Global Information Assurance Certification Paper

Prepared for the SANS Security Essentials (GSEC) Practical Assignment
Version 1.4b [Option 2]

TITLE: CASE STUDY: THE ANTI-VIRUS JOURNEY…FINDING THE BEST PRODUCT FOR OUR ENVIRONMENT

ISSUE STATE: 2.0

ISSUE DATE: 2nd February 2004

AUTHOR: Rosalind Nash

LIST OF CONTENTS

ABSTRACT

The International Computer Security Associations (ICSA) reports that 500 new viruses are released monthly (1). The need for consistent antivirus protection within any organization is crucial. Yet, viruses, Trojans, worms and malware continue to cost many companies downtime and money. An organization change along with the latest virus scares was the catalyst for reevaluating our company's Antivirus (AV) software solution. This paper provides a description of the journey taken by our company to assess the best AV protection for our environment. Our ultimate goal was to commit to a single vendor AV package. The content of this paper addresses questions such as; should we try to prevent the threat at the door or react to the intruder after it's in, and what specific features of AV are vital to protect the organization?

1. INTRODUCTION

The size and sophistication of the Sapphire/Slammer worm that hit early in 2003 could scan 30,000 machines per second (2). There are still some questions as to whether the Blaster worm was responsible for one of largest power grid failure in years (3). Viruses have caused problems for 51% of all corporations (4). These statistics are staggering but so is the cost to combat these problems. In 2000, the ICSA reported the cost associated with fighting viruses for a typical company to be between $100,000 and $1 million annually (5). A recent survey revealed it cost $52,000 per incident to address a virus attack (6) and this could quickly exceed $1 million annually.

As the figures escalate, businesses have to decide the most effective way to combat the hundreds of harmful viruses and attacks that will continue to negatively impact them. Although, no AV package can guarantee absolute protection against viruses, worms, Trojan horses or malware, the lack of consistent antiviral protection is asking for trouble. Without a solidly configured AV package, organizations are confronted with the realities that they could loss data, allow backdoor access into their networks or simply be left with the feeling of being invaded.

To address viruses, worms, Trojans and malware, our organization decided to take a proactive approach to AV—commitment to a single antiviral package to be used corporate-wide.

1.1 THE COMPANY SNAPSHOT BEFORE THE JOURNEY

The managerial structure of the company had recently changed. The transformation was migrating from many individialized IT groups to one network with one IT department. In addition, the change required that all functions of the IT department be critiqued. As part of our one network model and the barrage of new viruses released monthly, the antivirus solution throughout the organization was at the top of the list of things to be assessed.

The distributed network administration resulted in our organization having licenses for at least three separate AV software packages (Panda Enterprise Suite, McAfee Active Defense and Symantec Antivirus Enterprise). Even though the diversified approach is not necessarily bad, our organization encountered the dilemma of several workstations and servers being left out of the AV protection loop. The problem was in our organization structure as well as the

Windows domain structure. Although this set-up was dangerous, our company managed to escape any costly consequences.

1.1.1 Root domain

The Root domain was the primary organizational distinction of the company, as well as the primary domain in the forest. There were seven Wintel networked domains—which spread across nine physical locations. This domain had approximately 400 computer accounts and 36 servers. The main email server was also located in this domain. In general, most of the domains were responsible for their own AV protection. Although, the Root domain was responsible for a couple of the smaller domains' AV and other machines, which were physically located in buildings where other Wintel networked domains resided. The Root domain used two different software packages—Symantec Antivirus Enterprise and Panda Enterprise Suite. Symantec was the predominately used package; it was deployed on all of the servers and most of the workstations. However, Panda was used on the majority of the workstations in the Root domain's IT department.

When I took over the AV administration a year ago, all 36 servers under the Root domain were being used as Symantec parent AV servers; although three-fourths of the AV servers did not have any client under them. I spend many hours reconfiguring the AV deployment and reducing the AV parent servers to ten. There were six parent servers in the Administration building—which is the main physical location of the Root domain. The building has five floors and each floor pointed to a parent server and the other Symantec parent server was the quarantine server, where all infected files for the Root domain were sent. The other four AV parent servers were physically located in different outlining buildings, where there were client workstations, in close proximity. This set-up was done to reduce network traffic.

1.1.2 Division B domain

The Division B spanned across three physical locations and was the second largest Wintel networked domain within the organization; it contained approximately 75 workstations and four servers. All servers and most workstations in this domain were protected by McAfee Active Virus Defense package.

1.1.3 Other domains

Little was know about the AV products used in the other Wintel networked domains. Although, the Root domain also retained the liability of protecting a few of the workstations and three servers

physically located within some of the buildings of these networked domains.

1.2 DURING THE ANTIVIRUS EVALUATION PROCESS

To accomplish the task of determining the AV software package solution for the organization, an AV committee was formed. The first stage of the project was to gather information about several AV products.

The committee flagged several issues that had to be addressed in order to effectively evaluate the products:

(a) Effective protection in light of our current network design

(b) Methods of virus attack

(c) Mandatory verses wanted features and

(d) Centralized management.

The committee realized that the structural design of the network is an important aspect of security and rectifying the vulnerabilities of our current network design would take time. Therefore it was imperative that the AV strategy incorporate one of the key elements addressed in the SANS Security Essential course, “defense-in-depth”. Consequently, the method of attack for the selected AV needed to be multidimensional. The committee believed that the ultimate strategy would stop viruses before they ever entered the network. Since 90% of all viruses are obtained through email (4), the email perimeter was a high priority. Though the boundary line of attack is the perfect scheme, the group felt the selected product should offer a tactical approach to protect desktops and servers after viruses have entered the environment.

The products being reviewed were the AV software packages owned by our company and Trend Micro Enterprise Protection Strategy—which was recommended by one of the committee members who had used it in a previous job. Since the McAfee Active Defense solution was already being used within the organization, a decision was made to make the McAfee Console Manager available to committee members to evaluate and get a feel for the product.

After gathering product information, reading several product reviews, discussing features, issues and problems with the owned licensed products, Panda Enterprise Suite was eliminated because of its inability to function with some in-house developed applications.

Shortly thereafter, McAfee was eliminated because the product lacked friendly usability.

Since I had been the AV Administrator for the remaining owned AV product, Symantec, I was the individual responsible for the evaluation phase. The next stage of the project was to compare the features of Symantec Antivirus Enterprise to Trend Micro.

A 30-day evaluation copy of Trend Micro was obtained; only portions (i.e. OfficeScan Corporate Edition, Control Manager and ServerProtect) of the software was installed and configured on a makeshift server. In addition, the ScanMail portion of Trend Micro was installed on an e-mail relay server, which was placed in front of the Exchange server. This setup allowed the ability to thwart viruses at the email perimeter, by scanning all incoming mail. This deployment was optimal over, installing ScanMail on the Exchange server, because Symantec was already installed on the Exchange server. Secondly, we did not want to radically change our current set-up in the event Trend Micro was not chosen as our corporate-wide AV answer.

The server installations progressed fairly well, although a couple of issues surfaced (1) the required installation of Microsoft Internet Information Services (IIS) on the makeshift sever and (2) the incompatibility of Windows 2003 server with the Management Console of Trend Micro. Both of the Windows servers were downgraded to 2000 and IIS was installed on the makeshift server, but not fully patched for security holes. The client installation was carefree; initially 12 machines were used. But as the users began voicing opinions about the product, other clients were added from several of the Wintel networked domains.

1.2.1 Needed anti-virus features

There were specific features thought to be important for the selected package, such as:

(a) The ability to work with Window clients including NT—this was a mandatory feature since our company was primarily a Microsoft shop. The product had to work with Microsoft NT because applications being used on the network still required NT.

(b) Easy to install, deploy and use. The committee felt this feature was important for a couple of reasons. First, if the product was easy to use, it decreased the learning curve and training time. From the administrator prospective, the easier the product was to use, the greater the likelihood the AV software would be

configured to best protect the environment. Secondly, ease of use provided improved productivity for the administrator, technician and end user.

(c) Option to interpolate with Microsoft Exchange 5.5 and 2000, which included the ability to:

(i) Exclude mail stores—this became an important feature after the initial scan of the mail stores. Once the mail stores had been scanned, it would be a waste of resources to rescan them, when all new emails will be scanned prior to being allowed entrance into the network. This does a couple of things, it preserves the CPU and eliminates investigating the same issues.

Additionally, the committee discovered other files to exclude from being scanned repeatedly—the quarantine viruses and the recycle bin—for the same reasons for excluding the mail stores.

(ii) Manage the Exchange server remotely. The committee accepted as true that availability is crucial in security management. Therefore, having instant access remotely to address issues quickly helps mitigate virus exposure and potentially saves the organization time, productivity and money.

(d) Network and workstation based solution.

(e) Notifications, which included the abilities to:

(i) Notify email senders and recipients of problems.

(ii) Administrator notification of alerts and outbreaks.

A dependable alerting mechanism is invaluable; it provides an administrator with the opportunity to respond quickly to a virus outbreak or potential problems.

(f) Logging and reporting with the ability to:

(i) Create logs of alerts and errors.

(ii) Have database for logs and text logs.

(iii) Central log folder.

(iv) Standardized activity reports.

(v) Graphical reporting.

Logs and audit trails are extremely important to investigating problems.

(g) Automatic updates of definitions and policies. The committee considered this is a mandatory feature. First, it frees up the

administrators making them more productive. Besides automation reduces vulnerabilities.

(h) A central administrator console, which allows for control of servers, workstations and quarantined viruses.

(i) On demand scanning—allows for scanning of floppies and CDs prior to usage or any suspicious files.

(j) Technical Support—having consistent support as well as an escalation process from the vendor is added value for our environment.

1.3 RESULTS AND RECOMMENDATIONS

At the onset of the evaluation, I thought selecting one AV product for our organization would be a piece of cake; since both Symantec and Trend Micro offered similar feature sets (See Appendix B). Moreover Symantec was the "known" product that I had spent countless time tweaking and configuring for the Root domain's use for over a year. In spite of this, I endeavored to evaluate the products on their merit and not take the road less traveled.

To my surprise, there were several features of the Trend Micro that made this product a good choice for our corporate-wide AV protection solution:

(a) The ease of client installation was great; the help desk technicians liked the speed of installation with the product.

(b) The centralized management and configuration. When the help desk technician installed the Trend Micro, if the workstation that the product was being installed on was in a different Wintel networked domain, it automatically added the domain and placed the machine under that domain in the Console Manager.

(c) Notification and logging. There were several notification features that made great impressions. However, the one that stood out the most was the user warning about out-of-date virus pattern files; something the previously used product fell short on. During the testing phase, several machines did not get their virus pattern files updated properly, for various reasons (i.e. some individual computers were turned off longer than the seven day update periods due to vacation/absences; others workstations were intentionally disconnected from the server; etc.). The Micro Trend icon in the Icon Tray would begin flashing a red exclamation mark until the updates occur. The flashing red exclamation drew the user's attention, which in turn stimulates a call to help desk to find out what the

problem could be. In our environment, this was considered a plus, because this enabled the IT department to help educate users, this also provided the users with the feeling that they have played a part in securing company resources and the network.

(d) Processor overhead for the clients and servers was minimal, which won points from users, especially from the application developers. Additionally, the Trend Micro Console Manager generated very little network traffic.

(e) Firewall integration. The product integrated with some of the common firewall; which will provide our organization with another level of virus perimeter protection. Although this feature was not tested during the initial evaluation, much research has been done on this aspect of the product, so that it can be deployed later.

(f) Trend Micro offered a separate product to protect the server within a network, which is a greater level of protection than the desktops.

There were two features that the standard version of Trend Micro did not offer; which are attributes the committee initially felt were wanted and handy (i.e. notifying email senders of potential problems and graphical reporting). These features are good ones, but the committee decided if the product would provide optimal protection, then we could function without those conveniences. Although with a separate module of Trend Micro—the Control Manager—makes graphical reporting available.

In spite of the fact that, sender notification was not an inherent feature of Trend, I found that some sender notification did occur, just indirectly. When an incoming email was forced into isolation because of a virus; the recipient of the email was notified that an email message from a certain party was quarantined. If the recipient felt the email message was important, we observed a couple of things transpire (1) the recipient contacts our help desk to obtain additional information about the isolated message and/or (2) the recipient contacts the sender and informs him/her of the problem, therefore in a roundabout way some senders are notified.

Up to now, the overall attributes of the Trend Micro product were buzzing in our environment, yet there was one small snag. During the initial fact-finding phase of this project, there was no mention of Trend Micros' ability to integrate with Microsoft Exchange 5.5, which was currently being used within our organization. The problem our company was facing was if Trend Micro were to be selected as the corporate-wide solution, the company would have to upgrade to

Exchange 2000, at minimal. This was a huge problem because upgrading the Microsoft Exchange would require a major investment in time and money, which could not be afforded at this time. To obtain clarity and a possible solution or a work around for this issue, a call was placed to the Customer Service department of Trend Micro Company. The Customer Service Representative was helpful and pointed out that Trend Micro did offer integration with and support for Exchange 5.5. This removed the only other obstacle Trend Micro would have to overcome to be selected as our single vendor AV system.

1.4 AFTER THE EVALUATION—GOING FORWARD FROM THE TEST

Once the decision was made to use Trend Micro as the corporate wide AV, Trend Micro Company was called to obtain an extension on the 30-day evaluation. Now the committee needed to decide on the most effective deployment strategy. For our environment placing the software on a dedicated server was selected as the best solution. The dedicated server approach was beneficial because it reduced the administrative work and provided a simplified solution to our AV strategy.

Prior to full corporate deployment, support for three AV products (i.e. Trend Micro, McAfee and Symantec) was required, because many of the users did not want to migrate back to their previously used AV solution. To speed up the deployment process, a special purchase order was cut to get the necessary equipment. Upon the arrival of the purchased licenses and the hardware, the configuration process began. The operating system, Windows 2000, was installed. In order to run the Console Manager of the OfficeScan portion of the Trend Micro, the Microsoft Internet Information Services (IIS) had to be installed on the Trend Server, at this time it was important to secure IIS; given the known security holes with Microsoft IIS 5.0 (8). The IIS Lockdown Tool was run to ensure the security of the server. However, after running the IIS Lockdown Tool against the Trend Micro server, access to the Console Manager was lost. This was a hurdle we needed to overcome quickly. The initial approach was to search Trend Micro's knowledge base, in hopes that a solution was available. Through a bit of trial and error, we discovered that special configuration was required since the html-based interface is a requirement for the Console Manager. The urlscan.ini filter was edited to allow .exe and .dll internally; also this file required an additional verb "POST", to be added to IIS Verbs section of the urlscan.ini file.

As soon as the obstacle was overcome, we continued with the process of securing the server. To further guarantee that all necessary security actions were taken with this server, several analyzers were run against the server (i.e. Microsoft Baseline Security Analyzer, Network Mapper, Nessus, etc.); the appropriate service patches were applied, unnecessary ports were closed and service disabled.

1.4.1 Corporate-wide deployment discovery

After the primary Trend Micro server was deployed, the focus shifted to the email server deployment. During the operation, Symantec was removed from the Exchange server and Trend Micro was installed prior to removing the evaluation e-mail relay server from the picture. The process went smoothly, but the discovery made after the scanning of the all the mailboxes was astonishing. There were over 700 viruses found in various mailboxes that no previous notification had been made by the former AV product. This information was difficult to absorb at face value, so I poured through the archived notifications for answers. There were no answers to be found, so I was left with two possibilities:

(a) The package had failed to adequately protect our company at the email perimeter or

(b) I failed to optimally configure the package.

Of course, my ego wanted to believe that option b was not correct, but no matter which scenario was correct, the fact remained that this was troubling information.

1.4.2 A discovery after the deployment

Now that the deployment of Trend Micro was successful and things appeared to be running smoothly, the company network was experiencing excessive traffic, which generated a bit of concern. A couple of network analyzers were run to get an epitome of the problem. The majority of the traffic was coming from two machines on the network, the assistant AV administrator and my workstation. The first thought was that these desktops had contracted a virus, but no notification had occurred. After some investigation and the process of elimination, the problem was isolated to the Symantec System console, which was on the administrators' workstations. Neither of us remembered to uninstall the management console of Symantec from our workstations, as a result Symantec continued attempting to communication with previously configured clients.

1.5 CONCLUSION

In conclusion, AV protection is a must because viruses and their kin are serious problems and will continue to plague businesses. The decision made by our organization to commit to a single vendor strategy for AV protection was a smart choice. The selected AV package helped us discover over 700 viruses and their kin that were lurking around in our environment, which could have caused major problems. Even if we had not found the dormant viruses, the ease of use alone has been enough of a benefit for our organization to migrate to Trend Micro Enterprise Protection Strategy. This strategy may or may not be the appropriate solution for every organization. However, this journey helped our company form a cost-effective strategy that was a good fit.

Moreover, this voyage awoke me to a fact I sometimes forget. Keeping an open mind, along with open eyes can only enhance the security of any network, whether implementing an AV solution or a different project.

2. **APPENDIX A—FEATURES COMPARSION [9]**

FEATURES	Symantec AntiVirus Enterprise	Trend Micro Enterprise Protection Strategy
OPTIONS		
Microsoft Exchange 5.5	X	X [7]
Microsoft Exchange 2000	X	X
Central installation of servers	X	X
Central installation of workstations	X	X
Automatically excludes mail stores		
Automatically excludes quarantine		X
Automatically excludes recycle bin		
NOTIFICATIONS AND UPDATES		
Notifies email recipients of potential problem	X	X
Notifies email senders of potential problem	X	
Sends administrator email	X	X
Sends administrator page	X	X
Send administrator SNMP trap	X	X
Logs alerts	X	X
Logs errors	X	X
Outbreak alert	X	X
Central alert manager	X	X
Push updates or policies	X	X
Automatic client software updates	X	X
ADMINISTRATOR CONSOLE (CENTRAL CONTROL)		

FEATURES	Symantec AntiVirus Enterprise	Trend Micro Enterprise Protection Strategy
Integrate control of servers	X	X
Integrate control of workstations	X	X
HTML-based	X	X
MMC-based (Windows)	X	
Quarantine manager	X	X
Automatically uploads new viruses to vendor for analysis	X	X
Administrator can manage Exchange server product remotely	X	X
Works with Windows clients without a separate agent	X	X
LOGGING AND REPORTING		
Can log client infections	X	X
Can log server infections	X	X
Central log folder	X	X
Graphical reports		
Windows NT/2000 event logging	X	X
Database log		X
Text log	X	
Standardized activity reports		X
Ad hoc query of reports		X
TECHNICAL SUPPORT		
Toll-free number	X	X
Email Support	X	X
Web support	X	X
Service contract	X	X

LIST OF REFERENCES

1. Trend Micro, Inc. "The Real Cost of a Virus Outbreak, http://www.trendmicro.com/NR/rdonlyres/02A09EAE-3758-41C9-8ED0-1FAF851BA256/2774/realcostwhitepaper.pdf (March 1, 2002)

2. Moore, D; Paxson, Vern; Savage, Stefan; Shannon, Colleen; Staniford, Stuart & Weaver, Nicholas. "Sapphire/Slammer Worm Shatters Previous Speed Records for Spreading through the Internet, California computer experts report", http://www.sdsc.edu/Press/03/020403_SAPPHIRE.html (February 4, 2003)

3. Schneier, Bruce "Did Blaster cause the blackout?", http://zdnet.com.com/2100-1107_2-5118123.html (December 9, 2003)

4. "Inova Stats", http://www.inova.com.br/velop/escudo/e_estatisticas.htm

5. Featherly, Kevin. "Virus Threats Bad and Getting Worse – ICSA Survey". http://www.computeruser.com/news/00/10/24/news7.html (October 24, 2000)

6. Mimoso, Michael. "Cost of virus cleanup goes up." http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci941270,00.html (December 15, 2003)

7. Trend Micro's Customer Service Representative (personal communication, 2003)

8. Howard, Michael. "Secure Internet Information Services 5 Checklist", http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/chklist/iis5chk.asp (June 29, 2000)

9. "Summary of features—Corporate Antivirus Tools", http://common.ziffdavisinternet.com/download/0/1984/summary.pdf