

Re: Anyone using AV, Spam, & content filtering devices?

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-04/msg03294.html>

- *From:* Andrew Hodgson <me3@xxxxxxxxxxx>
 - *Date:* Thu, 19 Apr 2007 18:56:01 +0100
-

On Mon, 16 Apr 2007 08:18:02 -0500, Leythos <Void@xxxxxxxxxxx> wrote:

On Mon, 16 Apr 2007 06:10:55 -0700, Gary V. wrote:

I know I am not going to stop using trend this is just a what if. If the one device could stop "all" incoming then why have it on the server. I guess would still need away to clean a virus if/when it gets to the server. Anyways

You need to understand that AV solutions are "reactionary" for the most part.

Removing content before it reaches your network is not reactionary, but it is not a 100% reliable method – as an example, I can remove all EXE files and depending on the solution a person could email an EX_ file and then the idiot on the lan could save and rename it to EXE and you could be compromised.

Urm, if your appliance based solution allows this then it is worthless. The system I believe is being talked about in the op's message was some type of appliance with a disk, running an antivirus system etc. For example, I run Sophos suite on our box, Sophos AV on the workstations, but ClamAV on the appliance based solution in front of the SBS. ClamAV is very good at getting fishing attacks, whereas Sophos catches some bits that ClamAV doesn't touch.

Andrew.

.