While I agree with your general argument, I have a lot of concerns for your second example. Which by the way, was exactly what I was telling people three years ago. Now with experience, I can give you some advice:

- Yes, if you scan shared folders on Unix boxes you're not preventing any infection spreading from one Unix or NAS box to the next, because there are close to none for them. However, what about files stored there infected with Windows malware that are being accessed by Windows boxes? AV scan of NAS/Unix shares can prevent those servers acting as infection vectors.
- Oh, yes, you're redundantly doing the AV on both the servers and the client workstations, so why you cannot remove one of them? This is a good question, but again you have not give it enough thought.

Look, if you can absolutely-positively-without-any-doubt be sure that no one is ever going to plug into your network a machine that does not have AV up to date (or is not sensible to such attacks, such as a Unix box) then you can remove the AV engine on the file server and leave it to the workstation to do the virus scan.

Somehow I think that the technical measures to prevent someone to plug into your network a non sanctioned equipment are going to be way more costly and difficult to implement. And no, just banning that as company policy is not going to work, people regularly bring equipment from home and plug it into the Ethernet port just to see what happens.

In fact, if I had to remove one of the two AV engines, it would be the one on the workstations. Workstations can be easily replaced and if they go down affect only a single person. Yes, there can be critical data stored on an individual desktop or laptop, but logic says that it should be a minor impact compared to losing a whole file server.

So keep hammering your server with weekly, no, make it daily, AV scans. File servers are there to be hammered, after all they are designed for... serving files. And consider AV scanning your file server just another of those security layers you correctly mention as the foundation of good security.

However, using such a bad example does not invalidate your argument. Yes, there are more than a fair share of completely useless security policies out there, and people prefer to keep them rather than taking the risk of thinking by themselves. I agree fully with that. Just as your bad example shows, if you don't think enough about them you may find yourself in an awkward position if something bad happens.

Or better yet, use a sensible security professional. Which I am not (security professional, I mean)

Source: https://faq.remarkbox.com/06d85e3c-9ee0-11e7-bece-040140774501
Snapshot: 2026-05-06T01:10:07Z
Generator: Remarkbox 763cacb