

Re: McAfee and Comcast

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.basics/2007-08/msg00074.html>

- *From:* Gregory <Gregory@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 2 Aug 2007 04:40:09 -0700
-

Thanks Vanguard, you have been a great help !! I'm going to mix this cocktail and install it. Was it you who mentioned the Grisoft AVG Anti-Rootkit? I read a review, and they said to be careful, it is BETA. What did they mean? Is this program too big or powerful for my laptop? HP Pavillion xv5330us 7.9 lbs.
— Intel Pent. 4 3.2 GH
Gregory 512 MB 80 GB Hard Drive

"Vanguard" wrote:

"Gregory" wrote in message
news:6DC0230F-FACA-447A-8726-0F1396EDE594@xxxxxxxxxxxxxxxxxxxx

PC.World tested Firewalls and ranked Comodo Firewall 2.3 first with 9,350 points out of possible 9,625. Jetico came in second with 9,125 points and Zone Alarm was a distant third. All free. The test included free and "for-hire" firewalls !!! You were dead right Vanguard ! I tip my Hat to you.

Just don't get too lured by Comodo products. I trialed their v2.0 anti-virus software and it is severely bloated, consuming 97MB total (real + virtual memory). It is still beta and supposedly to be released sometime the end of July (well, that's gone and still it's beta). Unless they address their memory bloat, I won't be using it. The reason I wanted to check it out is both their anti-virus and firewall include HIPS (host intrusion protection system) which would integrate well together. I suspect part of the HIPS that will go into their anti-virus product will be from their BOClean product but that isn't what I'd call a full-fledged HIPS product. Their firewall uses HIPS to regulate what can call what to get a connection while the HIPS in their anti-virus/spyware product will regulate what can load what into memory. Just be ready for lots of prompts. They have their white- and blacklists (and Safety Net Monitor has its learn mode you use on a clean

Re: McAfee and Comcast

host) but they can be daunting the first few days with all the prompts and you having to analyze what they're telling you.

I had suggested ProcessGuard but have since changed to using System Safety Monitor. Both are free and another HIPS product. ProcessGuard was the gold standard but System Safety Monitor goes further but has a smaller memory footprint than ProcessGuard. I'm just using the free versions so not all the security features are there. Don't bother with using any HIPS program if you can't understand what the prompts mean. Saying "yes" to all prompts obviates the point of using the product. So now my security cocktail is:

Active programs (constantly running):

System Safety Monitor
AVG anti-virus
Comodo firewall
Windows Defender

Inactive programs (those I run manually for on-demand scanning):

Lavasoft Ad-Aware
Spybot S&D
SuperAntispyware
AVG Anti-Spyware (ewido)
SpywareBlaster (only for AX disable & bad sites but never for cookies)
HijackThis

Protected environments:

VMWare Server
Sandboxie (becomes nagware after the 30-day trial)

I no longer use a-squared because their coverage has waned severely. Nothing a-squared found wasn't already discovered by ewido. Trojan Hunter is very bad and asked that their product be withdrawn from the anti-malware review performed at av-comparatives.org (<http://www.av-comparatives.org/seiten/ergebnisse/atreport2006.pdf>). I certainly wished this site did comparisons more often of anti-malware products but I suppose they're busy enough with testing the anti-virus programs (some of which don't even make it to their list). Of note, however, is that such tests that rank purely on coverage of known pests doesn't reflect how well they work against zero-day pests, and HIPS products work by regulating what can run or what can connect rather than cure an already infested host. Any product that you don't know how to use is a waste of disk space and like buying an elephant gun to shoot a mosquito (i.e., not an appropriate choice). It has to be a product you can use or one to which you can become self-educated to use properly.

Security is the antithesis of ease-of-use. The more secure is a host, the less easy it is to use that host (i.e., more security means more stuff in your way). That's why I decided not to go paranoid and have a slew of various anti-virus, anti-spyware, anti-malware, HIPS, and

Re: McAfee and Comcast

whatever else security products running. I'd actually like to USE my computer and have it remain responsive. I try to find a cocktail of products that gives me reasonable security but without a lot of wasted overlap and still lets me use my host. So far, the above cocktail of 4 active security products has given me with a decent but not onerous level of security without severely impacting the responsiveness of my host. All running software impacts your host to some degree so going extreme is self-defeating.