Global Information Assurance Certification Paper

What to Look for in your Anti-Virus Solution?
David Poston
22 June 2002

Introduction

Vendors, Vendors, Vendors, what are all of the Anti-Virus sales people talking about? Is there a real difference among the Anti-Virus Vendors? Who should I choose?

http://www3.ca.com/virus/ Computer Associates
http://www.f-secure.com/ F-Secure
http://www.mcafee.com McAfee
http://www.pandasoftware.com/ Panda
http://www.sophos.com/ Sophos
http://www.symantec.com Symantec
http://antivirus.com Trend Micro
and the list goes on……

An Anti-Virus Vendor is trying to sell you a product to help secure your environment. Now choosing the best one is the challenge. There should be a couple of thing to look for that the vendor isn't telling you, yes reporting is nice, but reporting does not stop viruses. I hope to bring these points to light.

How easy to deploy?
Is it hard to update?
Does it catch viruses?
Once I find something what can I do with it?
Am I finding everything that I should?
How much does it cost?

I hope to clear some of these questions, and ask some more. I hope to assist you in making a logical choice in selecting an Anti-Virus product, unless you just want a vendor shirt, mug, or other freebie.

Client and Server

Lets start at the client/server level; I'm assuming you have determined a need for protection against malicious code impacting this host. I'm also assuming that we are not talking about any retail anti-virus products, enterprise/corporate products only. When I do mention servers in this section, I am referring to protecting the servers local operating and files systems only, Not MS Exchange or Lotus Notes etc. This should be a pilot implementation on a test network, no production machines. You are loading code for the 1st time. Will it work? Will it crash my server? Will I see a Blue Screen? I hope you understand, if not you will find out.

Read the documentation 1st (RTFM), you now should be ready to start the evaluation process. Some Anti-Virus vendor have one product for clients and another for servers, some have the same product for clients and server. Do you really want to manage two pieces of software? Two software packages have more administration overhead, helpdesk cost, virus administration cost, and twice the software inventory to maintain.

During deployment you may/will need administrator access to load the management console, if it has one. A management console may deploy anti-virus software or just manage it once deployed. Some products require an agent to be deployed, then anti-virus software. Here we go again with maintaining, updating, and managing another piece of software. I bet your corporate base-line/imaging group is going to love this? Also why would you need to buy additional software to manage your anti-virus product? Shouldn't this be included?

A virus policy needs to be set, type of protection, scanning time, schedule updates, and client/server/agent check in times, alert messages and any other configurable settings that need to be adjusted.

Now it is time for deployment, there are numerous ways to deploy anti-virus software, through the console, agent deployment, creating an .exe or .msi package, MS SMS, Tivoli, Zen Works or off of the cd. There may be more ways not list or some not supported by every vendor, but you've read the manual, and know the deployment methods.

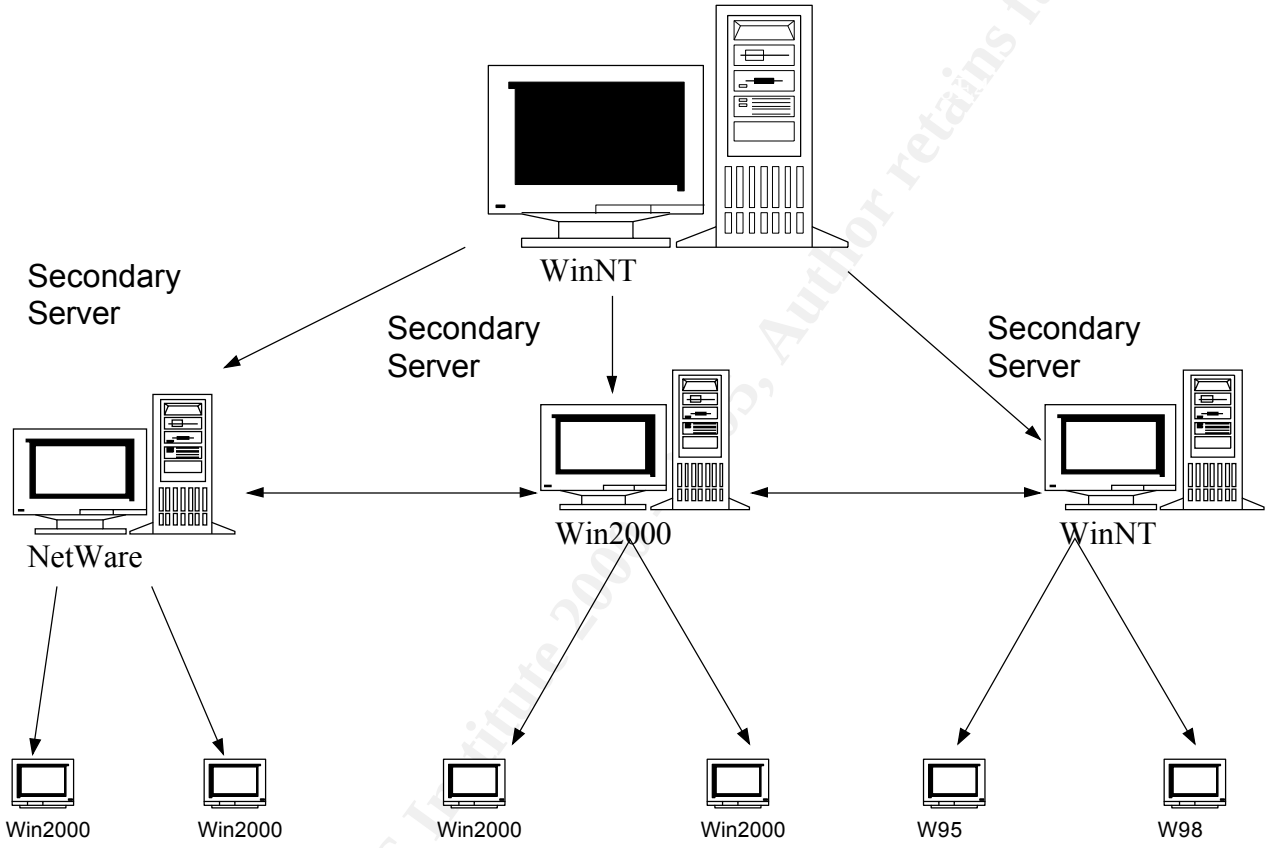
Clients/agents report to a server, for anti-virus policy changes, definitions/dats, and reporting of infected clients. This client to server scalability is different for each vendor. One vendor claims that they can support 250,000 clients to one server. If this has some type of random polling period between the client and server, it may work. During an outbreak where you need to tell every client to update itself, this is a major bottleneck. 250,000 clients trying to access one server on one a network, downloading a 50K file, will have a major impact on LAN traffic.
250,000 clients to one server reference was found at:
http://corporate.mcafee.com/content/software_products/avd_compare_epolicy.asp

Once the clients receive this policy, it may state that the client go to another server and then download definitions/dats files which range in size from 100K through 5 meg. Will you network be able to take this load? If you're a small company a small server will work, what happens over 5000 users? You will need to upgrade to a multi-processor server.

What happens if your one and only server crashes? Rebuild the server as

fast as possible, with the same name and IP address. Hopefully a bad set of definitions/dats didn't cause the crash to this server or how will you deploy new definitions/dats to all of your clients? One server is one point of failure.

Another way to deploy configuration changes or definitions/dats files is a hierarchical deployment. Having a master server that communicates to secondary servers that communicates to clients. This distributed type system allows for a faster and more scaleable deployment of virus policy or definitions/dats files. Current servers deployed in your environment may be used in this deployment method, without the need to purchase additional hardware.



Definitions/Dats

Has an anti-virus vendor ever release a set of definitions/dats files that were corrupt or alerted on a false positive, or cause a system to crash? A false positive is when the anti-virus software says a file is infected when it's not. This could be a major problem if this is a system file and your policy states to delete infected files that cannot be cleaned. When you or a user reboots I'm sure you will find the problem. The answer to the above, is yes; all of the vendors have

released a bad set of definitions/dats files. Now the problem is how do to deal with it. Here are a few solutions:

1. Wait another 3 hours or so for the vendor to release a new set of definitions/dats files. How can this impact the CEO's desktop, companies file servers, or even you company's public web server?
2. Remove and reload the anti-virus software, this will need a reboot or two. Then only update the definitions/dats files to a known good state. How many hours could be lost if this was one of your choices?
3. A better answer is to have the ability to roll the definitions back through the console to previous sets of known good definitions/dats files, then distribute to all of their clients. This would be a lifesaver compared to the choices above.

Depending on anti-virus software a user may need to be logged in to the machine before definitions/dats files are downloaded to the client. This may leave a machine unprotected for several hours while definitions/dats files are available. Network bandwidth is impacted at the time users start logging into the network. There is now competition between definitions/dats files, smtp, http and other normal traffic, when users start logging into your network. A better way, after of definitions/dats files have been tested, is to update the clients during off peak work hours. This will provide better protection, and your able to deploy definitions/dats with or without users logged in. During off peak hours, will also speed up the deployment process, due to less network activity.

Engine

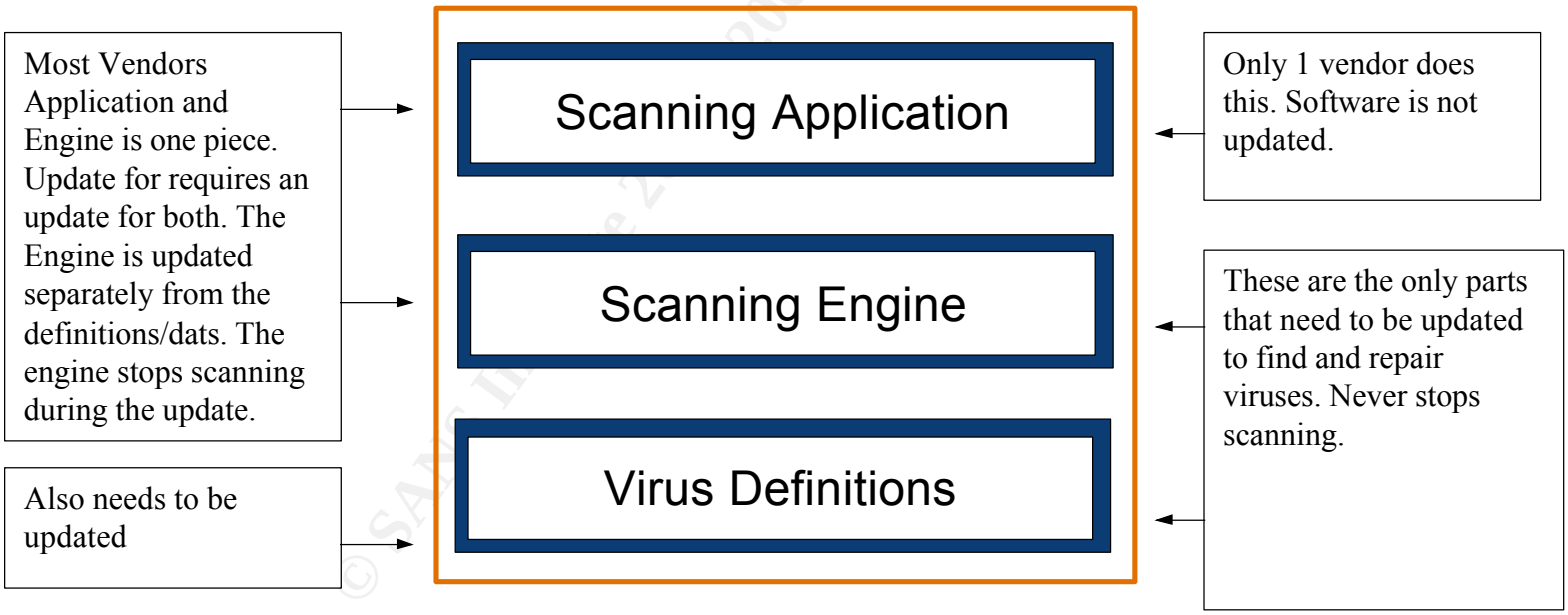
Lets start by discussing what an engine is. There are three pieces to all anti-virus software: the application loaded on a client, the engine (this is what does the scanning, virus finding and repair) and definitions/dats files (the patterns the engine uses to find virus).

New viruses are found on a daily, if not hourly basis. Definitions/dats files are release on a daily/weekly basis. The problem faced is that definitions/dats files may find a new virus, but cannot due any thing with what it has found. The current engine is not capable of repairing the virus or files infected. Now a new engine is required to solve our problem. The vendors release a new engine; it is our responsibility to deploy it to our clients and servers. This may be a separate update from the normal virus definitions. We may have another file to deploy, ranging from 1 to 5 Meg. You will need to deploy the engine to a local update server or servers, and tell the client to retrieve their updates. Also if you have separate desktop and server software, they require different engines, and Please don't put the wrong engine on the wrong product. If you are running another type of virus protection, http, ftp, or smtp, these also may require separate engine upgrades. This also may be a software upgrade, so we need to

let the imaging group know that we have updated the base-line image again.

I have another question, have you noticed with some of the newer viruses; they try to disable the anti-virus software and desktop firewalls? Does you anti-virus solution STOP scanning during an engine update? If it does please see the question above. Why are you paying for your protection to be stopped? Next, you may be required to reboot all clients that have upgraded the engine. So if you have an outbreak, during the middle of the day, and need to update your engine, and then reboot all clients, what do you do?

Wouldn't be great if there were a simpler process? Let me explain, one vendor has the capability, with the way the engine is designed to seamlessly update the engine when the definitions/dats files are updated, no special process. They also never stop scanning during an update. No reboot for this process either. This engine is also common across all of there antivirus products, and all languages supported. This anti-virus software is updating the engine, across all platforms, during normal definitions/dats files updates, and is not a separate process. Depending on the definitions/dats deployment method, the size of the updates with the engine range from 300K to 3.5 Meg.



Virus Handling

Now after we have definitions/dats files, and a new engine deployed, what are the options when we find something. The 1st action should be to clean, but what if that fails? The file will be locked by the anti-virus software, the user

can see the file, but has no access to it, and receives a message from the operating system that the user cannot access the file. Now a virus administrator will need to go to the pc, unlock the file and take an action. One vendor had an option to let the user decide the action to be taken, but that option is out, that is why we have a virus policy, and we don't want to rely on users input. One option is to delete, but we've discussed that option if the file is an operating system file or your company's database. Some software may move the infected file to a network share, who has access and can download the code from this server? The options above were clean or delete or move or let the user decide, but only one option, only severely limits the options and protection you may choose to enforce the virus policy.

These options apply to all viruses, macros and non-macros. You may need to take different action for the different type viruses including Win32 viruses.

Szor, Peter. "Attacks on Win32" The Eighth International Virus Bulletin Conference, October 1998, Munich/Germany, page 57-84 Ref: http://www.peterszor.com/attacks.pdf

Szor, Peter. "Attacks on Win32 Part2" Virus Bulletin Conference September 2000, Orlando/USA, page 101-121 http://www.peterszor.com/attacks2.pdf

Lets look at another option to the ones above, virus software should allow you to choose an action and if that action fails the go to a secondary action. Example, if I find a virus, and try to clean it, if unable to clean then encrypt and send to another server which is the repository for all malicious code, not just a moved to a share. This option alerts the user something was found, but they have no decision, the rules are predefined. You may decide that you may need separate action for macro and non-macro viruses.

Hopefully your not the 1st to every report a potential new virus, what do you do? How do you submit a file to a vendor? One-way is to password protect a zip and ftp it. Some vendors have a limit on the size of zips of 3 or 4 Meg. If your suspected file is larger how do you get it to the vendor for analysis? Also why are you sending possible privacy act, private, or classified information to an anti-virus vendor? I would rather strip only the malicious from a file and submit it for analysis. This could be automated and the code sent to the vendor for analysis. The vendor could automatically generate definitions/dats files and sent back to the customer for testing and deployment. This would eliminate the manual submissions, reducing administrative cost.

Being able find malicious code is extremely important, but virus handling once something is found is also important, unless the virus administrator has nothing else to do, except chase viruses.

Certifications

All virus vendors tout they are this 1st to market with new definitions/dats during an outbreak. One of the major 2 or 3 vendors are normally the 1st to release definitions/dats. On occasion, a vendor may need to release 2 or 3 sets before they can clean viruses, 1st set to detect, 2nd or 3rd to clean. Getting a new set of definitions/dats to a customer is important for a vendor, so is detecting viruses that have been out for weeks, months, or years.

Virus Bulletin is an independent Anti-Virus testing company.

Ref: http://www.virusbtn.com

Virus Bulletin does testing of anti-virus products on different platforms and publishes the results of which vendors are really catching malicious code from the wildlist. There are two types of viruses, a zoo virus, which is created in a lab by vendors to test products. Virus generating tools over the Internet that may create a possible virus may also be classified as a zoo virus, because it has not been written at this time. There are also in the wild viruses, written by people to cause harm. These are everywhere and what you hopefully will catch and not be infected with one.

Link to the WildList
http://www.wildlist.org/

VB 100% awards are posted on a quarterly basis, the latest is testing is done on Windows XP. If your anti-virus vendor is not passing checks for viruses that are in the wild, are you using the right product? Also some vendors may not enter every category because they may offer products in that category, for example, Linux, Win 3.1 or Netware or a console to run on a certain platforms. Look for anti-virus vendors that are not failing these tests!

The VB 100% logo is awarded to products that detect all In the Wild viruses during both on-demand and on-access scanning in **Virus Bulletin**'s comparative tests. The product must also produce no false positives.

Results table

Key:

Pass
Fail
No entry

NetWare
Sep *01*
Windows NT
Nov *01*
Windows ME
Feb *02*
SuSE Linux
Apr *02*
Windows XP
Jun *02*

Aladdin Knowledge Systems

Alwil

CAT Quickheal

ICSA is another independent group that test and certifies products to work and be stable.

http://www.icsalabs.com/

The goal for ICSA Labs Certification is to enhance and improve security implementations of network and Internet computing, which will improve commercial security and its use of appropriate security products, services, policies, techniques, and procedures. Certification enforces overall confidence in computing and drives enhanced security measures while at the same time, decreasing the intrusion of security measures in everyday life. Certification also promotes user acceptance of increased security while improving the ease of use, and the invisible, automatic, and seamless integration of security technology in everyday computing.

Ref: http://www.icsalabs.com/html/certification/index.shtml

West Coast Labs is another third party that test and has certification for anti-virus products. West Coast has two levels of certification.

> For a product to be certified to Anti-Virus Checkmark, Level One the product must be able to detect all those viruses which are" In The Wild ". This gives a clear and independent indication to end users of those anti-virus products that can be relied on.

http://www.check-mark.com/cgi-bin/redirect.pl

> For a product to be certified Anti-Virus Checkmark, Level Two the product must comply with Anti-Virus Checkmark, Level One and, in addition, disinfect all viruses on the "in the wild" list which are capable of disinfections.

Ref http://www.check-mark.com/cgi-bin/redirect.pl

Protection

What is your vendor providing definitions/dats file for now, other than malicious code? We know and virus, worms, and trojans. Where you aware the anti-virus vendors also check for 2 Microsoft Stolen certificates. There is becoming a blur between some of the new viruses and network attacks. Hopefully your vendor is a security company, to protect you from these new viruses/network attacks. Some vendor initially did not write a definitions/dats for Nimda. Nimda started as a network hack, and evolved into malicious code. Now for every network hack that could have been prevented with applying the current patches to the Operating Systems users want the anti-virus to fix it for them.

> **E**xperts called the recent Goner computer worm a perfect example of a "blended threat" -- one that combines the evils of an Internet virus with the opportunity for a hacker to take over a PC and turn it into a zombie. In response, antivirus and security professionals are increasingly coming together to answer the challenge with their own blended defense.

Ref: http://www.newsfactor.com/perl/story/15233.html

> According to Vincent Weafer, director of Symantec AntiVirus Research Center, part of the problem stems from hackers and virus writers using known vulnerabilities in systems to their advantage.

Ref: Weaver, Vincent Director of Symantec Anti-Virus Research Center
http://www.scmagazine.com/index2.html
SC Magazine, May 2001, Viruses Preparing for the Onslaught

Do you really need more than one vendor? Depends on the vendor that you pick. If your vendor catches all viruses, check VB100 Awards, ICSA, and West Coast Labs, I don't see a reason any longer for the defense in depth. If you are unsure about the vendor you have, that's probably the reason you have two vendors.

Price

Now we are at the last step, the all mighty $$$$$$. Why would you buy an inferior product based on price? When you buy a car do you choose the cheapest one on the market? Probably not, I'm also not saying that because it is the most expensive it is the best. There is a level of quality and support you should be paying for, it not you will not receive it. Are you really saving money buying the cheaper product? Consider what the vendors have told you, ask the questions above and make a choice. You may need to sell the choice to you management, for a better product.

Conclusion

Anti-Virus vendors are only showing the nice features, be aware there are other feature you need to look for in an anti-virus solution. Make sure your anti-virus product has deployment features compatible in your environment. Understand all involved in updating the definitions/dats files and engine, and what to do if the definitions/dats are corrupt. Look at the certification web sites to ensure you products is catching the viruses in the wild. Look for a product that is able to manage a virus when you find one. Make sure you're not getting caught up in a price war; the best product may not be the cheapest. The better product may cost a little more now, but a lot less later.

References

http://www3.ca.com/virus/ Computer Associates
http://www.f-secure.com/ F-Secure

http://www.mcafee.com McAfee
http://www.pandasoftware.com/ Panda
http://www.sophos.com/ Sophos
http://www.symantec.com Symantec
http://antivirus.com Trend Micro
http://corporate.mcafee.com/content/software_products/avd_compare_epolicy.asp

Szor, Peter. "Attacks on Win32" The Eighth International Virus Bulletin Conference, October 1998, Munich/Germany, page 57-84 Ref: http://www.peterszor.com/attacks.pdf

Szor, Peter. "Attacks on Win32 Part2" Virus Bulletin Conference September 2000, Orlando/USA, page 101-121
http://www.peterszor.com/attacks2.pdf

http://www.virusbtn.com
http://www.wildlist.org/
http://www.icsalabs.com/
http://www.check-mark.com/cgi-bin/redirect.pl
http://www.newsfactor.com/perl/story/15233.html

Ref: Weaver, Vincent Director of Symantec Anti-Virus Research Center
http://www.scmagazine.com/index2.html
May 2001, Viruses Preparing for the Onslaught