



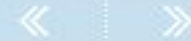
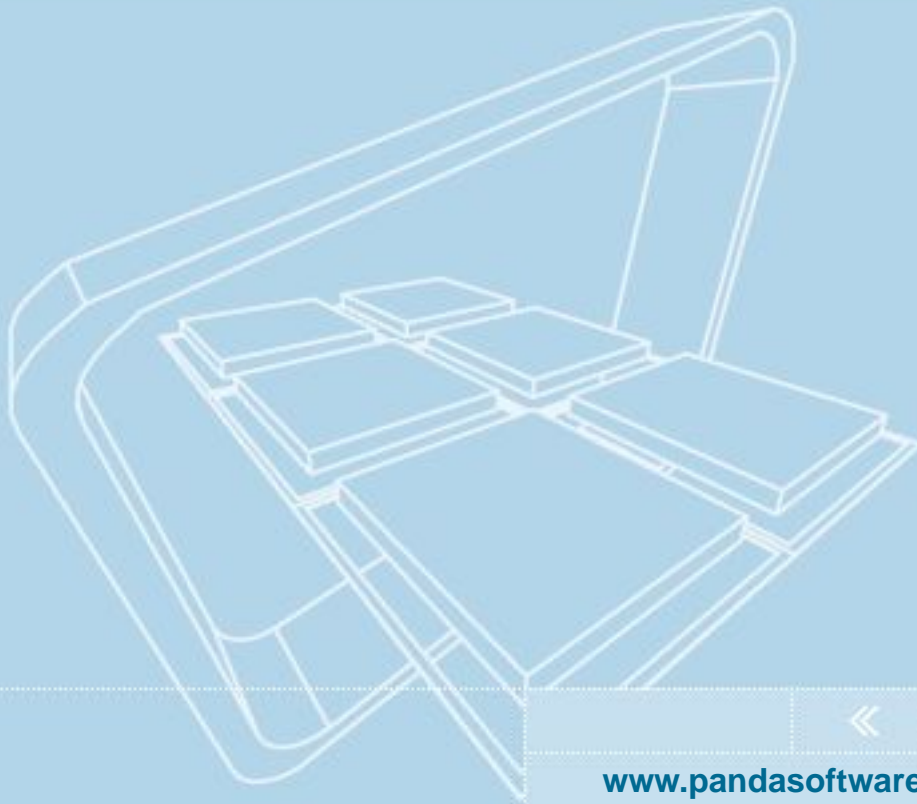
White Paper

Antivirus Technologies for Corporate GroupWare Environments

Index

| | |
|--|---|
| ▶ Antivirus Technologies for Notes/Domino | 3 |
| ▶ Hook Driver | 3 |
| ▶ Extension Manager | 5 |
| ▶ Antivirus Technologies for Exchange | 6 |
| ▶ AntiVirusAPI (AVAPI 1.0) - McAfee, Trend, Symantec | 6 |
| ▶ ESE API - Sybari, Trend | 7 |
| ▶ MAPI - Panda Antivirus for Exchange Server | 8 |
| ▶ Virus Scanning API (VSAPI 2.0) - Panda Antivirus for Exchange 2000 | 9 |

Note: This document simply aims to highlight the similarities and differences in terms of functionality and implementation between the different technologies used by various commercial antivirus products in corporate installations in Exchange and Notes/Domino platforms. The products mentioned are produced by Network Associates, Panda Software, Sybari Software, Symantec and Trend Micro.





Antivirus technology for Notes/Domino

There are currently two technologies used by antivirus products for servers in corporate Notes/Domino environments: **Hook Driver** and the new **Extension Manager**.

This document aims to analyze the differences in functionality and implementation of these technologies in corporate Notes/Domino environments.

Hook Driver

Hook Driver is the first and oldest antivirus technology provided for scanning and disinfecting document databases in Notes and Domino environments.

Antivirus products based on Hook Driver technology hook onto the Notes system and monitor its tasks. The antivirus has to recognize when the server has performed a task and intercept this task and its content (mail or document) in order to scan and, if necessary, disinfect it.

Although Hook Driver technology has a way of hooking onto the server databases, the fact that it does not offer a functional interface integrated with the Router (MAIL.BOX) represents an important limitation.

In the case of antivirus products that scan the document and Router (MAIL.BOX) databases, the antivirus based on Hook Driver needs to extract documents and mail from the Notes system, scan and disinfect them and then reinsert them in the Notes / Domino environment mail flow.

Another limitation of this technology is that the antivirus can only hook the task that manages the normal user databases and not other tasks such as:

- Mail Router
- Replication between servers tasks
- HTTP (Domino) server
- Other server tasks

In order to scan these tasks, in particular the mail Router, it is necessary to create procedures that are not recommended by the manufacturer Lotus.

The commercial antivirus solutions for Notes/Domino servers that use Hook Driver technology are: **McAfee, Symantec, Trend Micro and Sybari**.

We are now going to examine the consequences of using an antivirus product based on Hook Driver technology.

The risks involved in using Hook Driver technology in antivirus products for Notes or Domino servers are quite significant, above all because of the load and limitations this technology presents when natively accessing server tasks. The main risks are as follows:

- **Difficult to install:** one of the characteristics of using Hook Driver technology is that the clients (network administrators) need to manually create a Cross Certificate for each server in which they want to install the antivirus. A Cross Certificate is a digital authorization that a company generates in order to allow another entity to access its Notes servers. In other words, the antivirus manufacturer needs authorization to be able to access the company's servers, with the security problem that this involves. In addition, creating cross certificates is not an easy task and as this process must be carried out in each server, it makes the task of installing the antivirus in servers more difficult.
- **Unnecessary load on the server:** the antivirus solutions that use the Hook Driver technology extract documents from the Notes system, copy them to a temporary file in the hard disk, scan and disinfect them in the hard disk and then reinsert them in the Notes system flow. All of these read and write disk operations significantly slow down the performance of the Notes / Domino servers.



Index



www.pandasoftware.com



- **Corrupt messages in the Router:** as the Hook Driver technology does not have an antivirus interface integrated with the Router, the antivirus solutions based on this technology need to create an additional task that accesses the MAIL.BOX in the Notes system. This additional task searches for new messages in the original MAIL.BOX queue every portion of a second. If it finds one, it scans and disinfects the message using the following process:
 - Marks the message as 'dead' in the original MAIL.BOX.
 - Figures out that the message must be scanned.
 - Extracts the attached file to a temporary file in the hard disk.
 - Scans the file in the hard disk, where it will also be disinfecting if necessary.
 - Reinserts the file in the MAIL.BOX document.
 - Removes the 'dead' mark.

Figuring out that there's a new message in the Router and marking it as dead has to be done quickly (faster than the Router) so that the antivirus can get to it before the Router hooks it in order to send it. There is a risk that the Router could hook the message from the queue before the antivirus can mark it as dead.

The Router (MAIL.BOX) is not designed to be accessed by several tasks at the same time, which means that Hook Driver antiviruses are breaking this 'rule' of Notes / Domino functionality, therefore the probability of the database being corrupted is quite high, as there are two tasks modifying the database and they could corrupt the indexes. Below is an example of a typical scenario:

- The Router recognizes the message as 'live'.
- At the same time, the antivirus marks it as 'dead'.
- As the Router thinks that it is live it tries to route it, but it has already been marked as dead, which means that a message marked as dead reaches the next server. This message will be permanently blocked in the next server.

Altering the process of the Router like this could result in queue backlog problems.

- **Difficult to manage:** the antivirus solutions for Notes / Domino environments based on the Hook Driver technology cannot truly be managed remotely and centrally, as the antivirus must be installed in each server one by one, in the majority of cases from the server console itself. In addition, some of them do not have an administration interface and in order to make simple changes to the antivirus configuration, files such as NOTES.INI must be modified manually.
- **Reliability:** if an antivirus based on Hook Driver has a problem with the databases (not only because of the antivirus, but also because of corruption, due to a problem with cross certification, etc), the Hook Driver technology will cause the whole server to block. In other words, the antivirus operations are not independent of the Notes server.

Index



www.pandasoftware.com



Extension Manager

'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 technology and Hook Driver is the high level of integration that Extension Manager allows in server tasks (in databases, Router 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.

There are significant advantages to using this new technology in antivirus products for servers. We will look at some of the main advantages in more detail:

- **Easy to install:** with Extension Manager technology it is not necessary to manually create cross certificates for each server that needs protecting. Thanks to this advancement, it is possible to install, configure and manage the server antivirus in a way that is truly centralized and remote.
- **Optimized performance:** thanks to the combined use of Panda Software's VirtualFile technology and Extension Manager technology, the antivirus can scan absolutely all traffic (documents and mail) in memory. Hook Driver technology however, needs to extract the files to a temporary file in the hard disk, which significantly slows down the server. The antivirus based on Extension Manager optimizes server performance by quickly scanning in memory.
- **Native integration in the Router:** Extension Manager technology natively integrates external applications in the Router, which is non-existent in Hook Driver technology. The difference is huge, above all in terms of server performance and mail scan efficiency.
- **Centralized and remote administration:** as cross certificates do not need to be created manually between each server and with the antivirus manufacturer, the solution based on Extension Manager allows the antivirus to be managed (installed, configured, updated, monitored, etc.) in a way that is truly automatic, centralized and remote.

Panda Antivirus for Notes / Domino is, as of today, the first and only antivirus on the market to use Extension Manager technology, recommended by Lotus.

[Index](#)

www.pandasoftware.com





Antivirus Technologies for Exchange

AntiVirusAPI (AVAPI 1.0) - McAfee, Trend, Symantec

- ScanMail and Norton use both AntiVirusAPI (AVAPI 1.0) and MAPI technologies. Although they market this as an advantage, they are actually loading two residents (Services under Windows NT) in each server instead of one. This considerably reduces server performance.
- Although the antivirus can be managed remotely through these products, it can only be managed in one server at a time. These products are not designed for large scale installation with remote offices and WAN links.
- Neither of these products can scan the content of RTF, HTML or RTFHTML messages, nested messages or embedded OLE objects.
- As these products rely on the first version of the AntiVirusAPI (AVAPI 1.0), these antivirus products cause many problems not only when detecting viruses, but also limiting functionality and performance of the Exchange server. Many of the problems that these antivirus products can cause are documented in the Knowledge Base on the Microsoft web site, for example:
 - Information Store Crashes When Using Antivirus Application Programming (AVAPI)
 - Internet Mail Service Does Not Deliver Message After You Install Virus Scan Software
 - Inaccessible attachments
 - Messages that seem to be stuck in the Outbox
 - Autoforward Rules May Be Disabled When Using Antivirus API
 - Increased latency of directory and public folder replication
 - Offline folder (*.ost) synchronization time-outs
 - Move Mailbox Utility Does Not Work When Antivirus API Is In Use
- However, to our knowledge, there is no technical problem documented about Exchange antivirus products based on MAPI.
- The following, taken from Microsoft's Website, summarizes the risks of installing a product based on AVAPI 1.0, as are ScanMail, GroupShield or Norton:

If you are considering a move to third-party products that use the antivirus API, you must be aware that issues may arise that may seem related to performance of the information store. Based on the architecture of the antivirus API, the speed at which attachments are scanned is bound by the vendor's implementation of the scanning DLL. In addition, because third-party vendor's solutions run in process with the information store service, issues (such as memory or processor use and access violations in the Store.exe program) may become harder to troubleshoot because there is no way to distinguish between the information store and the vendor's DLL.

Index



www.pandasoftware.com



ESE API - Sybari, Trend

- Sybari and Trend use a series of undocumented calls to the Microsoft ESE API. What they do is to hook the Exchange server .EDB file. Although this method has its advantages by scanning the read and write methods of files, it also runs more risks than other antivirus products.

- Curiously the biggest criticism of this technology comes from Microsoft, who say in one of their web pages on antivirus strategies for Exchange server:

No software or hardware should preempt or modify the Exchange Server services' method of reading to and writing from the data files. This might cause the Exchange Server services to stop working or corrupt the data files.

- Sybari is not an antivirus manufacturer. It uses third party antivirus scan engines, which means that the client indirectly depends on other companies for updates, virus alerts and technical support for problems with the scan engine.
- For obvious reasons, there have been rumors that Microsoft will not support Exchange clients who have Sybari Antigen installed.

[Index](#)



www.pandasoftware.com

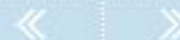


MAPI - Panda Antivirus for Exchange Server

Is the most effective and best performing antivirus solution for companies and institutions of all sizes. Panda has implemented advanced antivirus functionalities and techniques that offer stability and performance required by the most demanding corporate Exchange installations.

- Our antivirus is optimized for better server performance. Through the use of MAPI, it achieves better server performance than other antivirus solutions. This is due to the fact that antivirus solutions based on AVAPI 1.0 completely stop the functioning of the Exchange server until the antivirus returns the messages.
- The Panda Antivirus for Exchange Server solution offers the most centralized management of Exchange servers available on the market. From Panda Administrator it is possible to remotely install, configure and update multiple Exchange servers at the same time from the network administrator's workstation. Other solutions can only manage the antivirus protection of Exchange servers one by one.
- Panda detects viruses in places other antivirus solutions can't reach: body of messages in any format (such as RTF, HTML y RTFHTML), embedded OLE objects, and many more compressed formats and nested messages at all levels.
- There is a mistaken concept in the market about antivirus products based on MAPI, as it is often said that outgoing messages slip past them. Although this may be true for other antivirus solutions based on MAPI, this is not true for Panda, as we offer the only antivirus based on MAPI that as well as disinfecting the Information Store, also scans and disinfects the Internet Mail Connector (the SMTP stack), protecting both incoming and outgoing mail in real-time.
- Panda Antivirus for Exchange Server includes a heuristic scan engine for detecting unknown DOS, Win32 and Macro viruses. Other products do not include a heuristic scan or only scan one of these three types of files.
- In their web site Microsoft refers to a model installation of Exchange Server in a large organization. About the antivirus solution for the installation they say: "The solution suggested [...] is to install the Panda corporate anti-virus system, because of its level of integration with Microsoft Exchange."
- Panda Antivirus integrates its own technology for intelligent CPU monitoring, called AutoTuning. Thanks to this technology we optimize server performance to the maximum during on-demand scans, without interfering in the slightest way with the normal operations of Exchange.
- Panda Software works in collaboration with Microsoft on many occasions, providing antivirus know-how to Microsoft developments, such as Virus Scanning API (VSAPI 2.0), which Microsoft is going to launch with Service Pack 1 for Exchange 2000. This collaboration offers clients Panda solutions that are totally compatible and perfectly integrated in Exchange environments.
(<http://www.microsoft.com/exchange/thirdparty/ISV.htm>)

Index



www.pandasoftware.com



Virus Scanning API (VSAPI) - Panda Antivirus for Exchange 2000

Panda Software has been working in collaboration with Microsoft for over a year, promoting the new technology Virus Scanning API (VSAPI 2.0) available with Service Pack 1 of Exchange 2000.

Panda Software is using VSAPI 2.0 in the new Panda Antivirus for Exchange 2000, whose Beta version release will be announced soon.

In this way and by responding to market demand, we provide administrators with the two antivirus solutions that use the most advanced technology, thereby demonstrating the continuous commitment to antivirus protection for e-mail of Panda Software:

- Panda Antivirus for Exchange Server (MAPI): Exchange 4.0/5.0/5.5
- Panda Antivirus for Exchange Server (VSAPI 2.0): Exchange 2000*

* Note:

Contact your Panda Software representative to obtain the Beta versions of Exchange 2000 (VSAPI 2.0).

[Index](#)



www.pandasoftware.com

