

INFORMATION SECURITY

WWW.INFOSECURITYMAG.COM

Help!

Vendors promise solid tech support, but our test found long hold times and poor advice.

By Ed Skoudis

What really *sells* security managers on one AV vendor over another?

There's no mystery behind antivirus technology. Gateway and host-based applications scan files against signatures for known viruses and apply heuristics to detect the unknown. With persistent maintenance, and a little luck, AV applications can catch most malware.

But product loyalty is built through customer support. When security managers are happy with their vendors, they say, "They've been right there whenever we've run into problems." Robust, exciting technology may be the spark that brings vendors and customers together, but support is the stuff of long, happy relationships.

With a malware storm always on the horizon, you'd expect AV vendors to have among the best customer support programs. The last thing you'd expect is having to wait an eternity on an 800-number listening to Burt Bacharach melodies only to tell your problem to a call center operator with a checklist of questions and stock responses.

But that's exactly what *Information Security* found disturbingly often in our review of leading AV vendors' customer support.

As a follow-up to our technical review of desktop AV products, *Information Security* investigated the state of the AV industry's customer support, putting five vendors to the test: Computer Associates, McAfee, Symantec, Sophos and Trend Micro. We graded each on the entire support experience, putting the greatest weight on the ability to solve our test problems (see "Report Card," p. 34).

After several dozen support phone calls over three weeks, we can report bright, not so bright and downright dark spots. Some vendors have sharp techs who think on their feet and solve problems with professionalism and enthusiasm. Others subject customers to intolerably long waits, staff with limited knowledge and, in a few cases, advice that actually compromises security.

Support Call Scenarios

Information Security tested each of the vendors with support calls based on four different scenarios, which we constructed with varying complexity and likelihood of occurrence. This allowed us to test each support staff's competency and the consistency of quality service. The "problems" were as follows:

1. Installation. We wanted to measure the vendors' troubleshooting capabilities when confronted with an unusual, yet fairly simple, installation problem. We created a folder with the same name as the one the AV installer creates. We then changed the permissions on the folder so that even the machine's administrator couldn't write to it, causing an error message.

2. Personal Firewall. We configured a third-party personal firewall to block the AV's signature update requests, while allowing all other traffic (browser, Windows FTP client, ping, DNS lookups, etc.). We didn't tell the support personnel we were running a personal firewall until they explicitly asked. This is a common problem, so we expected a quick, easy solution. Boy, were we surprised.

3. Disinfection. We installed the AFX Windows Rootkit on our test lab systems. We chose this malware for two reasons. First, it employs several techniques that make it difficult to delete and forces many AV tools to quarantine rather than remove it; we wanted to see how the technicians advised us to get rid of the malware, or whether they'd let it sit in quarantine. Second, attackers frequently use rootkits to mask other forms of malicious code.

4. Custom Malware. We created a simple five-line script that disabled each product's real-time protection shortly after system boot. We wanted to see how the support staff would handle malicious code that disables its tool, and whether its troubleshooting processes could even identify it. We tried to make it obvious, naming our script "stop.bat,"

and placing it in the C: directory. We ran it using the "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" registry key, a common method for activating malicious code every time the system boots or a user logs on. The script caused each product's AV system tray icon to change appearance, indicating that real-time protection was disabled.

TECHNICAL PROWESS

Troubleshooting Skills

This is the ultimate test: Could the vendors quickly solve our problem with a minimal amount of pain?

We frequently got the distinct feeling that the support techs were simply reading opaque troubleshooting instructions from an online manual. On several occasions, support personnel at CA, McAfee, Symantec and Trend Micro admitted that was exactly what they were doing. Most of them seemed knowledgeable only about their software, with little understanding of the underlying Windows OS and its impact on their products.

Vendors' troubleshooting effectiveness is reflected in this report, in part, by how long each spent dealing with, unraveling and resolving our scenarios. Sophos and CA were the quickest, while Trend Micro was generally far slower. McAfee and Symantec were mixed bags.

Overall, Sophos, which places customer support as the cornerstone of its business, was the best. We were greatly impressed by the troubleshooting skills of its technicians, whose knowledge about their product and Windows is solid. But Sophos wasn't perfect, as we'll see in our next comparison criteria.

CA's processes and patient, polite support techs worked well, resolving three of our four scenarios within an hour. For example, CA quickly settled the tricky custom malware issue by having us use the built-in Windows XP restore function to set our system configuration back to before we installed the malicious script. Nevertheless, CA's techs never identified the original problem, likely leaving other systems exposed to the same attack.

Our problems were most pronounced with Trend Micro. In dealing with our custom malware scenario, Trend Micro's technician incorrectly concluded that the system tray icon indicated that the AV client couldn't communicate with the AV server. We protested, saying that we thought the real-time scanning was disabled. He disagreed and spent an hour on the phone troubleshooting the wrong problem, followed by another hour analyzing results we sent via e-mail, before admitting his error.

Some of the solutions offered were dramatic—and misguided.

After two hours dealing with our installation problem, a Symantec technician advised us to reinstall the OS, even though we simply faced a permission problem in a single folder. After we carefully reread the Symantec diagnostic tool's error message—which said the administrative user didn't have privileges to access the Symantec Antivirus folder—the technician finally understood the issue.

Similarly, the McAfee technician advised us to uninstall the product to solve the custom malware challenge. When

COMPARISON SUPPORT ON THE LINE

ANTIVIRUS VENDORS (with location of support centers)

SUPPORT PROBLEM	COMPUTER ASSOCIATES (India)	McAFEE (Plano, Texas)	SOPHOS (Lynnfield, Mass.)	SYMANTEC (Eugene, Ore.)	TREND MICRO (Philippines)
Installation Failure: Created a folder with a name used by the AV tool, but without write permissions.	Time: 73 min. Resolution: After trying to uninstall the tool, per the support tech's instructions, we installed it into a folder with a different name.	Time: 24 min. Resolution: Instructed us to add write permissions to the folder; we deleted it and then reinstalled tool.	Time: 51 min. Resolution: Instructed us to add write permissions to the folder; we deleted it and then reinstalled tool.	Time: 135 min. Resolution: After repeated attempts to remove and/or reinstall, we were advised to reformat the drive and reinstall the OS. Finally, we added write permissions to the folder, deleted it, and then reinstalled tool.	Time: 180 min. Resolution: After hours of trying to delete logs and nonexistent services, folders and registry keys, we were told to delete the problematic folder and reinstall the tool.
Personal Firewall Issue: Configured a personal firewall to block signature updates.	Time: 31 min. Resolution: After reconfiguring and restarting service, the support tech quickly isolated the firewall problem.	Time: 258 min. Resolution: Downloaded new signatures several times, reinstalled AV tool and ran a diagnostic script. The support tech finally discovered the firewall.	Time: 17 min. Resolution: After verifying network activity, the support tech said, "This sounds like a firewall problem." He then helped reconfigure the firewall.	Time: 186 min. Resolution: After hours of repeated removal and reinstallation of the AV tool and license key, the support tech discovered the firewall.	Time: 184 min. Resolution: After hours of analysis, escalated to second-tier support, which discovered the firewall within 30 minutes.
Rootkit Removal: Installed a difficult-to-remove rootkit that is often quarantined but not automatically deleted.	Time: 36 min. Resolution: Instructed us to reconfigure the AV tool away from defaults so that it could automatically delete the rootkit.	Time: 44 min. Resolution: Instructed us to tweak configuration to delete the rootkit files.	Time: 31 min. Resolution: Instructed us to boot system in safe mode to run a script that deleted rootkit files. Advised us to install antispyware tool and a personal firewall.	Time: 28 min. Resolution: Instructed us to boot system in safe mode to delete rootkit files by hand, and advised to reinstall operating system.	Time: 55 min. Resolution: Downloaded and ran a custom cleaning script, which removed rootkit.
Custom Malware: Installed a script, "stop.bat," that disables AV real-time scanning during system boot, making the AV system tray icon indicate no protection.	Time: 45 min. Resolution: Instructed us to use the XP system restore capability to set machine configuration back one week, removing our stop.bat registry key for startup. The support tech never detected malicious script.	Time: 93 min. (plus four days to analyze diagnostics) Resolution: After reinstalling the tool twice, the support tech finally pointed out a strange "stop.bat" startup file, but didn't tell us what it did.	Time: 69 min. Resolution: The support tech misdiagnosed problem, saying that we faced a "bug" in the product that made the AV appear to be disabled, leaving us infected and without protection. He never detected malicious script.	Time: 63 min. Resolution: Instructed us to reconfigure the AV tool to start up despite presence of malicious script. The support tech never detected script.	Time: 288 min. Resolution: The support tech never solved problem despite several days analysis of system diagnostics. He never detected malicious script and left it running.

we tried, the automated uninstall script failed, a curious anomaly that wasn't part of our scenario. She then walked us through the painstaking process of manually removing a dozen registry keys and files. That also failed, due to default permission problems—also not our doing. After an hour of trying to manually delete the AV tool, our technician advised us to run a diagnostic program, which—after four days—finally identified the real issue. McAfee also told us that there was a strange file called stop.bat, without venturing any opinion about what it might be doing.

First, Do No Harm

Although the people we dealt with were security vendor support staff, some of them left us...well...insecure.

When resolving tricky problems, a technician sometimes has to temporarily weaken security settings. That's fine—as long as they restore them when they're done. In some cases, though, the AV vendors' support techs failed to instruct us to restore security settings after resolving our problems, leaving us vulnerable.

Even worse, Sophos—which was simply stellar resolving our first three problems—left us compromised and wide open to new attacks in dealing with the custom malware issue, in which our script disabled the AV tool's real-time scanning. The Sophos tech said this was a known bug that makes it *appear* as though real-time scanning is disabled. He didn't even have us take the elementary step of verifying the status of real-time scanning in the services control panel, which would have shown that the protection was disabled. If a sysadmin accepted this diagnosis, he'd have an infected system *and* no working AV.

For two of our scenarios, McAfee technicians advised us to give full control to everyone on the machine for McAfee-related registry keys and/or folders in the directory structure. This was part of an attempt to uninstall the McAfee product before trying to reload it. That's a problem, since granting blanket permissions like that could allow ordinary users to change configurations or alter executables.

Of more concern, Trend Micro technicians advised us to give everyone full control on the central server's shared folder, including scripts used for installing the package and scanning for malware. With these permissions, an attacker could use the Trend Micro installation files on the server to spread malware to clients. Additionally, Trend Micro told us to wipe out our AV logs in unsuccessful attempts to fix three of our four test problems. That hamstrung subsequent troubleshooting and wiped out any records of prior infections. Trend Micro also recommended we give all local laptop users admin-level privileges, a bit of advice that we're uncomfortable applying across an enterprise, because some users simply don't understand the security implications of their actions.

In the course of our testing, some AV technicians gave us very helpful suggestions, particularly during our rootkit scenario. In particular, a Symantec technician advised us that there were likely bigger problems on our system because a rootkit is designed to hide other forms of malicious code. She recommended that we reinstall the operating system from scratch—solid advice, and music to our ears, although reformatting the drive, then reinstalling

the OS is the best solution to be sure the rootkit is eradicated.

The Sophos technician also cautioned us about rootkits. Although he didn't recommend a reinstall, he advised us to add an antispyware tool and personal firewall.

Help Yourself?

Telephone support is not the only medium we tested. We also looked at the usefulness of online help.

Each vendor site includes searchable knowledgebase articles, a virus encyclopedia and a library of signature updates. We researched each of our scenarios using the knowledgebases, entering the same keywords into each search engine. The results for every vendor except Symantec were pathetic. CA, McAfee, Sophos and Trend Micro yielded few matches and little insight. Symantec's knowledgebase, however, provided useful tips in resolving our personal firewall, rootkit and custom malware problems.

The vendors' virus encyclopedias looked quite similar, but Sophos provided the most detail about the dozen different trial specimens for which we searched.

THE USER EXPERIENCE

"Please Hold"

The quality of the hold music aside, nothing is more frustrating and unproductive than waiting for your turn to talk to a support technician.

We clocked the initial hold times of our calls for each scenario. If a problem required multiple calls, we averaged the initial hold times. While there's no standard for acceptable hold times, we set our expectations at 10 minutes. We didn't include times we were placed on hold after being assigned a technician; we assumed the tech was working on our problem.

Despite subjecting us to a mix of AM radio-style ads and pop music, CA was the quickest at getting us off hold: an average of four minutes per call. CA was the only vendor that asked us to rate the severity of our issue before asking us to hold: general issue, minor problem, major problem and critical system outage. For our tests, we split the level of urgency between minor problems (installation and personal firewall) and major issues (disinfection and custom malware).

In sharp contrast, Symantec left us in hold purgatory—an average of 41 minutes—while the other three vendors averaged around 10. To help manage expectations around these lengthy holds, a Symantec dispatcher would tell us the current number of callers ahead of us and the maximum hold time so far spent by a caller. No other vendor tried to manage our expectations in this way, but it was cold comfort as we waited...and waited.

"We'll Get Back to You"

When presented with a particularly troublesome issue that couldn't be solved within an hour or two, some vendors resorted to e-mail support. They often had us download and run a diagnostic program, and return the results to them for review, one would suppose, by a higher-tier analyst.

Sometimes we waited 24 hours or more for an e-mail

In computing overall grades, "Troubleshooting Skills" was given by far the greatest weight, followed by "Reducing Security." The remaining criteria received equal, lesser consideration.

Vendor	Computer Associates www.ca.com	McAfee www.mcafee.com	Sophos www.sophos.com	Symantec www.symantec.com	Trend Micro www.trendmicro.com
Troubleshooting Skills	B- Resolved three of four scenarios within one hour.	C Sometimes efficient, sometimes ineffective for long stretches.	B+ Techs had the understanding and skills of a solid sysadmin—with one glaring exception on the custom malware issue.	C- Sometimes efficient, sometimes ineffective for long stretches. Instructions to reinstall the OS for folder permissions issue was problematic.	D Spent a long time resolving issues. Often, the first two or three "solutions" didn't work, forcing more calls.
Introduced Security Problems	A Never weakened security.	B Tweaked permissions on laptop to give full control to folders and registry keys.	D On custom malware problem, advised us that AV protection was still running when it was disabled and left malware running.	A Never weakened security.	C- Told us to add full control for everyone to server file share, and advised us to give all users local admin rights.
Additional Useful Advice	F None	F None	A Advised us to get antispyware and personal firewall after removing rootkit.	A Advised us to reinstall OS after removing rootkit.	F None
Online Knowledgebase	D Provided little help in resolving our scenarios.	D Provided little help in resolving our scenarios.	D Provided little help in resolving our scenarios.	B Contained useful advice for resolving three scenarios.	D Provided little help in resolving our scenarios.
Virus Encyclopedia	B Contained a reasonable level of detail.	B Contained a reasonable level of detail.	A Provided the most detail for the malware we researched.	B Contained a reasonable level of detail.	B Contained a reasonable level of detail.
Average Hold Time	A 4 minutes	B 12 minutes	B 10 minutes	F 41 minutes	B 10 minutes
Follow-Up E-mail Response	A All e-mail was received on time.	B- Some e-mail took two hours when one hour was promised, plus four days to analyze results from diagnostic scan.	A Never resorted to e-mail support; all issues resolved by phone.	B Some e-mail took two hours when one hour promised.	B Some e-mail took two hours when one hour promised.
Ease of Understanding (language, call audio volume)	B- Only one call was difficult to understand. Call center located in India. Sometimes hard to hear.	A- No language difficulties. On occasion, difficult to hear.	A No language or audio difficulties.	A No language or audio difficulties.	C- Consistent problems understanding language. Call center located in Philippines. Often difficult to hear.
Professionalism	A- Very polite.	A- Very polite.	A Extremely polite.	C Bordered on rude on three occasions.	A Extremely polite.
Overall Grade	B Consistently satisfactory experience.	B- Some room for improvement on troubleshooting.	B Very good support, marred by one instance of very bad advice.	B- Needs to improve troubleshooting, reduce hold time and improve professionalism.	C- Disappointing across the board.

response. For our custom malware issue, a McAfee technician asked us to run a diagnostic program and e-mail the results. McAfee's response came four days later; the malware remained active, and our system was exposed the entire time.

Because of their thorough troubleshooting process and level of experience, Sophos technicians never needed to resort to e-mail. CA e-mails all arrived within an hour, as promised. Symantec once promised they'd call us back within an hour, but didn't—we called them two hours later. We received Trend Micro's follow-up e-mails within two hours, although many of them were promised within one hour.

Can You Hear Me Now?

McAfee, Sophos and Symantec all use U.S.-based support centers. CA and Trend Micro centers are located overseas. Frankly, we didn't care where the technicians were located, as long as they were easy to understand and the phone connection was acceptable.

We had no problem hearing or understanding Sophos' and Symantec's technicians. McAfee's volume was a bit low and sometimes difficult to hear. All of CA's India-based technicians had a distinct accent and the audio volume was somewhat low. Still, we couldn't understand their advice on only one occasion.

Trend Micro was a much more significant problem, however. The accents of its Philippines-based staff were difficult to understand, a problem significantly compounded by the low audio volume. We had to ask the technicians to repeat statements several times.

Professionalism

Most of the support personnel were friendly and polite, almost to a fault. Symantec was the exception. Its technicians weren't exactly rude, but we got the distinct feeling we were being rushed or that they were annoyed during three scenarios:

- In troubleshooting the installation problem, our initial technician was clearly rushing, speaking quickly and impatiently. He even told us that he wouldn't wait for us to run a script and reboot because he had to deal with other calls.
- The technician helping with the personal firewall issue sounded annoyed that we didn't realize the firewall was the cause of the problem.
- While troubleshooting the malware issue, our support tech got a bit feisty after telling us to reinstall the tool. We asked him if we should install it from the CD. "Where else are you going to install it from?" he retorted in an irritated tone. We explained that we thought he might have us download the product, a technique used by all of the other vendors when they suspected the installation, and perhaps our CD, was corrupt.

Our experience was similar when we called Symantec for product and pricing information.

(Good) Help Wanted

Across the board, we were surprised by the difficulty some vendors had in solving several problems that we considered quite simple. Equally surprising, none of the vendors offered consistently good advice.

Overall, Sophos and CA were the top performers. We were most impressed with Sophos' quick solutions and professional troubleshooting capabilities, although its response to our malware scenario left us vulnerable and infected. CA provided prompt, reasonable responses to most of our issues, although the overseas call center did raise some communications issues.

Symantec and McAfee demonstrated moderate troubleshooting skills, but Symantec's excessive hold time was simply unacceptable. Trend Micro was clearly the weakest, with troubleshooting, language and audio problems severely limiting the effectiveness of its support.

We expected much better troubleshooting skills across the board, as well as some modicum of sys-admin skills and basic security knowledge. We didn't get that in the majority of our calls. Under-scoring this problem is that the apparent focus of AV support is to just get the tools installed and running, sometimes with little understanding if the tool is functioning properly.

AV support has a long way to go before it achieves what we consider acceptable levels. It's not hard to figure out what's needed: The prescription for success is more or less distributed among the vendors we reviewed.

Sophos technicians displayed the technical savvy and problem-solving ability we expected from all of the vendors. Realistically, scaling that type of support to larger vendors like Symantec or McAfee would be a tough task, but stepping up the caliber of their support staffs would provide a competitive advantage.

CA demonstrated a model for quick, efficient response, without frustrating delays. Symantec's calls were clear and its technicians easy to understand; there's no excuse for poor audio quality or support personnel who are hard to understand. All the vendors need to improve their online help—if customers can solve problems themselves, they'll be happy and the vendor will have fewer calls.

"Good service is good business" is an axiom most businesses learned a long time ago. For AV vendors, it seems the message hasn't quite sunk in. ■

ED SKOUDIS, CISSP (ed@intelguardians.com), is cofounder of Intelguardians, a security consulting firm, and is a member of the Information Security Testing Alliance. He's the author of *Malware: Fighting Malicious Code* (Prentice Hall, 2003).



SOPHOS