB drives and devices to the system, allowing the user to specify that a password must be entered before a drive can be mounted, to disable *Windows*’ notoriously dangerous autorun set-up, to scan USB drives or mount them read-only, and even to whitelist trusted drives.

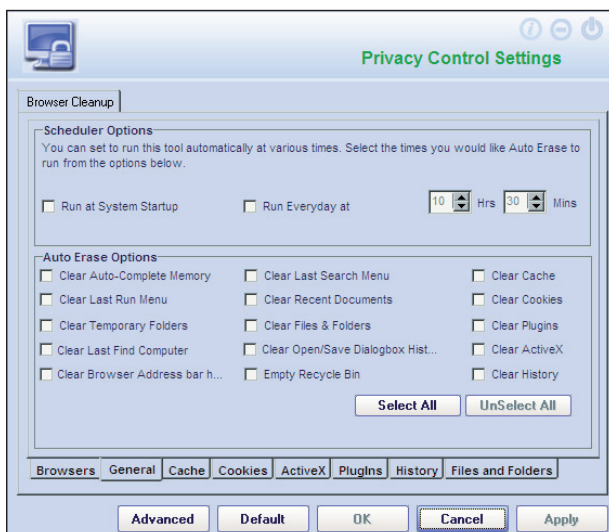
The final section of the main protection tab, ‘Privacy Control’, provides automated removal of browsing history and other traces. The single page of the control interface provides scheduled cleanup settings, along with the ability to

browse and delete or block specific cookies, remove browser plug-ins and helper objects, peruse browsing history, purge caches and even add cache folders for purging. All of these options cover all installed browsers (with the apparent exception of *Google Chrome*). Yet again, the design is straightforward and easy to understand and use.

The entire set-up can be protected with an administrator password, allowing parents or owners to maintain tight control of their machine, whoever is using it.

One final section merits some comment: a tab on the main screen labelled 'Tools'. Here, the main tool is a system information monitor, which displays a vast range of data on the system being watched. Full details of hardware and drivers are covered, similar to the information provided by the standard *Windows* 'System Information' tool but considerably more user-friendly, and combined with a range of other items such as lists of installed software, shared folders and drives, startup items, and running processes. Most, if not all of the information here is available from various normal *Windows* components or free tools available from *Microsoft* (particularly since its acquisition of the *Sysinternals* product set), but having so much together in a single, simple interface is a boon for the power user.

Also listed under 'Tools' are options to report a bug or defect to the manufacturer, and to download the latest 'hotfix' – presumably managed separately from simple detection updates, possibly as system restarts may be required to get them running. Finally, there is a scanner which checks through the registry and system areas and resets any significant changes to the *Windows* defaults. This chugs through the system resetting various options, such as settings for displaying hidden system files and so on, to the *Windows* defaults.



## CONCLUSIONS

Having had considerable experience of *eScan* products from numerous VB100 outings, we have always found it to be a solid and well-designed implementation of the *Kaspersky* detection engine, a pleasure to test with its stability and straightforward, sensible layout. Having expected a suite version to include the standard additions of firewall and anti-spam and little else, we were both surprised and impressed by the full range of additional tools available. The application control and parental control options, the privacy monitor and system analysis tools, the mail and web policy enforcement and much more were all unexpected delights. That just about every component seemed to work solidly and without fuss was another bonus, but the clarity and simplicity of the configuration system really puts the product into the top league. Providing such user-friendly design, making the more sophisticated areas of the product accessible to any user regardless of their technical ability without compromising on the finely graded configurability, is truly a remarkable feat.

Reading back through this review, parts of it may come across as gushing and over-enthusiastic, but I am genuinely most impressed with this suite. It seems to provide, for home users, levels of control over their systems usually only available to enterprise network admins running a range of security products and custom client lockdown scripts. I can only recommend that users, guided by what will hopefully be a decent help system when it comes on line, spend the time to plough through the vast range of options and settings dialogs to get the most out of the great degree of control available here. Even with its default set-and-forget settings, the suite provides a top-class level of protection, but with so much more to offer it would be a shame to see any of it go to waste.

### Technical details

*MicroWorld eScan Internet Security Suite* was variously tested on: *Intel Pentium 4 1.6 GHz, 512 MB RAM, running Microsoft Windows XP Professional SP2; AMD Athlon64 3800+ dual core, 1 GB RAM, running Microsoft Windows XP Professional SP3 and Windows Vista x64 SP1; Intel Atom 1.6 GHz netbook, 256 MB RAM, running Microsoft Windows XP Professional SP3.*



*MicroWorld Technologies Inc.,  
33045 Hamilton Court East, Suite 105, Farmington Hills,  
MI 48334-3385, USA  
Tel: +1 248 848 9081/9084 Fax: +1 248 848 9085  
Email: sales@mwti.net, Web: http://www.mwti.net.*