

Antivirus Taste Test: One Man's Quest for (Nearly) Objective Rankings

Security Consultant Chaz Sowers did a semi-scientific comparison of antivirus software. The results may surprise you.

» [Comments \(6\)](#)

By Chaz Sowers CISSP, CISM

May 20, 2009 — [CSO](#) —

Editor's Note: Chaz Sowers wants reliable, independently tested antivirus software with few false positives. But what really constitutes an "independent" test? Unsatisfied with lab ratings, he built his own malware testbed and put 35 AV products through the paces. Here is the story behind one man's AV rankings; your results may vary.

I started my research with an online company that just recently rated the "top" 14 AV products. They promised "independent comparatives of antivirus software" while at the same time stating that "since 2008 [they charge] a fee for various services we provide."

Call me a skeptic. But when a testing lab accepts money from a company to test its product, I have to wonder about the independence of the findings.

Even assuming the test results are truly independent, this business model excludes smaller companies that are unable or unwilling to pay the testing fees. A quick search online found over 40 AV products, many from companies I had never heard of before. I wondered how the lesser known ones might fair against the better known ones.

Since I already have a day job (as senior security architect at Vangent Inc., provider of information management and strategic business process outsourcing services) and didn't accept money from anyone for these test results, I decided to share my independent and unbiased comparison of AV products.

The results may surprise you.

Testing methodology, disclaimer and other stuff

My testing methodology was as unbiased as I could make it. After all, I had a vested interest in finding the best AV solution for my own computer. Of course my testing falls short of the double-blind scientific method, but I think it holds up well for publication in mainstream media. Remember this above all: I was searching for an AV product that would identify and delete the highest number of the test malware that I have. My emphasis in testing was on a high number of detections and my testing penalized software that reported a large number of "false positives."

Software

I used a fresh install of Windows XP, running in a Sun Virtual Box virtual machine, to run all tests. The installation of Windows was fully patched and updated (including SP3) as of Jan. 8, 2009. Each AV program was copied to the main machine from a shared folder and was the only program on the virtual machine not part of a regular Windows install. The test data resided on a logical D:\ drive and consisted of 36,438 pieces of malware. All of the malware has been, or currently is, in the wild. The virtual machine was restored to the previous, pristine state after each test.

Hardware

The system used for testing consisted of a AMD Sempron 2600-Plus processor, Asus A7N8X-E motherboard, 3 GB of 184 pin DDR RAM, a Seagate 190GB SATA hard drive, and an nVidia video card. The test bed was installed with Ubuntu Linux (version 8.10 Intrepid Ibex) which ran a copy of Sun's Virtual Box (OSE 2.1.0). Most AV programs ran without incident on the test bed but a few had problems which are detailed in the table that follows.

Source

I found a list of AV vendors on [this website](#), which I augmented with additional AV found [here](#). The Wiki site had 35 unique AV product listings, including proprietary, freeware and open source. There were names that I have known for over 16 years as well as ones that I had never seen before. Of these listings, I eliminated those whose parent company no longer existed, those for operating systems other than Windows, those for whom I could not download an evaluation copy, and software at (or very near) the end of its life. What remained are the AV solutions evaluated here.

Download

All AV software was downloaded directly from the vendor's website (where possible) or from a trusted source (C-Net or SourceForge) where the vendor did not directly support downloading. In all instances the software I downloaded was fully functional but time-limited software and would be the same that I would install and keep. For the companies that offered free versions of their products, I still chose the trial version of the commercial product.

Disclaimer

Ultimately these findings are the true and factual results of my experiences with the software and hardware listed above. They should not be used as the sole basis for purchasing Antivirus software and none of these products is endorsed by me or any of the professional associations through whom I have certifications.

Here are my findings:

- **AV: Arcabit Infections found:** 28,944. **Comments:** This AV software come from Poland and the GUI feels like it. There are a few poorly translated buttons (Pauza for Pause, for example) but overall a very intuitive interface and easy to use. The scanner was screaming fast, taking only 27 minutes and 34 seconds to evaluate all the files in the malware folder.
- **AV: Ashampoo Infections found:** 32,291 **Comments:** Decent product but the name definitely isn't ready for Prime Time. I doubt that their enterprise solution would be taken seriously because it's too easy to dismiss an AV solution called "a shampoo." The funny name aside, their AV product performed better than some very big names (Norton, Panda and Kaspersky) and proved to be very good.
- **AV: Avira Infections found:** 35,846 **Comments:** Took about 2 hours to plow through all the test data which ranks it as average in speed. Identified a very respectable 98.37 percent amount of malware but even this high percentage leaves 592 infections on the computer.
- **AV: AhnLab Infections found:** 21,301 **Comments:** AhnLab doesn't offer an AV-only product. This one is an integrated Internet Security package with "virus, work, hacking and Phishing" protection. Unfortunately, against my mix of malware this software finished third to last, and worst of all AV products that found more than 10,000 pieces of malware.
- **AV: Avast Infections found:** 36,124 **Comments:** Found 36,124 total malware but only after running the program twice. After the first scan produced such a small number of results, I re-ran the AV and this time it found additional infections. In truth, if I didn't have previous experience with this AV and a high respect for it, I probably would not have run the test a second time. If I had reported the first scan this software would have finished dead last instead of near the top. After two scans it did finally find 99.14 percent of infections. But, I ask, how many people will run AV software twice in a row?
- **AV: AVG Infections found:** 110 **Comments:** Yeah it really only identified 110 items. I ran the test 4 different times, from the context menu and from the software's GUI, changing the options to allow more time to scan and even specifically pointing it to the folder that contains about 20K well known viruses. It still came up with only 110.
- **AV: Bit Defender Infections found:** 36,105 **Comments:** After a rocky start the software showed its true ability by finding 36,105 pieces of malware. That's a total of 99.08 percent and ranks the software in third place.
- **AV: Bull Guard Infections found:** 31,608 **Comments:** Worked fairly fast, taking only 15 minutes to flag 31,608 pieces of software However, the product froze the computer when I tried to use the GUI to remove the flagged malware.
- **AV: CA Infections found:** 24,996 **Comments:** Unfortunately CA only found 68.59 percent of my malware. If I were a "black hat" I would certainly want to know which enterprises are using CA Antivirus.
- **AV: Clam Infections found:** 22,247 **Comments:** Despite being a huge supporter of open source software, I'm afraid that a 75-percent success rate is too low for me to consider seriously. Missing 25 percent of the test data translates into 9,109 pieces of malware and I don't think many people would think twice about paying 50 beans for the extra protection.
- **AV: Comodo Infections found:** 36,492 **Comments:** By far and away this was the fastest AV scanner that I tested. Comodo scanned thought all 36,438 malware in only 6 minutes. However, it appears that this speed comes at a price. The software flagged and "removed" 54 more instances of malware than were actually on the computer.
- **AV: Dr. Web Infections found:** 34,114 **Comments:** Spartan and quirky user interface. The aforementioned notwithstanding though, this software found 93.62 percent of all the malware. And it did this in only 14 minutes! I was impressed!
- **AV: Dr. Web CureIt Infections found:** --- **Comments:** This is the free version of the Dr Web software product. It took the Spartan interface and stripped it down to basically an "on" and "off" button. The software promises to "quickly scan and cure" computer infections. In my case, though, after scanning for 7 hours and 10 minutes it found 137,286 infections after scanning only 7,711 files. Extrapolating this data, the scan would have taken 34 hours and found almost 600,000 infections. I pulled the plug.
- **AV: eScan Infections found:** 36,146 **Comments:** Surprisingly, this unknown (at least to me) AV vendor found the second highest number of malware. The scanning times were average but it outperformed many other better known brands with 99.19 percent detection. Ranks in second place.
- **AV: ESET Infections found:** 23,746 **Comments:** Took 4 hours to scan all malware but the accuracy of the scanner has this product finishing in the bottom half of the test. This software recognized only 65 percent of all malware. Clam the free AV performed better.
- **AV: File Sentry Infections found:** 111 **Comments:** Yes, after running the test twice, reinstalling and running again, the AV still only found 111 malware. I wonder if AVG and File Sentry are using a common AV engine. This would explain the very low, and almost identical number of infections found. It does not however explain the overall poor performance of these two AV products.
- **AV: F-Prot Infections found:** 32,635 **Comments:** I received the error message that the "maximum entry count reached". The "Report" window in the GUI had about 500 entries before the error appeared. This scanner ran longer than most taking 12 hours and 5 minutes to scan all data files.
- **AV: F-Secure Infections found:** 36,692* **Comments:** On my fourth attempt at installation I finally got something that looks like it might scan for malware. The previous 3 installations failed at various points and the software failed with no error message or notification. After the software did run, it found an extra 2,642 files to scan and discovered 254 more instance of malware than actually existed on the computer.
- **AV: G Data Infections found:** 36,423 **Comments:** Highest success of any AV solution tested, identifying 99.95 percent of all the malware in my data file; downside is that everything is in German and the GUI is a little bit quirky.
- **AV: Hacker Eliminator Infections found:** 1 **Comments:** Yes, this software found exactly 1 piece of malware. Perhaps this is a limitation to the trial version because the set up screen said "will not remove Trojans unless you purchase a license." Regardless, by finding 1 malware, it performed better than in did in another report where it identified absolutely zero.

- **AV: Hauri Infections found: 35,325 Comments:** The scanner said that it scanned 63,828 files but I only had 36,438 pieces of malware for it to look at. The only possible explanation I have is that it scanned the 27,390 files in the Windows directory in addition to my malware. Nevertheless, if we believe the scanner results, this AV identified 97.21 percent of my malware collection.
- **AV: Kaspersky Infections found: 20,289 Comments:** I read about Kaspersky Labs often, and I have to admit that my expectations were high for this product. Sadly, this was another major AV company that failed to impress me. The software only identified 55.68 percent of the malware.
- **AV: McAfee Infections found: 36,512 Comments:** McAfee found 74 more malware than existed on the computer. Assuming that these 74 extra files were "false positives" and not the software alerting on Windows Updates, then this product had the most false positives of any I tested.
- **AV: Norton (Symantec) Infections found: 20,404 Comments:** The program installed easily and ran quickly, finishing in about 25 minutes. I was shocked though at the low number of malware that it flagged, so I restored the virtual machine and reinstalled NAV. After running it a second time I got the exact same results. So I tried a third time. Sad to say, what I thought would be the Gold Standard, only identified 56percent of the malware. But it did find this 56 percent three times in a row.
- **AV: Panda Infections found: 31,719 Comments:** Sixteen hours, 4 installs and 7 reboots after I started, I finally was able to get the software to scan. It found only 87 percent of the malware on the system. Lots of work for a disappointing low result.
- **AV: PC Tools Infections found: 30,023 Comments:** Endorsements from Dr Phil and www.MajorGeeks.com aside, this AV only caught 82.39 percent of malware on my computer. Not a much better than Clam (the other free AV in the test) and far from what I would install to protect my computer.
- **AV: Protector Infections found: --- Comments:** I was excited to try an AV product from India. Unhappily this one brings up a "nag screen" with each infection it discovers, requiring the user to "click here" to continue. Needless to say, I no intention of clicking through 36,438 nag screens. Plug pulled!
- **AV: Rising Software Infections found: 27,991 Comments:** After almost giving up to make this product work, it finally installed and ran on my last attempt. This AV was one of the faster ones, chewing through all my test data in only 47 minutes. However, it only managed to identify 27,991 of the items it scanned.
- **AV: Sophos Infections found: --- Comments:** The software froze the computer and I was unable to run the test. I followed the same procedure I used with other AV software like reinstalling using different options, but the software still wouldn't run. It seemed like it was trying to call a service that wasn't running, but for whatever reason, the software either "failed silently" or froze the computer.
- **AV: Trend Micro Infections found: 35,182 Comments:** I don't know what the software meant when it said that "35,001 targets checked" when it should have counted 36,438. It also said "35,182 potential threats found" but it didn't delete them.
- **AV: Trust Port Infections found: 36,171 Comments:** Despite their Web claims of 99.9percent detection, this software only detected 99.26 percent on my tests. Still, it was pretty darned impressive. They use a unique approach by licensing AV engines from 4 other companies which they roll up into their own GUI (AVG, DrWeb, Norman, and Virus Blok ADA). Certainly an excellent AV choice, but still second to G Data in terms of malware identification.
- **AV: Virus Blok ADA (also called VBA) Infections found: 22,417 Comments:** The software has a very Spartan GUI and didn't appear to provide a summary report. In fact I'm not sure that a reporting option even exists. And since this AV identified only 61.52 percent of my malware, the lack of a reporting function doesn't really matter.
- **AV: Zondex Infections found: --- Comments:** This AV software hails from Australia and I was curious to see how an "Auzzy" product would stack up. The interface feels a lot like Windows 3.1 and settings cannot be adjusted like many other products. Twice the GUI crashed and stopped running. When restarted, it pegged CPU usage at 100percent.
- **AV: Zone Alarm Infections found: --- Comments:** It was the slowest of all AV products tested, scanning only 162 files an hour (2.7 files per minute). I was curious as to why it was so slow until I checked my firewall logs (not ZA or Checkpoint). Apparently the product "phones home" with each and every possible infection. At this rate the test would have taken over 9 days to complete. I pulled the plug after 30 hours.

Products not tested (and why)

- **Inca:** Also know as nProtect, the site is mostly in untranslated Korean (hover your mouse over the "Products" icon and see for yourself). I was trying to read the few English words on the site and guess where the link to the software was when the site launched a java script that pegged my CPU usage at 100 percent. Given this experience I chose not to download or test this AV.
- **Graugon:** A program that uses the Clam AV engine, and after seeing how effective this engine is, I chose not to evaluate this product.
- **Norman:** The Trust Port AV software uses the Norman AV engines in its product. Since the engine was already being tested (sort of) I chose not to test it again. They also appear not to have a free evaluation copy of their software.
- **Virus Chaser:** Another AV product from the People's Republic of China. For the most part, the site was better translated than the others from Korea and China. However, having said that, the link on the site to download the software is either broken or deliberately severed. I tried many times over the course of a week to download the software.
- **Microsoft OneCare:** Cheap shots at the software giant aside, this product is at the end of its life. Microsoft plans to roll out a new anti-malware product in a few months code named "Morro." Since I decided at the beginning of these tests not to evaluate any AV that is (or will be shortly) discontinued, MS was left out.

RANK -- AV Product -- Malware Identified -- Percentage of Total

- 1. -- G Data -- 36,423 -- 99.95 percent
- 2. -- Trust Port -- 36,171 -- 99.26 percent
- 3. -- eScan -- 36,146 -- 99.20 percent
- 5. -- BitDefender -- 36,105 -- 99.08 percent
- 6. -- Avira -- 35,846 -- 98.37 percent
- 7. -- Hauri -- 35,325 -- 96.94 percent
- 8. -- Trend Micro -- 35,182 -- 96.55 percent
- 9. -- DrWeb -- 34,114 -- 93.62 percent
- 10. -- F-Prot -- 32,635 -- 89.56 percent
- 11. -- Ashampoo -- 32,291 -- 88.61 percent
- 12. -- Panda -- 31,719 -- 87.04 percent
- 13. -- BullGuard -- 31,608 -- 86.74 percent
- 14. -- PCTools -- 30,023 -- 82.39 percent
- 15. -- Arcabit -- 28,944 -- 79.43 percent
- 16. -- Rising Software -- 27,991 -- 76.81 percent
- 17. -- Clam -- 27,247 -- 74.77 percent
- 18. -- CA -- 24,996 -- 68.59 percent
- 19. -- ESET -- 23,746 -- 65.16 percent
- 20. -- VBA -- 22,417 -- 61.52 percent
- 21. -- AhnLab -- 21,301 -- 58.45 percent
- 22. -- Norton (Symantec) -- 20,404 -- 55.99 percent
- 23. -- Kaspersky -- 20,289 -- 55.68 percent
- 25. -- File Sentry -- 111 -- 3.04 percent
- 26. -- AVG -- 110 -- 3.01 percent
- 27. -- Hacker Eliminator -- 1 -- 0 percent
- 4 or 24 -- Avast -- Make sure to read the footnote for this entry in the individual assessment. Avast had either 99.14 percent or 57.67 percent success.

These AV products were eliminated because they reported more malware than actually existed on the computer (false positives): Comodo, DrWeb CureIt, F-Secure and McAfee.

These AV products were eliminated because they caused miscellaneous problems on the test bed (read the individual entries for details): Protector, Sophos, Zondex and Zone Alarm. I offer no explanations why these AV products did not work. I simply report the results that occurred in my test bed.

- [Email](#)
- [Print](#)
- [Comments](#)
- [Digg This](#)
- [SlashDot](#)