

Antivirus Solution Evaluation

Rutgers University

March 2006

Overview

For the past several years, Rutgers University had contracted with McAfee, Inc. to provide the campus with an antivirus solution for desktops, servers, and e-mail. Based on feedback from users, we became increasingly aware of the fact that the product's effectiveness had begun to diminish rapidly. We, therefore, began to evaluate antivirus solutions from other major vendors in the enterprise market. In doing so, we believe that we found the best solution that can truly fit the needs of Rutgers University. The solution is from Trend Micro, Inc.

Evaluation Requirements

Over a period of several months, we researched and evaluated enterprise-class solutions from the major antivirus vendors: McAfee, Trend Micro, and Symantec as well as the smaller, well-known vendors F-Secure and Sophos. In researching and evaluating solutions, we looked to see if the software met any or all of the following key requirements:

- Ability to produce new virus signatures quickly
- Dispersed/distributed manageability
- Unified client features
- Client transparency
- Support for all Windows Oses and Linux
- Web-based management console
- Company strength and overall AV strategy
- Ability to integrate with other solutions such as Cisco NAC
- Proactive notification on potential outbreaks and/or problems
- Ability to clean up after viruses and/or spyware have infected a system
- Ability to quickly prevent outbreaks while new virus signatures are not yet available

Ability to Produce New Virus Signatures Quickly

The period between when a virus is discovered "in the wild" and when a signature or pattern file is available for clients is extremely critical in our environment. The longer it takes us to get and distribute new pattern files, the more likely we are to have clients getting infected.

Dispersed/Distributed Manageability

The ability to provide Unit Computing Specialists and/or departmental administrators access to manage their own clients was also an important feature to us. With the diversity in departmental IT policies, it is necessary to be able to give people the ability to set policies for their department differently than we may define at the global level. Furthermore, departments need the ability to provide customized reports on systems under their control to their management.

Unified Client Features

The ability for client software to provide antivirus, anti-spyware, SPAM filtering, and firewall support in a single package was very high on the list of requirements. Packaging all of these features together under a single client not only reduces desktop and system tray clutter but typically takes up fewer system resources in terms of CPU and memory.

Client Transparency

Another aspect that we looked at was how the client itself performed while a system was under heavy usage. Real-time scanning and monitoring needed to be as unobtrusive as possible. This also meant that any error messages or warnings that popped up as viruses were found needed to be easy to understand and answer. It was very important that the client be as transparent and easy to use as possible to our users.

Support for All Windows Oses and Linux

There is a great deal of variety among systems within the University. Therefore, it was important that any solution support the full range of Windows operating systems from Windows XP and 2003 all the way back to Windows 98 and Windows 95. In addition, adding support for protecting the growing number of Linux desktops and servers was also desired.

Web-Based Management Console

Enterprise management tools needed to be web-based for ubiquitous access. Not all system administrators run Windows on their desktop, so use of a Windows client-based management system is not desired in our environment. Furthermore, the console needed to be able to provide granular control over systems being managed.

Company Strength / Overall AV Strategy

Another factor in selecting an antivirus solution was how strong the company itself was. Fiscally weak or unsound companies tend to get bought out by larger corporations who may then change the levels of service a product provides even during a contract. Companies also needed to have a strong strategy and focus on antivirus and system security as part of our evaluation.

Ability to Integrate with Other Solutions Such As Cisco NAC

Network security is another area of focus when selecting an antivirus solution. The ability of a solution to integrate with third party solutions such as Cisco's Network Admission Control is an important feature. Because the vast majority of the network at Rutgers is controlled by Cisco equipment, it is vital that any possible solution be able to integrate with the existing network infrastructure.

Proactive Notification of Potential Outbreaks and/or Problems

Limited human resources prevent us from watching any system 24x7x365. Therefore, it is critical that any solution be able to watch systems and automatically notify system administrators of possible outbreaks or issues on the network. The ability to email or page an administrator or administrators when there appears to be an anomaly on the network was determined to be vital in our list of requirements.

Ability to Clean Up after Viruses and/or Spyware

Obviously another factor that must be considered when evaluating antivirus solutions is how well the product is able to clean a system after an infection. If a solution simply detects a virus but doesn't clean it up well, it doesn't really save an administrator any time or effort. The solution should be able to successfully clean a majority of infections without having to rebuild the system.

Ability to Prevent Outbreaks Until New Virus Signatures Are Available

Many vendors have begun to discuss "zero-day" protection, but few actually do much about it. The ability to prevent an outbreak from occurring when there is no virus signature or pattern file available is extremely important. Hundreds of systems could potentially become infected in the time it takes a virus to be detected "in the wild" to the time a new pattern is available. A feature we considered key was the ability for software to keep systems protected even though they were unable to detect the virus.

Evaluation Results

We were able to fully evaluate McAfee and Trend Micro on each of these criteria. McAfee had been in place for the past few years, so our experience with that proved to be very useful in evaluating other solutions.

Symantec was only evaluated on a few of these criteria because of our past experience with the company and its software. Symantec's antivirus solution is extremely invasive in the fact that it installs registry keys and files all over a system's drive. On many occasions, the software fails to uninstall itself properly leaving a mass of problems behind. Its separate LiveUpdate process complicates matters concerning software and virus pattern updates and requires its own install/uninstall process. Symantec's track record for success has declined significantly over the last several years due to some major acquisitions. We felt that the company has diversified itself so greatly in what it does that it no longer provides the focus on its antivirus solutions that it once did. As a result, their products have suffered greatly over the past several years. Furthermore, Symantec no longer supports downlevel Windows 95/98/ME clients, which still make up a significant amount of systems both at the University and at home.

Sophos and F-Secure were not evaluated on many of these criteria either because they were ruled out early in our evaluation process for several reasons. First and foremost is the size of the company. Although both companies are important competitors to McAfee, Symantec, and Trend, we felt that neither company was in a position to provide us with the trust and support needed when committing to a multi-year contract. There is a large concern that the company may be purchased by a larger corporation, such as a Symantec or Microsoft, at some point while we are under contract. This typically causes products to suffer during the acquisition phase and often even afterward. Furthermore, smaller companies have fewer resources. We were concerned that fewer people were dedicated to providing technical support as well as staff dedicated to continued product development. Both companies might be viable contenders in a smaller business world and even on a smaller scale at the university level. However, we didn't feel that either vendor could provide the confidence and support levels we need at Rutgers.

Ability to Produce New Virus Signatures Quickly

From our experience, McAfee had been lacking on their ability to quickly protect against some of the most prevalent viruses. There were several times during the course of our contract where viruses were infecting our systems because their pattern files did not protect against high-threat viruses. Furthermore, there were a few instances of McAfee producing DAT files that caused false positives to be reported. Trend Micro typically produces a pattern file within a matter of 30 to 60 minutes once a virus has been detected in the wild. Symantec, Sophos, and F-Secure vary on their turnaround time, but were all generally more than an hour.

Dispersed/Distributed Manageability

McAfee's ePolicy Orchestrator server is a fairly resource intensive application. Each server requires its own database that can grow to many gigabytes in size, and there is no easy way to consolidate reports from multiple servers in order to provide an overall picture of antivirus at the University. Furthermore, McAfee's solution was not very simple for administrators at remote locations to set up and configure. There was a steep learning curve when it came to managing an ePO server. Trend Micro's solution is simple. Sites can set up their own servers simply by using a web server. The setup and configuration is very straightforward, and each site can report to a master server at the global level making it easy to run enterprise-wide reports. Symantec, Sophos, and F-Secure were not evaluated on this feature.

Unified Client Features

Trend Micro's product has integrated antivirus, anti-spyware, anti-spam, and firewall support. A single agent installed on the desktop manages antivirus, anti-spyware, and a client firewall. This is significant because not only does it reduce clutter in the system tray, but it takes up far fewer system resources while it is running. By having everything integrated in one package, there are fewer processes to debug and cause issues on a system, which provides a much more cost-

effective solution. McAfee, on the other hand, required you to run a separate antivirus, desktop firewall, and management agent all at once. Some clients are more memory and CPU intensive than others, but the McAfee solution takes significantly more resources to run than Trend Micro. Symantec has a fairly integrated solution as well, however, its client uses more resources than the Trend solution. Sophos, and F-Secure were not evaluated.

Client Transparency

Hand-in-hand with unified client features is client transparency. As previously stated, Trend's solution is much more compact and robust than what McAfee was providing. Trend requires less memory while running and virtually no CPU cycles. McAfee, on the other hand, could cause a system to grind to a halt when it performed a full system scan or even while scanning a large attachment in e-mail. This had a sizeable impact on users who worked with large files on an almost daily basis. Many of them had to turn off real-time antivirus scanning, which defeated the purpose of having an antivirus solution installed in the first place. Trend has proven its ability to scan large files on even our oldest systems with virtually no interruption to users. Moreover, Trend has a much simpler interface than McAfee. Their interface is very straightforward and easy enough for most users to figure it out without any help from documentation. McAfee had a list of complex tasks and schedules for users to try and figure out, which often caused them to configure their systems incorrectly, leaving them vulnerable to attack. Symantec has an equally if not more complex interface to its software as well. F-Secure and Sophos were not evaluated on this requirement.

Support for All Windows Oses and Linux

McAfee and Symantec instantly failed this requirement because they have already dropped support for Windows 95, 98, and ME-based systems. Many of our clients were left with no supported protection after last June when McAfee discontinued their Win9x line of products. Although not as critical as Windows 98/ME support, F-Secure no longer supports Windows 95 systems either. Only Trend Micro and Sophos currently met the needs in terms of support for the various operating systems that we feel are important to protect at Rutgers. Many of our students continue to run Windows 98 and ME on their home computers, so it was important for us to be able to provide them with some method of protection from viruses that we can manage for them.

Trend's solution also provides support for Linux and Netware systems.

Web-Based Management Console

McAfee's management console was a 32-bit Windows client application. This severely limited administrators in what choices they had for supporting their clients. While most system administrators do run Windows-based operating systems, some use Linux or even Mac OS as their operating system of choice. Furthermore, access to the management console was not nearly as ubiquitous as it could have been with a web console. All of Trend's management and reporting interfaces are available through a standard web browser. Any administrator can access and manage any client under their control from anywhere so long as they have access to the Internet. This eliminates the need for administrators having to download and install a client on each PC they work on. What is even more important is that the web-based Trend console is far easier to understand and navigate as well as faster than the McAfee management console, which often broke and needed to be reinstalled. Symantec, Sophos, and F-Secure were not evaluated on this requirement.

Company Strength / Overall AV Strategy

While Symantec is a strong company overall, their focus has diversified so much over the years that we felt they were no longer able to provide an effective antivirus solution. Several of their key acquisitions in the past few years have not been antivirus-related, so we did not feel they were truly focused on providing world class enterprise support. McAfee has been shifting most of their focus from software to hardware appliances over the past year or so. This has caused their software to lag behind their competitors' solutions greatly. We have seen the effectiveness of their product degrade tremendously over the past 3 years mainly because they have lost their

focus on providing a good antivirus software solution. While both Sophos and F-Secure are well-known, they are considerably much weaker vendors in the antivirus arena. One very important aspect to us was that the company we chose would be unlikely to be purchased by larger vendors such as the Symantecs and Microsofts of the world. Because Sophos and F-Secure are comparatively small, there does exist a possibility that either or both may be purchased by a larger corporation. As has been our experience, this is typically disastrous as the products tend to suffer overall. Another issue with smaller companies is support. They typically have much smaller support teams and fewer resources dedicated to technical support. Some even outsource their support infrastructure. This can cause major problems when trying to solve an issue in a timely fashion. We not only needed a good software solution but also strong technical and sales support.

Trend Micro is not only a fiscally sound company, grossing over \$600 million in revenue last year alone, but they also are dedicated to their focus on a total system security solution. Rather than buying smaller companies, Trend has chosen to partner with them so they can focus on providing the best solutions available and let their partners continue doing what they do best. Trend has an excellent support infrastructure, most of which is located right here in New Jersey. This gives us excellent access to both their sales and technical support teams whenever we need them.

Ability to Integrate with Other Solutions Such As Cisco NAC

All of the solutions we evaluated were able to integrate with Cisco's NAC.

Proactive Notification of Potential Outbreaks and/or Problems

The only solution we looked at that provided the ability to automatically monitor system activity and notify administrators of potential problems was Trend Micro. During our testing, Trend's OfficeScan server was able to detect a high number of viruses on a particular machine and immediately notified us of a potential problem. This is an extremely helpful tool. It allows us to find a potential problem and stop it before the infection spreads throughout the University. McAfee's ePO server has no feature comparable to this. One would have to manually run reports to find similar information. None of the other vendors had features that were comparable to Trend's robust reporting in this situation.

Ability to Clean Up after Viruses and/or Spyware

McAfee did a very mediocre job in cleaning up many of the viruses it encounters. Oftentimes, the software could not even clean a virus from the system completely. There have been many occasions, however, where a system was infected with multiple viruses, and McAfee was unable to detect all of the viruses correctly. McAfee also has had a very poor track record when it comes to cleaning up spyware. Most of our users have had to resort to 3rd party products such as Ad Aware or Spybot Search and Destroy to remove spyware from their system. Trend Micro has been very successful at not only detecting viruses and spyware but also cleaning up the infection. Many of our tests and other independent tests show that Trend has become the foremost effective product in detecting and cleaning spyware. This is a significant characteristic of Trend's product as spyware and adware has become as much if not more of a problem than viruses at the University. Symantec, Sophos, and F-Secure have average track records for detecting and cleaning viruses and spyware but they were not individually compared.

Ability to Prevent Outbreaks Until New Virus Signatures Are Available

The only vendor we have found that has a robust method to prevent viruses from spreading while there are no pattern files available is Trend Micro. Their Outbreak Prevention Services allow us to quickly deploy policies to servers and workstations that help us to stop viruses before they begin. One policy allows email servers to automatically quarantine specific attachments. Another policy may prevent new shares from being created on a workstation. Trend analyzes each threat individually and provides their clients with an outbreak prevention pattern within 10 minutes of a known exploit. Coupled with the fact that these patterns can be deployed automatically to clients, this greatly reduces our exposure to infection from rapidly spreading viruses. McAfee, Symantec, Sophos, and F-Secure cannot provide such robust capability in their products that we have found.

Conclusions

Over the past 3 years we have had a chance to fully evaluate McAfee's antivirus solution. While the solution had been working, it was only marginal at best. In the past year or so, performance degraded and the software began to lag behind many of its competitors. In evaluating solutions from other vendors, Trend Micro stood out in all of our testing.

Symantec, Sophos, and F-Secure were evaluated briefly, but it was quickly determined that their solutions could not meet the demanding needs of Rutgers. Symantec has a poor performance record and has shown their lack of focus on antivirus by purchasing several non-AV companies such as Veritas. Furthermore, their solution is extremely invasive in systems and often does not uninstall itself properly. Sophos and F-Secure stand the possibility of being purchased by larger companies and have more limited resources than many of the larger vendors do. There are fewer staff dedicated to research and development as well as technical and sales support.

Trend Micro has consistently been an industry leader in the realm of antivirus and system security. Some of Trend's largest clients are other universities such as Penn State and companies such as AOL, GM, Nissan, John Deere, and AT&T. They have an impeccable record in providing software that's robust and reliable. Their software would provide Rutgers with a complete system security solution. Their cross-platform solution includes antivirus, anti-spyware, anti-spam, and firewall packages. They have a highly configurable and distributed management infrastructure for handling even the most complex environments. The software's automation capabilities not only reduce the amount of human resources needing to be dedicated for support but provide added protection from viruses and threats.

From our findings and feedback from our users, it was our conclusion that Trend Micro was the only antivirus solution that could meet the ever changing and demanding needs of the Rutgers University environment.