Sophos Anti-Virus: Competitive Analysis

Test report prepared under contract from Sophos Anti-Virus

Executive summary

Sophos Anti-Virus commissioned VeriTest, a division of Lionbridge Technologies, Inc., to perform a competitive analysis of their anti-virus software version 3.75 against the following four competitors.

- McAfee VirusScan 7.0
- Reliable AntiVirus (RAV) 8.6
- Symantec AntiVirus Corporate Edition 8.6
- Trend Micro OfficeScan 5.5

The applications under test are enterprise antivirus applications. They provide the user with a way to deploy antivirus software out to multiple network clients and then monitor them for any virus activity.

Key findings

❑ In our test configurations, we found that Sophos required the least amount of time to install on a single test client (29 seconds) and 15 test clients (1 minute and 59 seconds)

❑ In our test configurations, we found that Sophos provided the most frequent virus definition updates in both manual and automatic testing configurations and provided smaller files for download than the competitive products thus saving download and installation time.

❑ In our test configurations, we found that Sophos required the least amount of time of the products we tested to complete the full drive scan taking only 2 minutes and 18 seconds.

❑ In our test configurations, we found that Sophos Anti-Virus required the least amount of disk space of the products we tested taking only 12.5 MB for a default software deployment.

This testing focused on the following three areas for each product tested:

- Ease of product installation
- Scheduling accuracy and total time for scheduled scans
- Procedures for updating virus definitions

Testing the ease of installation consisted of following the manufacturer's documentation to deploy their software to 15 individual network-based clients. During this phase VeriTest recorded the time to deploy the software to one client, the time to deploy to 15 clients, and the amount of disk space taken by the application on each client after deployment. To test the scheduling accuracy and total time required to complete scheduled scans we configured each product under test to perform a full system virus scan at an allocated time. We repeated this test on three consecutive days and recorded the total time to complete each scan. To test the capabilities of each product under test with regard to virus definition updating, we performed manual and automatic updates with all applications for 10 consecutive days. Please refer to the Test Methodology section of this report for complete details on how we conducted these tests.

In our test configurations, we found that Sophos Anti-Virus required the least amount of time to install to both a single client and to fifteen clients compared to the other products tested. We were able to deploy the Sophos anti-virus product to a single client in 29 seconds and to all 15 test clients in 1 minute and 59 seconds. We found that McAfee required the most time to install in both deployment configurations taking 13 minutes and 6 seconds to deploy and install to one client and 13 minutes and 21 seconds to deploy to all fifteen clients.

In addition, we found Sophos Anti-Virus 3.75 required the least amount of disk space in our test configurations after the default software deployment taking only 12.5 MB. In contrast, we found that Trend Micro Office Scan 5.5 required the most disk space of the five applications tested, requiring 38.2 MB of disk space after a default deployment. Included in the disk space used by Trend Micro Office Scan 5.5 is a 20 MB reserve file that gets installed on the system by default. This reserve file is placed on the system to allow the application room for updates. The use of the reserve file can be removed by deselecting the reserve file option from the advanced settings of the client administration in the Trend Micro OfficeScan Management Console.

When testing the capabilities of the products under test to schedule and complete virus scans, we found that all of the products tested performed the scheduled scans without errors. However, the time to complete these scans differed between the products. Sophos Anti-Virus 3.75 required the least amount of time in our test configuration to complete the full drive scan taking only 2 minutes and 18 seconds. This is compared to Symantec AntiVirus Corporate Edition 8.6, which required the most time to complete the full disk scan of the five applications tested taking 6 minutes and 19 seconds.

When comparing the frequency and size of virus definition updates provided by each manufacturer on their website, we conducted both manual and automatic virus definition updates for 10 consecutive days. The process of providing frequent virus definition updates allows the user the opportunity to stay up-to-date with protection from the most recent viruses. In our test configurations, we found that Sophos provided the most frequent virus definition updates in both the automatic and manual update testing compared to the other products under test. In addition, we found that in all cases Sophos and RAV provide the user with smaller update files, which take less time to download and install.

In addition to recording the manufacturers update procedure, we also evaluated their email notification process. To do this, we subscribed to the email notification process for each of the manufacturers that offered this as a free service. All of the manufacturers offered this as free service except Symantec. Symantec does offer this service but it is part of a platinum level service agreement that must be purchased through the manufacturer. Sophos is the only manufacturer that provided a virus update email notification on a daily basis to coincide with their definition updates. Each day that a virus definition update was available, we received email to notify us that an update was available.

Please refer to the Test Results section of this report for complete test results.

Testing methodology

Sophos Anti-Virus commissioned VeriTest, a division of Lionbridge Technologies, Inc., to perform a competitive analysis of their anti-virus software version 3.75 against the following four competitors.

- McAfee VirusScan 7.0
- Reliable AntiVirus (RAV) 8.6
- Symantec AntiVirus Corporate Edition 8.6
- Trend Micro OfficeScan 5.5

The applications under test are enterprise antivirus applications. They provide the user with a way to deploy antivirus software out to multiple network clients and then monitor them for any virus activity.

This testing focused on the following three areas for each product tested:

- Ease of product installation
- Scheduling accuracy and total time for scheduled scans
- Procedures for updating virus definitions

Please refer to the Appendices for a complete list of the hardware and software used for the tests.

Ease of installation and Deployment

For each application we followed the manufacturer's documented installation procedure to deploy a default installation of the software to multiple clients. We recorded the following information during the deployment: deployment file size, time to deploy application to all 15 clients, and the time to install software on only one client.

For the deployment process we used the following tools:

- McAfee – McAfee ePolicy Orchestrator 2.5.1
- RAV – RAV Deployment Tool 1.1
- Sophos – SAVAdmin in Enterprise Manager 1.1
- Symantec – Symantec System Center for SAV version 8
- Trend Micro – OfficeScan Management Console 5.5

For the deployment test we configured a test bed with one server and fifteen clients. The server was configured as a domain controller with Microsoft Windows 2000 Advanced Server with Service Pack 4. All fifteen clients were configured with Microsoft Windows 2000 Professional with Service Pack 4. The server and clients were networked together with 100Mbps Ethernet connections through an Extreme Networks Summit 48 switch. The server and client network adapters and the switch ports were set to auto negotiate line speed and duplex resulting in connections of 100 mbps using full-duplex. The server was configured as a Windows 2000 domain controller with DNS enabled.

For the software deployment, we used the manufacturer management console and/or deployment tool listed above on the server to deploy the software to all fifteen clients. To obtain the total time for the deployment we recorded the start time of the deployment and end time for the software installation on each of the clients. We then subtracted the start time from the end time of the last client installation. The result gave us the total time to complete the deployment and software installation on all fifteen clients.

To ensure the system clocks were the same on all systems we configured the clients to synchronize their clocks with the server clock. To do this we used the "net time" command with the following syntax: "net time \\server /SET /YES" (where "server" refers to the actual computer name of the server).

For the deployment start time on each application we used the system clock on the server and recorded the displayed time when we executed the deployment. There were differences in the way each application reported the software deployment completion. If possible we used the event recorded in the Windows Event Log to indicate when the deployment completed. However, not all applications recorded an event so we relied on other means to show the completion time.

To ensure that each application had successfully completed the installation we installed Sysinternals' Filemon for Windows on each client. We had this program running on the server and all clients during the deployment. After the deployment was complete we used the Filemon log to verify the time when the setup process finished installation. We noted the deployment completion time when the application was successfully installed, all setup processes had stopped running, and the antivirus program was active. The following sections provide the specific details of how we measured the time to complete the deployments using each application under test.

McAfee VirusScan 7.0:

First we installed and configured the McAfee ePolicy Orchestrator 2.5.1 console with the default installation. Then we configured our domain within the directory. To configure the domain, we created a new site and named it the same as our domain name. After creating the site, we allowed the console to discover the clients in the domain by using the "All Task > Update Domain" option from the menu that appears after right clicking on the site name.

After the site was configured, we started the software deployment by right clicking on the site name and selecting "send agent install". This opened the send agent install window. For the deployment we used all of

the default deployment settings except for the suppress agent installation GUI option and the force install installation options. We deselected the suppress agent installation option on the send agent install window so that we could see the GUI menu on the clients during the ePolicy installation. We chose to do this as verification that the installation was being performed on all clients. The installation option that we changed from the default setting was "Force Install VirusScan Enterprise". This option is not selected by default; however, the manufacturer's instructions recommend that this option be selected. We recorded the start time of the deployment when we clicked OK on the send agent install window. To obtain the start time we had the date/time properties window open on the screen. We noted the exact time that we clicked the OK button and recorded the hour:minutes:seconds.

To record the end time, we used the timestamp of the 11707 event logged in the Windows Event Log (shown in Figure 1) by the client when it completed the installation. Figure 2 shows the properties of this event. We verified the accuracy of the event log timestamp with the timestamp in the ePolicy Orchestrator Agent Log on the client found in the ePOAgent folder. We verified on each client that the software was indeed installed and active on the system. To do this we opened the McAfee console from the start menu on the client and verified that the client reported an active on-access scan.
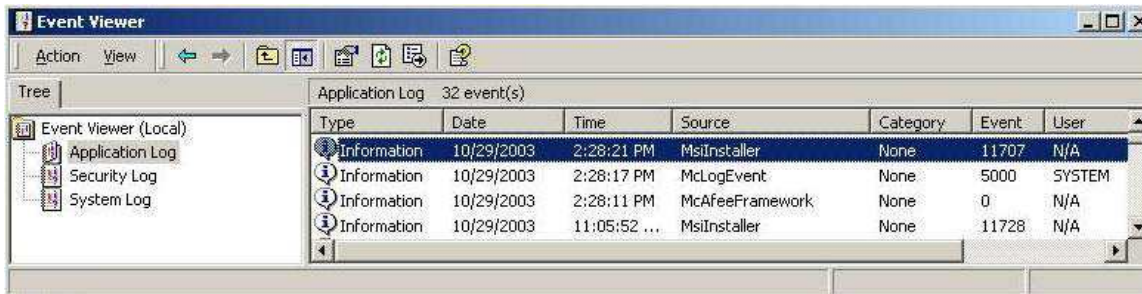
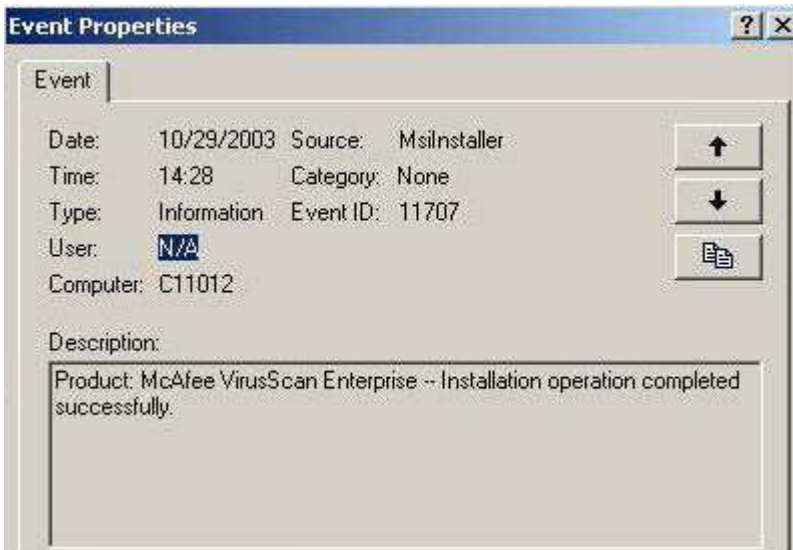**Figure 1: Event Viewer from a client after software installation.**

Figure 2: Properties of the event logged into the Event Viewer.

Sophos AntiVirus 3.75:

For the deployment of Sophos we first configured the Sophos Enterprise Manager. Then we configured the CID (central installation directory) for the software deployment. For both the Sophos Enterprise Manager and CID, we used the default configuration options. Once the configuration of the management console was complete, we used the SAVAdmin utility to deploy the software to all clients.

We opened the SAVAdmin utility and expanded the network neighborhood option within the SAVAdmin window until our configured domain was shown. This identified all systems in the domain on the right hand side of the SAVAdmin window along with their Sophos installation status. All clients showed that no Sophos software was installed on their system. We selected all fifteen clients for software installation by clicking on them with the mouse cursor while holding down the ctrl key. This allowed us to choose multiple installations simultaneously. To deploy the software, we performed a right mouse click on one of the selected systems and then choose "install SAV" from the menu that appeared. We kept all the default options for the deployment except for the account name and password. We did have to enter this information into the deployment option window. Once we entered this information we started the deployment task by selecting OK.

To record the start time of the deployment we used the timestamp when we clicked OK to begin the deployment. To record the end time of the deployment process, we noted the file creation time of the SWEEP.LOG file on each client. This log file is created once the Sophos software has completed the installation on the client machine. We recorded the creation time for the SWEEP.LOG file by right clicking on the file and choosing properties. Figure 3 illustrates the properties of the file and its creation date. We verified on each client that the software was indeed installed and active on the system. To do this we opened the Sophos console from the start menu on the client and verified that the client reported active**.**
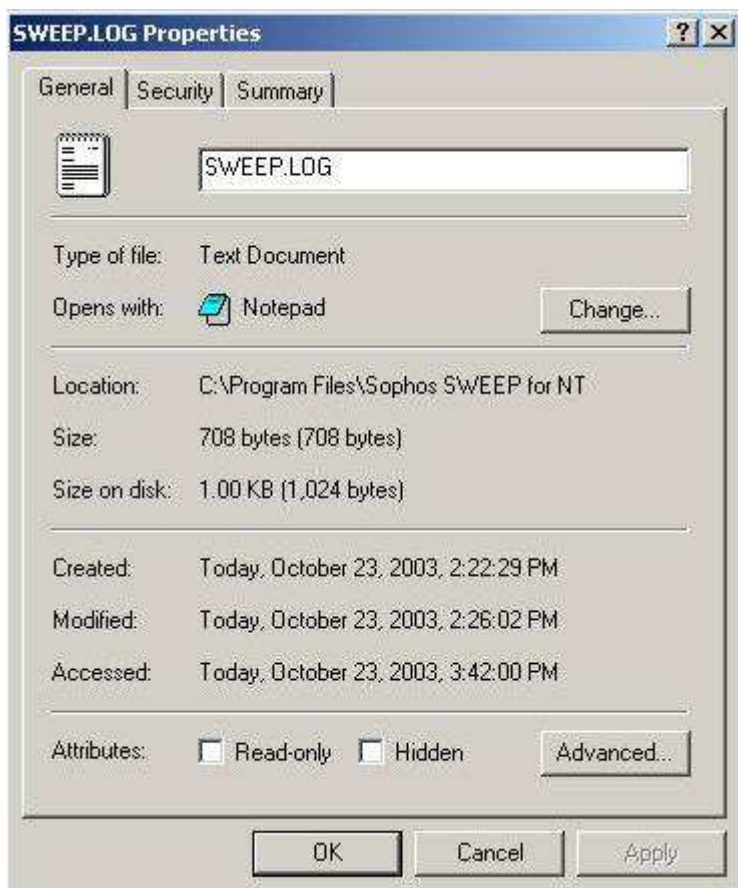

Figure 3: SWEEP.LOG from a client after installation.

Symantec AntiVirus Corporate Edition 8.6:

We installed and configured the Symantec Management Console on the server. After installing and configuring the Symantec Management Console, we installed the Symantec Antivirus software on the server. To do this we used the AV server rollout option found on the tools menu within the management console. Once the server was installed, we started the client deployment from within the management console.

To start the client deployment, we used the NT client install option from the tools menu within the Symantec Management Console. After clicking on this option, a software installation wizard appeared to guide the user through the installation task. We choose the default options on all screens except for the Select Computers screen. On this screen we selected all fifteen clients and then selected the server that they would belong to for update purposes. At this point we clicked finish to begin the deployment. We recorded the start time on the system clock when we clicked finish to begin the deployment.

After the software installation was complete on the client, the system logged an 11707 event (shown in Figure 4) into the Windows Event Log. Figure 5 shows the properties of this event. We used the timestamp of the event as the stop time of the deployment. We verified that the installation was successful by opening the application from the start menu. When the Symantec console opened, we verified that the auto-protection was running.
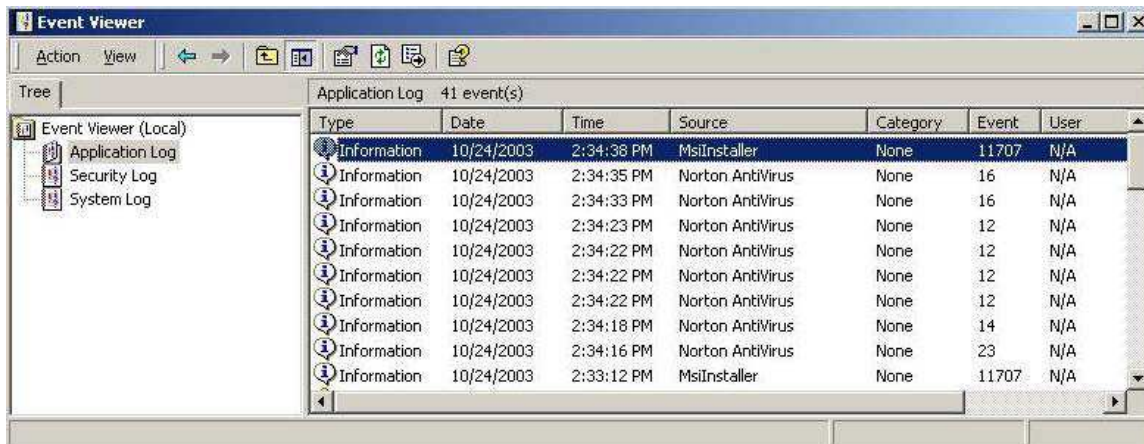
Figure 4: Event Viewer from a client after software installation.

Figure 5: Properties of the event logged into the Event Viewer.

Reliable AntiVirus 8.6:

RAV does not have a management console available to deploy their software, so we used their stand alone deployment tool to install the anti-virus package to all clients. For the deployment, we copied the deployment tool and the client software into a directory on the server, and then we executed the deployment executable to begin the installation.

We accepted all of the default options for the installation except for the remote computer selection. At this screen, we selected all fifteen clients for the deployment. After we selected the clients, we clicked next to continue. We proceeded through the remaining options by accepting the defaults. On the last screen we clicked finish to begin the deployment.

For the start time, we recorded the time on the system clock when we clicked finish to begin the deployment. To get the exact time on the system clock we opened the date/time properties and noted the hour:minute:second time in the window.

At the completion of the RAV installation on the client the system shows a Messenger Service popup message in the middle of the screen. The displayed message is as follows: "RAV AntiVirus Desktop for Windows has been installed on your computer. To start using the antivirus protection, you will need to restart your computer." Figure 6 shows the event properties from the application popup from the Messenger Service that was logged into the Windows Event Viewer. Here you can see the contents of the message in the description portion of the event properties. Therefore we included the system reboot time into the deployment for the RAV application. This was only done with the RAV application because it was the only one that states a system restart is required to start using the antivirus protection. Because we were recording the total time until the system was actively protected, we included the reboot time as part of the deployment.

Figure 6: Event Properties showing the message that a system restart is needed.

To perform the system reboot we created a script with Rational Visual Test 6.5 to restart the computer at the completion of the RAV client software installation. To trigger the system restart we created the Visual Test script to look at the C:\winnt\task directory. RAV places a task entitled "rav_install" in the task directory for the installation process. When the installation is complete on the client the "rav_install" task is removed from the task directory. The Visual Test script was designed to check for this file in the task directory. Once the task was located the script waited until the file was removed from the task directory. After the file was removed from the directory then the Visual Test script initiated a system reboot. Please refer to the appendix for the contents of the Rational Visual Test script.

To record the stop timestamp for the RAV deployment we used the timestamp of the 6005 event logged in the Windows Event Log (shown in Figure 7). This event is when the Event log service was started. Figure 8 shows the properties for this event and illustrates that the service was started. We used this timestamp because Windows has successfully loaded when the Event Log service starts so the system restart process has completed.
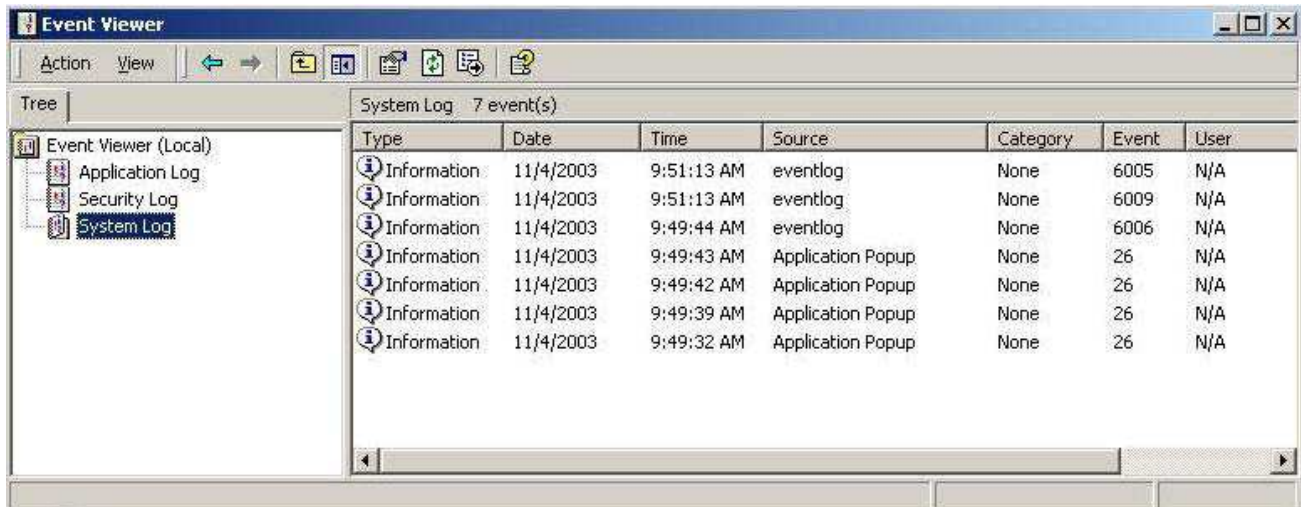
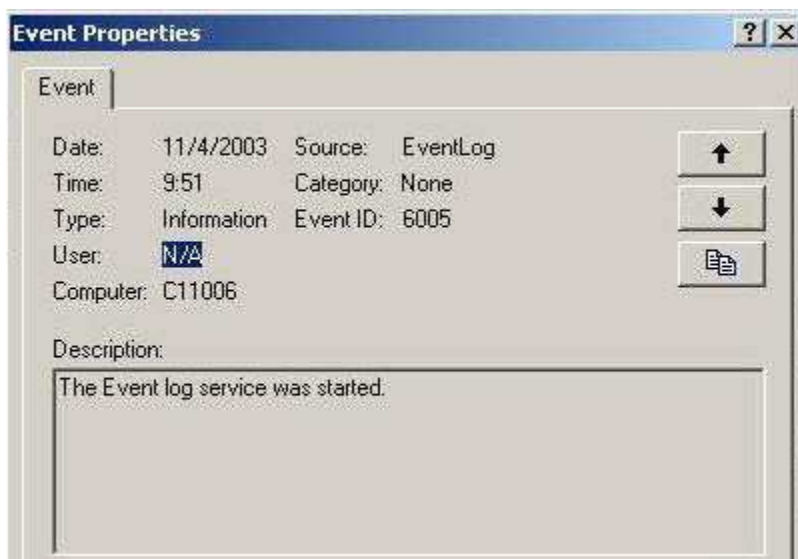**Figure 7: Event Viewer from a client after software installation.**

Figure 8: Properties of the event logged into the Event Viewer.

Trend Micro OfficeScan 5.5:

First we installed and configured the Trend Micro Office Management console. After configuring the management console on the server, we performed the deployment with the NT Remote Install feature found in the Client Administration menu of the management console. To start the deployment, we expanded the network in the NT Remote Install GUI interface so that all fifteen clients were shown. Then we selected all clients for deployment and selected Apply to begin the deployment. To record the start timestamp we had the date/time properties window open at the time of deployment. We recorded the time showing on the clock when we clicked Apply for the deployment to begin.

For the stop timestamp, we used the management console user interface. The management console places checks on top of the clients when the deployment and software installation is completed, see figure 9 for illustration. When all clients have completed the installation process we noted the time in the date/time properties window and recorded that as the completion time. We relied on the management console for the stop time because there was no obvious indication on the client that the installation process was complete. We verified on each client that the software was indeed installed and active on the system. To do this we opened the OfficeScan console from the start menu on the client and verified that the client reported an active status.
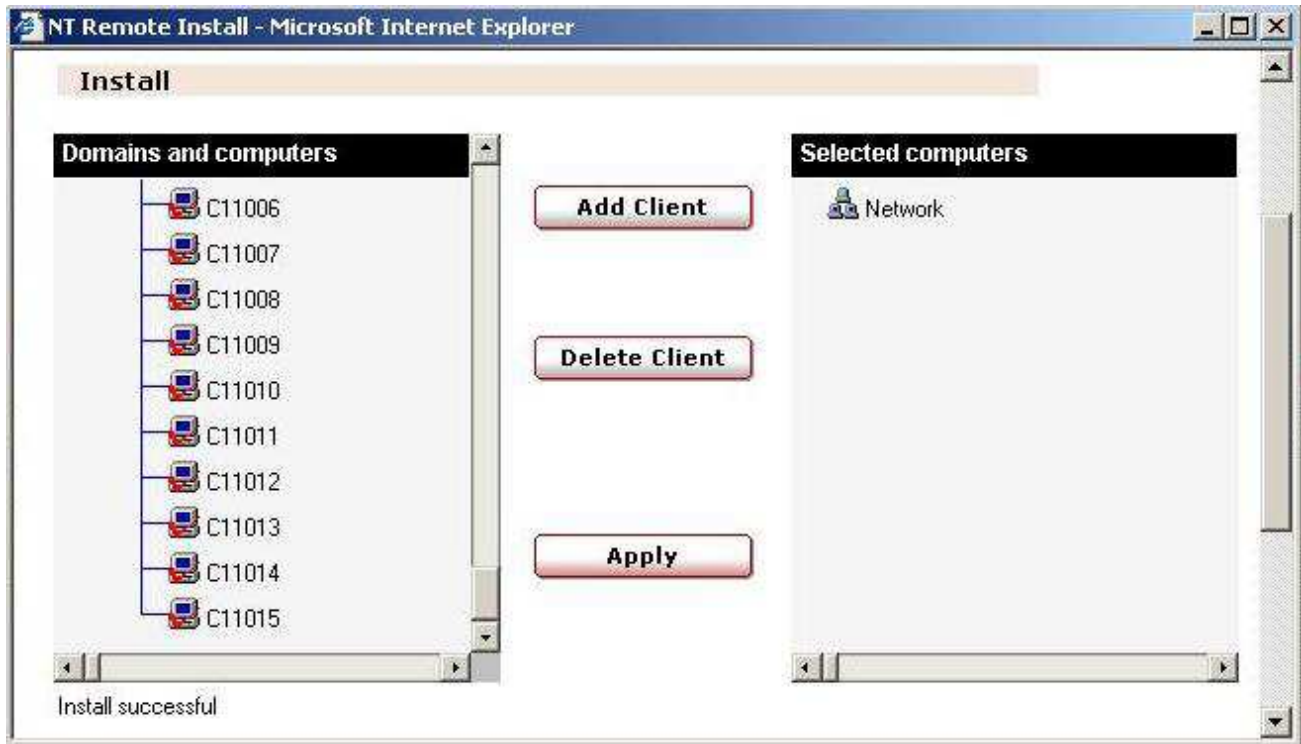
Figure 9: Trend Micro NT Remote Install window showing installation successful.

To ensure the stop timestamp was accurate we installed the Sysinternals' Filemon for Windows executable on the server. We had this program running in the background to record the processes running during the deployment. We verified the stop timestamp by recording the time that the installation process stopped running according to the Filemon results. When the OfficeScan processes was not longer running we knew the installation was complete. We used this console for the timestamp because Trend Micro does not record an event into the event viewer when it has completed the installation. Figure 10 and 11 show the Filemon logs from the server and client and illustrates the stop timestamp.

Figure 10: Filemon log of the server showing the ending timestamp of the deployment.

Figure 11: Filemon log from the last client to have software installed. This confirms the end timestamp for the deployment.

Evaluating Scheduling Speed and Accuracy

These tests evaluated the scheduling accuracy and speed of each application's scanning ability. For this testing we configured two computers for each application. These computers were networked together by connecting them through a 100 Mbps network switch. We configured the computers and the switch ports to auto negotiate resulting in 100 mbps, full-duplex connections. One of the computers was configured as a domain controller server with Microsoft Windows 2000 Advanced Server installed. The other system was configured as a client in the domain with Microsoft Windows 2000 Professional installed. Both of these systems had Service Pack 3 installed. We installed the antivirus applications on configured computers by performing a default installation for each application.

To test the scheduling accuracy we configured each application to execute a scheduled scan of the system's hard drive. This scheduled scan was to begin at the same time everyday for three days. To ensure that each application began the scan at the scheduled time we physically checked each system at the scheduled time and made sure the application was scanning the system's hard drive. In addition, we recorded the total time to perform the scan by using a stopwatch. We started recording the time when the antivirus application started scanning the system and stopped when the application showed that it was complete.

Virus Definition Updates Capabilities

In this testing, we compared the frequency and size of the provided virus definition updates available from each vendor. We performed both manual and automatic update testing for this phase. For the manual testing the test bed was configured identically as described above for the scheduling speed and accuracy testing. For each of 10 consecutive days, we checked the vendors' website for virus definition updates. If new updates were available we manually downloaded and installed them according to the manufacturer's instructions. For each download, we recorded the file size and verified its relevancy. To determine the relevancy of the file we compared the update information for that day's virus definition update to the update from the previous day. If the file was not adding any additional virus definitions then it was noted as not relevant because no actual update was required.

In addition to comparing the frequency of the updates on the vendors' website we compared their email notification. We subscribed to the vendors' email virus and product update notification located on their website and we evaluated and recorded the frequency and content of email messages that we received from the vendor.

For the automatic update testing we compared the frequency and size of the provided virus definition updates available through each vendor's automatic update process. For this testing the test bed was configured with ten test systems. Five of these systems were configured as servers running Windows 2000 Advanced Server with Service Pack 4 and the other five were configured as client systems running Windows 2000 Professional with Service Pack 4. We connected the ten systems via network through a Summit 48 network switch that was segmented into five different virtual networks. We connected them so that only one client and one server were on each of the five virtual networks. All five servers had two network adapters installed in the system. One of the network adapters was connected to the Summit 48 for the isolated network with the client and the other network adapter was connected to the Internet. This adapter connected to the Internet was to allow the server a way to pick up daily updates from the vendor's website.

We scheduled each of the five anti-virus programs to check for updates at 12:00 PM every day. Each application was setup to automatically check for updates and then download and deploy the new updates to their client system. Each day we recorded the file size of the automatically downloaded update. The configuration for each application as well as the procedure used to verify the update is outlined below for each application under test.

Reliable AntiVirus 8.6:
For RAV we installed RAV for Windows on the server and then installed the RAV desktop client on the client system. On the server we used the configuration center within the RAV GUI interface to setup the server

update. We changed the "Server Update" configuration window from its default setting by selecting the "enable server update" option. We changed this setting so the update would download to a shared folder to allow the client to receive the update for this server. We selected the following location for the shared folder: C:\RAV Update. To do this we first created the C:\RAV Update folder and then enabled sharing on this folder. After sharing the folder we browsed to it from within the RAV Server Update Configuration Center user interface and selected it as the default update location.

After creating the server update location we created a task to check for updates every day at 12:00 PM. To create this task we used the RAV Scheduler found on the RAV GUI "tools" drop down menu. We also set the source location for the update to be downloaded from to the server. For the source location we used the FTP site on RAV's website. This link is a default option stored in the RAV Update source update location.

To perform the update on the client machine we configured the update source to be the shared folder on our server. We pointed the update location on the client to the C:\RAV Update folder that we shared out on our server. In order for the client to receive updates on a daily basis we setup the RAV Scheduler to check for updates on our server every day at 12:15 PM. We selected 12:15 PM instead of 12:00 PM so that the server would have time to download the updates to the appropriate location.

Each day we checked in the C:\RAV Update folder on the server and recorded the size of the updated files. To verify that the update was run we looked at the update.log. This file was found on the server at the following location: C:\Documents and Settings\Administrator\Application Data\GeCAD\RAV8 Desktop. We then looked on the client machine and verified that it had performed the update and received the updated files as well.

Sophos Anti-Virus 3.75:

We configured the software as outlined in the manufacturer's documentation. We installed and configured the Sophos Enterprise Manager to monitor all activity. In Enterprise Manager we set up a schedule to check for updates at 12:00 PM each day. The client was setup to check the server for updates every 60 minutes. We set the server to place all the updates into the central installation directory on the server.

Each day we checked the message log in the Enterprise Manager to verify that the system received updates. We looked in the central installation directory to see what updates we received. To get the total size of the files downloaded we added the file size of each file that had been modified that day and calculated the total. After this we looked at the log file on the client to verify that the update was transferred to the client.

Symantec AntiVirus Corporate Edition 8.6:

We installed the Symantec System Center console on the server and then used it to manage all installations. We installed the client from within this console by choosing Tools > NT Client Install. We selected during the installation for the client to check for updates on the server every 60 minutes. We configured the server to check for virus updates every day at 12:00 pm. We verified in the event log that the automatic download took place and was successful.

After the system downloaded the latest update we looked in the C:\Program Files\SAV folder and recorded the size of the XDB file that had been downloaded. This XDB file is what the Symantec application downloads and then uses to run the virus definition update on all clients. The XDB file uses the following naming convention, VDnnnnnn.XDB, where nnnnnn is the definition date and version. The information below explains the contents of the XDB file. This information was taken out of Symantec support document number 2002080815034048.

The XDB file is a ZIP file that contains the following:

- The current VDB file, but only with files needed by managed computers.
- A Catolog.dat file, used to decide which files in the VDB file are needed by various target computers.
- A number of microdefs patch files, ending in .IDB, each of which converts an older set of definitions to the current definitions. The IDB files are named VDnnnnnn.IDB, where nnnnnn is the version of the definitions that this IDB can be applied to. IDB files are also ZIP files.

McAfee VirusScan 7.0:

For McAfee we installed the ePolicy Orchestrator version 2.5.0 SP 1 on the server. Then we created a new group in the directory section of the ePolicy Orchestrator. After this we allowed the application to discover the client and server in the domain and record them in the newly created group. This allowed us to see each system in the ePolicy Orchestrator and to deploy the VirusScan software to each system. We deployed the software with the manufacturers default options.

To allow the server to automatically receive updates we installed McAfee AutoUpdate Architect 1.0.0 on the server. Then we setup the directory structure for the automatic update process. This directory structure consisted of two repositories, namely the source and master repositories. We configured the source repository to use the NAIHttp repository for the download of the updates. We configured the master repository to be a shared folder on the server.

For the automatic update process we configured a pull task that would download the updates from McAfee's website at 12:00 PM each day and place them in the shared folder on the master repository. Then we configured the client system to perform an auto update each day at 12:30 PM by checking for updates in the shared folder on the master server.

We insured the update process took place by looking in the AutoUpdate log each day. This log file detailed the time and steps taken during the update process. The log also detailed if the update was needed or not. If there was no update available the clients log would show that it was running the latest engine.

Each day we recorded the sizes of the files that were downloaded to the master repository. The downloaded files consisted of two types, the engine and the DAT files. We recorded the size of the folder and if there was a change in the files since the previous day.

Trend Micro OfficeScan 5.5:

We installed OfficeScan Corporate Edition on the server. After the installation on the server we used the OfficeScan Management Console to deploy the software to the client. We created a shared folder on the server for the automatic updates to download the software to. This shared folder contains a folder entitled "download" that has the engine and pattern updates. Each day we verified the contents of these folders and recorded the size if an update occurred.

We configured the automatic update with the OfficeScan management console. We configured the server to perform a daily update at 12:00 PM. Then we configured the client update so that if an update was received during the server update it would immediately deploy it to the client. We verified the update process with the logs for both the server and client in the OfficeScan management console.

Test results

This section provides the complete results for all testing we conducted. Please refer to the Test Methodology section for complete details of how we conducted each test.

Ease of installation and Deployment Test Results

This testing identified the overall experience of installation and deployment by recording the following information for all products tested:

- Time to install software on only one client
- Time to deploy application to all 15 clients
- Any problems encountered during deployment
- Deployment file size after installation

For each application we followed the manufacturer's documented installation procedure to deploy the software with the default settings and tools to multiple clients. We used the manufacturer management console and/or deployment tool on the server to deploy the software. Refer to the methodology for details of steps used for each application.

Figure 12 shows the results for the deployment of the software to one client. Sophos Anti-Virus required the least amount of time taking only 29 seconds to deploy and install their software. McAfee VirusScan required the most time taking 13 minutes and 6 seconds to install the software. Trend Micro OfficeScan took 30 seconds, Symantec AntiVirus took 1 minute and 45 seconds, and Reliable AntiVirus took 2 minutes and 2 seconds to install their software on one client. We did not encounter any issues with the application installation with any of the software installations.

Figure 12: Total time to deploy software to one client. (Time is recorded in minutes: seconds)

Figure 13 shows the software deployment times for each application deployed to 15 clients. Sophos Anti-Virus required the least amount of time to deploy their software to all clients requiring only 1 minute and 59 seconds. McAfee VirusScan required the most time to deploy their software requiring 13 minutes and 21 seconds. Reliable AntiVirus took 2 minutes and 15 seconds, Symantec AntiVirus took 2 minutes and 23 seconds, and Trend Micro OfficeScan took 6 minutes and 52 seconds to deploy their software to all 15 clients. We did not encounter any issues with the application installation with any of the software installations.
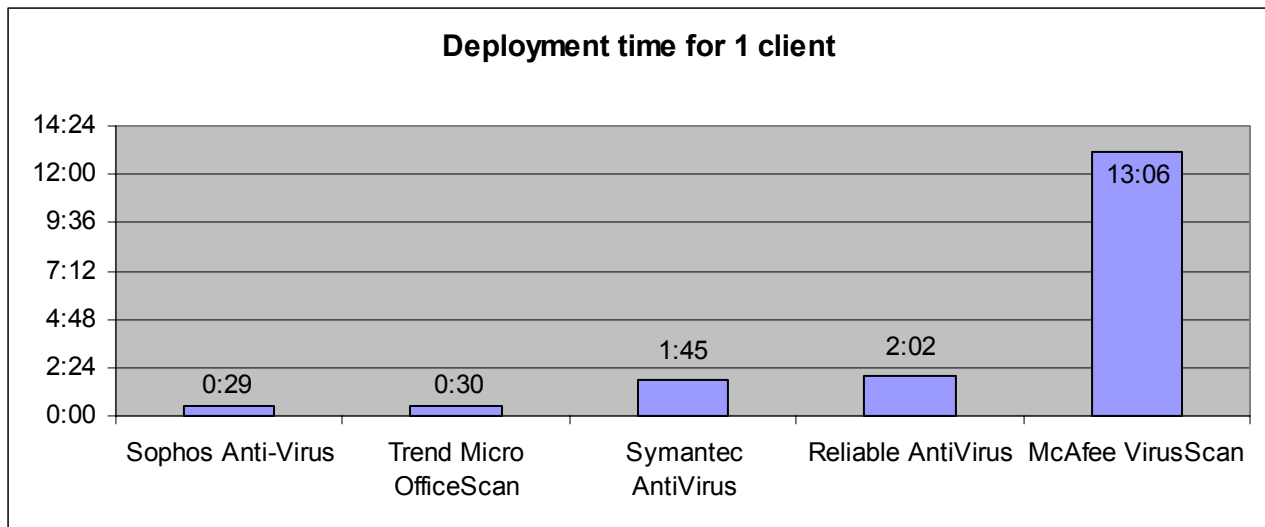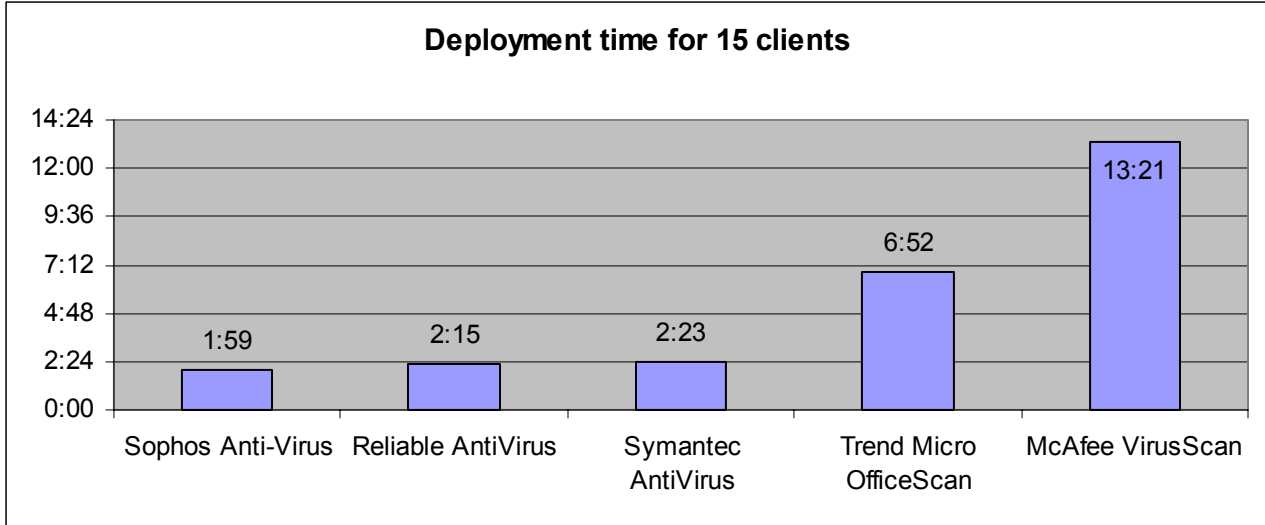
Deployment time for 15 clients

Application	Time
Sophos Anti-Virus	1:59
Reliable AntiVirus	2:15
Symantec AntiVirus	2:23
Trend Micro OfficeScan	6:52
McAfee VirusScan	13:21

Figure 13: Time to deploy software to 15 clients. (Time is recorded in minutes: seconds)

Figure 14 shows the total disk space used on the client system by each application under test after completing the software installation. Sophos Anti-Virus required the least amount of disk space at only 12.5 MB. Trend Micro OfficeScan required the most disk space at 38.2 MB. Included in the disk space used by Trend Micro OfficeScan is a 20 MB reserve file that gets installed on the system by default. This reserve file is placed on the system to allow the application room for updates. Installation of the reserve file can be deselected within the Trend Micro OfficeScan Management Console. The other applications required the following amount of disk space: Reliable AntiVirus required 13.1 MB, McAfee VirusScan required 21.2 MB, and Symantec AntiVirus required 34.3 MB.

Total Disk Space Used on Client by Application

Application	Disk Space (MB)
Sophos	12.5
RAV	13.1
McAfee	21.2
Symantec	34.3
Trend Micro	38.2

Figure 14: Total disk space used by application
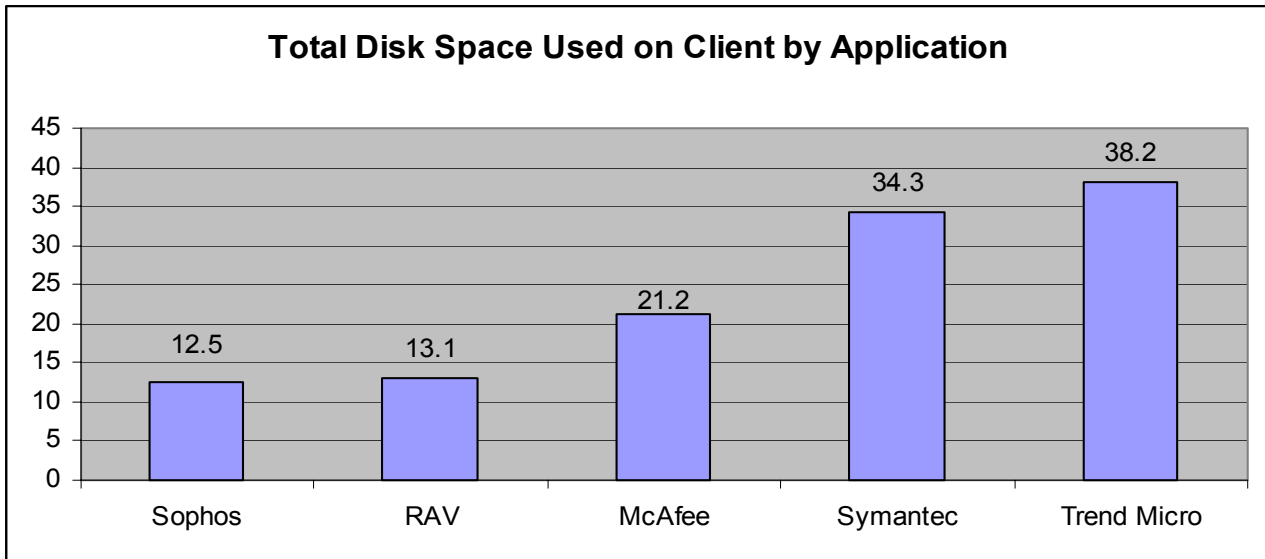
Scheduling Speed and Accuracy Test Results

In these tests, we evaluated the reliability and speed of each applications scanning ability. To verify the reliability of each application, we configured them to perform a full system scan at a specific time each day for three consecutive days. Figure 15 illustrates that Sophos Anti-Virus required the least amount of time to

perform the full system scan at 2 minutes and 18 seconds. Symantec AntiVirus required the most time to complete the full system scan requiring 6 minutes and 19 seconds.
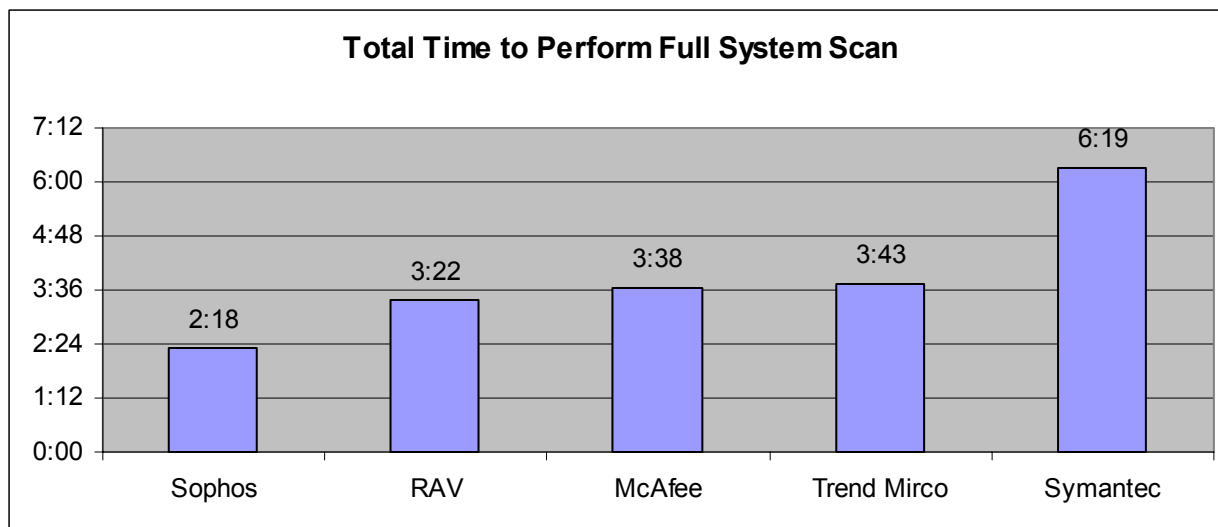
Total Time to Perform Full System Scan

Figure 15: Total time to perform a full system scan. (Time is recorded in minutes: seconds)

Virus Definition Updates Capabilities Test Results

In these tests we compared the frequency and size of virus definition updates provided by the manufacturer for each application under test. We did this by performing a manual and automatic update. For the manual update testing, we visited each manufacturer's web site and downloaded the latest virus definition update available. We performed this task once a day for ten consecutive days. For each download, we recorded the file size and verified its relevancy. To determine the relevancy of the file we compared the update information for that day's virus definition update to the update from the previous day. If the file was not adding any additional virus definitions then it was noted as not relevant because no actual update was required.

The results for the ten consecutive days of testing are shown below in Figure 17. The first day of testing, we downloaded a full update for each application under test in order to update each software application to the latest virus definitions available. For the remaining days of testing we only downloaded the daily updates for those products that provided this feature. Sophos Anti-Virus and Reliable AntiVirus were the only manufacturers that offer the daily update feature. The difference between the full and daily update is the full update includes all virus definition updates since the product was released. The daily update only provides the virus definition updates since the previous day. The advantage this offers the user is that download and installation times are shorter for the daily updates because they are significantly smaller compared to performing a full update.

Figure 16 shows the total cumulative file sizes for the manual download performed for 10 consecutive days. Sophos Anti-Virus' cumulative download totals were the lowest totaling only 136 KB. Symantec AntiVirus' cumulative totals were the greatest amount totaling 50513 KB. The cumulative totals for the other applications were as follows: RAV totaled 2216 KB, McAfee VirusScan totaled 8432 KB, and Trend Micro OfficeScan totaled 13178 KB. Figure 17 shows that Sophos and Symantec provided virus definition updates for 8 of the 10 days of testing. More frequent virus definition updates allows the user the opportunity to stay up-to-date with protection from the most recent viruses. In addition, Sophos and RAV provide the user with smaller update files, which take less time to download and install.
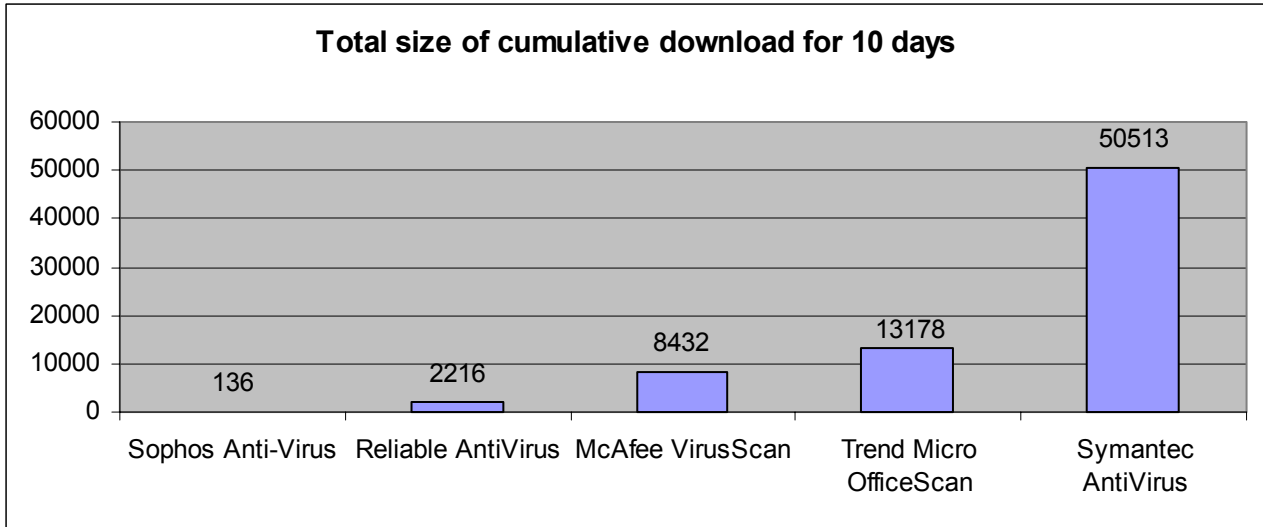
Total size of cumulative download for 10 days

Figure 16: Total size of cumulative manually downloaded files for 10 consecutive days. (File size is recorded in KB)

	7/14	7/15	7/16	7/17	7/18	7/19	7/20	7/21	7/22	7/23
McAfee	2,080	n/a	n/a	2,112	n/a	2,112	n/a	n/a	n/a	2,128
RAV	2,200	n/a	4	n/a	n/a	3	4	n/a	5	n/a
Sophos	108	4	2	2	6	n/a	n/a	5	7	2
Symantec	7,879	6,138	5,937	6,057	6,053	6,004	n/a	n/a	6,203	6,242
Trend Micro	6,730	n/a	3,217	n/a	n/a	n/a	n/a	n/a	n/a	3,231

Figure 17: Manual virus update file size in KB. (N/A symbolizes that no relevant update was available that day)

For the automatic update testing we compared the frequency and size of the provided virus definition updates available through each vendor's automatic update process. To do this we scheduled each of the five anti-virus programs to check for updates at 12:00 PM every day. Each application was setup to automatically check for updates and then download and deploy the new updates to their client system. Each day we recorded the file size of the automatically downloaded update.

Figure 18 shows the total cumulative file sizes for the automatic updates performed for 10 consecutive days. RAV's cumulative download totals were the lowest totaling only 417 KB. Trend Micro OfficeScan's cumulative totals were the greatest amount totaling 27300 KB. The cumulative totals for the other applications were as follows: Sophos totaled 419 KB, McAfee VirusScan totaled 10340 KB, and Symantec AntiVirus totaled 12466 KB. Figure 19 shows that Sophos provided virus definition updates for 6 of the 10 days of testing. More frequent virus definition updates allows the user the opportunity to stay up-to-date with protection from the most recent viruses. In addition, Sophos and RAV provide the user with smaller update files, which take less time to download and install.
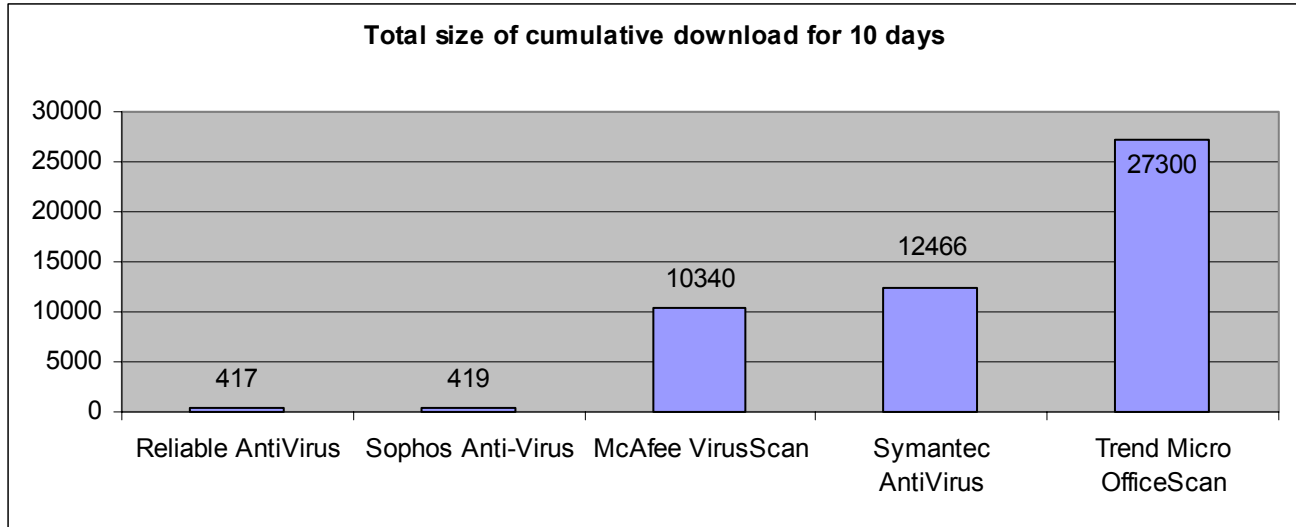
Total size of cumulative download for 10 days

Figure 18: Total size of cumulative automatic downloaded files for 10 consecutive days. (File size is recorded in KB)

	10/8	10/9	10/10	10/11	10/12	10/13	10/14	10/15	10/16	10/17
McAfee	n/a	5,170	n/a	n/a	n/a	n/a	n/a	n/a	5,170	n/a
RAV	n/a	98	n/a	n/a	n/a	n/a	101	102	n/a	116
Sophos	2	83	82	n/a	n/a	n/a	82	84	n/a	86
Symantec	n/a	6,173	n/a	n/a	n/a	n/a	n/a	n/a	6,293	n/a
Trend Micro	6,810	n/a	6,560	n/a	n/a	n/a	7,070	n/a	6,860	n/a

Figure 19: Automatic virus update file size in KB. (N/A symbolizes that no relevant update was available that day)

In addition to recording the manufacturers update procedure, we also evaluated their email notification process. To do this, we subscribed to the email notification process for each of the applications that offered this as a free service. All of the manufacturers offered this as free service except Symantec. Symantec does offer this service but it is part of a platinum level service agreement that must be purchased through the manufacturer. Therefore, we do not have any results pertaining to Symantec's email notification process.

Sophos is the only manufacturer that provided a virus update email notification on a daily basis to coincide with their definition updates. Each day that a virus definition update was available, we received email to notify us that an update was available. In addition to the notification, the email included a link to Sophos' webpage that described the virus update in detail. McAfee also sent us an email notification on the days that their updates were available but their update only informed us that the update was available. The McAfee update did not have much information regarding the virus definitions included in the update or any link to explain about the associated viruses.

Trend Micro sent out a weekly virus report. This report included information about the ten most prevalent viruses for that week. In addition, they included all the information regarding one virus to help educate the recipient about different viruses. Lastly, they included the information about the latest virus and software dates so the recipient could easily identify if they were running the correct versions or not.

RAV did not send us any email notification regarding virus definition updates for the entire ten days of testing. We subscribed to the RAV email notification on their website. After we subscribed, we received an email notifying us that we had subscribed to their outbreak notification list. The email did not inform us that any further action was required, but we never received any other information from RAV.

Appendix

A. Software used for testing

- McAfee VirusScan Enterprise 7.0
- McAfee ePolicy Orchestrator 2.5.1
- Rational Visual Test 6.5
- RAV AntiVirus 8.6
- RAV Deployment Tool 1.1
- Sophos Anti-Virus version 3.70
- Sophos SAVAdmin in Enterprise Manager 1.1
- Symantec AntiVirus Enterprise Edition 8.6
- Symantec System Center for SAV version 8
- Sysinternal Filemon for Windows v6.07
- Trend Micro OfficeScan Corporate Edition 5.5
- Trend Micro OfficeScan Management Console

B. Hardware used for testing

Dell / PowerEdge 350	
Processor / Speed / # of CPUs	Pentium III / 850 / 1
System RAM / Type / # of Slots	256 MB / SDRAM / 1
L2 Cache	256 KB
BIOS / Version / Date	PowerEdge 350 Bios / A08 / 3-19-2001
HD Make / Model / Size	Maxtor / 5T010H1 / 10 GB
HD Controller	Intel 82371AB/EB PCI
Graphics Adapter	ATI Rage XL
NIC / Driver	Intel Pro 10/100 MB
CD-ROM Make / Model	TEAC CD-224E
Operating System	Microsoft Windows 2000 Advanced Server
Service Pack Installed	SP 3 or SP 4

Figure 20: Server systems

Dell / PowerEdge 350	
Processor / Speed / # of CPUs	Pentium III / 850 / 1
System RAM / Type / # of Slots	256 MB / SDRAM / 1
L2 Cache	256 KB
BIOS / Version / Date	PowerEdge 350 Bios / A08 / 3-19-2001
HD Make / Model / Size	Maxtor / 5T010H1 / 10 GB
HD Controller	Intel 82371AB/EB PCI
Graphics Adapter	ATI Rage XL
NIC / Driver	Intel Pro 10/100 MB
CD-ROM Make / Model	TEAC CD-224E
Operating System	Microsoft Windows 2000 Professional
Service Pack Installed	SP 3 or SP 4

Figure 21: Client systems

Extreme Networks / Summit 48	
Software Version	4.1.19b2

Figure 22: Network switch

C: Rational Visual Test script used for RAV deployment

```
'$INCLUDE 'RECORDER.INC'

SetDefaultWaitTimeout(Timeout)
        Global returnstatus      As Long
Scenario "svs"
        'Minimize the Visual Test window.
        If GetHandle(GH_HWNDCLIENT) Then WMinWnd(GetHandle(GH_HWNDCLIENT))

        ' Check the resolution that this script was recorded on.

    returnstatus = 0
    while returnstatus <> -1
        returnstatus = EXISTS ( "c:\winnt\tasks\rav_install*.*" )
    sleep 1

        Wend
        while returnstatus = -1
        returnstatus = EXISTS ( "c:\winnt\tasks\rav_install*.*" )
    sleep 1

        Wend

        sleep (2)
        EXITWINDOWS

End Scenario
```

VeriTest (www.veritest.com), the testing division of Lionbridge Technologies, Inc., provides outsourced testing solutions that maximize revenue and reduce costs for our clients. For companies who use high-tech products as well as those who produce them, smoothly functioning technology is essential to business success. VeriTest helps our clients identify and correct technology problems in their products and in their line of business applications by providing the widest range of testing services available.

VeriTest created the suite of industry-standard benchmark software that includes WebBench, NetBench, Winstone, and WinBench. We've distributed over 20 million copies of these tools, which are in use at every one of the 2001 Fortune 100 companies. Our Internet BenchMark service provides the definitive ratings for Internet Service Providers in the US, Canada, and the UK.

Under our former names of ZD Labs and eTesting Labs, and as part of VeriTest since July of 2002, we have delivered rigorous, objective, independent testing and analysis for over a decade. With the most knowledgeable staff in the business, testing facilities around the world, and almost 1,600 dedicated network PCs, VeriTest offers our clients the expertise and equipment necessary to meet all their testing needs.

For more information email us at info@veritest.com or call us at 919-380-2800.