7 Ways to Tell If It's Time to Change Your Anti-Virus Software

When you're responsible for Internet security and anti-virus protection in your organization, you know how critical AV software is.

The threats keep changing and growing at exponential rates. Every day 30,000 new threats and 3,500 new viruses appear. And, if you've had any recent issues with Internet security and malware, you may already be wondering if your AV software is really getting the job done.

So how can you tell if it's time to change your AV software? That's where this list can help. It spotlights specific objective metrics and activities you can check to see how well your current AV software is performing. Besides helping you **benchmark your current software, it also establishes a starting point for evaluating new AV options when you decide you need to make a change.**

1. **Anti-malware protection measurement**
   Anti-virus testing labs such as AV Comparatives, Cascadia Labs, Virus Bulletin, and others run different AV software products through a series of tests, and report comparative scores for how well each product performs each kind of detection. These involve 2 kinds of AV detection: reactive which detects known viruses, and proactive which detects unknown viruses (heuristics).

   The higher your AV product's reactive score, the better you're protected against known threats; and the higher its proactive score, the more you're protected against potential threats.

2. **Anti-virus update frequency**
   The number of new malware threats and viruses each day is exploding, which makes the frequency of AV updates a very important component of protection. Current products range from less than one update a day to more than 21 a day.

   With 3,500 new viruses appearing every day, if you get updates only once a day, you're exposed to 3,500 new threats between updates!

3. **Impact of scanning performance**
   Anti-malware products perform several different kinds of scans: boot, on-access, on-demand, email, and full file system scans. Except for system scans – which can be scheduled for non-working hours – all of these scans occur real-time when users are at their desks. Again, test labs measure how fast different AV products perform each kind of scan, and report the results.

   The faster your AV software runs these scans, the more work users can get done.

Every day 30,000 new threats and 3,500 viruses appear. Are you protected?

Get more information from these industry resources!

www.av-comparatives.org

www.virusbtn.com/vb100

www.kaspersky.com/cascadia

www.anti-malware-test.com

4. **Resource usage**
   It's probably fair to say that virtually all AV products use significant system resources when they're actively executing detection scans.

   The benchmark for resource usage is how fast your AV product completes its scans and returns resources to the system. Checking scan performance results from various test labs will tell how long each product ties up system resources.

5. **Helpdesk calls**
   This can be seen as an indirect indicator of anti-malware protection and scanning impact in your organization. Tracking the volume of AV calls to your helpdesk over time will show whether AV issues have been increasing. Plus, if your helpdesk records include call notes, you may be able to identify specific AV problems.

   The more your help desk is burdened with AV calls, the less likely your software is getting the job done.

6. **Support levels and access**
   An objective measure for evaluating product support is how often your AV support delivers "first responder resolution." Although this may be the universal goal of support organizations, many AV companies do not structure product support to enable "first responder resolution."

   The closer your AV product support comes to achieving "first responder resolution," the less time you have to spend waiting in support queues.

7. **Management**
   Complexity is the biggest issue to consider when it comes to AV management. If your AV software has manual processes for configuration and managment, they tend to be more labor-intensive and error-prone.

   Using AV software with product wizards to automate and simplify product configuration and management requires fewer staff hours, and reduces training requirements.

Summary:
Software changes are always tough, and AV changes even more so because of their impact if something goes wrong. With budgets tight as well, it's critical to demonstrate that change is needed. This checklist is intended to be a useful starting point for determining whether a change in your AV software is needed, as well as framing the most desirable features to look for in a new AV solution.

For more information on how Kaspersky can help you assess your current anti-virus solution, please contact smbsales@kaspersky.com or call 866-563-3099.

500 Unicorn Park
Woburn, MA 01801
866.563.3099
smbsales@kaspersky.com

www.kaspersky.com
www.threatpost.com