

alt.computer.security: Re: Norton 2005 Int Security, Trend PCcillin or Zone Alarm ????????

Re: Norton 2005 Int Security, Trend PCcillin or Zone Alarm ????????

Source: <http://www.derkeiler.com/Newsgroups/alt.computer.security/2005-02/0139.html>

From: winged (winged_at_nofollow.com)

Date: 02/06/05

Date: 06 Feb 2005 12:14:43 EST

Anonymous wrote:

- > *Hi*
- >
- > *I've got a PC hardwired and a Laptop wirelessly off a Belkin F5D7630-4A*
- > *wireless router (with WEP 128 bit encryption).*
- > *Os is XP with SP2.*
- > *Mainly use Firefox 1.0 but IE if necessary.*
- >
- > *I currently run Norton Internet Security 2004 on both machines but the*
- > *update period is about to expire.*
- >
- > *I want security I can run on both machines.*
- > *I don't mind paying a bit.*
- > *Don't want something I've got to remember to update and I need a degree in*
- > *computer science to operate.*
- > *I want something that updates semi or completely automatically*
- > *Broadband is connected quite a lot*
- > *I don't do gaming but do do a little peer to peer.*
- >
- > *Zone alarm and Trend PC-cillin seem to be getting good reviews at present.*
- >
- > *Anyone got any ideas or know where I can find unbiased reviews?*
- > *Can I install on both machines without paying for a second licence?*
- >
- > *Any assistance greatly appreciated.*
- >
- > *(Also have AdAware, Spybot Search and Destroy and the new MS Anti Spyware*
- > *(which hasn't found anything the others haven't))*
- >
- > *Please reply to group.*
- >
- > *Thanks*
- >
- >

I have used all three products, all have positive and negative points.
System overhead is higher than standard firewall applications. There

Re: Norton 2005 Int Security, Trend PCcillin or Zone Alarm ????????

again my version doesn't time out so this is a factor in my consideration. Symantec products do not remove (uninstall) well. Some manual extraction of the product from the registry should be made when uninstalling. One might consider rebuilding the system when removing it. I can block many malware threats however I object it is not turned on by default and requires a user to dig to find where to turn it on. Why do use it? Because I have learned its Quirks and I use the logging capabilities extensively. Since I use a layered firewall topology it is my 3rd line of defense. Additionally since this is the product we use in the corporate environment, I use it to remain intimate with its functionalities.

McAfee's product is very competent and has a lower system impact than Symantec. My exp indicates they are a bit slower on response to new threats than Symantec however I am not sure the threat 0 day to response time is enough different to warrant non-consideration. It uninstalls fairly well however it too leaves tread marks in the registry after uninstall. This product can be centrally managed however I prefer the Symantec plug-in to the AV server console.

Zone alarm Pro is much better than "free" version, one needs the ability to build pipes. It has the advantage of not timing out and has some nice intelligent blocking features. It does not have some of the filtering capabilities of either the McAfee product or Symantec s. It has the advantage of having a smaller footprint than some of the other products and is considered easier to use by many. I have had issues, in the past, with this product and VPN products. I have also had issues layering topology with Virtual machines. It is problematic if a VM is layered behind the ZA firewall. This may be an issue of the VM product and not a deficiency of the firewall itself. There are a couple pipes that are opened by default in the product that are difficult to close completely. I can't directly address current uninstall issues as I have not tested the current generation of this product. This product is not designed for central management and can allow users to block communications that the network gods have deemed required. The tool is well designed for the home market.

Micro Trends PC-Cillin is very good (possibly the best in home network environment). It is much better than the other products finding and stopping non-viral type attacks. It does port and packet inspection and has a higher probability of catching something inside, trying to get out or modifying registry entries. Its notification of aberrant activity is better than any of the other products you mentioned (IMHO). The hooks it uses to monitor registry interaction impact CPU performance however if you are on a recent generation machine, the overhead will not be noticed. You will see impacts to the throughput of a machine that increases noticeably with a high speed connection on a slower machine (ie below 1 ghz). All things considered, in a non-corporate environment, this might be the tool of choice. There are issues in central management of this product. You will see issues in doing simultaneous engineering across desktops where bandwidth requirements are very high

alt.computer.security: Re: Norton 2005 Int Security, Trend PCcillin or Zone Alarm ????????

in the form of stutters when high data volumes are being transferred even on a fast machine).

The key is to find a product that meets your needs and you can be comfortable in learning its functionalities. It is hard to say what product is best without knowing your specific requirements and testing.

I can't address licensing issues as I strive to ensure my software is appropriately licensed. I do not know what the license policies are for the various products nor have I seen articles that address this issue on a comparison basis.

In a broadband environment I would ensure I had an external hardware firewall between the pc (home network) and the Internet. Software firewalls may not stop attacks made against the physical layer, data link layer, the network layer, or the transport layer of the IP protocol. There are flaws with a number of NIC cards in manufacture that can allow compromise of information where the NIC is directly exposed to communication. A hardware Firewall can help protect against this type of attack. Additionally a hardware firewall can help protect the inside from various types of IP spoofing (protects from spoofing internal trusted address) attacks from outside of the network.

Winged