Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Choosing Your Anti-virus Software

The first step to choosing anti-virus software is to understand how they work. That will give you a better idea of the features they offer and make your way through the technical terminology used by anti-virus vendors and experts. Understanding what your anti-virus software can and cannot do will help you have the right expectations and will help you tell the difference between serious anti-virus software and the others.

Copyright SANS Institute
Author Retains Full Rights

AD
Take control of vulnerability threats Now!
Request a Free Trial
Secunia
Stay Secure

Jacqueline Castelli
Sans Security Essentials GSEC practical assignment Version 1.3 (December 12, 2001)

Choosing your anti-virus software

Introduction

In today's connected world, anti-virus software is more than ever a necessity to protect your computer against viruses, worms and other types of malicious code. It is by far the easiest way to give your computer a minimal level of protection. Yet, the process of choosing which anti-virus software is best suited for your protection is not so easy. That task is made challenging by numerous misconceptions that surround the anti-virus world and some of the questionable claims made by some vendors. If you surf anti-virus vendors' web sites, for example, you will soon find out that many of them are the best, that many have the biggest market share or that many are the only vendors with a 365x24 support. The marketing war raging among those vendors and sometimes the lack of knowledge of their own competitors makes it rather difficult for the end-user to make a knowledgeable choice.

Whether you are a home user or an IT professional in charge of security in a large corporation, it is easy to be mislead by information provided by the different vendors and sometimes, even by the press. Therefore it is important that you understand how anti-virus software work and what the important criteria are, when choosing of such a solution. It is also important that you know how and where to find relevant information when making your decision.

Understanding how anti-virus software work

The first step to choosing anti-virus software is to understand how they work. That will give you a better idea of the features they offer and make your way through the technical terminology used by anti-virus vendors and experts. Understanding what your anti-virus software can and cannot do will help you have the right expectations and will help you tell the difference between serious anti-virus software and the others.

How does an anti-virus detect viruses?

There are several technologies used to detect viruses. Viruses and malicious code in general, are nothing more than code. So, if we know what the code of a virus looks like, we will be able to identify the virus when we see it. That is the first technology used by anti-virus software. It is called signature matching. The anti-virus product contains a database of virus signatures and will detect a virus any time it sees code that matches an entry in the database. That is probably the most efficient way to detect viruses. The drawback to that technology is that we need to have seen the virus before and have written a signature for it to be able to detect it. That requires the user to keep the virus signature database as up to date as possible.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

To work around that weakness, anti-virus software can use two other technologies: Heuristic and Integrity Checksum. The philosophy behind Heuristic technology is to be able to detect viruses or malicious code for which a signature does not exists yet. That result is achieved by using a database of virus behavior signatures. If the Heuristic technology analyzes the code for any routine or subroutine matching a virus behavior signature, we will call it static heuristic. If the heuristic technology lets the code run into a virtual machine to analyze the behavior, we will call it dynamic Heuristic. The issue with Heuristic technologies is that they can trigger false positive, where a clean file is reported as being infected.

The integrity checksums are based on the assumption that a virus needs to make a modification to a system in order to infect it. The simplest example is that a virus needs to modify a file by overwriting or adding its code to the file, so that, when the file is run, so is the viral code. The integrity checksum method consists of taking a checksum of clean files or disks. Any change to the checksum indicates that the files or disks have been modified by what could be a virus. Not only can that method generate false positives, it is also inefficient against macro viruses or virus like Code Red that can insert itself into memory and run without being saved to a file.

If the malicious code goes through all the scanners, there is a last line of defense offered by some anti-virus products: the activity blocker. It will block all activities that could be caused by a malicious code. The activity blocker will alert you, for example, if a process is trying to format your hard drive or write to the boot record of your hard drive.

When does the AV detect a virus?

Usually, anti-virus software has two ways of operating. First, a real-time or on-access scanner, which is memory resident (or service or daemon), monitors the system activity at all times for the presence of viruses. A hook to the operating system alerts the real-time scanner when a file is accessed, allowing the scanner to check the file. It has the advantage of offering constant protection but it will only check files when they are accessed. If an infected file resides on the disk and is not accessed, the real-time scanner will not detect it. Then, an on-demand scanner can be started by the user at any given time to check a file, folder or the content of the entire hard drive for viruses. The on-demand scanner can check every single file, but it only offers a good assessment of your system at a single point in time. On demand scan can be scheduled to check all the files for viruses on a regular basis.

What anti-virus software can and cannot do

- 100% protection

  No anti-virus software in the world will provide you 100% protection, no matter what they claim. Viruses and malicious code are often ahead of anti-virus researchers. Melissa, FunLove, CodeRed, Nimda and many other viruses have

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

proven that fact. That is because of the way anti-virus software work. Remember, they need to have the virus signature to be able to detect it. And most of the time, for new types of viruses, the heuristic technology does not quite work. That is also the reason why it is vital to be up to date on the virus definition database. However anti-virus software will provide a solid protection against all the existing viruses (about 60 000 to date) and will provide you with a quick fix when a new one comes in.

- Repair viruses

  If a virus is detected will my anti-virus software be able to repair it? Well, it depends. It depends on the virus that has caused the infection. Some viruses, especially macro viruses are easy to clean, because they don't damage the host file. It is easy for the anti-virus software to remove only the malicious code and repair the file. Some other viruses overwrite the content of the host file to replace it with its own code. That is the case of the Love Letter virus. In such a case, the infected files cannot be repaired. The only option is to delete the files and restore them from a backup. Last but not least, some other malicious code, like Nimda, not only infect files, they also make modification to your system. They replace system files, and/or make registry changes. To get rid of viruses of that kind, the anti-virus is not sufficient. You need removal tools, available on most vendors' web sites, to undo what the virus has done and clean up your system.

Evaluation criteria

Now that we know how anti-virus software work and what they can do for you, let's take a look at the important criteria to consider when choosing anti-virus software.

Detection

The one most important thing you want the anti-virus to do is to catch viruses. But how do you know that it works as advertised. If it is easy to see the results in a word processor or compiler, how do you know that your anti-virus software is really catching viruses? That question actually encompasses two questions. The first one is to know how many viruses the software actually recognizes, which is commonly known as the detection rate. The second question is to know under which circumstances the software is able to see the virus. Can it see viruses if they come through a network share, via email or if they are already running in memory? There are three things you could do and shouldn't do to get the assurance that your anti-virus software is indeed reliable.

First, you could be tempted to test the anti-virus yourself, to go on the net looking for virus libraries and throw them at the anti-virus. Well, I would strongly discourage you from doing so, even if some vendors include such a methodology in their white papers. As Eicar (European Institute for Computer Ant-Virus Research) states: "Using real

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

viruses for testing in the real world is rather like setting fire to the dustbin in your office to see whether the smoke detector is working." You are not a virus expert and you never know what can happen. What if the anti-virus does not catch them all and they start deleting data on your hard drive or start spreading in your enterprise. That could cost you your job. Anti-virus experts themselves take all the precaution when dealing with viruses, ensuring, for example, that all infected media they handle are destroyed after being reviewed.

Second, if you really want to know that the anti-virus is doing something, you can download at www.eicar.org a safe anti-virus test string. Most anti-virus software will detect the eicar file as being infected. That is a secure way to check the anti-virus ability to see viruses under different circumstances.

Finally, you can rely on external sources to verify the anti-virus detection rates. In order to understand what detection rates really mean, you need to know the difference between viruses in the wild and viruses In-The-Zoo. The In-The-Zoo viruses are lab viruses that have not been encountered in the real world. The In-The-Wild viruses are viruses that have been infecting computers worldwide. A list of the In-The-Wild viruses is kept by the WildList Organization International and can be found at http://www.wildlist.org.

- The Virus Bulletin at www.virusbtn.com , for example, awards a 100% logo to products that pass their testing. It consists of testing anti-virus on-demand and real-time scanners against the list of the viruses found in the wild. The products able to detect a 100% of the In-The-Wild list are awarded.

- The West Coast Lab offers two levels of checkmarks for anti-virus products. Vendors have to pay to have their products tested. The first level is passed if the product detects 100% of the virus listed in the WildList. To obtain the level 2 checkmark, the anti-virus has to pass level 1 and has to be able to repair all reparable viruses of the WildList without altering the system stability. The checkmarks can be found at http://www.check-mark.com/cgi-bin/redirect.pl. The West Coast Lab also provides test results for anti-virus software ability to catch Trojan horses.

- The ICSA (International Computer Security Association), division of TrueSecure, offers certification for On-Demand/On-Access anti-virus products, anti-virus products cleaning, anti-virus product for Internet Gateway E-mail, anti-virus products for Microsoft Exchange and Lotus Notes, anti-virus products for Security Service Providers, Internet Service Providers and anti-virus scanners. Anti-virus vendors also have to pay a fee to have their products tested. To be certified an On-Access or Real-Time scanner, for example, has to detect 100% of the viruses listed in the current In-The-Wild List, detect 100% of the viruses listed

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

in the ICSA Labs Common Infectors Test Suite, detect 90% of macro viruses in the ICSA Labs Virus Collection and not cause false positives. An exhaustive list of the certification criteria for each type of anti-virus product can be found at: http://www.icsalabs.com/html/communities/antivirus/certification.shtml. A list of all testing results can be found at: http://www.icsalabs.com/html/communities/antivirus/index.shtml

Technology

It is also very important to know what kind of technologies is included in the product. Below is a list of technical features you should be looking for in anti-virus software.

- Product compatibility with your hardware and software configuration

  It may sound obvious but make sure that the anti-virus software you choose works in your environment. Some vendors will advertise their latest and greatest version that works only with the latest operating systems release. So before you go ahead and purchase the product, make sure that you meet the software requirements. That information can be found on different vendors web sites.

- On-Access or Real-Time scanner

  That is an absolute must. The On-Access or Real-Time scanner is your watchdog. It will give you the ability to catch viruses as soon as they try to infect a system. The On-Access scanner should be able to scan all areas of the systems, including the file system, boot record, master boot record and memory.

- On -Demand scanner:

  That will make sure that all the files on your system are virus free. It is always good to run an on-demand scan after you have updated the virus definitions to make sure no virus has gone undetected. That could happen if, for example, you receive via email an attachment that is infected with a virus that does not have a signature yet. If you save the attachment on your hard drive without executing it, you have a virus dormant on your system. If you never access that file again, only an on-demand scan with new virus definition would catch that virus.

- Heuristics

  Heuristic technology will give you protection against basic unknown viruses.

- Ability to scan all types of files and not only some specific extensions

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

If you have the right virus definitions and you are not looking at the right files, viruses will still be able to infect your system. In the past, program files were the only way to spread a virus. Since then, virus writers have found ways to use files other than executables to spread viruses and new threats can infect any type of files. Therefore, looking at all files has become very important.

- Script blocking:

  Script based viruses, such as the mass-mailing script worms I Love You and Anna Kournikova are more and more common. The scanning engine should be able to recognize VBScripts and JScripts to detect and stop those malicious scripts.

- Ability to scan email attachment

  A lot of viruses now spread though email. Some of them, like the KAK worm can spread on a vulnerable system without even requiring the user to access the attachment. That is why anti-virus software with email scanning ability is a plus.

- Ability to scan within compressed files

  Even though a virus cannot be run when compressed, it is always good to be able to detect it before it enters the system. You should also check how many levels deep the anti-virus software can go. Yet, the deeper the scanner goes, the more it will impact the system's performances. In some instances it can even crash the system or the anti-virus software itself. Rob Rosenberger, (http://www.vmyths.com) has showed that a recursive compressed file can cause a denial of service attack on anti-virus scanners. So, don't be fooled by vendors who claim being able to scan 99 levels deep because you should never use such a feature. Three to five levels should be enough.

- Ability to detect Trojan, malicious active-X controls and Java applets

  Anti-virus software should not only detect viruses and worms but also protect you against malicious code in Trojan horses, ActiveX controls and Java applets. Today, most anti-virus software includes those features.

Maintenance

- Viruses definition updates

  We have seen how critical it is to keep the virus definition database up to date. Consequently, you should choose anti-virus software that is easy to update and for which new definition databases are available frequently. Weekly is currently the standard even though some vendors will make beta virus definition database available daily to the public. Some vendors now offer daily tested definitions.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

You should also consider which mechanisms are available to you to update those virus definitions. Are they available on a web site, can you download them directly from the product, can you be notified when new virus definitions come in? How big are those updates? If you have a slow Internet connection, updating can be a painful process. If you are in a corporate environment, the update has to be small enough to have minimal impact on the network bandwidth. In any case, you'd probably want to lean towards smaller updates. Some products have the ability to only download the difference between what's new and what's already installed.

The ability the vendor has to quickly release virus definitions for new threats is also a factor to consider. Vendors will claim to have been to first one to have new definitions or signatures for such and such virus. The reality is that none of them is always first. The major vendors often beat each other from a couple of hours. To go around that issue, some companies have chosen a multi-vendor strategy. Their philosophy is that one of their vendors will be first and will provide them with protection while the other vendors are still working at their virus definitions. Even though technically attractive, that strategy has the drawback of increasing the cost of ownership; forcing the company to use multiple management consoles, to learn different products and methodologies and to maintain multiple vendor relationships.

Yet, more important if you are in a corporate environment is the speed of deployment of those new virus definitions. Once you have those definitions in your hands, how long is it going to take to update all your systems? You may want to look at an anti-virus solution that allows you to update virus definition fast.

- Product upgrades.

  All anti-virus products will have to be updated eventually. Check if updating the anti-virus software requires uninstalling the older version before installing the new one. If
  You are a home user, that may not be an issue, but if you are responsible for a number of systems, that task can become quite costly.

  Apart from new versions to assure compatibility with new operating systems, anti-virus software sometimes have to be updated to be able to detect new types of viruses. Anti-virus software is made of three parts: a user interface, a scanning engine and a virus definition database. The scanning engine is the brain of the product. It knows where to look for viruses and uses the virus definitions database to match what it scans with virus patterns. If a new type of virus comes along, the scanning engine may have to be updated to start looking at areas of files or systems it did not monitor before. That was the case for the Remote Explorer virus, for example, that had the originality of compressing and hosting the original file within itself. It is important that the scanning engine of the anti-virus you

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

choose can be easily upgraded. You definitely don't want to have to install or deploy a new version of your anti-virus software in the midst of an outbreak. To make that type of upgrade easier, some vendors offer scanning engines integrated with virus definition databases.

Performance

Anti-virus software will always have an impact on systems performance. Even though it is difficult to define, it is an important criterion. Does the anti-virus scanning slow down the boot process, does it increase the time required to access a file? How does it impact the memory and CPU usage? How much of a memory footprint does the On-Access scanner use? Just like for detection rates, you can choose to perform some tests for yourself, or you can rely on third party testing.

- Basic guidelines for performance testing

  Some of the things you can easily test yourself are the time needed for different types of scans and the memory and the CPU usage. You can time how long an On-Demand scan takes for each product. You can also time how long it takes to open a big file when the On-Access scan is turned on.

  To monitor the memory and CPU usage, you can some tools such as Perf Monitor (which comes with Windows by default). Check the CPU and memory usage during an On-Demand scan. Check the CPU and memory usage when accessing a big file without the On-Access scanner turned on and then, with the On-Access scanner enabled.

  A lot of factors have an effect on performance. Therefore, when you are conducting your own testing or reading results from third parties, make sure you are comparing apples to apples. One of the factors impacting performance, for example, is the type of files you are asking the anti-virus software to scan. Scanning all files versus scanning some extensions only will definitely make a difference in the testing results. However, some anti-virus software will by default scan all files, where some others will, out of the box, scan only specific extensions. The heuristic technology is resource intensive. Make sure, when you are testing that the same level of heuristic protection is enabled on each product. You should also check if the product, by default, excludes any folders or type of files from being scanned. The most important thing to keep in mind is that all the products you test have to be configured in the same way. Otherwise, your testing results will be biased.

- Third party testing results

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Unfortunately, unlike for the detection rate, there is not institution or association that measures anti-virus impact on systems' performances. Yet, if you look for anti-virus and performance testing in a search engine on the net, you should be able to find some reviews.
The following links will give you the most recent results.
.
http://antivirus.about.com/library/reviews/winscan/aatpavwin.htm and http://antivirus.about.com/library/reviews/winscan/aabybavwin.htm?PM=ss14_antivirus will give you anti-virus software reviews, including performance reviews.

In its June 26th 2001 review, PC Magazine offers a review of different anti-virus software. The results can be found at:
http://www.zdnet.com/products/stories/reviews/0,4161,2766399,00.html

Manageability

META Group says: "If you can't centrally manage your virus protection software, then you don't have virus protection." That is true of corporate environments. Central management of your anti-virus solution should allow you to rapidly deploy new virus definition updates, establish policies and enforce them, verify the protection on clients and server and view alerts, reports and logs. You should also make sure that the management feature of the solution is scalable in your environment and that is does not impose heavy extra traffic on your network.

Technical support

- Different levels of support

  Important also is the ability the vendor has to support you. You should ask for the different level of support available. A home user and an anti-virus coordinator in a big corporation don't have the same need. The vendor should be able to offer a level of support that is in line with your need and your means.

- On-Line support

  You should also find out if they have on-line support. Will the vendor let you send them virus samples if you have suspicion on some files?

- Alerts

  Does the vendor offer a virus alerts? That is a very important feature. If a new virus is detected in the wild, is it important that your vendor has the ability to alert you, so that you can take the necessary actions to protect yourself or you company as fast as possible. In some cases, it is critical to be alerted and to receive

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

information about a virus before signatures are available. An early alert and understanding of what the virus does will allow you, for example, to add the appropriate filter on email gateway to keep the virus away.

Third party tests and reviews

One of the things you can do to select anti-virus software is to review what journalists, testers and users have to say about the products.

- PC Magazine will provide you with editor's reviews and users ratings. You can find those at: http://www.pcmag.com/category/0,2999,s=1594,00.asp

- Secure Security Magazine on-line will also give you some software reviews at http://www.scmagazine.com/
  Click on View articles, Category Index, Anti-Virus

- PC World
  http://www.pcworld.com/home/index/0,00.asp
  Make a search on "antivirus" in the review section.

- Consumer Search
  http://www.consumersearch.com/www/computers/antivirus_software

Product vulnerabilities

Introducing a new security product in your environment should not open any security holes. It is consequently always interesting to take a look at the list of vulnerabilities listed for the products you are considering to acquire. The Security Focus vulnerability database at http://www.securityfocus.com/corporate/products/vulns.shtml will provide you a list of software vulnerabilities. You will find out if the anti-virus scanner can be bypassed in any way, or it is opens your system

Vendor profile

At last, you should check the vendor's profile. If you are making a decision for an entire corporation, you might want to check who is going to become your business partner. You can check on their position on the market by checking information provided by the Gartner group of IDC. Be aware that you may have to pay to get that information and that the Gartner group collects information from resellers to determine anti-virus sales, where IDC asks the vendors for that information. As a result of the latest method, you may find a total market share of over 100%.

You should also consider how big the company is, how long they have been on the market and how long they have been in the anti-virus business.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Where to find more information: Anti-virus vendors list

Below is a list of anti-virus software vendors with their respective web sites, where you will be able to find product information and download evaluation products.

Aladdin Knowledge Systems
Home page: http://www.ealaddin.com

Command Software Systems
Home page: http://www.commandcom.com
Download evaluation: http://www.commandcom.com/try/try_before_you_buy.html

Computer Associates
Home Page: http://www.cai.com

F-SECURE Corporation (Formally Data Fellows Corporation)
Home page: http://www.europe.f-secure.com
Download evaluation: http://www.europe.f-secure.com/download-purchase/list.shtml

Dr Solomon's Anti-Virus Software Ltd (Now McAfee)
Home page: http://www.drsolomon.com

GFI Software Ltd
Home page: http://www.gfi.com
Download evaluation: http://www.gfi.com/pages/files.htm

InDefense
Home page: http://www.indefense.com
Download evaluation: http://www.indefense.com/downloads/index.html

Kaspersky Labs
Home page: http://www.kaspersky.com
Download evaluation: http://www.kaspersky.com/download.html

McAfee
Home page: http://www.mcafee.com
Download evaluation: http://download.mcafee.com/eval/evaluate2.asp

Network Associates
Home page: http://www.networkassociates.com
Download evaluation: http://www.nai.com/naicommon/buy-try/introduction/default.asp

Norman Data Defense Systems UK Ltd
Home page: www.norman.com/us
Download evaluation: http://www.norman.com/downloads.shtml

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Panda Software International
Home page: http://www.pandasoftware.com
Download evaluation: http://www.pandasoftware.com choose downloads, and downloads again.

RAV (Reliable AntiVirus)
Home page: http://www.ravantivirus.com
Download evaluation: http://www.ravantivirus.com click on free downloads

Reflex Magnetics Ltd
Home page: http://www.reflex-magnetics.co.uk
Download evaluation: http://www.reflex-magnetics.co.uk/downloads/downloads.htm

SOPHOS
Home page: http://www.sophos.com

Symantec Corporation
Home page: www.symantec.com
Download evaluation: http://www.symantec.com/downloads

Thunderbyte (Now Norman Data Defense Systems)
Home page: http://www.thunderbyte.com

Trend Micro Inc
Home page:www.trendmicro.com
Download evaluation: http://www.antivirus.com/download

VET Anti Virus Software Ltd
Home page**:** http://www.vet.com.au
Download evaluation: http://www.vet.com.au/html/software/full.html

VirusBuster Ltd
Home page: http://www.virusbuster.hu
Download evaluation: http://www.virusbuster.hu/letoltes.en.shtml

Sybari Software, Inc.
Home page: http://www.sybari.com
Download evaluation: http://www.sybari.com/download/eval.asp

Conclusion

There is no best anti-virus product. The choice of your anti-virus solution should depend on your needs, your environment and your goals. Vendor information is always useful, but it is not wise to rely solely on them. In order to make the right choice, you should see for yourself, and you should look at vendor information as well as at alternative sources

© SANS Institute 2002, Author retains full rights.

of information.

© SANS Institute 2002, Author retains full rights.

References

"A Credibility Model for AntiVirus Industry Sefl-regulation"
http://conference.eicar.org/past_conferences/2001/papers/other/Wells.pdf

"A Guideline to Anti-Malware-Software testing"
http://conference.eicar.org/past_conferences/2000/papers/Tuesday/Virus%20and%20Malware/other/Marx.pdf

"Beyond Detection Rates - What Users Want "
http://www.virusbtn.com/vb2000/Programme/papers/joost.pdf

"Antivirus Software Testing for the Year 2000 and Beyond"
http://csrc.nist.gov/nissc/2000/proceedings/papers/038.pdf

Virus Bulletin
http://www.virusbtn.com/

ICSA
http://www.icsalabs.com/html/communities/antivirus/index.shtml

Virus Test Center of the University of Hamburg
http://agn-www.informatik.uni-hamburg.de/vtc/en0110.htm

In the Wild viruses
http://www.wildlist.org

West Coast Lab Checkmark information
http://www.check-mark.com/cgi-bin/redirect.pl

What is Wild?
http://csrc.nist.gov/nissc/1997/proceedings/177.pdf

"Reviews and Evaluation of Antivirus Software: The Current State of Affairs"
http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper019/final.PDF

Anti-Virus reviews
http://antivirus.about.com

Symantec "Lower IT costs through better Anti-Virus management"
http://securityresponse.symantec.com/avcenter/reference/nvxwp2b.pdf

Trend Micro "Virus Protection Selection Criteria Guide"
http://a1984.g.akamai.net/7/1984/537/0000787/download.antivirus.com/ftp/white/vir_prot.doc

McAfee "Evaluating Anti-Virus Solution Within Distributed Environments"

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

http://vil.nai.com/VIL/white-paper.asp

Anti-virus Product Evaluation Criteria
http://www.emory.edu/ITD/DESKNET/AV/criteria.htm

Computer Associates: "Choosing Antivirus Software"
http://www3.ca.com/Solutions/Collateral.asp?ID=910&PID=

The Yellow Pages of White Papers: Anti-Virus White Papers
http://www.itpapers.com/cgi/SubcatIT.pl?scid=276

"Email Infrastructure Vulnerabilities - Simple & effective exploits based on computer security myopia"
Rob Rosenberger
http://www.chi-publishing.com/isb/backissues/ISB_2000/ISB0509/ISB0509RR.pdf

© SANS Institute 2002, Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**