Anti-Virus Software Solution at JPL

David P. Gilliam, Ph.D.

The Jet Propulsion Laboratory, California Institute of Technology
Pasadena, CA. 91109

Abstract:

The growth of inter- and intranets and the sharing of information has led to a rise in the transmission of viruses, especially among the PC and MAC platforms. Due to the rising cost of fighting comptuer viruses, virus protection is essential for any organization. However, virus protection is difficult and costly to implement and maintain. The Jet Propulsion Laboratory has had problems maintaining current virus protection software and pattern files and there has been an increase in calls for assistance with virus problems. The problem was NASA-wide. NASA asked the JPL Network and Computer Security Group to lead an effort to search for a comprehensive solution to this problem. After careful research and testing, a single-vendor solution was selected. Following the vendor selection, the product was re-tested for deployment, and issues and problems were documented and resolved with the vendor. The deployment, although not without difficulties, was successful. Several lessons were learned in this effort to find and deploy a single-vendor, multiple-platform software solution that may benefit other organizations facing a similar situation.

Key words:

Anti-Virus, JPL, NASA, Evaluation, Software Deployment, Software Solution, Datawatch® Virex VET, Dr. Solomon's Anti-Virus Toolkit, McAfee NetShield Viruscan, Symantec Norton Anti-Virus, Intel LANDesk® Virus Protect

Author:

David P. Gilliam, Ph.D.
Jet Propulsion Lab
4800 Oak Grove Dr., MS 144-210
Pasadena, CA 91109-8099
Phone: (818) 354-0900
FAX: (818) 393-1377
E-mail: david.p.gilliam@jpl.nasa.gov

Anti-Virus Software Solution at JPL

• Abstract

The growth of inter- and intranets and the sharing of information has led to a rise in the transmission of viruses, especially among the PC and MAC platforms. Due to the rising cost of fighting comptuer viruses, virus protection is essential for any organization. However, virus protection is difficult and costly to implement and maintain. The Jet Propulsion Laboratory has had problems maintaining current virus protection software and pattern files and there has been an increase in calls for assistance with virus problems. The problem was NASA-wide. NASA asked the JPL Network and Computer Security Group to lead an effort to search for a comprehensive solution to this problem. After careful research and testing, a single-vendor solution was selected. Following the vendor selection, the product was re-tested for deployment, and issues and problems were documented and resolved with the vendor. The deployment, although not without difficulties, was successful. Several lessons were learned in this effort to find and deploy a single-vendor, multi-platform software solution which may be of benefit to other organizations facing a similar situation.

• Background

1. Multi-vendor, multi-platform problem

   Maintaining current virus protection software and pattern updates is a monumental problem for any large organization, especially when the organization supports multiple platforms and operating systems (OS's). The training of helpdesk personnel to support the software on the different platforms is a major cost in dollars and time. In the past, vendors have provided solutions for a single platform. Today vendors are attempting to provide solutions across platforms as seen by Dr. Solomon's recent acquisition of Datawest's Virex.

   Traditionally, the Jet Propulsion Lab (JPL) allows and supports multiple OS's and platforms. There are approximately 10,000 Personal Computers (PC) and Macintosh (MAC) worstations, and over 600 Novell and Windows NT servers. In addition, there are numerous unix workstations and servers of varying kinds, mid-range, mainframes and super computers. The decision as to what type of hardware and software to purchase for these systems traditionally has been left up to the individual organizations and projects based on their particular requirements. However, JPL has been moving to standardize its micro computer hardware, OS's and core software.

One major component of standardization is in the area of virus protection software. JPL had a variety of anti-virus software for the different platforms and OS's and a number of systems, including servers, had no protection at all. Virus protection was left up to the users or System Administrators (SAs) to make sure that their systems were protected. The Network and Computer Security (NCS) Group had one full-time and two part-time personnel assisting users and SAs with virus assistance calls.

2. Lack of consistent knowledge-base and regular updates

At JPL, calls for assistance with viruses continued to increase. SAs needed assistance for installing and maintaining anti-virus software on their servers. A knowledge-base for the various anti-virus products was not available making assistance in installing, configuring and troubleshooting anti-virus software difficult and time-consuming. JPL was in a reactive mode of operation. Throwing more personnel at handling the virus calls was deemed only a temporary, quick-fix solution. What really was needed was a good pro-active solution.

3. Need for single-vendor solution across PC and MAC platforms

The number of NT servers being deployed at JPL increased steadily during the past three years. JPL had no supported anti-virus software for them. There were also problems with maintaining updates for the supported anti-virus software on the other systems. A comprehensive solution for the PC and MAC workstation and server platforms was needed to alleviate the growing problem, especially installing and maintaining current anti-virus software and pattern files. The problem was also a NASA-wide issue, and the JPL NCS Group was asked to lead the effort to find, if possible, a single-solution package, compatible with NASA usage at no additional cost. Searching for a comprehensive product was difficult. Even more difficult was the planning for a major deployment of the anti-virus software for more than 10,000 micro computers and 600 servers.

• Evaluating & Selecting a Cross-Platform Product

1. Search for a single-vendor solution

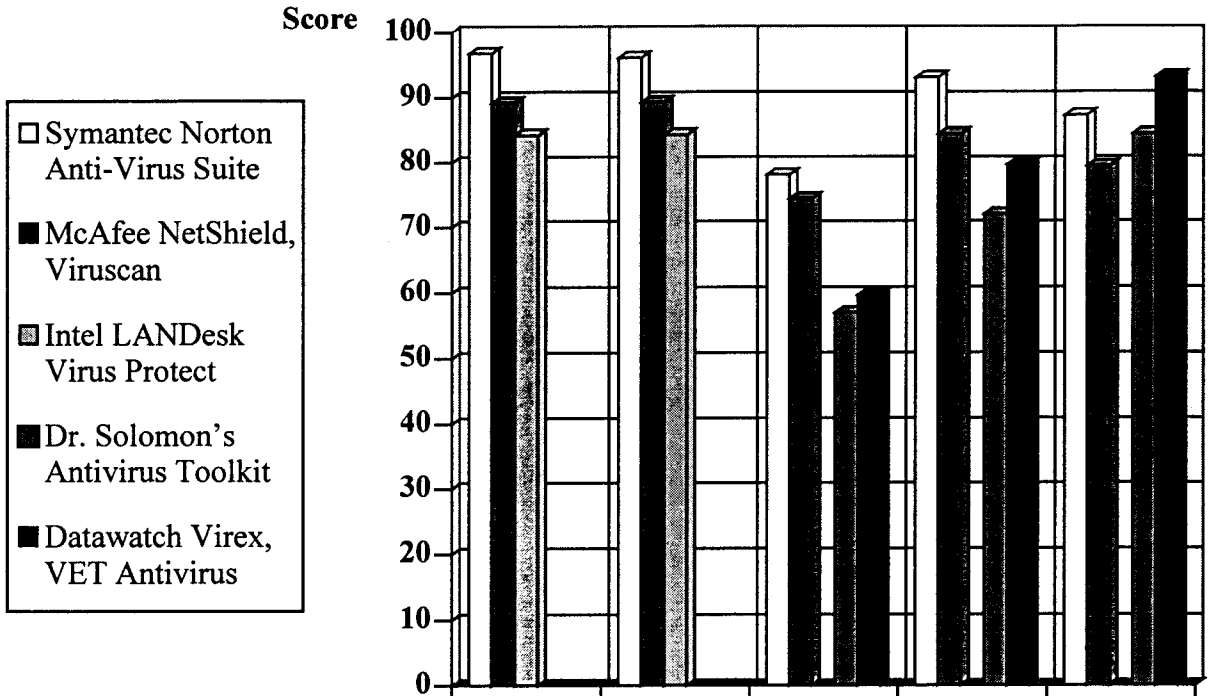
The NCS Group evaluated the needs of the JPL and NASA communities for virus protection. Requirements were developed and major anti-virus software vendors were contacted describing the requirements. Vendor packages that met the general requirements were selected for evaluation: The primary vendors were: Virex/VET Anti-Virus by Datawatch® (Version9.4.1); Dr. Solomon's Anti-Virus Toolkit (Version 1.07); Intel LANDesk® Virus Protect; McAfee Netshield/Viruscan; Symantec Norton Anti-virus (Version 2.0).

Four products made it to the final evaluation for DOS/Windows and MAC: Datawatch® Virex and VET, McAfee Viruscan, Dr. Solomon's Anti-Virus Toolkit, and Symantec Norton Anti-Virus. Three products made it to the final evaluation for the servers: Symantec Norton Anti-Virus, McAfee Netshield, and Intel LANDesk® Virus Protect.

2. Evaluation criteria

The evaluation was based on the criteria and weighting shown in the *Appendix*. The evaluation included multiple platform support, regular update procedures (including live update capabilities), on-going development, helpdesk support, scanning capability against a set of known viruses to determine error rate detection, cleaning, responding to system infection, scan rates, memory requirements, etc. The primary categories and weighting were: Performance—40%, Reliability—20%, Maintainability—20% and Costs—20%. A lab was set up on a self-contained network which included Novell 3.12, Windows NT 4.0 SP3+ server, Windows 95, Windows3.x/DOS, and a PowerMac 8100 OS 7.5. Testing was performed against specified criteria on a stand-alone network. The final results were:

Evalution Results



Product	Novell	NT	Windows 95	DOS/ Windows	Macintosh
Symantec Norton Anti-Virus Suite	96.8	96.1	78.1	93.1	87.3
McAfee NetShield, Viruscan	89.2	89.3	74.4	84.4	79.4
Intel LANDesk Virus Protect	84.2	84.3	NA	NA	NA
Dr. Solomon's Antivirus Toolkit	NA	NA	57	72	84.4
Datawatch Virex, VET Antivirus	NA	NA	59.7	79.7	93.2

Symantec Norton Anti-Virus Suite scored the highest in all categories except for the MAC platform where Datawatch Virex scored the highest. Since the scores between Symantec and Datawatch were close on the MAC platform and a single-solution vendor for anti-virus was preferred, the Symantec product was selected as the best choice for the JPL and NASA environments on the PC and MAC workstation and server platforms.

3. Some general comments

Intel LanDesk:

a) The package does not maintain its own activity logs. If a large number of viruses are discovered on an NT server, it can quickly fill up the NT logs. Any activity occurring after the log is full will not be recorded until the Administrator clears the application log. b) The package supports the Simple Network Management Protocol (SNMP). c) The package provides the option of executing a program upon a virus alert. d) The package only offers workstations protection if they are logging into a Server that is protected.

McAfee Vhsield:

a) The auto autoupdate feature requires the writing of a script (Symantec performs this operation with a push of a button). b) The Product Support Group can be reached easily by email. c) On a server, the product gives the option of executing a program once a virus is detected. It also allows the assigning of priorities to alerts. d) The product supports SNMP.

Symantec Norton Anti-virus:

a) The product can monitor floppy disks when working with them, including the scanning of the disk on shutdown if it is left in the drive. b) Symantec provides relay of alerts via email or a server setup to centrally process all alerts. c) The product always makes backup files before attempting a repair. d) It provides an automatic live update feature that monthly updates pattern files. It also allows modification of the update host file to access another update site. The live update proxy server function, however, does not work with firewalls.

Datawatch VET Antivirus and Dr. Solomon's Anti-Virus Toolkit:

These two products were management packages for workstation anti-virus software and not true Server products. They manage the installation and updating of anti-virus software on Windows 3.x, Windows 95, and Windows NT workstations with the intent that if the workstations can be kept clean, then the Server will be safe. In a homogeneous environment such an assumption would be safe. However, in the NASA environment there is a heterogeneous mix of platforms including Unix workstations running Microsoft Office products. With the advent of macro viruses (esp. Microsoft Word and Excel Macro Viruses), the scheme of protecting the workstations with the view that the servers will also be protected, is no longer true. Neither product made it to the final Server evaluation.

4. Final selection for NASA-wide site license

After rigorous testing and evaluation of the products against the JPL and NASA requirements, Symantec's Norton Antiv-Virus software was selected. While all the products performed well, Symantec performed the best overall. Out of the twenty-five criteria requirements, Intel and McAfee met twenty-two of them and Symantec met twenty-four.

- **Re-testing of Selected Product for Deployment Issues/Problems**

1. Testing for deployment

After the selection process, a deployment plan was implemented. Symantec had just released a major upgrade to its product shortly after its selection. Testing on the new version was needed immediately since the anti-virus deployment was scheduled.

Testing was extended to include other OS's and platforms. Besides the original OS's (NT 4.0 SP3+ server, Novell 3.12, Windows 95, Windows3.x/DOS and MAC 8100 OS 7.5.1), testing included Windows 3.1x/DOS, NT 3.51 SP5, NT 4.0 SP3+ workstations on various brands of PCs, other MAC workstations with OS 7.1 through 7.6, and a Novell 4.11 server. Not tested were multi-processor NT and Novell Servers due to lack of their availability. Deployment issues were the focus of this testing—uninstalling previous anti-virus software, installing the Symantec software, standard configuration parameters and update procedures. The testing included identifying problems and concerns during and following installation on the various platforms and OS's. The issues and problems were noted and incorporated into the user documentation. A knowledge-base is also being developed for keyword searching.

2. Deployment test team

Testing was divided between the NCS Group, JPL Helpdesk Core Product Group and SAs who volunteered to assist. During the deployment test phase, several problems were encountered that were not discovered in the evaluation phase.

3. Problems encountered

The following problems, some specific to JPL, were discovered:

a) The live update process needed to be re-configured to access a local ftp site for updates rather than the Symantec site so that updates could be tested prior to their release to the JPL community.

b) There were no live updaters for MACs or for Novell servers. A work-around solution for MACs was to send out messages to MAC users when updates were available on the MAC support server for downloading and rely on the users to get the new files; the solution for Novell servers in the NDS Tree, was to have the software installed in the same location on all servers (SYS:System\Nav directory), then have the updates

replicated to the servers from the master server. For Novell servers not in the NDS Tree, the SAs would be notified of updates so they could manually download them.

c) Security firewalls required a work-around for accessing the local ftp site. Unfortunately, the proxy server option did not function in the live-updater. The solution for this problem was to rebuild a specific live update package for workstations behind a firewall. For each firewall, the live update parameters would include the name of the ftp site (Number field) and the Login Name. Since the live-update software would not allow special characters in the Login Name field (*viz.* the '@" symbol), an additional step was needed which had the proxy server transpose a '!' into an '@' symbol. The proxy server name was placed in the Number field. All PCs behind the firewall were given this new update host file.

d) MACs needed to have the initial memory size increased to 4MB or greater to install the product with the later virus pattern files. The original size caused the MAC to fail during installation due to memory constraints. The problem was not discovered during the initial phase as the pattern files were smaller. This memory increase had to be built into the software and repackaged into a compressed format. The Symantec Anti-Virus for Macintosh (SAM) intercept updater was used to allocate additional memory space for itself to accommodate the larger virus pattern files. The Administrator Tool was used to create a complete package for the MAC that included the standard software, updated pattern files and the SAM intercept updater.

e) PCs using Win3.1x/DOS running Lotus cc:Mail needed to have the win.ini file modified in the Symantec section, changing the Share from 1 to 0.

f) Due to limited resources, testing was not performed on dual processor servers or workstations. Testing was also not performed on NT Alpha stations.

- **Deploying the Product**

1. Deployment documentation

Documentation with screen images both for uninstalling old products and installing the new product was written and tested for the JPL/NASA environment. The documentation required several review and testing cycles to ensure that it was easy to follow, especially for the novice, to limit the number of Helpdesk case calls for basic installation assistance. More attention could then be focused on the expected virus calls that the anti-virus software would find during installation and on other user specific issues or problems.

2. Deployment process

The deployment process required enlisting support of the SAs, to augment the Helpdesk support personnel. The number of available Helpdesk personnel was insufficient to handle the expected large number of virus and installation calls on initial deployment. It was decided that support from the SAs was essential for a successful deployment.

Two information sessions, one for the general community and one for SAs were given. At both sessions handouts were distributed which briefly described where to get the anti-virus software and the installation documentation, and how to install the product on each of the PC and MAC platforms. The sessions were well received and the SAs agreed to assist in deploying the product. Enlisting the support of the SAs was critical as they would be the ones performing the majority of installations.

Another critical area was having sites readily available where SAs and users could download and install the software. JPL did not want a huge network load increase from users accessing the servers all at once. The load on the servers and the backbone by a large number of users trying to install the product simultaneously could potentially cripple other networking activities. Three platforms were setup for providing the software: a) Helpdesk servers for MACs and PCs; b) Andrew File System (AFS) for users on AFS servers; c) Security web server. This last platform proved to be the most effective means for providing the software. It created less network load, fewer problems and glitches during installation. The product was zipped into a single compressed executable which then could be downloaded and executed on a server or workstation. Running the setup from the Helpdesk servers resulted in installation problems for users when the network load was high.

- **Helpdesk & Troubleshooting**

Problems encountered:

1. Uninstalling the current anti-virus software on MACs required manually removing the extensions, including the hidden files of the software. However, it should be noted that no problems were encountered if they were not removed.

2. Uninstalling the McAfee Vshield anti-virus software on PCs created problems if the user was also using Remedy and removed the shared files. Remedy had to be re-installed if the shared files were removed. The uninstall documentation included a warning about this problem and suggested that shared files not be removed.

3. During the deployment phase, the Helpdesk support staff was to be trained on how to download and install the anti-virus software. The NCS Group and the Core Products Support Group were to be used for second level support. However, the reality was that the NCS Group handled the majority of the calls and trouble-shooting issues as the SAs and the Helpdesk personnel were concurrently being outsourced and were in a stage of transitioning to a new contracting company. The result was a lack of training for Helpdesk personnel.

4. Maintaining current updates lagged. Since updates needed to be tested for the JPL environment and there were insufficient personnel to do this during the outsource transition period, updates were slow to be placed on the JPL ftp live-update site.

5. An installation on a dual processor ALR NT40 server caused the server to crash. The only way to resolve the problem was to reinstall the product during a non high-use time and get a core dump from the server and send it to Symantec for inspection.

6. It was discovered after the deployment, that scanning of MAC volumes on an NT server would only catch macro viruses. Symantec acknowledged the problem and suggested that MAC volumes on servers be regularly scanned using a protected MAC workstation.

7. The script for performing the live updates needed revision to make sure the registry on NT and Windows 95 machines acknowledge the latest date and time stamp of updates.

8. The helpdesk server required upgrading to handle the heavier load of requests and accesses due, in part, to being the primary point for obtaining virus protection software. This problem was not discovered until several users began performing simultaneous installs from the server. The Security web server then became the primary source for the software.

• Lessons Learned

Many lessons were learned in tackling a major deployment of a core software product.

1. Testing needed to be more inclusive prior to deployment. The problems encountered with the Macs, Mac volumes on the NT servers, and the Dual Processor NT stations could have been caught with more time and resources used in the testing phase.

2. The training of Helpdesk personnel should be completed prior to the deployment. Some of the users felt they were going in circles getting someone from the Helpdesk to come out and support them with the installation when they had problems. Also, more Helpdesk personnel should be assigned to answering calls for assistance during the initial deployment phase.

3. The Helpdesk server was not robust enough to handle a large number of simultaneous requests to perform a software setup. A better solution was creating a compressed executable package that could be downloaded from a web server then executed.

4. Having three sites for downloading/installing the software proved a problem for configuration control. A replicated web site on a fast server with pointers to it from the other locations appears to be a more viable solution for making sure that all users are getting the latest supported software and documentation.

• Acknowledgements

I wish to thank members of the NCS Group for their inputs and assistance: Brent Mead, NCS Group Supervisor, who led the effort in evaluating and procuring the cross-platform anti-virus software and ensuring the deployment dates were met, Tom Dearmond, Group Leader, Bahram Chaudhry, Russell Kirkpatrick, Charles Mobley, Behshad Sedighi and Josef

Sherif. I also wish to thank the team of software evaluators for their efforts: The Core Products Group Leader, Alan Stepakoff who led the testing and deployment effort, Darrell Duley, Jeff Knecht, Jack Kobzeff, Joel Petz, Saeed Shapourifar, Martin Short and the tireless efforts of Doug Gordon who also setup the FTP update site.

APPENDIX

Criteria For Screening Anti-Virus Software

Performance (Weight 40%)

Performance is a key issue for the use of any type of software, it is particularly important when deciding on a virus protection package. There are a number of performance issues that must be addressed when considering an anti-viral package. The following are critical criteria:

1. Is this package user friendly? (Wt. 1.9)

    a. How easy is it to install? (Wt.38)
    b. How long does it take to install? (Wt.38)
    c. Can it be uninstalled? (Wt.38)
    d. How easy is it to use? (Wt.38)
    e. How long does it take to run? (Wt.38)

2. Does this package provide memory resident virus protection? (Wt. 1.9)

3. Can this package support non-direct disk access (e.g. zip, jaz, Bournulli, tapes)? (Wt. 1.9)

4. Can this package be configured to automatically (timed run/off peak hour) schedule hard drive scanning? (Wt. 1.9)

5. Does this package provide boot sector protection? (Wt. 1.9)

6. Does this package provide virus alert capabilities (workstation and network)? (Wt. 1.9)

7. Is this package capable of providing centralized network administration? (Wt. 1.9)

8. Does this package have the capability of automatically preempting scanning for more critical system tasks? (Wt. 1.9)

9. Can this package be configured not to allow infected files to be copied or run? (Wt. 1.9)

10. Does this package detect and eradicate viruses including variants, e.g., polymorphic, stealth, multipartite, and encrypted viruses? (Wt. 1.9)

11. Does this package detect and eradicate macro viruses? (Wt. 1.9)

12. Does this package allow files to be selected for scanning by type using custom as well as standard file extensions? (Wt. 1.9)

13. Does this package create activity logs? (Wt. 1.9)

14. Can this package be configured to scan for virus-like activity (unknown viruses)? (Wt. 1.9)

15. Is this package capable of inoculating files? (Wt. 1.9)

16. Is this package capable of restoring files? (Wt. 1.9)

17. Can this package be configured to deny network access unless anti-virus software is running on the workstation? (Wt. 1.9)

18. Does this package provide transaction monitoring? (Wt. 1.9)
What impact does this have on server performance?

19. Is this package capable of interoperating with existing software products? (Wt. 1.9)
What impact does it have on installed (running) software?

20. Is this package capable of scanning compressed and archived files? (Wt. 1.9)

21. Does this package allow for the creation of a rescue diskette? (Wt. 1.9)

Reliability (Weight 20%)

The reliability of the anti-viral package is an important issue. How consistent is this anti-viral package compared to similar products?

1. Is this package self-examining? (Wt. 5)

2. Does this package perform consistently on different configurations? (Wt. 5)

3. What is this the detection rate of this package? (Wt. 5)

4. Does this package give false positive indicators? (Wt. 5)

Maintainability (Weight 20%)

Maintainability of the software is another issue that must be addressed. The following are maintenance issues that must be addressed:

1. Does the vendor stay abreast of current virus threats; covers all known viruses; releases periodic product updates? (Wt.10)

2. Is this package capable of automated distribution of software releases? (Wt.10)

Cost Factor (20%)

Cost of the product to NASA is a major concern. Famililarity of users and helpdesk personnel within NASA on the anti-virus product must be considered. Their training/re-training has to be taken into account as a factor of cost. The following considerations need to be addressed:

1. What are the initial costs?

2. What are the maintenance costs?

3. Will the vendor give price breaks on use of their other vendor anti-virus products with the evaluated product?

4. Will the vendor give price breaks to use their product over a product already in use at a NASA center?

5. How many NASA Centers use the vendor's product?

6. Are NASA Centers satisfied with the vendor's product?

Detection Rate Results for Two Platforms: The tests were run on a Compaq Deskpro 4000.

NT 4.0 SP3+ SERVER, DETECTION RATES:

PRODUCT	# OF FILES SCANNED	# OF VIRUSES DETECTED	TIME
McAfee NetShield	7,430	5,974	28 min.
Intel LANDesk Vprotect	8.083	5,952	24 min.
Symantec Norton Anti-virus	7,621	5,891	28 min.

WINDOWS 95 DETECTION RATES:

PRODUCT	# OF FILES SCANNED	# OF VIRUSES DETECTED	TIME
Dr. Solomon's Toolkit	6,452	6,053	14 min.
McAfee Vshield	7,474	5,975	21 min.
DataWatch VET/Virex	7,005	4,639	10 min.
Symantec Norton Anti-virus	7,610	5,890	20 min.