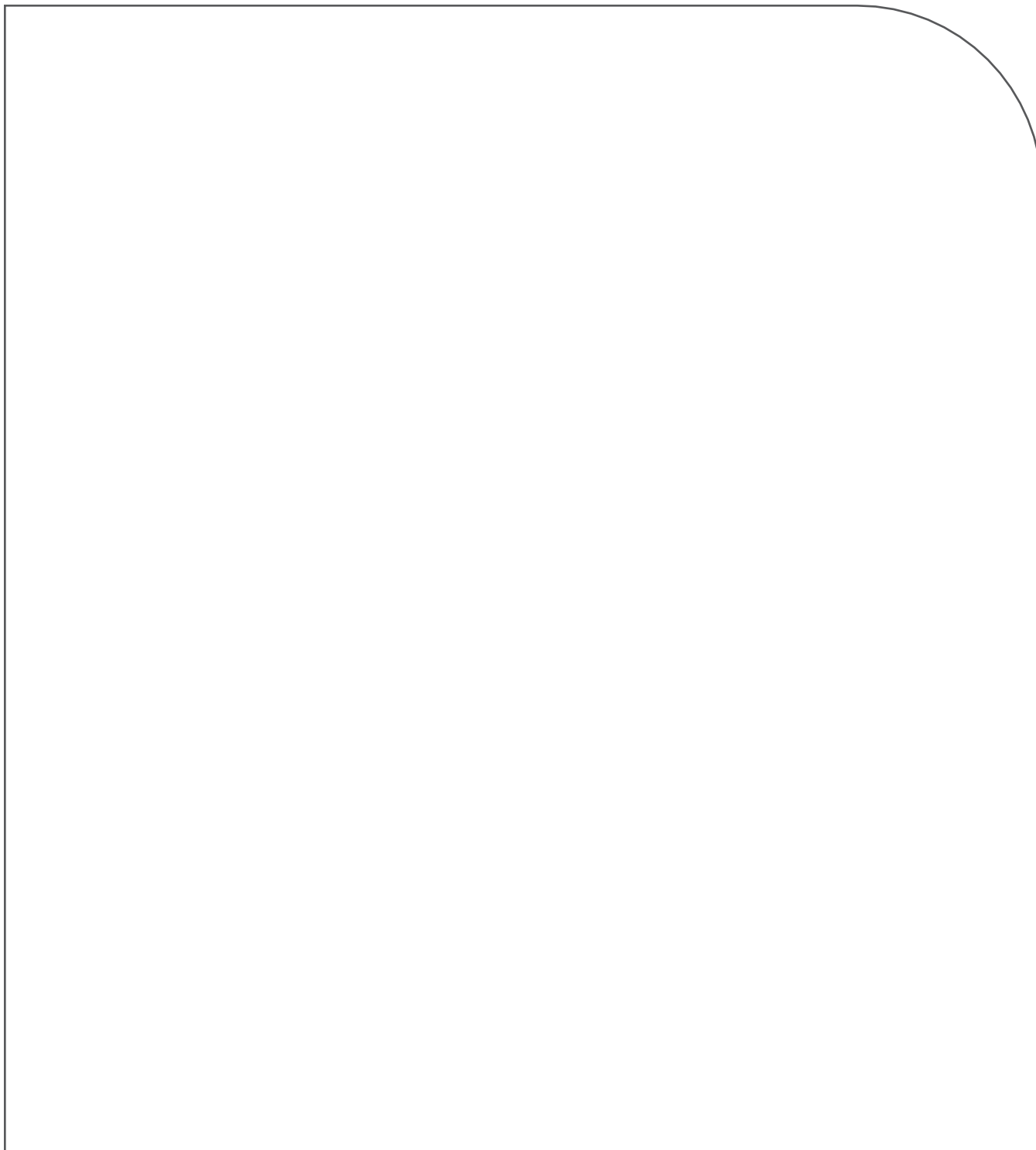


## **GroupShield and the Microsoft Virus Scanning API**

An Anti-Virus Solution trusted worldwide.



## Table of Contents

Summary .....	2
GroupShield and the Microsoft APIs .....	2
The Microsoft anti-virus API 1.0.....	2
GroupShield 4.5 and the anti-virus API 1.0 .....	2
The Microsoft virus scanning API 2.0 .....	3
API 2.0 On-access scanning.....	3
API 2.0 Proactive scanning.....	4
API 2.0 Background scanning .....	5
How GroupShield works with the Microsoft virus scanning API .....	3
Exchange 2000 Message Routing and the virus scanning API 2.0.....	6
Benefits of using GroupShield with the Microsoft virus scanning API .....	6
Further Information.....	7

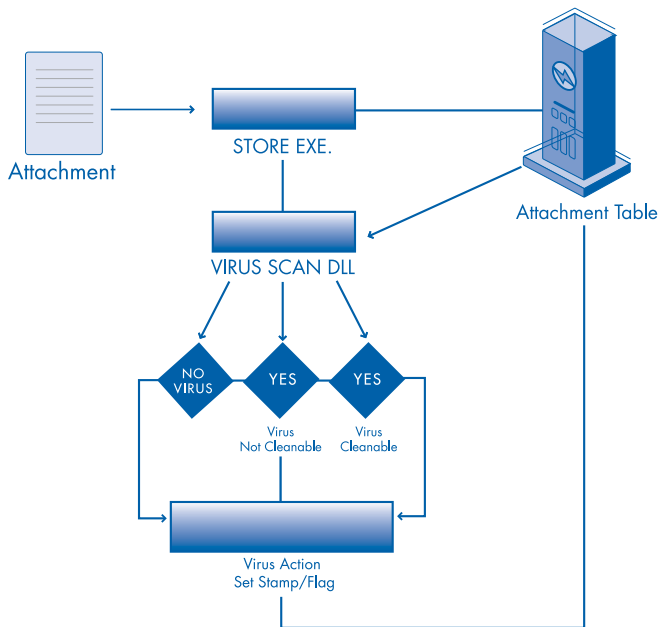
The information in this guide has been provided by Network Associates, Inc. To the best knowledge of Network Associates, Inc., these companies offer the types of products described. These companies are solely responsible for their software, distribution, and support services. Network Associates, Inc. disclaims any and all liabilities for and makes no warranties, expressed or implied, with respect to these products, including, without limitation, the implied warranties of merchantability and fitness for a particular purpose. Distribution of these products, or information concerning these products, does not constitute Network Associates, Inc. endorsement of the products, the companies, or support services. Product information is subject to change without notice.

## Executive Summary

This paper provides an overview of the Microsoft Exchange virus scanning API and how it is used by McAfee GroupShield. For information concerning other aspects of GroupShield—such as clustering and competitive comparisons—please refer to other documents.

### GroupShield and the Microsoft APIs

GroupShield is McAfee’s award-winning solution for groupware content security. By working closely with Microsoft, GroupShield was the first product released to utilize the Microsoft antivirus 1.0 and 2.0 APIs. 1.0 was introduced as part of the Microsoft Exchange 5.5 Service Pack 3 and was also used in the initial release of Microsoft Exchange 2000. With Service Pack 1 for Exchange 2000, Microsoft updated the API to improved functionality and performance, and in doing so, renamed it from “antivirus” (AVAPI) to “virus scanning” API (VSAPI) 2.0.



### The Microsoft antivirus API 1.0

The antivirus API 1.0 was introduced in Exchange Server 5.5 SP3 to provide high-performance scanning of attachments in the Exchange Server information store. While antivirus scanning solutions had been available using MAPI, inaccurate scan-timing and periodic server loading meant it was

possible for attachments to be delivered to users before being scanned. To combat this vulnerability, the antivirus API provides low-level hooking into the Exchange stores and ensures that all attachments are scanned before a client can access them. In addition to scanning, the antivirus API also provides the ability to selectively repair, mark as suspicious, or replace any attachment. Any time an attachment is opened, modified, or sent by a user, the antivirus API ensures that the attachment is completely scanned before allowing it to continue on to delivery or storage.

Server performance is significantly improved over other solutions, such as MAPI based scanning or other inter-process communication methods, because the API provides a means for the virus scanning to run in process with the information store. By scanning at the store level, attachments need only be scanned once, rather than multiple times as they move from one user to the next.

### GroupShield 4.5 and the antivirus API 1.0

GroupShield 4.5 was released to use the new Microsoft API, but because 1.0 did not scan message body text or provide attachment sender and recipient information, GroupShield 4.5 continued to use MAPI for on-demand scanning. However, additional solutions were required for on-access scanning, so the Message Body Scanning and Resolve Names utilities were developed for the Microsoft Exchange 5.5 platform. The Body Scanning utility provided on-access scanning capabilities to protect against message-borne threats, so that the Resolve Names utility could then be run as required on the log and quarantine log.

In the initial release of Microsoft Exchange 2000, Microsoft continued to use the antivirus API 1.0 until 2.0 could be released as part of the first service pack. To provide interim protection against message body threats, McAfee developed the SMTP Scanning utility that would scan in-bound messages from other servers.

## The Microsoft virus scanning API 2.0

While the antivirus API 1.0 provided improved scanning of attachments, version 2.0 added functionality and addresses previous shortcomings. The virus scanning API 2.0 was released as an upgrade to Microsoft Exchange 2000 in Service Pack 1 and featured the following enhancements:

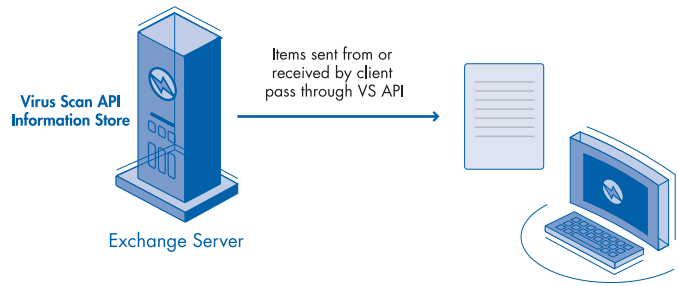
- Scanning of all message items, not just attachments
- Message details including sender and recipient information
- Native MIME/MAPI content scanning
- Proactive scanning
- Priority-based queuing
- Multithreaded queue processing
- Per-Messaging Database configuration options
- Enhanced background scanning
- Event logging
- Virus scanning API-specific Performance Monitor counters

### Important Note:

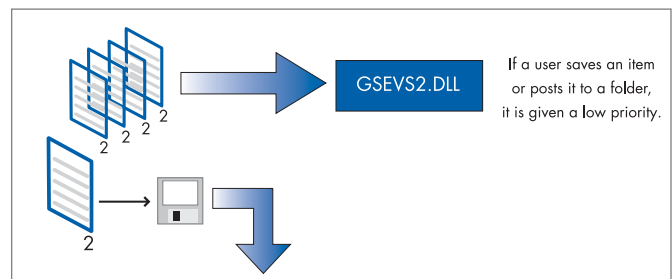
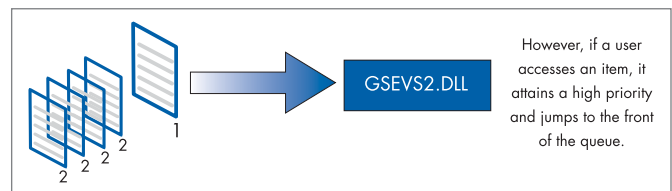
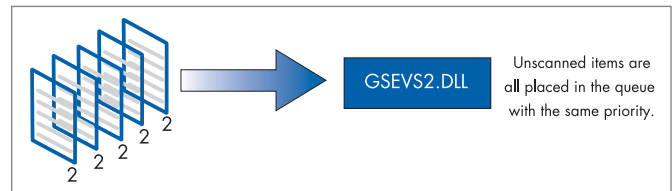
McAfee and Microsoft use different terms to describe scanning that takes place when an item is being requested by a user or process. McAfee refers to this realtime scanning as "on-access," whereas Microsoft uses the term "on-demand." To maintain consistency with other McAfee materials, this document will use the McAfee convention.

### API 2.0 On-access scanning (aka Microsoft on-demand scanning)

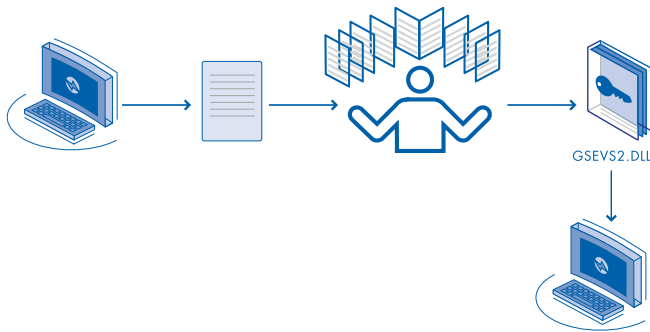
As in virus scanning API 1.0, virus scanning API 2.0 continues to support on-access scanning. As clients attempt to gain access to Exchange items, either by using an Internet protocol-based client such as Post Office Protocol version 3 (POP3), Outlook Web Access (OWA), Internet Message Access Protocol, Version 4rev1 (IMAP4) or by using a conventional Messaging Application Programming Interface (MAPI) client, a comparison is made to ensure that the message body and attachment (if present) have been scanned by the current virus signature file. If the content has not been scanned by the current vendor or signature file, the corresponding item is submitted to GroupShield for scanning before that item is released to the client.



### Global Scanning Queue

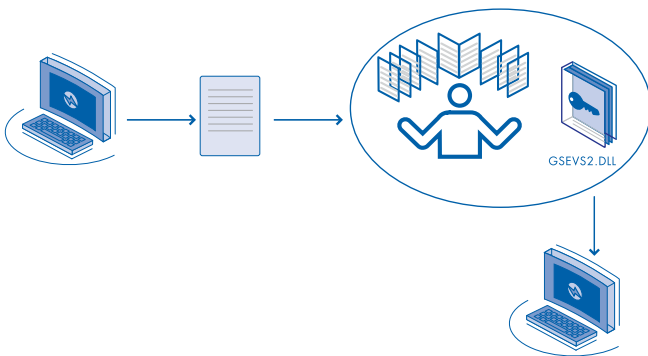


In virus scanning API 2.0, a single queue processes all of the message body and attachment data. Items that are submitted to this queue as "on-demand" (Microsoft terminology) are submitted as high-priority items. This queue is now serviced by a series of threads (the default number of threads is:  $2 * \text{number\_of\_processors} + 1$ ), with high-priority items always taking precedence. This allows multiple items to be submitted to GroupShield simultaneously. In addition, client threads are no longer tied to "time-out" values that are waiting for items to be released. After items are scanned and marked safe, the client thread is notified that the item is available. By default, the client thread waits up to three minutes to be notified of the availability of the requested data before a time-out occurs.



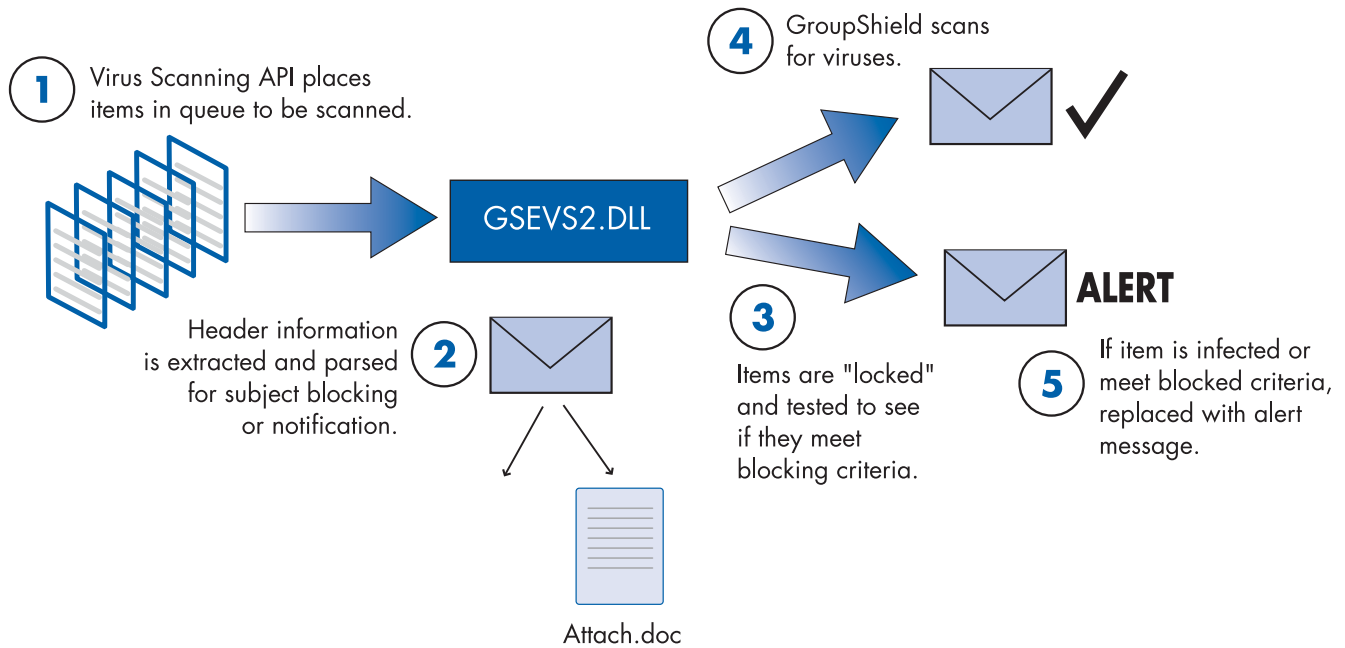
### API 2.0 Proactive scanning

A new feature in virus scanning API 2.0 is proactive scanning of messages. In virus scanning API 1.0, message attachment information was only scanned as it was accessed. In virus scanning API 2.0, items are submitted to a common information store queue as they are submitted to the information store. Each of these items receives a low priority in the queue, so that these items do not interfere with the scanning of the high-priority items. When all of the high-priority items have been scanned, virus scanning API 2.0 begins to scan low-priority items. The priority of the items is dynamically upgraded to high priority if a client attempts to access the item while the item is in the low-priority queue. A maximum of 30 items can exist at one time in the low-priority queue, which is determined on a first in, first out basis.



### API 2.0 Background scanning

Background scanning navigates the series of folders that comprise each user's mailbox and public stores. As items that have not been scanned by the current virus signature file are encountered, they are submitted to GroupShield. Each Messaging Database (MDB) receives one thread to conduct the background scanning process. After the thread completes a pass of all the contents, the thread waits for a restart of the information store process before conducting another pass. As all the contents in a folder are scanned, a flag is set at the folder level so only new and unscanned folder contents will be scanned after a restart. A background scan can also be initiated by GroupShield after an Engine or DAT update.



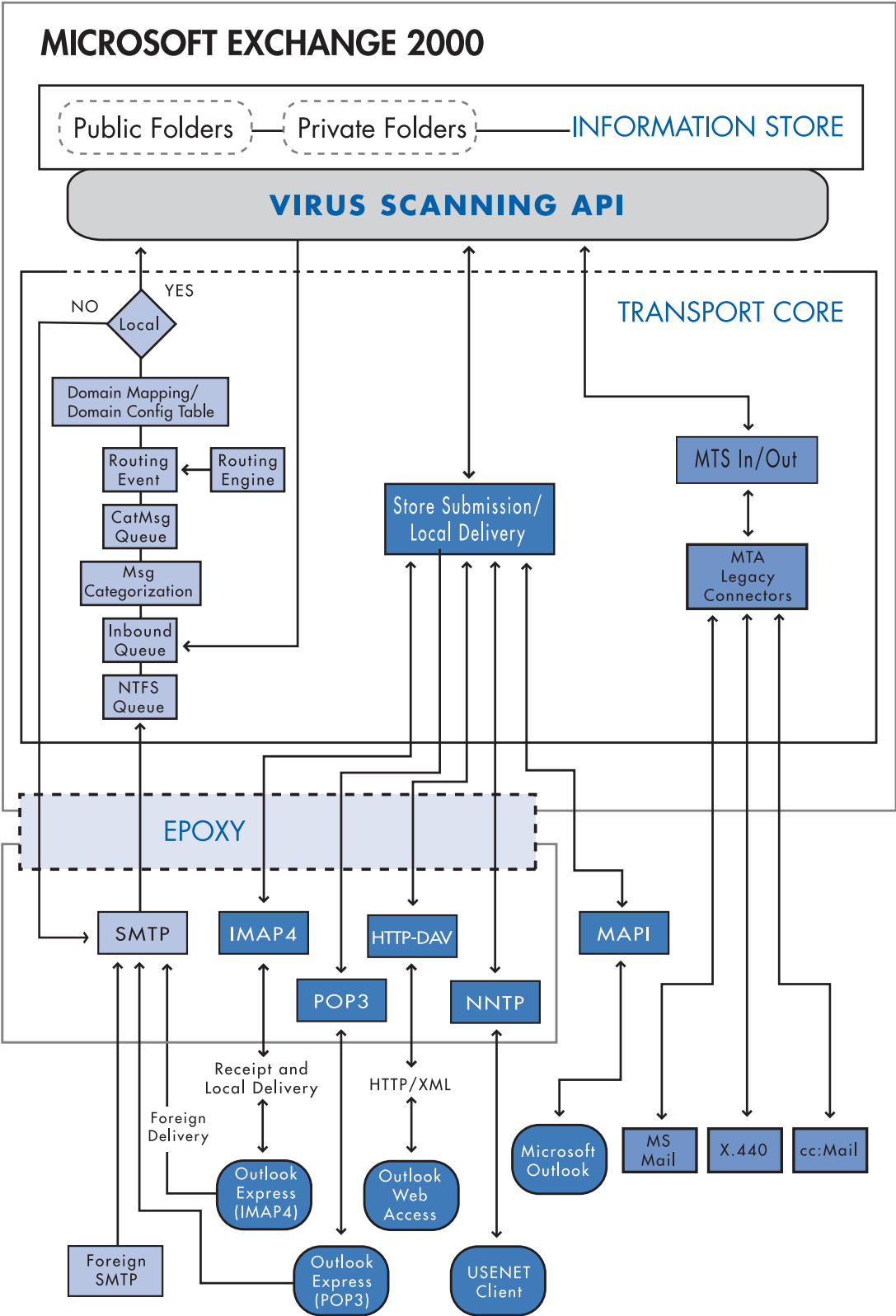
### How GroupShield works with the Microsoft virus scanning API

As items are written and read from the Microsoft Exchange stores, the virus scanning API passes them to GroupShield for scanning prior to routing. After scanning, the item is either delivered, cleaned, or quarantined as required, and the results are noted in the information stores.

### Exchange 2000 Message Routing and the virus scanning API 2.0

The following page contains a diagram that illustrates how messages are routed through Microsoft Exchange 2000 from various email clients and external sources. From this diagram, it can be seen that all messages are routed through the Microsoft Exchange virus scanning API, with the exception of external SMTP traffic.

So long as SMTP messages are being delivered to or sent from the local Exchange 2000 server, they will be scanned. However, SMTP messages sent from a POP3 client or from another server to a non-local recipient will not be scanned. Customers with multiple Exchange servers should, for Best Practice reasons, use GroupShield on each server. If they are using POP3 clients, they should ensure that VirusScan is used to provide scanning of outbound messages from those users.



## Benefits of using GroupShield with the Microsoft virus scanning API

- Ensures that all Microsoft Exchange items (messages, attachments, files, etc.) are thoroughly scanned before being delivered to internal users or sent to external recipients.
- Single-instance scanning of items, even if one email is sent to multiple recipients.
- GroupShield for Microsoft Exchange 2000 can be administrated to provide real-time protection to Exchange 2000 servers without requiring the Exchange services to be stopped and restarted.
- Scans all protocols passing to and from the Exchange 2000 server, including: SMTP, MAPI, HTTP, POP3, IMAP4, Installable File System (IFS), X.400, etc.
- Provides the highest level of scanning performance with lowest possible server resource utilization.
- Uses the Microsoft approved and preferred method of scanning Exchange stores to provide the best possible scanning while ensuring compliance with other Microsoft APIs, integrity of data, and stability of the Exchange services.

## Further information

### Microsoft Knowledge Base articles @

<http://search.support.microsoft.com/>

- Q285667 XADM: Understanding Virus Scanning API 2.0 in Exchange 2000 Server SP1
- Q263949 XAMD: Understanding How the Antivirus API Scans Attachments
- Q285696 XADM: Virus Scanning API Performance Monitor Counters In Exchange 2000 Server SP1
- Q294336 XADM: Event Logging in Exchange 2000 Server SP1 for Virus Scanning API 2.0

### Microsoft TechNet articles

<http://www.microsoft.com/technet/>

- Products & Technologies > Exchange Server > Resource Kits > Chapter 13—Virus Protection

Digital Press @ <http://www.bh.com/digitalpress>

- Microsoft Exchange Server for Windows 2000: Planning, Designing, and Implementation, by Tony Redmond

All Network Associates products are backed by our PrimeSupport program and Network Associates Laboratories. Tailored to fit your company's needs, PrimeSupport service offers essential product knowledge and rapid, reliable technical solutions to keep you up and running. Network Associates Laboratories, a world leader in information systems and security, is your guarantee of the ongoing development and refinement of all our technologies.

3965 Freedom Circle | Santa Clara, CA 95054 | 888.847-8766 main



YOUR NETWORK. OUR BUSINESS.

[networkassociates.com](http://networkassociates.com)