

PRODUCT REVIEW

MICROSOFT SECURITY ESSENTIALS

John Hawes

Microsoft Security Essentials, the long-awaited replacement for the *Windows Live OneCare* package, is finally with us. When the globe-straddling giant began its push into the anti-malware sphere a few years back, some initial poor test results dented the launch of *OneCare*, and sluggish performance and general lack of user interest were immediately apparent. Despite a much improved version 2, *Microsoft* quickly decided to give up on the product – and its retirement and replacement were announced almost a year ago. The new project, codenamed ‘Morro’, excited a great deal of debate and no little controversy around the topic of free AV – and the debate continues to rumble on now that *Security Essentials* is available to the public.

One question which has received little attention amongst the hype and hyperbole surrounding the launch of *Security Essentials* is: what is meant by ‘free AV’? We know from correspondence with our readers that some people always run some high-quality, multi-function suite without paying for it. They do so quite legally, simply by switching from one free trial to another every few months. Others get free access to security software via a value-added model. Should I need one, I could get myself set up with an expensive security suite at no charge thanks to extras thrown in with my bank account, my ISP, my phone line or TV provider, or any of a number of others.

Of course, none of these are completely free – the trial option requires considerable investment of effort, while the value-added path depends on having paid for the original product or service. What about the people who don’t have the time or inclination to regularly reinstall software, and who can’t afford the kind of service contracts that throw in extras? For them, the most common answer is the free-for-home-use model, under which developers make pared-down versions of their software available free of charge, on the condition that it is only for personal use.

The free-for-home-use field is currently dominated by the three ‘A’s: *Alwil* (*avast!*), *AVG* and *Avira*. Many other providers also release parts of their product range without charge, but it is these big three which dominate. According to a recent blog post by *Alwil*’s CEO, 50% of the world’s 500 million consumer machines run one of the three, compared to 20% running one of the ‘market-leading’ brands, *Symantec*, *McAfee*, *Trend Micro* and *Kaspersky*¹. The business model is a simple one, providing the

¹ <http://blog.avast.com/2009/10/02/and-what-about-microsoft-security-essentials%e2%80%9494mse/>

companies with wide market penetration and excellent brand recognition. A small fraction of users of free products will upgrade to paid editions, while the widespread distribution of the free products also provides the companies with an additional source of fresh samples that’s pretty hard to beat. All this can be achieved for no more than the cost of a little server space and bandwidth for updates, and a few man-hours for the monitoring of help forums (which are essentially fan-maintained).

So where will *Security Essentials* find its place? Clearly *Microsoft* has slightly different goals here – the firm has little need of additional publicity, and it seems unlikely that many users of *Security Essentials* will be tempted to upgrade to its corporate big brother *Forefront* (*Security Essentials* is targeted squarely at home users). There will, of course, be some advantage to be gained from the increase in new samples flowing into the company’s labs, but with such massive presence in all sorts of areas, this should not make a great impact.

The stated aim of the product is to provide protection for those users currently running their machines unprotected, particularly in less developed nations (some reports have estimated as many as 50% of users are not running up-to-date security software²). As always when *Microsoft* takes steps in the security world however, many sceptical commentators have viewed such altruistic claims with suspicion, muttering that such efforts may simply be part of an ongoing campaign to counterbalance the company’s reputation for insecurity in its operating systems. Despite making great strides in recent releases, that reputation lingers thanks to the continual discovery of new flaws and vulnerabilities in many areas – perhaps inevitably, given the breadth and scope of the company’s product range, and the armies of hackers beavering away looking for cracks to crowbar open.

Once the decision to retire *OneCare* had been taken, releasing the *Security Essentials* product seemed almost to have no downside for *Microsoft*. The interface will likely require little maintenance, support will likely be kept to a minimum, while the engine teams and malware analysts will already be hard at work maintaining *Forefront* – so it could just be that the proclaimed altruism is genuine, and the improvement of the firm’s security image just a side effect. There are similarly few downsides for users – the product is available free of charge to those who want it, and even if it is only taken up by a tiny fraction of potential users and only provides minimal protection, it will still contribute positively to the overall security picture. The uptake may well depend on the quality of the product, but will also doubtless be influenced by promotion, marketing and the response of users.

² http://www.theregister.co.uk/2009/09/29/ms_security_essentials/

SECURITY ESSENTIALS: PROMOTION, INFORMATION AND SUPPORT

The initial announcement of the retirement of *OneCare* and its replacement with a free offering attracted considerable interest, and a public beta release was heavily oversubscribed with many more users trying to get hold of it than expected. However, the final full release came with less of a fanfare, with interest somewhat depleted after almost a year of waiting, a staggered release into different territories and the impending release of *Windows 7* all factors in the relative quietness of the product's emergence.

Considerable attention was paid by the technical branches of the media however, with a mixed bag of early reviews appearing in the weeks following the official public launch. Many commented favourably on the product's simplicity and ease of use, while some – rather unfairly – criticized the absence of the full range of additional layers of protection, such as firewall and HIPS protection, found at the more advanced end of the suite market. Despite the somewhat tepid reaction, downloads were reported to have reached 1.5 million within the first week.

The product can be acquired from the microsite located at www.microsoft.com/Security_Essentials. The landing page is pretty simple and straightforward, with a big download button taking centre stage along with some basic information about the product. The fact that the product is free only for home users of genuine licensed copies of *Windows* is clearly highlighted; business users are directed to *Forefront*, while those seeking more information on malware are provided with a link to the Malware Protection Center (MMPC) portal. A selection of certification badges appeared soon after the site went live.

The most prominent buttons on the page are for help, support and an installation video (the use of which involved allowing scripting in the browser and, to view the video, installation of *Microsoft's Silverlight* system). An option was provided to download the video as a WMV file and watch it the old-fashioned way, but it appeared to be beyond the abilities of several older copies of *Windows Media Player*³.

A resources tab provides more links to the MMPC, the EULA and privacy policy (for the SpyNet system, which we'll come to later), and the system requirements – the product claims support for *Windows* versions from *XP SP2* up via *Vista* to the new *Windows 7*, and needs 140MB of hard drive space, a 500MHZ processor and 512MB of RAM (rising to 1GHz and 1GB for the *Vista* and *Windows 7* version). This all seems pretty reasonable, given the

³ Further product information and videos are at <http://www.microsoft.com/presspass/presskits/microsoftsecurityessentials/materials.aspx>

requirements of the operating systems, and hopefully few users will find themselves unable to use the product through a lack of computing power.

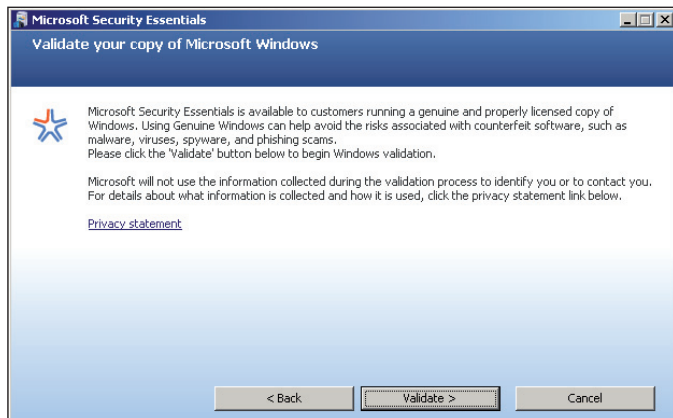
The final part of the page – probably the most important once users have acquired and installed the product – is the support area. This is already well stocked with FAQs, guides and how-tos alongside the videos mentioned earlier, and also provides access to a community-driven forum for resolving more specific problems. This seems to have generated some useful content already, and appears to be well staffed by some helpful and knowledgeable pros alongside the user community. With no proper manual apparent, there seems to be ample information available to steer users through any potential issues they might have, while a proper online support-case submission system is also provided for more troublesome matters, alongside a new threat reporting system.

The whole thing is smooth and slick (some issues with the videos notwithstanding), but there was one thing that did stand out like a sore thumb throughout the site: just about every page appears to carry advertising. Some layer of ad filtering managed to block the advertising on most systems we used to visit the site, but this spoiled the smooth clean lines with clunky block messages. I suppose we could have allowed the ads to see whether they would fit in nicely with the look and feel of the surroundings. Either way, though, the idea that help – even for a free product – is a suitable place for advertising seems rather uncomfortable, and somewhat dents the supposed altruistic ethos behind the project.

USER EXPERIENCE

With the product downloaded – a small initial file which took seconds to download with a fast connection – the installation process is pretty straightforward. It sails lightly and quickly through the standard set-up steps, with the only less usual one being a check for the genuineness of *Windows*. As honest, well-behaved people we did not have any unlicensed or pirate copies of *Windows* to hand to observe how it would respond in such circumstances, but on legitimate systems it trips through nice and quickly (even more so if the Genuine Advantage set-up has already been performed). The check for the legitimacy of the running *Windows* system has proved controversial, with some commentators arguing that the bulk of the audience *Microsoft* is aiming for – those running unprotected systems in less advanced regions – are likely also to be running unlicensed copies of *Windows*. However, the decision not to allow these users to protect themselves does make some business sense.

At the end of the installation process the product connects back to base to update itself, and offers to run a full system



scan once it is complete. In our tests the update never took more than a couple of minutes, even with a less than ideal web connection or having waited several weeks after the initial download. Once installed, a rather lumpy icon (which, after a few moments of staring, we deduced represented a square castle flying a large flag) appears in the system tray to indicate protection is in place.

The product itself is remarkably simple and clear, with a main page offering bare data on the protected status of the system (a bar turning red if any kind of threat has been observed), and a few buttons for different kinds of on-demand scans. An update tab provides some information on update status and a button to run a fresh update; a history tab reports details of threats detected and how they have been treated; and a settings tab provides some configuration options – with rather more choice available than might have been expected. There is a sensible set of defaults and a selection of useful options – including the exclusion of certain areas, types of files and even running processes from scanning – but there is not quite the in-depth configuration available as seen in the most sophisticated products. The scheduler allows only a single job, and as in so many systems is set to run in the middle of the night on a Sunday; some users may want to adjust this, particularly if using laptops or saving energy by shutting down at such times.

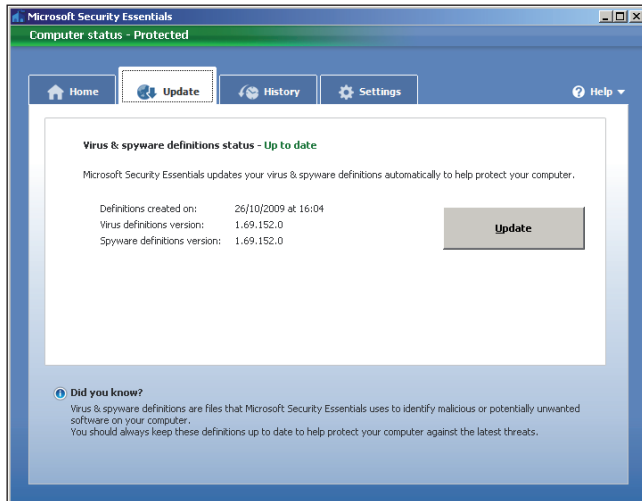
The most interesting part of the settings tab are the controls for the ‘SpyNet’ system, yet another online community-reporting system designed to gather information on what is being detected. The default ‘basic’ setting provides *Microsoft* with minimal details of any detection that occurs, mainly limited to what was detected and when. Meanwhile the ‘advanced membership’ option allows the product to upload much more detailed information including filenames and locations of dangerous files. There is no option to run without reporting data to base, which may worry some users from a privacy angle, but in most circumstances even the advanced setting is unlikely to

breach anyone’s privacy. As such systems help measure and monitor the malware problem, providing useful information on how infections function and spread, I would recommend that any user not crippled by paranoia enable the advanced mode.

Running the product for a while and putting it through our standard set of speed measurements showed it had a reasonably low footprint, not interfering with normal usage even while scanning, thanks to judicious use of prioritization. A full set of speed measurements were taken in direct comparison with the last VB100 test – which was admittedly on an unsupported server platform, but this seemed not to impede the product’s operation and showed that it fitted fairly neatly into the upper end of the range for speed and overheads, with both on-demand and on-access speeds around a third faster than those recorded for big brother *Forefront* across the board. We got similar results on *XP* and *Vista*, and should have more accurate and complete results available, including details of *Windows 7* performance, once the product has been through a full VB100 comparative in a month’s time. As well as standard on-access and on-demand scanning, the product also checks web downloads and email attachments specifically as they arrive by integration with standard *Windows* functions for this. Here, a noticeable but totally acceptable additional delay was added to the download.

We did note a fairly hefty slowdown of the system in a couple of cases, particularly when running on low-end netbooks at the bottom end of the supported power range. This was most evident during boot-up and recovering from hibernation, and was quickly diagnosed – when the product is installed, its updating system is integrated with *Windows Update*, which on some systems I have found it best to run manually thanks to this slowdown during boot-up as new patches are downloaded. Enabling the update system for the malware definitions also enables the full *Windows* updates, and led to the problems noted. In most cases of course, users should always have *Windows Update* active to ensure





they get the latest security fixes as quickly as possible, so this will not affect most users.

Having surveyed the product in its normal, fairly dormant state, it was time to see how well it fared in more challenging times.

PROTECTION CAPABILITIES

Continuing the process from the speed testing, we pushed the product through the full set of VB100 tests from the previous comparative (see *VB*, October 2009, p.17), albeit with definitions around a month newer than the official test deadline. We found detection scores as expected closely mirroring those achieved by *Forefront*, with the newer samples in the RAP sets covered much better thanks to the intervening time since the sets were gathered. Across the full trojan set and all of the RAP sets detection rates were steady and reliable, never dipping below 95%. The other standard sets were handled pretty impeccably, with no issues in the WildList set despite even larger numbers of highly complex polymorphic strains added in recent weeks. Several other variants of W32/Virut, which continues to show up high on our prevalence charts, were also tested and detected perfectly. Stability was excellent and the product behaved impeccably throughout, even when handling sets of strange and malformed files known to cause problems for some engines. We also liked the way the on-access scanner does not feel the need to bombard the user with alert pop-ups, instead going about its business simply and quietly and recording malicious activity in its main interface, to be reviewed at leisure.

There was one minor oddity in the history set-up though – one that perhaps is unique to the likes of us. Having run a scan of our full sets, we opted not to let the product plough slowly through the whole lot removing, cleaning and quarantining tens of thousands of files, so simply

closed the scan window. On checking the history area later, although it claimed to contain details of all threats detected, it reported nothing. We later found that reports seemed to make their way into the history only if they have been acted on in some way – either cleaned or allowed. As this is the default and probably most sensible way to operate, it seems unlikely that this will affect most users, but it is still perhaps a little misleading.

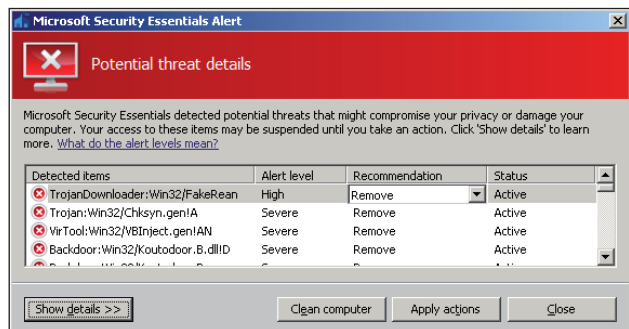
As well as the test sets used in the last comparative, we also built an updated RAP-style set from samples received shortly before and just after installing the product. Once again we saw some excellent detection rates – particularly impressive in the week +1 set which contained mostly items not seen by the labs before. The strong team being built up by *Microsoft* for its anti-malware department has already had great success as the scores achieved by the company's products, both in our own and other independent tests, have steadily increased in the last year or so to reach some extremely competitive levels – this trend shows no sign of abating any time soon. Our next test was to run the product against samples from the latest WildList, which again caused no problems.

Scanning our full clean sets produced no false positives, even in the batches of samples deemed too obscure or bizarre to include in our official set. *Microsoft's* products have shown a pretty clean performance in this area in our tests for some time now, with not a single false positive since *OneCare* first entered the VB100 several years ago – a pretty strong achievement perhaps helped by the firm's massive software certification programmes and penetrating ability to see what people are running on systems around the world.

All in all the basics of straightforward static anti-malware protection seemed to be provided to a very satisfactory standard. The set of tests we performed would easily have qualified the product for a VB100 award had it been under official conditions, and it looks pretty likely that, barring surprise disasters, certification will be achieved at the first attempt (which will hopefully be in the upcoming *Windows 7* test).

Cleaning seemed pretty solid too, with most of the handful of items we tested removed without difficulty. As is usually the case, a few innocuous remnants were left behind in some cases, along with a few registry entries and changes to the hosts file – this is par for the course though and few products will be brave enough to remove all possible side effects of some attacks for fear of damaging important existing settings.

Moving on to other features, we learned early on from the product literature and early reviews that there is a little more than basic protection here, with the SpyNet reporting system also featuring a level of cloud-based intelligence and even some behavioural monitoring, apparently watching unknown files for suspect behaviour, checking



for confirmations from other sources and automatically blocking new threats. We endeavoured to test this behaviour, having found a selection of newly gathered samples that were not being detected by the signature scanner which we ran on sacrificial systems with limited networking to allow the product to connect out while minimizing the potential danger of the malware. Unfortunately, despite our best efforts, we could find no confirmation of any additional protection provided by the cloud-based system – with each of the samples not spotted by the straight scanner allowed to operate as they pleased. We will keep an eye on this new technology and see how it develops.

CONCLUSIONS

Overall, *Security Essentials* proved a pretty decent product for the price bracket. Some commentators have complained about the lack of additional suite-type features, but there are still many similar standard anti-malware products on the market, with great demand for such protection even if paid for. The ability to pick and choose protective components remains important to many, while the prices of the more complete suites put them out of range for many others. We tried the product in combination with a number of third-party firewalls, spam filters and even behavioural monitors, with no sign of any clash or incompatibility, and we were able to provide ourselves with a fairly decent sense of security without spending a penny. Of course this takes some effort and perhaps a little skill, and for many users *Security Essentials* will in fact be their security be-all and end-all; while such an approach is not to be encouraged, it is far preferable to having no security at all.

Providing an extremely respectable level of detection of known malware, some top-notch heuristic and generic coverage of emerging threats, and a simple approach to usability which shouldn't baffle even the most technophobic, *Security Essentials* makes a strong addition to the line-up of free solutions on the market. If it is indeed taken up by the vast armies of unprotected systems out there, it should make quite some dent in the number of zombie systems attacking and spamming the rest of us.