More than 55,000 new malicious software programs are registered each day by AV-Test, an independent antivirus (AV) research institute. Any one of these can have a mild to devastating impact on an organization, ranging from wasted IT staff hours to damages to consumer confidence or losses of millions of dollars in the instance of a regulatory violation.

In fact, the average organization experiences a malware attack every 73 days, Osterman Research found in a 2011 study, in which 44% of participants said that a single malware attack had cost them as much as $10,000, while another 27% reported financial impacts as high as $50,000.

Too few IT decision-makers address malware threats adequately, chalk ing up security breaches as a cost of doing business, the researchers noted, adding, "The costs [of malware] are typically higher than many organizations realize, but with the right knowledge and technologies, it is possible to reduce the impacts of malware."

Canalys Research has likewise concluded that no organization is immune to the problem. "Security risks to businesses of all sizes are prevalent," analyst Nushin Hernandez said in a December 2011 report. "The need to secure sensitive data is more critical than ever."

The experts agree that AV software is a must-have for business PC users — though it’s necessary to take care in choosing one. As the following makes clear, user experiences with AV solutions can vary widely.

Survey

To further shed light on the current state of AV protection, a four-question poll was administered randomly over a three-week period between February and March 2012 to IT leaders, IT managers, software architects, and other enterprise technology decision-makers and influencers arriving at Slashdot. The following is a breakdown of their responses.

Question 1: Does your AV solution stop endpoint infections, or are you constantly reimagining and repairing machines due to unknown malware infections?

While keeping malware attacks from tying up IT staff hours is a main goal of AV software, for too many users this still isn’t the case.

![Survey Results Chart](chart)
Among 500 respondents, 34% reported that their AV solution stopped malware all of the time, and roughly another third, 33 percent, said theirs did so "a good majority of the time." That leaves another third of the pie that, despite their financial investments, are still more open to attacks than not.

Sixteen percent of respondents said their solutions stop malware "only part of the time," while another 17 percent said it rarely stops it.

While the good-news-to-bad-news ratio would seem to be 2 to 1, it's really quite the opposite. Were these same executives to invest in home security systems that wound up preventing burglars from entering their homes and threatening their families "a good majority of the time," they likely wouldn't think the systems were effective. Solutions that keep your business safe most of the time are likewise not to be considered a success.

**Question 2: Does your AV cause issues such as long scan times, slowed performance, and worker interruption that results in more Help Desk calls?**

In this instance, the most extreme options received the most votes, though still-generous numbers went to the options in-between, underscoring the inconsistency of experiences that AV solutions on the market can deliver.

Here again, roughly a third of respondents, 32%, are experiencing ideal results, with no issues of slow-moving machines or problems resulting in calls to the help desk, while just over two-thirds are dealing with various shades of the problem.

For 21% of respondents, slow solutions, whether just wasting workers' time or devolving to the point of involving IT staff, are causing issues "only occasionally." For 18% it happens "a lot," and for 28 percent — nearly 1 in 3 respondents — it happens "all the time."

Ideal solutions should of course block malware without affecting a machine's performance. The latter can particularly be an issue with older PCs — heavy AV solutions can intrude on processing power to a frustrating degree, so be sure to check system requirements before you buy or install a solution. Consider, when shopping, the size of the solution, as some can be more agile — and so less intrusive — than others.
Question 3: What have been the major management, control, and operational issues with your AV endpoint protection over the past 12 months? (Check all that apply.)

This question allowed a total of 502 respondents to choose all of the answers that applied to them, resulting in a total of 754 votes and a very mixed assortment of pie slices — though no slivers. Each listed problem was experienced by, at the minimum, 89 of the 502 respondents.

Particularly noteworthy here is that the problem that received the second-highest number of votes — 155 in all, for a 21% slice of pie — was "Still getting endpoint infections and breaches." This means that not only are AV solutions not working for approximately 1 in 5 users, but their workers, and bottom lines, are additionally suffering from side effects introduced by the software.

"Poor endpoint performance and user productivity," selected by 25% of respondents, was voted the number-one problem — again suggesting that slowed-down machines are more than simply an inconvenience.

The third-largest problem, chosen by 16% of all respondents, was that the "Solution is complex and difficult to manage," followed by "Poor vendor support," with 15% of the vote. "Definition updates have caused issues" was ticked by 12 percent of respondents, while another 12 percent selected "Poor remediation controls."

One consideration for how attacks may still be getting through is mobile devices that interact with PCs or the network. In 2011, malware began to target mobile platforms to a more significant degree, and the Android operating system — now the most-used mobile OS in the world — has particularly become a target.

With bring-your-own-device (BYOD) policies growing in popularity, and so Android-running smartphones and other consumer devices mingling with enterprise assets in increasing numbers, IT decision-makers will want to look for solutions that include a smartphone component. Specifically, they'll need to make sure that all mobile devices can browse the Internet securely, and that viruses or spam aren't being introduced through applications. Popular applications for social networking are common targets.
Question 4: What capabilities or features would you like to see in your 'perfect' AV solution? (Check all that apply.)

Again, respondents were able to choose more than one answer, and among 503 respondents a total of 1,264 votes were cast among the seven options. Again, too, speed was pointed to as a primary pain point.

Topping the list of desired capabilities or features, at 23%, was "Fast scan times that don't slow endpoints or users down."

Behind speed, another 16% percent of respondents said they'd like "No conflicts with existing, or other security software," while 15% said "Full visibility of applications and processes on each endpoint" and another 15% wished for "Built-in remediation tools."

Fifth on respondents' wish lists, selected by 14% of all respondents, was "Pro-active, responsive vendor support," followed by "No need for re-imaging endpoints," with just under 10% of votes.

Another 8 percent of respondents wished there were "No definition updates needed."

Many of these wished-for capabilities are actually already available; it's just a matter of finding the right solution. Regarding the issue of speed, some solutions can be a fraction of the file size of competing options. Consider how much memory is consumed during scans, and initial scan times, which can range from 20 seconds close to two minutes.

The second-most-desired feature — a lack of conflict with other security solutions — is also nothing to keep dreaming for. There are solutions designed to work around pre-existing security solutions or even to work with them, as a second layer of defense.

Likewise, some solutions already include a rollback feature that can restore a system to its previous condition after an attack, eliminating the need for reimaging — a task that can use up to 17 hours of an IT manager's time each month, keeping him or her from more pro-active, pro-business activities.
Management consoles can also make a tremendous difference, with some offering visibility into settings and policies at company-wide, group, or individual levels, as well as tools for remediating infected machines and remotely initiating scans — addressing two more top requests for a "perfect" solution.

Conclusion

AV solutions perform a critical function and remain essential to enterprise security, but as the survey makes clear, not all solutions are created equal. For many, there's much room for improvement, partly suggesting just how challenging the task at hand is.

With more respondents answering that their AV solution stops malware all the time than any other option, and more stating that their systems run quickly and quietly in background, rather than the alternative, the encouraging take-away from these responses is that there are indeed effective solutions on the market. IT manager simply need to be smart about their choices.

In sum, total malware accounts are skyrocketing toward 70 million this year — up from 46 million-plus in 2010 and just 17 million in 2008 — and are growing more sophisticated, say the experts, encouraged by a sweetening honeypot of more users with more connections to online assets. Downplaying the menace of online attacks, whether with crossed fingers or ineffective solutions, today is a tremendous hazard, and one that no business, regardless of size, can afford.

Your Next Step

To learn about the Webroot SecureAnywhere endpoint protection solution, click here.

For a 30-day free trial of Webroot SecureAnywhere, click here.

ii http://www.nwtechusa.com/pdf/m86-swg-wp.pdf