

Forum:[Hack Forums](#)

Thread: [What antivirus should I get? I have malwarebytes pro](#)

Ganja™ - March 10, 2014, 6:18 pm

Title say it all. I have malwarebytes pro + AVG(free) currently. I do not think this is enough protection since recent malware may be able to go though VMware and such. What would you recommend?

Aura - March 10, 2014, 6:20 pm

(Mar 10, 2014 06:18 PM)Ganja™ Wrote: [\[CITE\]](#) Title say it all. I have malwarebytes pro + AVG(free) currently. I do not think this is enough protection since recent malware may be able to go though VMware and such. What would you recommend?

It depends, we need more information on your current setup.

Do you want a free or a paid Antivirus ?

What version of Windows are you running ?

What are your computer specs ?

-Hyperion - March 10, 2014, 6:20 pm

Well you should never run 2 AV at a time they can conflict.

<https://hackforums.net/showthread.php?tid=4067069> you can see what other people use here personally I use and recommend Kaspersky to all my clients. MWB is good for running a scan once a week but its real time protection not that impressive. Edit: how did I know Aura would post here :P

RDCA - March 10, 2014, 6:23 pm

You shouldn't be using the resident scanner of MBAM simultaneously with an active resident AV (One that actively scans). I suggest you install Avira:

<http://www.avira.com/en/avira-free-antivirus>

Also, malware infecting a host machine is for the most part unheard of assuming the normal precautionary measures are taken.

xhflhkeuhwguu34 - March 10, 2014, 6:29 pm

There won't be an exploitation for VMWare. I assure you.

Ganja™ - March 10, 2014, 6:30 pm

Thanks all! I run windows 8 64bit. I had some trouble with kaspersky before. Maybe I should try again.

Yeah someone recommended me avira as well.

MechWarrior67 - March 10, 2014, 6:31 pm

I wouldn't run kaspersky if you have had trouble with your comp before. The .dll "klif" that kaspersky installs can cause BSOD rare but it still happens

I suggest sticking with MWB and getting something like Comodo or Avast?

Aura - March 10, 2014, 6:31 pm

(Mar 10, 2014 06:30 PM)Ganja™ Wrote: [\[CITE\]](#) Thanks all! I run windows 8 64bit. I had some trouble with kaspersky before. Maybe I should try again.

Yeah someone recommended me avira as well.

If you're running Windows 8 and you want a free solution, my vote goes to Avira as well. If you want a paid Antivirus, either Kaspersky or ESET, but my final vote will always goes to Kaspersky, it's just an amazing piece of software.

Tesseract - March 10, 2014, 6:33 pm

(Mar 10, 2014 06:23 PM)RDCA Wrote: [\[CITE\]](#) You shouldn't be using the resident scanner of MBAM simultaneously with an active resident AV (One that actively scans). I suggest you install Avira: <http://www.avira.com/en/avira-free-antivirus>

Also, malware infecting a host machine is for the most part unheard of assuming the normal precautionary measures are taken.

OP, malware bytes pro is just a filer after the AV doesn't catch something, usually small and intricate/particular malware or mal-programmed registry entries etc.

I'd also suggest Avira as a free solution to your problem.

For a purchased solution, i'd suggest ESET Smart Security 7 for your private needs. Also, I'd suggest sandboxing your VMWare player since you are so paranoid.

[Download Sandboxie by clicking here](#)

[Download ESET Smart Security 7](#)

Side note: THANK YOU FOR AGREEING AS A PERSON FROM MRT! Just validates me. Tell Aura that Avira is not adware.

RDCA: You remember me don't you? I'm that kid from SF.

http://www.supportforums.net/misc.php?action=username_history&uhuid=4502

(Mar 10, 2014 06:31 PM)Aur? Wrote: [\[CITE\]](#) If you're running Windows 8 and you want a free solution, my vote goes to Avira as well. If you want a paid Antivirus, either Kaspersky or ESET, but my final vote will always goes to Kaspersky, it's just an amazing piece of software.

Aura, don't be a hypocrite. You better go change that post you called Avira Adware. Please ?

(Mar 10, 2014 02:45 PM)Aur? Wrote: [\[CITE\]](#) Avira free is just a plain Adware and all of AVG addons (AVG Secure Toolbar included) are detected as PUPs and deleted by tools like AdwCleaner and JRT. It gives you an overall idea of how bad it is. McAfee we'll just not talk about it and Norton can comeback when it will learn that it doesn't have to use all the resources available on a computer in order to work.

Null Byte - March 10, 2014, 6:34 pm

(Mar 10, 2014 06:33 PM)MaiTriCks Wrote: [\[CITE\]](#) Also, I'd suggest sandboxing your VMWare player Um... What? ? I don't think that is going to change much.

Aura - March 10, 2014, 6:35 pm

(Mar 10, 2014 06:33 PM)MaiTriCks Wrote: [\[CITE\]](#) OP, malware bytes pro is just a filer after the AV doesn't catch something, usually small and intricate/particular malware or mal-programmed registry entries etc.

I'd also suggest Avira as a free solution to your problem.

For a purchased solution, i'd suggest ESET Smart Security 7 for your private needs. Also, I'd suggest sandboxing your VMWare player since you are so paranoid.

[Download Sandboxie by clicking here](#)

[Download ESET Smart Security 7](#)

Side note: THANK YOU FOR AGREEING AS A PERSON FROM MRT! Just validates me. Tell Aura that Avira is not adware.

RDCA: You remember me don't you? I'm that kid from SF.

http://www.supportforums.net/misc.php?action=username_history&uhuid=4502

Aura, don't be a hypocrite. You better go change that post you called Avira Adware. Please ? Avira free act like an Adware, doesn't mean it's not a good Antivirus. It's different.

TheMan321 - March 10, 2014, 6:35 pm

Avira would be the best antivirus to use.

AVG coming in second place.

Thats just my opinion.

T e s s e r a c t - March 10, 2014, 6:37 pm

(Mar 10, 2014 06:34 PM)Null Byte Wrote: [\[CITE\]](#) Um... What? ?wow2menycharsm8

Hey Hey. Don't judge. OP is super paranoid thinking the malware he may encounter can escape his VM. It is completely possible to sandbox a VM.

(Mar 10, 2014 06:35 PM)Aur? Wrote: [\[CITE\]](#) Avira free act like an Adware, doesn't mean it's not a good Antivirus. It's different.

Mhmm. Then why discuss that its Adware when its' functionality is phenomenal? It seemed you invalidated Avira as a plausible AV in the other thread.

-Hyperion - March 10, 2014, 6:38 pm

(Mar 10, 2014 06:37 PM)MaiTriCks Wrote: [\[CITE\]](#) Hey Hey. Don't judge. OP is super paranoid thinking the malware he may encounter can escape his VM. It is completely possible to sandbox a VM.

but stupid I have used vms for years and had virus test boxes and never had one escape. Kaspersky Pure is a beast built in root kit scanning to.

T e s s e r a c t - March 10, 2014, 6:43 pm

(Mar 10, 2014 06:34 PM)Null Byte Wrote: [\[CITE\]](#) Um... What? ? I don't think that is going to change much.

Really? Why not?

I'm pretty sure if the virus escapes the virtual machine it would be from directly copying an infected file out the virtual machine (&/or creating a live data stream) to allow for a breach [obviously] to the host machine not in the sandbox.

It could help cure the paranoia since the virus is most likely to escape into the Sandbox where the VM's process is being hosted within.

Null Byte - March 10, 2014, 6:46 pm

(Mar 10, 2014 06:43 PM)MaiTriCks Wrote: [\[CITE\]](#) Really? Why not?

I'm pretty sure if the virus escapes the virtual machine it would be from directly copying an infected file out the virtual machine (&/or creating a live data stream) to allow for a breach [obviously] to the host machine not in the sandbox.

It could help cure the paranoia since the virus is most likely to escape into the Sandbox where the VM's process is being hosted within.

In all my years I have never had a piece of malware escape the VM. I don't even think it's possible.

Tesseract - March 10, 2014, 6:48 pm

(Mar 10, 2014 06:46 PM)Null Byte Wrote: [\[CITE\]](#) In all my years I have never had a piece of malware escape the VM. I don't even think it's possible.

I've seen considerably knowledgeable individuals posting about malware escaping VMs. You really almost never know, so it would not hurt the OP's conscious decision to take one extra precautionary measures. I mean, if he is going to invest into his security, might as well right?

Aura - March 10, 2014, 6:48 pm

(Mar 10, 2014 06:37 PM)MaiTriCks Wrote: [\[CITE\]](#) Hey Hey. Don't judge. OP is super paranoid thinking the malware he may encounter can escape his VM. It is completely possible to sandbox a VM.

Mhmm. Then why discuss that its Adware when its' functionality is phenomenal? It seemed you invalidated Avira as a plausible AV in the other thread.

Nope, I actually recommend Avira for Windows 8 and Windows 8.1 users. All Antiviruses have their default, doesn't make them bad Antiviruses. Except for McAfee, Norton and AVG ?

xhflhkeuhwguu34 - March 10, 2014, 6:49 pm

There is a line. I will draw it for you.

VM

VM running in Sandboxie

VMWare is used in fortune 50 companies, an exploit would be devastating.

Tesseract - March 10, 2014, 6:50 pm

(Mar 10, 2014 06:48 PM)Aur? Wrote: [\[CITE\]](#) Nope, I actually recommend Avira for Windows 8 and Windows 8.1 users. All Antiviruses have their default, doesn't make them bad Antiviruses. Except for McAfee, Norton and AVG ?

Totally agree with you on the last 6 words ? Amen.

-Hyperion - March 10, 2014, 6:50 pm

(Mar 10, 2014 06:48 PM)MaiTriCks Wrote: [\[CITE\]](#) I've seen considerably knowledgeable individuals posting about malware escaping VMs. You really almost never know, so it would not hurt the OP's conscious decision to take one extra precautionary measures. I mean, if he is going to invest into his security, might as well right?

that only if it improperly configured or you copy files over etc. Vm having a hole is extremely rare and would not be used by your everyday virus .

cyberducky - March 10, 2014, 6:54 pm

Go with Avira if you are using windows 8, any other version of windows go with Kaspersky. Make

sure to turn of filesystem protection on MB so it does not conflict with the AV.

Ganja™ - March 10, 2014, 6:56 pm

Thanks all! About virus escaping from vmware and sandboxie, I have seen bad guys talk about it in other forums. Belive it or not, they said its possible. Thats enough reason for me to take extra caution. Also I recently downloaded not legitimate file so my paranoia was all my fault. I decided to get avira free for now. And try kaspersky in the future. I appreciate you all who helped me! Thanks very much

Null Byte - March 10, 2014, 6:57 pm

(Mar 10, 2014 06:53 PM)MaiTriCks Wrote: [\[CITE\]](#) Theres a reason why companies don't sandbox VMWare.

-snip-

Once again guys, tell OP he claims that VMs are not safe. I already know how safe they are. As long as you don't have a bridged connection enabled, nothing will happen. Refer to Xen0n's post please.

Tesseract - March 10, 2014, 6:59 pm

(Mar 10, 2014 06:56 PM)Ganja™ Wrote: [\[CITE\]](#) Thanks all! About virus escaping from vmware and sandboxie, I have seen bad guys talk about how to do it in underground forums. Belive it or not, they said its possible. Thats enough reason for me to take extra caution. Also I recently downloaded not legitimate file so my paranoia was all my fault. I decided to get avira free for now. And try kaspersky in the future. I appreciate you all who helped me! Thanks very much
THANK YOU FOR THE VOUCH.

All I needed was another person to agree and said he's seen knowledgeable people speak of such beautiful activities.

Sorry for the whole argument. Ganja, we're at that level.

You hear that Null, Aura, Xenon? Love.

Infer - March 10, 2014, 6:59 pm

You really can't go wrong with Kaspersky or ESET, I personally use ESET and haven't had any malware issues, some users will have more insight on this subject then I would.

Regards

Aura - March 10, 2014, 7:00 pm

(Mar 10, 2014 06:59 PM)MaiTriCks Wrote: [\[CITE\]](#) THANK YOU FOR THE VOUCH.

All I needed was another person to agree and said he's seen knowledgeable people speak of such beautiful activities.

Sorry for the whole argument. Ganja, we're at that level.

You hear that Null, Aura, Xenon? Love.

Why is my name even being mentionned ? What did I do ?

Null Byte - March 10, 2014, 7:00 pm

(Mar 10, 2014 06:59 PM)MaiTriCks Wrote: [\[CITE\]](#) THANK YOU FOR THE VOUCH.

All I needed was another person to agree and said he's seen knowledgeable people speak of such beautiful activities.

You hear that Null, Aura, Xenon? Love.

Escaping Sandboxie is easy to do with a simple DLL injection. I have yet to see a documented escape on a well-configured VMware box.

Tesseract - March 10, 2014, 7:05 pm

(Mar 10, 2014 07:00 PM)Null Byte Wrote: [\[CITE\]](#) Escaping Sandboxie is easy to do with a simple DLL injection. I have yet to see a documented escape on a well-configured VMware box.

I have yet to see a DLL injecting piece of malware that escapes a virtual machine. Well configured? It is just fine the way it is after you install VMware. What settings? Don't use Unity? Sure. Anti-viruses/malware for precaution? Sure.

K0FIN - March 10, 2014, 7:06 pm

I like Comodo. It's a pretty decent anti-virus, especially for being free.

Null Byte - March 10, 2014, 7:08 pm

(Mar 10, 2014 07:05 PM)MaiTriCks Wrote: [\[CITE\]](#) I have yet to see a DLL injecting piece of malware that escapes a virtual machine. Well configured? It is just fine the way it is after you install VMware. What settings? Don't use Unity? Sure. Anti-viruses/malware for precaution? Sure.

-I said DLL injection can escape sandboxie, not a vm. So in that regard you're proving my point further

-By "Well Configured" the main thing I mean is that you aren't using a bridged connection

(Mar 10, 2014 07:06 PM)K0FIN Wrote: [\[CITE\]](#) I like Comodo. It's a pretty decent anti-virus, especially for being free.

CIS is actually what I'm using right now. I'm in a love-hate relationship with HIPS right now.

Aura - March 10, 2014, 7:09 pm

(Mar 10, 2014 07:08 PM)Null Byte Wrote: [\[CITE\]](#) -I said DLL injection can escape sandboxie, not a vm. So in that regard you're proving my point further

-By "Well Configured" the main thing I mean is that you aren't using a bridged connection

CIS is actually what I'm using right now. I'm in a love-hate relationship with HIPS right now. Quite the arguing children. Recess time is over.

HA. Told you that HIPS could be fucking annoying sometimes. But it's the best feature of Comodo Firewall.

(Mar 10, 2014 07:10 PM)Xen0n Wrote: [\[CITE\]](#) Meh, it doesn't surprise me frankly that you can escape Sandboxie.

Go back to your vacation ban. I'm taking over SA to make it part of the Computing sector.

xhflhkeuhwguu34 - March 10, 2014, 7:10 pm

Meh, it doesn't surprise me frankly that you can escape Sandboxie.

Tesseract - March 10, 2014, 7:10 pm

(Mar 10, 2014 07:08 PM)Null Byte Wrote: [\[CITE\]](#) -I said DLL injection can escape sandboxie, not a vm. So in that regard you're proving my point further

-By "Well Configured" the main thing I mean is that you aren't using a bridged connection

CIS is actually what I'm using right now. I'm in a love-hate relationship with HIPS right now. I am proving your point because I already know malware can potentially escape a VM.

Null Byte - March 10, 2014, 7:11 pm

(Mar 10, 2014 07:10 PM)MaiTriCks Wrote: [\[CITE\]](#) I am proving your point because I already know malware can potentially escape a VM.

A virtual machine and sandboxie are two very different things.

I'm out of this thread now. I believe OP had his question sufficiently answered.

T e s s e r a c t - March 10, 2014, 7:14 pm

(Mar 10, 2014 07:11 PM)Null Byte Wrote: [\[CITE\]](#) A virtual machine and sandboxie are two very different things.

I'm out of this thread now. I believe OP had his question sufficiently answered.

Lol. Have a good day Nully ? No hard feelings right? ?

edit: *s

Null Byte - March 10, 2014, 7:17 pm

(Mar 10, 2014 07:14 PM)MaiTriCks Wrote: [\[CITE\]](#) Lol. Have a good day Nully ? No hard feeling right? ?

Oh yeah, no hard feelings man ?