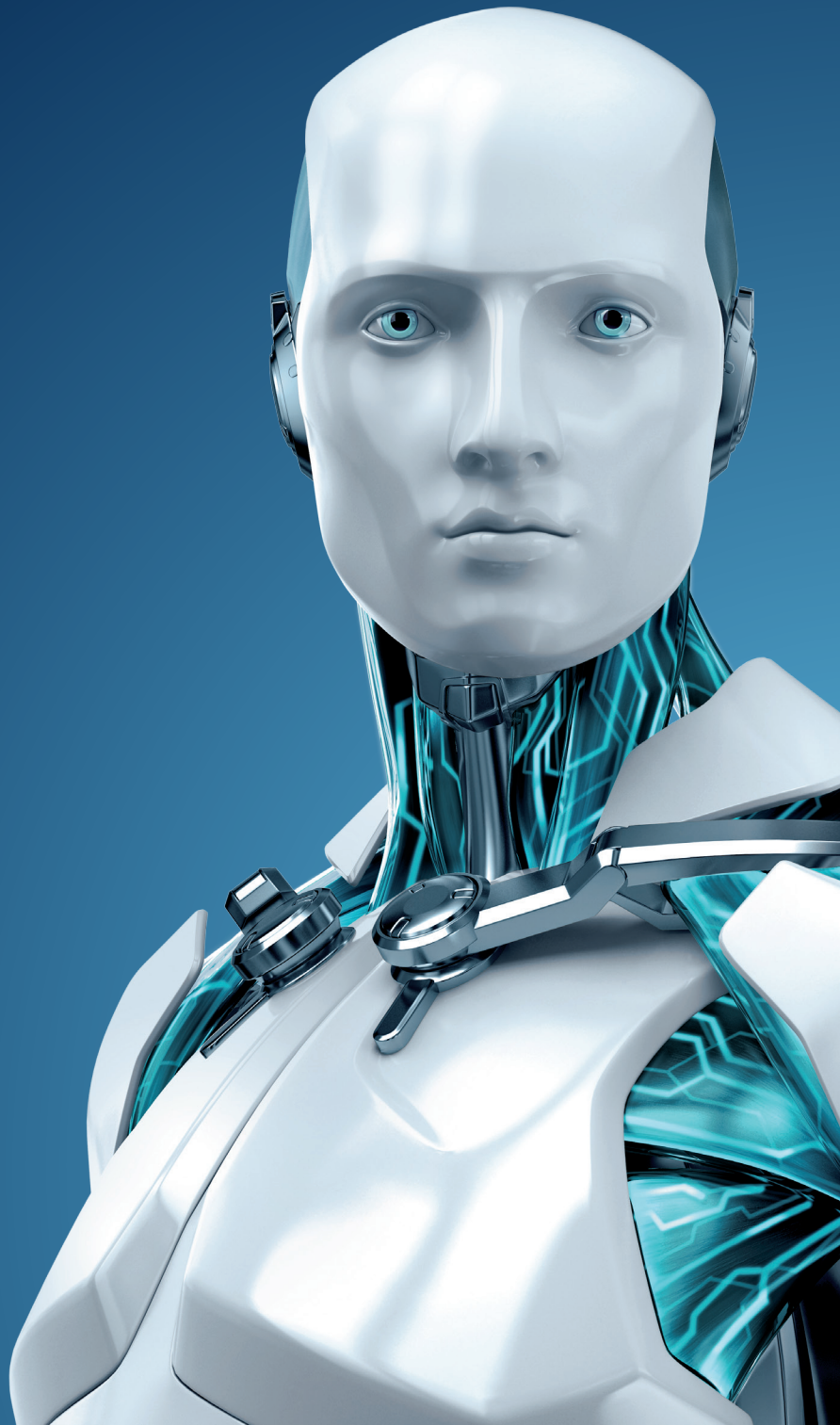
TECH BRIEF

10 ways to know it's time to change your antivirus



ENJOY SAFER TECHNOLOGY®

10 WAYS TO KNOW IT'S TIME TO CHANGE YOUR ANTIVIRUS

By Robin Dishon, ESET Staff

You likely have antivirus (AV) software in place at your business. (And if you don't, the never-ending stream of high-profile data breaches should be enough to convince you that you should have AV in place.)

But have you considered whether your solution is working as well as it should? Do you know what the signs are that indicate it's time to update or replace your antivirus software? Have you considered the fact that less-than-optimal solutions can cost you time and money, and degrade your security?

Here are 10 ways to tell it's time for a change:

1. When AV performance impacts productivity

If scans and updates slow your systems to a crawl, your productivity will benefit from a better solution, one that balances protection and speed. Not sure which brands are the fastest and most reliable? Check the findings of independent testing groups such as AV-Comparatives and Virus Bulletin.

You should also consider ease of management as well as ease of use and detection accuracy, particularly if you have a lot of systems to administer. You don't want managing your AV solution taking up all your time.

2. When employees complain about using AV

Any antimalware solution that runs slowly will be resented—and eventually bypassed—by employees. And when that happens, it affects both performance and security. When we learn of companies getting hit with a malware infection even though they say they have AV, for example, it often turns out this happened because one or more users had disabled the antimalware software on their company-issued phones or bring-your-own mobile devices.

3. When your AV under-delivers

Your AV can underperform in each of these areas: detection, performance, and usability.

Detection issues include not detecting a virus or other piece of malware as well as flagging non-malicious files as malware (false positives).

Performance issues include size of footprint and system resource usage. Higher system resource usage equals slower scanning. In a virtual machine, high system resource usage can contribute to AV storms. High bandwidth usage (when updating VSDs, checking cloud white/blacklists when scanning and determining which policies/rules to apply) can also result in slower performance for your entire network. In general, look for AV solutions that offer a light footprint that allows them to run unnoticed in the background.

Usability issues include pop-ups that require user intervention to resolve, wasting resources by demanding too much manual oversight. If the user isn't clear on what to do, user error can make the problem worse. Usability is also affected by manual processes in which the user has to initiate tasks and actively manage the antimalware solution rather than having automation built in. Putting the burden on the user, rather than automation, introduces a weak link and negatively affects your security posture.

4. When your AV alerts on too many files or links that aren't actually malicious, resulting in false positives

Some products achieve a high detection rate at the expense of being over-protective, but the resulting false positive results can waste valuable IT resources fixing a problem that doesn't exist.

According to a 2015 study by the Ponemon Institute, IT organizations are wasting valuable time and money hunting down false positives while advanced persistent threats evade preventive controls. Organizations spend an average of $1.2 million a year in time wasted responding to erroneous malware alerts, including false positives.

Like the boy who cried wolf, frequent false positives tend to result in employees ignoring credible warnings and failing to respond to real threats.

And worst of all, false positives can lead to deletion of legitimate files that the operating system or application program needs in order to function. One example of this occurred in 2010, when McAfee released an update that mistakenly attacked a legitimate operating system component known as SVCHOST.EXE. This false positive caused tens of thousands of Windows XP computers to crash or repeatedly reboot.

And in October 2011, Microsoft Security Essentials (MSE) removed the Google Chrome web browser, mistakenly flagging it as a Zbot banking Trojan.

To prevent false positives, the top AV companies use multiple procedures, such as advanced heuristics and DNA smart signatures, to determine more precisely whether a file is legitimate or not and lower the possibility of a false positive. Technology such as ESET's LiveGrid® checks a file's reputation against a database (whitelist/blacklist) that includes data collected from users all over the world. In addition, most AV solutions will have an exclusion list (that users can add) to exclude the file from being detected by the scanners (real-time or on-demand scan) if it was accidently detected.

5. When removing malicious files and dealing with false positives is too complicated

You want a solution that delivers silent quarantines and automatic removal of malicious files, not more work for your IT team. The Ponemon study mentioned above found that companies spend an average of almost 600 hours each week on malware containment.

- **The most time (229.9 hours per week) is spent cleaning and fixing and/or patching networks, applications and devices (i.e., endpoints) damaged or infected by malware.**

Another study estimated that enterprises around the globe spent about $500 billion in 2014 making fixes and recovering from data breaches and malware (source: International Data Corporation and the National University of Singapore).

6. When infections come back after you have removed them

This means the AV isn't doing a good job of cleaning or updating its detection often enough, a clear indication you're running inferior software. Again, we recommend checking the results of independent testing groups such as AV-Comparatives and Virus Bulletin and reading professional reviews.

7. When it's difficult to manage the solution across all your platforms and devices

You need a security product that's easy to manage so the burden of protection is minimal. A product that includes remote administration lets you control your entire network of workstations, servers and smartphones from a single location. The built-in task management system enables timely responses to malware incidents and lets you run reports, manage quarantined files, assign different privileges to users and enforce consistent security policies with ease.

8. When AV alerts or pop-ups interrupt presentations and sales demonstrations

You deserve uninterrupted access to your machine, with a malware solution that includes "silent" or "gaming" mode that is easy to use, as well as a good administration tool to restore regular mode when the presentation is over. For example, in some AV solutions there's a checkbox that enables presentation/gamer mode when running applications in full-screen mode automatically. During full-screen mode, all alerts and notifications are suppressed; once the user is out of full-screen mode, the presentation/gamer mode is disabled.

9. If getting technical support and customer service are inconvenient or communicating is difficult

If it's a pain to get reliable, customer-oriented support, it's time to think about an alternative AV product. Look for a solution that comes with free support that is provided from a location in your time zone, or close to it.

10. If you lie awake at night trying to figure out how to get world-class, fast-running, accurate AV protection that employees love and the bad guys hate

Then it's definitely time for a change.

Not sure which AV software is right for you? Take some new ones for a test drive with a free trial. You may want to try two or three brands of antivirus software to evaluate performance and customer support before you buy. See how they handle issues such as difficulties with installation, false positives or removing your current antivirus software.

ESET offers award-winning security solutions that can be customized for your business and industry, with products ranging from cross-platform endpoint security to secure authentication, data encryption and a single console remote management system. Test drive our solution with a free 30-day business trial.

ESET® develops innovative online security solutions used by businesses, governments and consumers worldwide. With a multilayered protection strategy ranging from gateway, server and endpoint defense to encryption, two-factor authentication and data recovery, ESET supports business continuity and individual privacy across multiple platforms. At the core is ESET's innovative heuristic technology, a proactive detection system that eliminates threats and shields networks, users, data and machines in real time. Our mission: to help the world Enjoy Safer Technology® every day.