



Why Is Panda Antivirus Better Than McAfee, Norton, and Trend Micro?

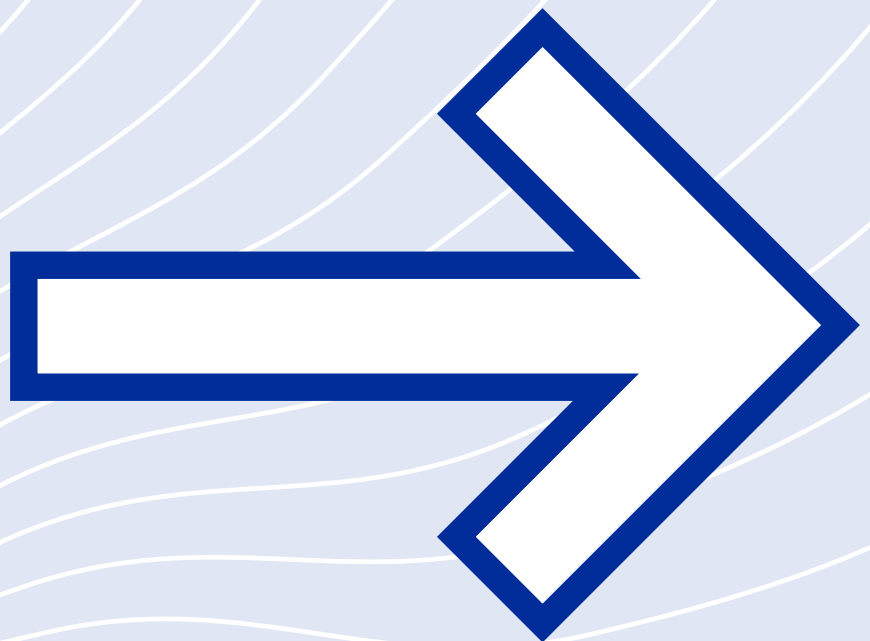




Table of Contents



Introduction	2
Most Advanced Antivirus Technology	3
Best GroupWare & Server Performance	7
Microsoft Exchange	8
Lotus Notes / Domino	9
Windows NT/2000 Server & Advanced Server	11
Truly Centralized Management	13
Product Awards & Certifications	14
Software As A Service	15



Introduction

Corporate antivirus protection is a constantly changing market which is driven by new virus technologies and the ability to seamlessly protect all possible virus entry points to the corporate infrastructure against new threats.

Over the course of the last few years we have seen how new virus technologies have radically changed their infectious and transmittal methods and this has raised questions about the validity of traditional antivirus solutions. Even though companies throughout the world have antivirus protection installed, the question is still raised every time a new breed of virus manages to slip through. The dangers of newer viruses no longer reside only in their ability to destroy information, but rather in the ability they have to bring down complete networks to their knees.

Antivirus solutions must no longer only deal with the “numbers game” of how many viruses they detect, but rather with issues such as **enterprise scalability**, server-based **performance**, and the ability to catch the newest viruses that use the **latest technologies**.

E-mail has quickly taken first place as the primary source of infection, which now represents about 90% of all corporate infections. It is obvious how viruses are using more advanced technologies to slip passed antivirus protection via e-mail, as is obvious how some antivirus solutions are not keeping up with the technology advances.

Not only must an antivirus solution keep up with new viral technologies, it must also do so without penalizing server performance or scalability. Any antivirus solution that does not keep up with these issues nowadays represents a threat to corporate security. It's as simple as that.

Panda Software has been developing antivirus technologies ahead of its time for the last three years, and has now **the most advanced server and groupware based centrally-managed corporate antivirus solution.**

Most Advanced Antivirus Technology

Panda Software takes pride in the fact that it develops 100% of the technology used by all its products. While other vendors are in the business of buying their core technology, Panda Software products enjoy a common, powerful, and stable, cross-platform antivirus engine and signature database.

This fact alone has allowed Panda Software to dedicate most of its Research and Development efforts to developing products that **prevent** new viral technologies, **instead of reacting** against them. On the other hand other vendors have to dedicate their R&D efforts to integrating different solutions developed by different vendors into a single suite.

The result is clear as shown by the innovations in antivirus technologies introduced to the market by Panda Software throughout its history, which has always driven the rest of the antivirus industry:

1994: First antivirus capable of automatically installing and updating protection to networked PCs

Known as RINSTALL (Remote Install), this product from Panda Software was the first one on the market to centrally manage and deploy antivirus protection and updates automatically to networked PCs.

1997: Creators of the client service concept of 24h-365d

In an antivirus industry where clients had to pay additional to receive special services from antivirus manufacturers, Panda Software introduced *24h-365d Global Virus Insurance*, the solution for corporate customers that merged software and service into a single packaged solution.

1997: First antivirus for Exchange & Outlook capable of scanning nested messages, OLE objects, etc

Panda Antivirus for Exchange/Outlook clients was the first home and corporate user e-mail solution for these platforms to automatically disinfect viruses from e-mail, regardless of their format (OLE objects, nested messages, compressed files at any level, etc.)

1997: Creators of revolutionary VirtualFile technology for optimized memory scanning

Adding antivirus protection to any system, whether this be a workstation, file server, groupware servers or gateways, adds a layer of performance degradation due to the nature of antivirus activity.

This is specially visible in corporate environments, where a single server has to service hundreds and many times thousands of clients. It is in these environments where antivirus products have to really be optimized in order to become truly effective. Panda Software realizes this and developed the VirtualFile technology to optimize its products much more than other available in the market.

VirtualFile is specially visible in antivirus protection by Panda for File Servers, GroupWare servers (Exchange & Notes), Proxy and Firewall antivirus. In these environments, Panda's products are the only ones in the market that scan and disinfect 100% in memory, while other products still extract files to disk in order to scan and disinfect them, degrading server performance dramatically as compared to Panda.

1998: Pioneers in making daily virus signature updates available

Thanks to the common antivirus engine that all Panda products share, Panda Software was the **first to provide daily updates** of virus signature databases for all its products and platforms. This was back in the beginning of 1998. Nowadays Panda Software is still the only antivirus vendor who regularly provides daily updates of its virus signature database.

Other vendors advertise their ability to update on a daily basis, but what they don't say is that the update is the same from one day to the other, so clients are not constantly being protected against the new viruses. We still see many antivirus vendors providing weekly or even bi-weekly updates. Some vendors do advertise daily and even hourly updates. These are not release updates which are Quality Assured but rather beta updates between their regular weekly or bi-weekly update schedule.

A completely automated daily updating facility is the starting point for any antivirus solution that claims to provide peace of mind and control over enterprise security.

Most Advanced Antivirus Technology

1998: First desktop antivirus to scan TCP/IP traffic

In mid 1998 Panda Software introduced Panda Antivirus Platinum, the first antivirus ever to scan at the Windows Winsock level the SMTP, POP3, HTTP, FTP, and NNTP traffic.

Other antivirus vendors such as Symantec, McAfee and Trend Micro still don't offer such a comprehensive protection at the protocol level for and Internet-connected community. Most competing antivirus products have specific applications or plug-in developments to their antivirus engine in order to protect the Internet traffic.

Because of this Panda Antivirus Platinum has been labeled by many as the “**Antivirus of the Internet Generation**”.

1998: Pioneers in scanning for viruses in e-mail message bodies

Panda Antivirus for Exchange and Outlook (both client and server) and Panda Antivirus Platinum were the first products of its kind to scan the body of e-mail messages.

For Exchange and Outlook e-mail platforms, Panda Antivirus was the first antivirus (in 1998) to ever receive a 100% In-The-Wild certification by West Coast Lab's CheckMark. It took competing products a year and a half to achieve such a certification (www.check-mark.com).

Even before VBS/BubbleBoy, the first e-mail body virus that activated itself by only reading an infected e-mail, Panda's products were prepared to handle the threat. It took competing products a long time to be able to stop this proof-of-concept virus.

An even more frightening example during the year 2000 was Kak.Worm, the virus which inserted itself in the HTML body of e-mail messages and infected users only by opening the message. Again, Panda Software's products could detect and disinfect this virus before users could even open the infected e-mail. For almost an entire year after Kak.Worm was first discovered, none of the competing products could stop their clients from its infection.

1998: First antivirus capable of scanning and disinfecting Outlook Express

In 1998 Windows 98 was released to the market. This new operating system incorporated Outlook Express as the default e-mail client, and so it became the de-facto e-mail program for home users and small companies alike. Today, many of the new viruses are designed to take advantage of the many security holes of Outlook Express and Internet Explorer. There are many examples of viruses specially written for this e-mail client, such as the Kak.Worm virus. The danger lies in the fact that Outlook Express can render a web view of e-mail messages, and thus execute malicious code.

1999: First antivirus for Exchange Server capable of protecting the Internet Mail Connector (SMTP stack)

The first antivirus for Exchange to be certified by either ICISA or CheckMark was Panda's. This was back in 1998. Since then further developments introduced into Panda Antivirus for Exchange Server have made it the first MAPI-based antivirus solutions that was able to scan and disinfect the Internet Mail Connector SMTP stack within the message transfer agent. This is the only MAPI-based antivirus solution that effectively scans and disinfects absolutely all inbound and outbound messaging traffic completely, guaranteeing 100% virus-free corporate environments.

In the meantime, other antivirus vendors are still extracting files to disk for scanning and disinfection, do not detect viruses in message bodies, have low performance metrics, and are not able to guarantee a 100% virus-free Exchange environment.

1999: First antivirus to use AutoTuning technology for performance optimization in Windows NT/2000 and Exchange servers

Hand in hand with its philosophy of providing corporate antivirus solutions that meet customer needs, Panda Software developed a new technology which was integrated into its server-based solutions in order to dramatically improve performance. AutoTuning is a Panda feature that automatically adjusts antivirus on-demand scan and disinfection jobs to the server's CPU load. It does this by watching the system processes and automatically adjusting itself to these processes.

While other antivirus products on the market reach 100% CPU utilization during certain antivirus scans, Panda's server-based products hover right along system processes without interfering with server operations.

Most Advanced Antivirus Technology

2000: First antivirus for Notes/Domino to use the new Extension Manager technology recommended by Lotus

'Extension Manager' is the most modern system developed by Lotus that allows a program to be run natively in a Notes or Domino server. The main difference between Extension Manager and the older Hook Driver technology, which most of the rest of the antivirus industry is still using, is the high level of integration that Extension Manager allows in server tasks (in databases, Router, Replication, and other server tasks).

In the case of antivirus programs, the Notes/Domino server itself informs the antivirus when to carry out its tasks.

An antivirus that uses Extension Manager technology allows all databases and all of the other server tasks to be protected natively, while those that use Hook Driver technology can only protect the task that manages the user databases, but not the task of the Router, Replication, etc. The access of Hook Driver technology is limited to three events, while Extension Manager accesses more than 160 events.

An antivirus that uses Extension Manager integrates perfectly in the Notes / Domino system, acting as another system thread rather than an external application that has to monitor and interrupt the Notes operations and processes every time it needs to act.

Panda Antivirus for Notes/Domino Servers is the first antivirus for this platform to make use of Extension Manager, which combined with Panda's VirtualFile memory scanning technology, improves server performance up to 300% over other antivirus products on the market for this platform. All other antivirus solutions for Notes/Domino server still extract attachments to disk in order to scan and disinfect them, dramatically penalizing server performance.

2000: First antivirus to provide SmartClean technology to repair system damages from virus infections

The sophisticated techniques used by the most recent viruses, worms and Trojan horses, besides infecting files and opening back doors into the computer, spread and execute their damaging payload by making changes to the system's configuration, such as modifying registry entries, system files, or dropping malicious files.

Traditional antivirus software detects and disinfects individual files, but cannot deal with the modifications made by the new viruses and Trojan hoses, which compromises system integrity.

Antivirus companies such as McAfee, Symantec, Trend Micro and others usually provide manual instructions or external per-virus utilities to completely clean these type of infections.

Panda Software is the first antivirus developer to provide a *SmartClean* technology within its products, which allows the original system configuration to be reset after it has been modified by a virus or Trojan horse. As well as disinfecting viruses, it resets the original system configuration values, after they have been changed or modified by a virus such as: COOL NOTEPAD, FUNLOVE, I LOVE YOU, KAK WORM, MATRIX, NAVIDAD, SHELL SCRAP, VERONA, PRETTY PARK or ANNA KOURNIKOVA.

The first antivirus product in the world to incorporate such a technology was Panda ActiveScan, the free online antivirus utility available from www.pandasoftware.com. Panda ActiveScan was launched in the year 2000. The first commercial antivirus product for the retail market in the world to incorporate this technology is Panda Antivirus Titanium (www.pandasoftware.com/titanium).

Trend Micro mistakenly announced that it was the first antivirus to provide such a technology which it calls Trojan System Cleaner:

http://www1.internetwire.com/iwire/release_clickthrough?release_id=27055&category=Technology

2001: First retail antivirus to incorporate SmartClean technology

During the second quarter of 2001, Panda Software launched Panda Antivirus Titanium, the first retail antivirus product in the world to incorporate SmartClean technology. To date, no other antivirus in the world includes this type of technology, and competing products and vendors must provide manual disinfection instructions and external utilities to completely disinfect a virus or trojan horse infection.

Again, Panda Software's R&D efforts have proven to advance antivirus technology to the next level and preventing infections rather than acting upon them after the fact.

Most Advanced Antivirus Technology

2001: Revolutionary new Heuristic approach for unknown viruses

Most antivirus products on the market advertise that their products can detect known and unknown viruses. Antivirus technology that detects unknown viruses is based on a "heuristic" engine, which basically interprets what an executable file will do to a system, and flags it as non-suspicious or suspicious.

There are four types of heuristic engines: for MS-DOS, Win32, Macro and Script viruses. Most competing antivirus products only integrate two or three of these heuristic engines, while Panda Software's products integrate all four heuristic engines, making them the most prepared to stop unknown viruses.

The latest addition to the Panda product line is the Scripts Heuristic, which is capable of stopping the newest and most lethal mass-mailing VBS viruses before they are even born.

Best GroupWare & Server Performance

As mentioned before, e-mail is now responsible for about 90% of corporate viral infections. This makes protecting GroupWare servers key and probably the most important part of the corporate security strategy.

In addition, even though corporations have gateway protection installed to prevent incoming viruses, the reality is that many corporate infections come from non-corporate e-mail systems such as web-based free e-mail services and outside POP3 accounts. Once downloaded directly to the desktop, the virus can easily and rapidly propagate via platforms that are prime virus breeding grounds, such as Exchange Servers and Notes/Domino systems.

Therefore antivirus protection is specially important in these GroupWare systems, since they are the main gateways between desktops and the outside world, and most of the new virus technologies take complete advantage of the low security mechanisms of such systems, for example, to mass e-mail themselves to the entire corporate Address Book in a matter of minutes or seconds.

Best GroupWare & Server Performance

Microsoft Exchange



Panda Software has been working with Microsoft and other large multinationals to make Panda Antivirus for Exchange Servers the most complete, reliable, and performance optimized antivirus solution for these platforms. This product has been developed by listening to the suggestions made by large corporations which do not find products scalable and reliable enough to meet corporate security needs.

Since 1999 Panda Antivirus for Exchange 5.5 Servers has been the first and only MAPI-compliant antivirus that has been able to scan and disinfect the Internet Mail Connector and message bodies, as well as OLE embedded objects. This product also stands out for being the most performance optimized and centrally managed. While other antivirus solutions on the market have been going back and forth between different Exchange technologies which over time have proven inefficient (such as AVAPI 1.0), Panda Antivirus for Exchange Server has remained the most stable and reliable solution.

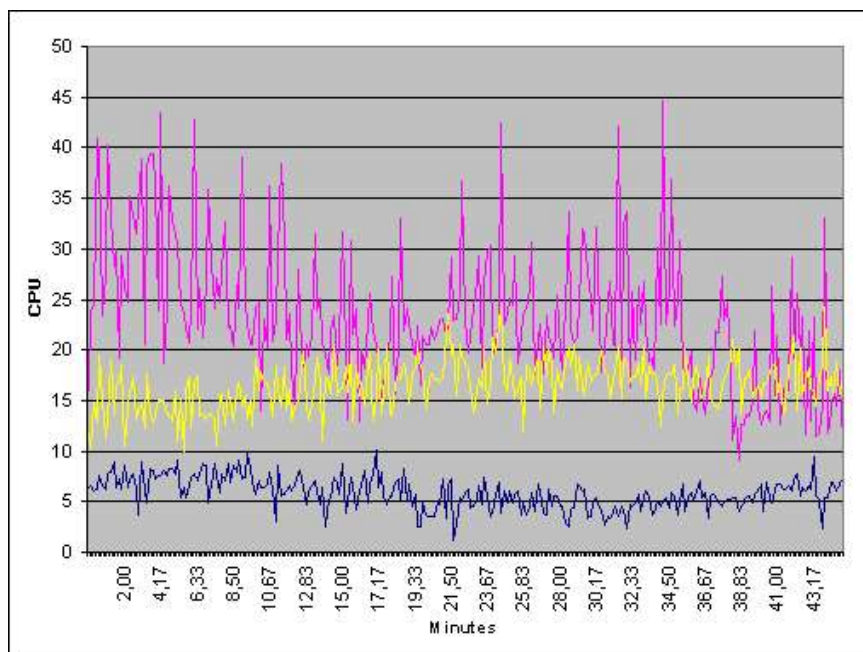
Interestingly enough, none of the competitors products such as McAfee's GroupShield, Trend Micro's ScanMail nor Symantec's Norton Antivirus for Exchange Servers can centrally deploy, update, manage, and monitor multiple Exchange Servers at the same time. Only Panda Antivirus for Exchange Server 5.5 can do this, which is specially useful in large corporate environments.

In addition to being the most centralized and complete solution, where Panda Antivirus for Exchange really stands out is in regards to performance. By using VirtualFile technology, Panda's products are the only ones in the market that scan and disinfect 100% in memory, while competitor's products extract files from the Exchange platform to hard disk, scan and disinfect them, and then re-insert them into the system. This method followed by our competition greatly reduces performances.

As an example, the following charts reflect internal comparative tests carried out with the latest versions of antivirus solutions for Exchange:

Tests performed by Panda Software using the latest versions of antivirus solutions for Exchange Server 5.5 available from the respective vendors website. Testing Profile included non-infected and infected files of all sizes. Same testing load and profile, such as number of messages, file sizes, number of minutes/hours, etc. was used for all products. Tests performed during May 2001.

Comparative of Panda AV for Exchange vs. McAfee (NAI) GroupShield



- Without Antivirus
- Panda Antivirus
- McAfee (NAI)

Best GroupWare & Server Performance

Lotus Notes / Domino



There are currently two technologies available today for antivirus solutions for Notes/Domino systems: **Hook Driver** and the new **Extension Manager**.

The Hook Driver was the first technology made available to antivirus applications in order to scan messages and documents from Notes/Domino platforms.

Its basic operation simply hooks into the Notes system and can only operate natively over the server task. This means that any antivirus solution based on Hook Driver technology must create and use other mechanisms to protect the rest of the tasks.

For example, in order to protect the Router, the antivirus must create a spooling mechanism of the MAIL.BOX database, which means that it is up to the antivirus to notice that the server has a pending task (such as an incoming or outgoing message), and intercept this task and its content (message or document) for its scanning and disinfection operations. This has been proven to be a less-than-ideal approach to Notes/Domino protection, due to the high risk of database and Router corruption and loss of messages. The same goes for other tasks such as server replication.

The main difference between the Hook Driver and the Extension Manager technology, apart from the fact that Lotus itself recommends it, is that the latter one permits a high degree of native integration into all server tasks (database, Router, replication, etc.). Panda Antivirus for Notes/Domino Server is the first antivirus in the market to make use of the Extension Manager since its first release in 1999.

Coupled with Panda Software's VirtualFile technology and the fact that other products extract files to disk in order to scan and disinfect them (while Panda performs these tasks in memory), Panda's is the most performance optimized antivirus solutions for Notes/Domino all around, as is proven by the following internal comparative tests:

Testing Profile

Lotus/Notes Server

Pentium III 866Mhz, 256MB RAM, 30GB HDD
Windows 2000 Advanced Server Service Pack 1, Lotus Domino 5.0.3

Client #1

Pentium III 550Mhz, 128MB RAM, 8GB HDD
Windows 2000 Advanced Server Service Pack 1, Lotus Notes 5.0.3

Client #2

Pentium III 550Mhz, 128MB RAM, 8GB HDD
Windows 2000 Server Service Pack 1, Lotus Notes 5.0.3, Macromagic 4.1q

Client #3

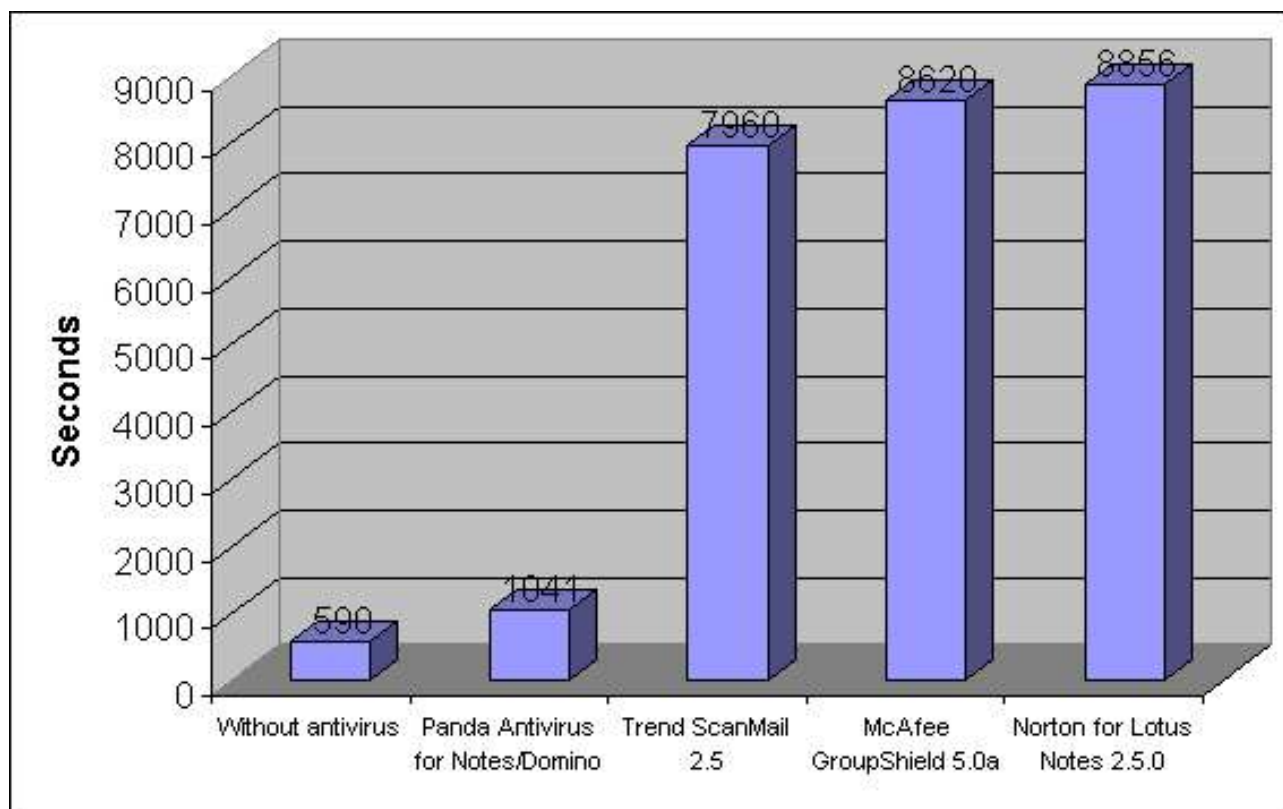
Pentium II 450Mhz, 256MB RAM, 8GB HDD
Windows 2000 Server Service Pack 1, Lotus Notes 5.0.3, Macromagic 4.1q

The Lotus Domino 5.0.3 server was started as a process with the following databases and configuration:

- BIGDOC.NSF
Size: 10.752 Kb
Contains a document with 11 DOC files of 1.545Kb each
- SMALLDOC.NSF
Size: 4.094 Kb
Contains a document with 40 DOC files of 93Kb each
- BIGEXE.NSF
Size: 13.568 Kb
Contains a document with 10 EXE files of 1.652Kb each
- SMALLEXE.NSF
Size: 3.840 Kb
Contains a document with 35 EXE files of 100Kb each.
- ZIP.NSF
Size: 3.994 Kb
Contains a document with 30 ZIP files of 133Kb each. Each ZIP file contains 3 EXE, 2 INI, 1 BMP, and 1 WRI file.

Best GroupWare & Server Performance

The test consisted of continuously opening-editing-closing the document contained in each of the databases up to 50 times. This was achieved with a macro generated by Macromagic version 4.1q. Results show seconds used by each antivirus solution to scan the document.



Tests performed by Panda Software using the latest versions of antivirus solutions for Notes Server available from the respective vendors website. Testing Profile included non-infected and infected files of all sizes. Same testing load and profile, such as number of messages, file sizes, number of minutes/hours, etc. was used for all products. Tests performed during May 2001.

Best GroupWare & Server Performance

Windows NT/2000 Server & Advanced Server



Panda Antivirus for NT/2000 file servers has been designed with one thing in mind: to perform optimally in heavily loaded systems.

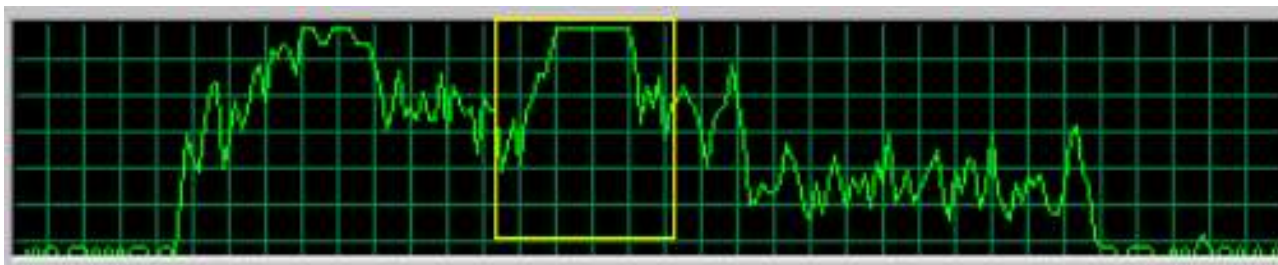
In order to achieve this the antivirus architecture of the real-time scanner and the on-demand functions is able to use the server's resources intelligently, so as to provide total protection against viruses and still be completely transparent to the Operating System and connected users.

To this effect there are three main advanced techniques used:

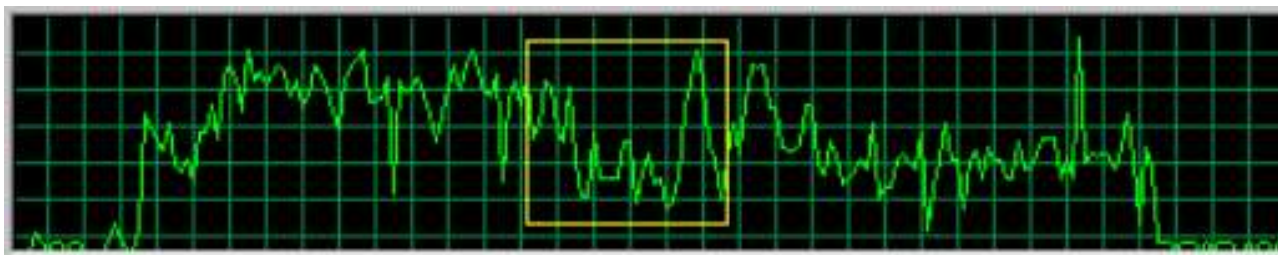
- 3-level cache of scanned files.
- AutoTuning that automatically calibrates the scan jobs based on the CPU load.
- Multi-channel operation that allow for parallel scans on servers with multiple CPUs.

By using these characteristics, it is safe to say that Panda Antivirus for NT/2000 Servers is the only antivirus specifically designed for performance optimization and scalability.

Competing NT/2000 Server Antivirus scan under heavy loads:



Panda Antivirus for Windows NT/2000 scan under heavy loads:



In addition, Panda Antivirus for Windows NT/2000 Server is armed with the following advanced features:

- Online disinfection of operating system files.
- NT Cluster-aware and fault tolerant.
- Optimized NTFS5 scans by using Journaling.
- Compatible with all Microsoft filters.
- Off-line scans with authentication.
- Compatible with NTFS5 and UDFS.
- Compatible with Windows 2000 characteristics such as Reparse Points, Single Instance Store, Encryption Engine (EFS), Mount Volume Points, etc.
- Tested with IOSTRESS, IFSTEST, and VERIFIER Microsoft test suites.

Best GroupWare & Server Performance

Comparative Test of Real-Time Scanners

Description:

Eight (8) consecutive executions of an application that recursively opens files are performed on a Windows 2000 machine. Results are shown in seconds used by each application to perform the scan job.

Testing Profile:

Hardware

4 CPU Pentium Pro 200MHz
515 MB RAM
4GB SCSI HDD

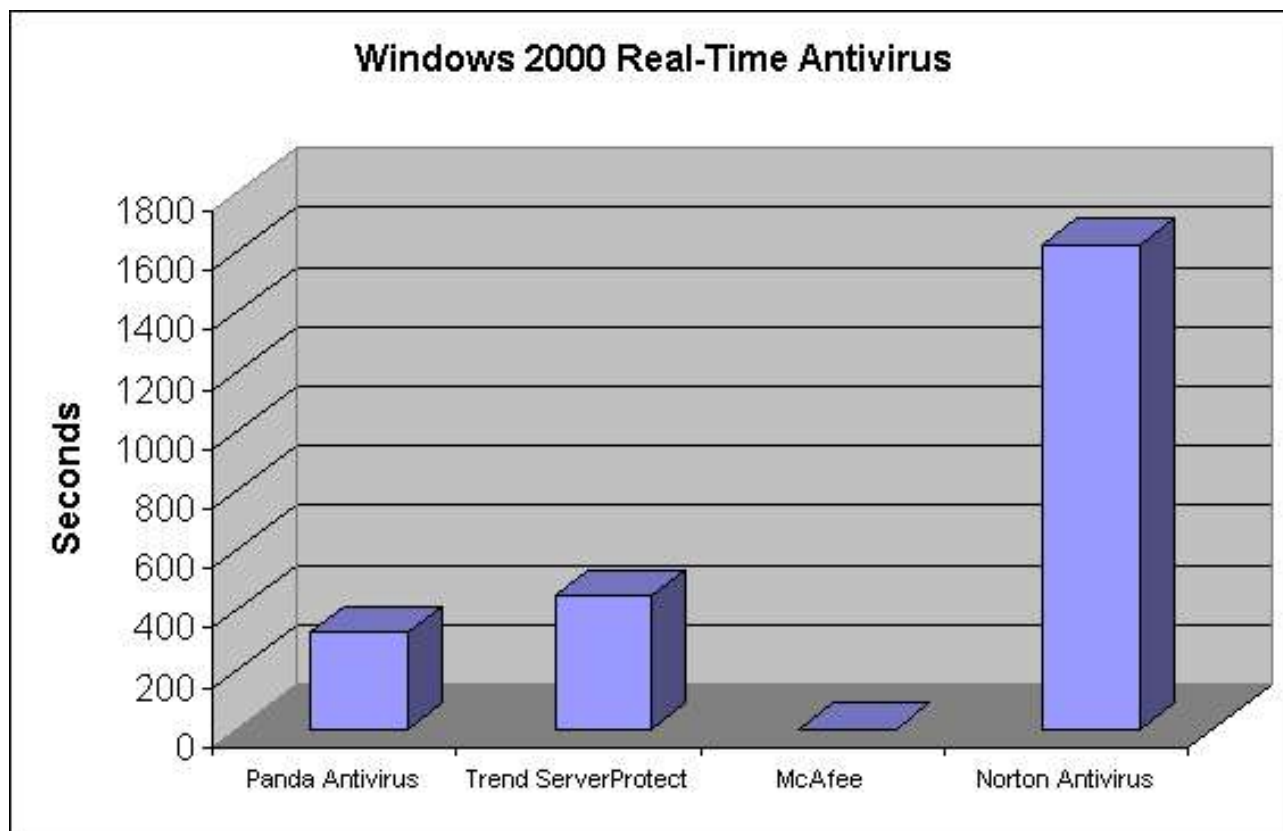
Files:

Total of 10.945
Executables: 235 (COM)
Executables: 9.950 (DLL, EXE)
OLE: 545 (DOC, MSI, XLS)
Other: 215 (PDF, DAT, BIN, HLP, LID, INS, TXT, BMP)

Products Tested:

- Panda Antivirus for NT/2000 Server
- McAfee 4.5.0
- Trend ServerProtect Management Console 5.2
- Norton Antivirus Corporate Edition
Program version: 7.51.847
Engine version: 4.1.0.6

Results:



Note: McAfee resident driver automatically deactivated itself after a long period of maximum load.

Truly Centralized Management

Medium and large sized corporations alike have software management needs that are outside the scope of antivirus and security products. Specially in environments where hundreds of servers and thousands of workstations are spread throughout the country or throughout the world in multiple remote offices, antivirus and security policies must take into consideration central deployment and ongoing management.

Panda's products are developed with one goal in mind: 100% central management. This is achieved thanks to Panda Administrator, the administrative console that is capable of centrally managing antivirus protection throughout the entire corporate infrastructure:

- Deploy to single or multiple remote servers and workstations simultaneously.
- Configure single or multiple remote servers and workstations simultaneously.
- Monitor multiple remote servers or workstations simultaneously.
- Update servers and workstations remotely and simultaneously.
- Consolidate multiple remote logs into a single, manageable virus log for statistical analysis and virus entry point troubleshooting.

While other solutions require one-by-one deployment to servers (specially GroupWare), Panda Administrator can deploy simultaneously to these servers, even with a pre-defined user configuration.

Product Awards & Certifications

Ever since 1997 Panda Software has constantly been achieving quality certifications from the most prestigious independent security organizations throughout the world, such as the International Computer Security Association (ICSA Labs), West Coast Labs' CheckMark, and Virus Bulletin.

In fact, Panda Software holds **more certifications than McAfee and Trend Micro** and other well known antivirus vendors.

It is true that many antivirus vendors hold many awards and certifications. However it is important to note how old these are, since they are no good if they relate to older products or versions which are no longer in the market. Recently, Windows 2000 Magazine named Panda Antivirus the best antivirus for Windows 2000 platforms. In addition, Chip China ranked Panda Antivirus the number 1 antivirus, ahead of competing products from McAfee, Symantec and others. The story repeats itself by the European VNU Labs which named us "Recommended Product" and other industry magazines, such as Windows Magazine, PC World, PC Actual, CRN, PC Week, PC Computing, Info PC ...

You can find out more about Panda Software's awards and certifications at www.pandasoftware.com/awards



July 31st 2001: PCWorld Magazine names Panda Antivirus Platinum "the Undisputed Champ".

July 2001

Secure Computing Magazine gives Panda Global Virus Insurance a 5-star rating.

Software As a Service

Panda Software has pioneered the concept that antivirus software and antivirus service and support are one and the same. Unlike other vendors who charge their clients additionally for technical support or special services, Panda's products are backed 100% by our own international technical support team day and night, 365 days a year.

■ Business Week

(<http://www.businessweek.com/smallbiz/news/date/9911/f991103.htm>):

"If you consider that Network Associates' 300-person customer support team services \$440 million of sales and Panda's 80-person team supports \$40 million in sales, it's clear how being small might translate into customer loyalty."

Since the date this article was release, Panda Software has more than doubled its technical support team to provide even better service to its client base.

■ European VNU Labs 2001 Antivirus Comparative

(<http://www.hispasec.com>):

"Panda Software is pushing hard internationally with an advanced product and a new service concept that is pulling the rest of the [antivirus] market."