Dray Agha is a PhD Researcher based in the Information Security Department at Royal Holloway University of London.

Anti-Virus/ Anti-Malware

Anti-virus (AV) and anti-malware (AM) protection are two distinct things.

- AV is mostly effective on the more 'classic' types of attacks, but new attacks may not yet be on the AV's watchlist.
- AM tends to be more clued up to the latest attack trends, but may not offer protection against classic, more mundane malware.

They both keep an eye out for the tactics, payloads (malicious code), and origins of attempts to infiltrate your computer. And then they thwart those attempts. They aren’t perfect however, as hackers are always coming up with new methods to bypass AV/AM protections.

Running both AV and AM at the same time sounds like it should be a great idea, but it isn’t! They would clash, cancel each other out in places, and make your computer slow. It’s better to have a consistent AV running, and to only run AM periodically or when you think your computer is acting unusually.

It’s hard to recommend any one company’s services, as it really is specific to your business use. You will have to do some homework and find an AV and AM that are best suited for your case. There are some things to keep in mind when you’re looking:

- There are providers who offer both AV and AM services.
- True does mean an AV or AM service will be bad. It’s best to read the description of the protection product you’ll be choosing, to make sure you’re picking what works for you. Picking what’s most expensive isn’t always appropriate for your computer.

Some AVs have been accused of leaving their payload is a Microsoft Word update, for example. A firewall makes sure that your Microsoft Word update is exactly that, and blocks a hacker whose dangerous payload is masquerading as a Word update.

A firewall can stop your programmes from working sometimes. But some hassle to turn the firewall off to make the programme work. Firewalls are extremely necessary as hackers automate their attacks to scour the globe, looking for devices that are vulnerable. One such vulnerability they look for is if the firewall is turned off, or poorly configured.

Not only can the hackers exploit these vulnerabilities, they can also use them to attack other devices on the network. They are security features that run in the background of our devices, and can sometimes stay in the background of our thoughts when we think about our cyber hygiene.

There is a persistent rumour that Apple devices don’t get viruses. This was once a half-truth. In the past, Microsoft Windows was more common worldwide and it made sense for hackers to craft attacks for Windows specifically. Apple devices have a different underlying structure to Windows, and hackers for one can’t just be used on the other.

“...... got to go to great lengths to have built-in security mechanisms, such as not letting unsigned software on the App Store. But it’s still advised to get anti-virus and AM for your Apple devices.

Firewalls

The purpose of a firewall is to be the wall of protection that separates your computer and hackers who want to ruin your day. Firewalls determine the origin of incoming data and do their best to block dubious packets that want to get through the wall.

Clueless attackers will try and disguise their dangerous malware to look like authentic data transfers from the web. The hacker may try and pretend their payload is a Microsoft Word update, for example. A firewall makes sure that your Microsoft Word update is exactly that, and blocks a hacker whose dangerous payload is masquerading as a Word update.

Security in the Background, The User up Front

Firewalls and AV/AM share in some of the things they ‘can’t do’, which all revolve around how proactive you are about your cyber security.

- Bad passwords: poorly chosen passwords, or using default credentials that devices and services come with, gives an attacker an open door through your protections, as they have found ‘legitimate’ access and do not need to send an attack.
- Social engineering: these protections are of little help with email scams or telephone scams. Email filters and training are your only protections here.
- Poor security configurations: protections can be undermined if you turn them off, or if you do not update them or other software on your device, as attackers can exploit these unpatched services.
- Unverified software: software that has been pirated or downloaded from unverified sources can be riddled with malware, and gives the hacker a method of attack that can bypass the protections.
- Sophisticated attacks: targeted attacks by sophisticated, well-funded hackers are very unlikely but still a possibility. These hacking groups are very capable of bypassing many protections.

Hackers prefer easy targets and will give up and move on if faced with obstacles. By ensuring that your background protections of AV/AM and firewalls are optimised for your business purpose, you are making the hackers job that bit harder.

Further guidance:

- https://www.virus Total.com/antivirus-product

Dray Agha is a PhD Researcher based in the Information Security Department at Royal Holloway University of London.