

Comparing E-mail Server Virus Protection Solutions, Part Two

Robert Grupe 2001-10-30

Comparing E-mail Server Virus Protection Solutions, Part Two

by *Robert Grupe*, Product Management, *McAfeeB2B Groupware*

last updated October 30, 2001

This is the second of a two-article series that is intended to help readers assess and evaluate anti-virus (AV) solutions. The [first article](#) looked at how users should assess their AV needs, as well as recommending a few features to look for in AV software. In this installment, we will take a look at AV product reviews and explore how users can evaluate AV products for themselves.

A Buyer's Guide to AV Reviews

Most of us like to own products that are publicly recognised as being 'the best', so we look for product awards and reviews to define which products warrant this valued designation. But lest you be lured into accepting these platitudes at face value and end up with a product that is ill-suited for your organisation, you really should take a bit more time to ask what is really behind the award. What is the purpose of the award? Who makes the selection and what are the criteria? Does the award reflect qualities that will contribute to your organisation's security protection?

Readers should approach product reviews with a critical eye. For instance, they should ask themselves whether the reviewers are recognised experts in the virus detection field and whether they are using industry-developed methods. Popular computing journals sometimes conduct product 'shoot-outs' that involve little more than installing the product and looking at the graphical interface. If you were looking for a new off-road vehicle, you wouldn't be satisfied with a review that simply looks at vehicles' appearances and options packages, would you? No, you would want to know how well it handled in deep mud, water, and on steep inclines. So why wouldn't you want the same kind of critical review for a product that you will rely upon to protect your core business communication systems?

Due to the specialised knowledge and large number of live computer viruses necessary to conduct a thorough evaluation, most AV product reviews are done quite poorly. The best thing that you can do is to educate yourself as much as possible, and then evaluate the products based on the specific requirements of your own organisation. The following is a list of things

that readers should be wary of as they read AV product evaluations.

1. The evaluation overemphasizes the user interface.

While usability is definitely an important aspect of your own selection criteria, when reading AV reviews, you need to keep in mind that user interface is a matter of personal preference. Some people like a command line, others a full screen, and while some people like lots of options and selection buttons, others like minimalist interfaces with few options.

2. Too few viruses are used to test detection.

Testing detection with too few viruses diminishes the effectiveness of the test. It makes it hard to differentiate between products because ones with poor detection capabilities will probably not vary greatly from better products. Furthermore, tests that use only a few specimens of each type of virus will not provide any meaningful indication as to a product's overall virus detection capabilities. The sample of virus types needs to be broad enough to ensure that there is not only protection from common mass-mailer and macro-scripts viruses, but also other types such as polymorphic, Trojans, and others.

3. Heuristic scanning on clean machines is not evaluated.

Heuristic analysis involves scanning a file for suspicious code to determine if it is 'virus-like' that is, if the code is suspicious. However, it's very difficult to define 'suspicious'. Code that might be perfectly legitimate (i.e. FORMAT.COM) could be suspicious if it is included as part of an infected file. Heuristic scanning is more susceptible to false alarms than other scanning methods, and so it is important to evaluate false alarm notifications since false alarms are often more time-consuming than real infections.

4. Only in-the-wild detection is evaluated.

There are two general terms used to classify viruses' in the wild (those which have been reported in the field) and 'zoo' viruses (those which haven't been seen outside research labs or ones that have been seen in the past but are not currently actively infecting significant numbers of users.) It is clearly very important for a scanner to be able to find viruses known to be infecting real users machines. Nevertheless, a scanner should also be able to find 'zoo' viruses that nobody knows about until one of these viruses is seen in the field. Unfortunately, some

vendors optimize their products to only provide protection against current in-the-wild viruses in order to improve their scanning speeds.

5. Virus repair capabilities are not evaluated.

Just as products may differ in the quality of virus detection or the number of false warnings they issue, they may also differ in their ability to restore infected data. Some reviewers feel that because not all products repair well, then this functionality shouldn't be evaluated. Often times, products with poor repair capabilities will argue that repairs are insecure and so everyone should just delete-and-replace.

6. Evaluations overemphasize scanning speeds.

Scanning speed is a valid consideration in the selection of AV solutions, but users should realize that products with poor detection will be quicker because they do not find as many viruses to report. Scanning small e-mail stores on high performance servers can also disguise significant variation between products, and so reliable test should be done using a disk full of viruses.

7. Evaluation uses different settings for different products.

In order to simplify their evaluations, some reviewers only test products based on their default installation settings. This can then lead to misleading results since vendors can have different philosophies as to what setting should customers specify in the configuration phase of installing their products. Within tests, it is preferred that the same settings are maintained when comparing speed and detection.

8. Evaluation does not test both 'on-access' and 'on-demand' scanning.

"On-access" scanning is scanning that is initiated each time a user or system accesses contents by reading or writing data. "On-demand" scanning is instigated either by a scheduled process or else manually by an administrator. Most users are protected by on-access scanning because it occurs each time a new e-mail arrives and each time the user accesses a message or attachment. On-demand scanning typically occurs after-hours or on weekends. The virus detection capability of a product's on-access scanning may be markedly different to its on-demand scanning, so both should be evaluated.

9. Results are reported to two decimal places.

While some test results will be reported to two decimal places, scanners that detect 99.43% are just as good as another that detects 99.34%. If scanners are this close in detection, it is likely that one will be able to detect the viruses the other missed by the time its next virus definition file is released.

Product evaluations and reviews can be a good starting point to find information about products that might be suitable for your organization, but readers should realize that not all reviews are as conclusive as they might appear. The best course is to use these reviews and awards as a starting point of discussion with vendors representatives, but then to conduct your own evaluation to select your own 'Editor's Choice'.

User Evaluation

Installation

Surprisingly enough, many people evaluate software by simply grabbing a distribution CD and popping it into a computer to see what happens. If after a short while they receive a 'finished' message, they figure everything has gone well. Of course that is ideal, but it doesn't always work like that in the real world. Usually security account permissions need to be considered, and other factors, such as operating system service patch level, groupware modifications, and add-on software, can all effect the successful installation and operation of the software.

Before beginning an installation, make sure that you have the latest version, scanning engine, and virus definition files. Always consult the 'readme' files and installation manuals. If you have any operating system or groupware versions not specifically mentioned in the documentation, ask the vendor's support services for advice. This is especially important when non-publicly released software patches have been added to your servers. Check your system security settings to ensure that the software will have the required and desired permissions.

Usability

Depending upon the make-up of your IT organisation, different people may be involved in the enterprise rollout, installation, configuration, and daily administration of your AV solution. You will need to determine what functionality is needed based on organisational procedures, policies, and personal preferences. But bear in mind that vendors sometimes have different approaches to the same issue - so try to be open and flexible.

The following is a short list of the areas that you might want to investigate:

- Installations: on a local server or remotely through your network; updates and reinstalls.
- Actions: blocking, quarantining, deleting, and cleaning; submitting suspected viruses to the vendor for analysis.
- Reporting: notification to administrators and users; summary reports.
- Scanning: file types and recursively compressed files.

Server loading

The additional tasks of scanning message traffic on your messaging server will increase the server's resource utilization. It is important to understand how that will affect your operations. No organization is exactly the same and there are no set figures that can predict how your AV scanning configuration will impact your servers. Factors that will affect the results of your test are things such as number of mailboxes, type of message traffic (message formats, messages per hour, message sizes, attachment sizes, number of attachments, types of attachments), number of infected items; detection, cleaning, and quarantining rules; reporting and alerting settings; type and number of processors; RAID configuration and performance; etc. The most reliable indication is to perform your own tests with a typical profile of your users and using your anticipated AV settings.

For Exchange servers, Microsoft has provided some MAPI Messaging Benchmark (MMB) profiles and a loading simulation tool (LoadSim) that can be used to evaluate server performance. After modifying one of the MMBs to more closely model your own users and messaging patterns, you can then use LoadSim to gather a baseline of performance data to be used in comparing AV solutions. Testing with real viruses is extremely risky and is not recommended without specialized procedures and expertise. Aside from the challenges of obtaining a large and meaningful enough collection of viruses, there is a very real danger of accidentally infecting the rest of your network. To address the need to be able to verify detection of viruses, the European Institute for Computer Anti-Virus Research (EICAR) has developed a benign file that can be use for simple virus verification testing. All AV products should be able to properly detect the EICAR virus, and so you can safely use it to verify AV software settings and reporting.

Speed testing

Speed of scanning should be tested on a clean, uninfected machine. For the most part, anti-virus software operates in a clean environment so it makes sense to test it under the conditions that prevail most of the time. Some scanners slow down to ensure accurate identification, but this is not seen during normal, everyday use of the product. Moreover, it doesn't really matter how long a scanner takes to scan an infected machine and remove the virus (or viruses) as this will not occur frequently. When it does, thoroughness not speed is the critical factor.

The following are some guidelines for valid speed testing:

- Ensure that the server is disconnected from your production network so other network loading or applications do not affect your results.
- Ensure that there are no other anti-virus scanners loaded during testing, since this could affect performance. For instance, a groupware server may have a file system scanner installed in addition the groupware scanner.
- Make sure the hard disk of the test machine is not infected and has a large data store. The wider the test-bed, the easier it will be to differentiate products by speed.
- Do not accept the scan time reported by the product at face value, as the product may not be measuring the same thing as you are.
- Consider the scan settings to use with each product. The obvious line to take is to use the scanner's 'default settings'. However, scanners are configured differently - one product's default may be another's option. Scanner A may enable compressed file scanning by default, but Scanner B may not. It would be unwise to reach the conclusion that Scanner B does not scan compressed files.
- After each test, do a complete rebuild and complete installation of each subsequent product. This avoids the risk of one scanner's files and reports interfering with subsequent scanner installations.

Final Considerations

Once your analysis of various vendors' products is completed, you will have a fairly good idea as to which product best suits the needs of your organisation. During your evaluations, the vendors should be able to provide you with assistance in optimally configuring their products and in analysing your results data to ensure that everything was set correctly.

When it comes time to compare costs, make sure that you include all the options that you will need. Content filtering and centralised administration are sometimes included as part of one

vendor's standard product, but for others they are additional costs. Another consideration is the cost basis whether it is number of nodes, seats, simultaneous users, or employees. Clarify what product updates are covered in the pricing (is it just for incremental releases or does it include major releases), and the term that you are covered for product updates, virus definition file updates, and support assistance. Support services can vary greatly, and so ensure that you understand the service level agreement included in the quotation.

Conclusion

Selecting virus protection for your organization's groupware is not simply a matter of reading a couple of magazine articles and asking some friends what they use. Each organization has its own unique requirements, and the best way to ensure you make the right decision is to do your own evaluation. AV solutions aren't quite install and forget yet; but by selecting a solution with good detection, recovery, and reporting, you can sleep easier at night knowing that you have done the best you can to avoid unnecessary operating disruptions.

Relevant Links

[Comparing E-mail Server Virus Protection Solutions, Part One](#)

Robert Grupe

[European Institute for Computer Anti-Virus Research \(EICAR\)](#)

[Wild List International](#)

[Yahoo listing of virus protection vendors](#)

[Microsoft Exchange 5.5 - Performance and Scalability](#)

[Microsoft Exchange 2000 Planning](#)

[Comparing MMB2 and MMB Workloads](#)

[Privacy Statement](#)

Copyright 2006, SecurityFocus