

Dead Trees

A PUBLICATION OF
QUESTIONABLE VALUE FROM
William Blinn
COMMUNICATIONS

179 Caren Avenue • Worthington • Ohio 43085
614-785-9359 • Fax 877-870-4892 • www.Blinn.com

December 2002

Antivirus Programs: There's more than just Norton

If I say "antivirus", chances are pretty good that you'll think "Norton" – and that's just fine with the folks at Symantec. With few exceptions, I've had Norton Antivirus on my computers for most of the last 10 years. Symantec makes a good product, backs it up with constantly revised definitions, and provides a lot of useful information on the company's website.

But Norton may not be the best for you.

Why not Norton Antivirus?

One problem with Norton Antivirus products involves installing, upgrading, and removing. Sometimes (in my experience "often" would be a better word) attempts to change the way Norton Antivirus works leads, sooner or later, to formatting the disk drive and reinstalling the operating system.

Another problem is the amount of system resources that Norton Antivirus uses.

And then there are the packages. Should I buy Norton Utilities, Norton Internet Security, or just Norton Antivirus? If I buy the "utilities" product, should I let the other applications run all the time or just start them when I need them?

Changing or deleting: BIG PROBLEM

I recently needed to add Norton Utilities to an existing installation of Norton Antivirus. The installation appeared to go all right until I rebooted the system. The antivirus product wouldn't start. I tried to install it again, but the installer told me it was already there. So I tried to uninstall it, but the uninstaller told me it wasn't there.

I deleted all of the Norton directories and Registry entries, but was never able to get the application to run properly until I formatted the drive, reinstalled the operating system, and ran the full Norton Utilities installation again.

A previous version of Norton Antivirus acted as a proxy server to process inbound and outbound mail. I had set up the e-mail program to look at pop3.norton.antivirus and had then then configured the account settings so that Norton would pass along the user ID and the password to the mail server.

Since I understood what was happening, the setup was easy. A user who didn't know what a proxy server was could have been left out in the cold.

When a new version of the program came out, Symantec had eliminated the proxy server. This wasn't mentioned prominently during installation, though. As soon as the program was on the computer, I could no longer receive mail.

Figuring out what had happened took only a minute or so and fixing the problem was quick and easy, but only because I suspected the cause and knew what to do to fix it.

In testing other antivirus programs, I've removed Norton Antivirus from each test machine. In one case, removing Norton Antivirus eliminated all network access. I might have been able to fix this, but I'd been planning to format the drive and reinstall the operating system anyway, that was my solution.

System resources

If you have Norton Utilities, the program may have suggested running the Disk Doctor or System Doctor at all times. These are enormously resource-hungry programs. There is no reason to run these applications as a matter of course and recent versions of Utilities have defaulted to not running them.

But even Norton Antivirus seems to make the machine a bit sluggish. It is, after all, watching any application that tries to write anything to any disk drive.

The dizzying variety

I've never been able to figure out whether Symantec offers so many packages to be helpful or to boost the company's bottom line. Norton Antivirus is in most of the applications and that's the one that everybody needs; the other products may or may not have value for you.

Whether you need the full utilities program or the Internet security applications is up to you.

Despite the shortcomings, Norton Antivirus is probably still the easiest product to use and the one most people have. For more information, see http://www.symantec.com/nav/nav_9xnt/.

The competition

When I started looking around, I found that there are several competing products and one of them is *free*.

McAfee

The best known competing product is from McAfee. This is a product I haven't used recently, but previous versions have always been competent in terms of catching and eliminating infected files. The McAfee product has generally been a little harder to install, though.

In McAfee's favor is SpamKiller, Thor Ivar's utility that seeks out spam and eliminates it. SpamKiller is now owned by McAfee

What the heck is this?

Dead Trees is the William Blinn Communications newsletter. It's published whenever I feel like it, although I generally feel like it when I'm preparing the month's invoices. If you didn't receive an invoice with this newsletter, kindly contact me and we'll rectify that situation. Please note that despite the name, of the publication, I bear no particular animosity toward trees. The name is simply an acknowledgment that paper is made from, well, dead trees.

and that gives the company a program that could open doors for its other applications.

For details, see <http://www.mcafee.com/> for information about McAfee's on-line services and about traditional applications that run on your PC.

AVG Antivirus

If you're on a limited budget and you don't mind getting an excellent product for free, take a look at AVG Antivirus from Grisoft (Czech Republic). You can pay for the product if you'd like a somewhat more robust interface, but the free version is surprisingly capable. It includes automatic virus definition updates and can, at your option, add a notice about the message being "certified" virus free. The message may be switched on for inbound or outbound mail, either all messages or only those with attachments.

The "certification" is perhaps a bit over the top because it depends on Grisoft always being ahead of virus writers and it depends on your having the latest definitions (you can turn off the automatic update feature).

AVG Antivirus is a breeze to install. This is an application that anybody could install without instructions. Even if you're running the free version, you do need a serial number. You get that by going to the Grisoft website.

The paid version costs \$40 for a single-user license. For corporate use, a multi-license option reduces the price (depending on quantity of licenses purchased) to \$32 (starting with 2 licenses) or to \$11 (for 100 licenses) with several intermediate prices.

The scanner component of AVG Antivirus is robust and offers all the standard options. The paid version (this is the free version) offers additional capabilities.

Volume users should also consider protecting their servers with AVG Server. The price is as low as \$38 if your network has just 2 users and as high as \$648 if your network has 100 users.

For more information, see <http://www.grisoft.com/>.

NOD32

Also worth a look is another Czech Republic antivirus program NOD32, \$40 (annual \$27 renewals) or \$30 for volume users. NOD32 is distributed in the US by Eset in California.

NOD32 is not an antivirus program for the timid. It must be installed as a proxy server. This is not particularly difficult if you have a single e-mail account. If you retrieve mail from numerous servers, though, the setup can be time consuming.

In my case, it was even more complicated.


To retrieve mail from the office, I have to run an application that establishes a secure connection and then performs "port forwarding" for POP3 and SMTP ports. To send or retrieve mail, my e-mail program connects to "localhost" (127.0.0.1), which forwards to port 21 (POP3) or port 110 (SMTP) at the office.

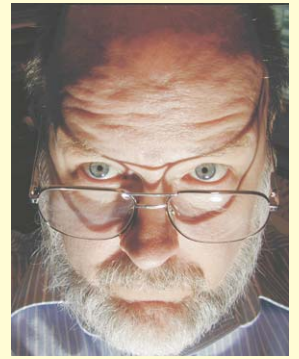
NOD32 would like to be localhost, too, but that's not possible. The help files explain how to get around this problem: For each e-mail system you need to communicate with, you need to create an entry in the POP3 scanner component of the software. For a single account, this is easy: You tell the scanner the address of your POP3 server (mail.foobar.com, for example) and tell it to listen on the POP3 port (110).

Those with multiple servers need to create multiple entries in the POP3 scanner. Each e-mail account gets a separate address. For example, the scanner communicates mail.foobar.com on port 110, but "listens" for your e-mail program on port 11010 of

The end? The beginning? Just another day?

Here we are at the end of another newsletter (well, top of the 4th and final column, anyway) and nearly at the end of another year.

By the time you receive the next issue of this publication, it will be 2003, so I'd like to take this opportunity to wish you a pleasant holiday season to round out 2002 and a happy, prosperous 2003. Be safe. Be well. Be kind. And enjoy. 



localhost (127.0.0.1). It communicates with mail.evileye.com on port 110, but "listens" for your e-mail program on port 11011 of localhost. The only difference is the port number (you assign the number – most values from 10500 and up are available).

For my office mail system, I had to set up the POP3 scanner to listen on a "high" port, but then to communicate with "localhost", which communicated with the port-forwarding security software, which then communicated with mail.atmyoffice.com. This sounds a lot more complicated than it is – it's really a lot like the old "bucket brigade" fire companies – and if you think of it that way, it's not at all confusing. But if "port addresses" and "IP addresses" and "port forwarding" frighten you, this may not be the right choice.

What I've found with NOD32 on one computer, the free version of AVG Antivirus on another computer, and the paid version of AVG Antivirus on a third computer is this: The computers boot faster and work better than when they had Norton Antivirus installed. Each of the computer has received numerous infected messages, but none of the messages got through to cause any harm.

The controls for the various components (three panels with various settings) look complex, and they are more involved than those for most other products; but the complexity provides for more flexibility.

For more information, see <http://www.eset.com/>.

WARNING: Pick only ONE

A peculiar American philosophy seems to hold that more is better:

- \$1000 is good, so \$2000 is better.
- The recommended dose is 2 aspirin, so 3 will relieve the headache faster.
- One antivirus program is good, so 2 will protect more.

While \$2000 is undoubtedly better than \$1000 and there might be instances in which 3 aspirin tablets are better than 2, installing multiple antivirus programs won't provide enhanced protection. You may get no protection at all.

The best solution is to pick an antivirus program that you have confidence in, follow the installation instructions, update the definitions regularly, and even then don't open an attachment if it comes from somebody you don't know or if it's and unexpected or unusual message from somebody you do know.

Safe is always better than sorry. 