



McAfee VirusScan Command Line User's Guide

Version 4.0.1

COPYRIGHT

Copyright © 1998 Network Associates, Inc. and its Affiliated Companies. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Network Associates, Inc.

LICENSE AGREEMENT

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (“AGREEMENT”), WHICH SETS FORTH GENERAL LICENSE TERMS FOR NETWORK ASSOCIATES SOFTWARE. FOR THE SPECIFIC TERMS OF YOUR LICENSE, CONSULT THE README.1ST, LICENSE.TXT, OR OTHER LICENSE DOCUMENT THAT ACCOMPANIES YOUR SOFTWARE, EITHER AS A TEXT FILE OR AS PART OF THE SOFTWARE PACKAGING. IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH THEREIN, DO NOT INSTALL THE SOFTWARE. (IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.)

1. **License Grant.** Subject to the payment of the applicable license fees and subject to the terms and conditions of this Agreement, Network Associates hereby grants to you a non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the “Documentation”). You may install one copy of the Software on one computer, workstation, personal digital assistant, pager, “smart phone” or other electronic device for which the Software was designed (each, a “Client Device”). If the Software is licensed as a suite or is bundled with more than one specified Software product, this license applies to all such specified Software products, subject to any restrictions or usage terms specified individually for any of such Software products on the applicable product invoicing or packaging.
 - a. **Use.** The Software is licensed as a single product; it may not be used on more than one Client Device or by more than one user at a time, except as set forth in this Section 1. The Software is “in use” on a computer when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that Client Device. This license authorizes you to make one copy of the Software solely for backup or archival purposes, provided that the copy you make contains all proprietary notices.
 - b. **Server Use.** To the extent that the applicable product invoicing or packaging sets forth, you may install and use the Software on a Client Device or as a server (“Server”) within a multi-user or networked environment (“Server Use”) for either (i) connecting, directly or indirectly, to not more than the maximum number of specified Client Devices or “seats”; or (ii) deploying not more than the maximum number of agents (pollers) specified for deployment. If the applicable product invoicing or packaging does not specify a maximum number of Client Devices or pollers, this license gives you a single product use license subject to the provisions of subsection (a) above. A separate license is required for each Client Device or seat that can connect to the Software at any time, regardless of whether such licensed Client Devices or seats are connected to the Software concurrently, or are actually using the Software at any particular time.

Your use of software or hardware that reduces the number of Client Devices or seats that connect to and use the Software simultaneously (e.g., using “multiplexing” or “pooling” hardware or software) does not reduce the number of licenses you must have in total. Specifically, you must have that number of licenses that would equal the number of distinct inputs to the multiplexing or pooling software or hardware “front end.” If the number of Client Devices or seats that can connect to the Software can exceed the number of licenses that you have obtained, then you must have a reasonable mechanism in place to ensure that your use of the Software does not exceed the use limits set forth in the product invoicing or packaging. This license authorizes you to make or download one copy of the Documentation for each Client Device or seat that is licensed, provided that each such copy contains all of the proprietary notices for the Documentation.

- c. **Volume Use.** If the Software is licensed with volume use terms specified in the applicable product invoicing or packaging, you may make, use and install as many additional copies of the Software on the number of Client Devices as the volume use terms specify. This license authorizes you to make or download one copy of the Documentation for each such copy of the Software you may make according to the volume use terms, provided that each such copy contains all of the proprietary notices for the Documentation. You must have a reasonable mechanism in place to ensure that the number of Client Devices on which the Software is installed does not exceed the number of licenses you have obtained.
2. **Term.** This license is effective for the period of time specified in the product invoicing or packaging, or in the README.1ST, LICENSE.TXT, or other text file that accompanies the Software and purports to set forth the terms of your license agreement. Where the provisions of the Agreement set forth here conflict with the provisions of the product invoicing or packaging, the README.1ST document, the LICENSE.TXT document, the product invoice, package, or the other text document will constitute the terms of your license grant to use the Software. Either you or Network Associates may terminate your license earlier than the period specified in the appropriate document in accordance with the terms set forth therein. This Agreement and your license will terminate automatically if you fail to comply with any of the limitations or other requirements described. When this agreement terminates, you must destroy all copies of the Software and Documentation. You may terminate this Agreement at any point by destroying the Software and Documentation together with all copies of the Software and Documentation.
3. **Updates.** During the term of your license, you may download revisions, upgrades, or updates to the Software when Network Associates publishes them via its website or through other online services.
4. **Ownership Rights.** The Software and the Documentation are protected by United States copyright laws and international treaty provisions. Network Associates owns and retains all right, title and interest in and to the Software, including all copyrights, patents, trade secret rights, trademarks and other intellectual property rights therein. You acknowledge that your possession, installation, or use of the Software does not transfer to you any title to the intellectual property in the Software, and that you will not acquire any rights to the Software except as expressly set forth in this Agreement. You agree that any copies of the Software and Documentation will contain the same proprietary notices that appear on and in the Software and Documentation.

5. **Restrictions.** You may not rent, lease, loan or resell the Software, or permit third parties to benefit from the use or functionality of the Software via a timesharing, service bureau or other arrangement. You may not transfer any of the rights granted to you under this Agreement. You may not copy the Documentation accompanying the Software. You may not reverse engineer, decompile, or disassemble the Software, except to the extent that the foregoing restriction is expressly prohibited by applicable law. You may not modify, or create derivative works based upon the Software in whole or in part. You may not copy the Software except as expressly permitted in Section 1 above. You may not remove any proprietary notices or labels on the Software. All rights not expressly set forth hereunder are reserved by Network Associates. Network Associates reserves the right to periodically conduct audits upon advance written notice to verify compliance with the terms of this Agreement.

6. **Warranty and Disclaimer**

- a. **Limited Warranty.** Network Associates warrants that for thirty (30) days from the date of original purchase or distribution the media (for example, the diskettes) on which the Software is contained will be free from defects in materials and workmanship.
- b. **Customer Remedies.** Network Associates' and its suppliers' entire liability, and your exclusive remedy, shall be, at Network Associates' option, either (i) return of the purchase price paid for the license, if any, or (ii) replacement of the defective media on which the Software is contained with a copy on non-defective media. You must return the defective media to Network Associates at your expense with a copy of your receipt. This limited warranty is void if the defect has resulted from accident, abuse, or misapplication. Any replacement media will be warranted for the remainder of the original warranty period. Outside the United States, this remedy is not available to the extent that Network Associates is subject to restrictions under United States export control laws and regulations.

Warranty Disclaimer. To the maximum extent permitted by applicable law, and except for the limited warranty set forth herein, THE SOFTWARE IS PROVIDED ON AN "AS IS" BASIS WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. WITHOUT LIMITING THE FOREGOING PROVISIONS, YOU ASSUME RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, NETWORK ASSOCIATES MAKES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES, OR THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS. TO THE MAXIMUM EXTENT PERMITTED BY LAW, NETWORK ASSOCIATES DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT WITH RESPECT TO THE SOFTWARE AND THE ACCOMPANYING DOCUMENTATION. SOME STATES AND JURISDICTIONS DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES, SO THE ABOVE LIMITATIONS MIGHT NOT APPLY TO YOU. The foregoing provisions shall be enforceable to the maximum extent permitted by applicable law.

Your purchase of or payment for the Software may entitle you to additional warranty rights, which Network Associates will specify in the product invoicing or packaging you received with your purchase, or in the README.1ST , LICENSE.TXT or other text file that accompanies the Software and purports to set forth the terms of your license agreement. Where the provisions of this Agreement conflict with the provisions of the product invoice or packaging, the README.1ST, the LICENSE.TXT, or similar documents, the invoice, packaging, or text file will set forth the terms of your warranty rights for the Software.

7. **Limitation of Liability.** UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT, CONTRACT, OR OTHERWISE, SHALL NETWORK ASSOCIATES OR ITS SUPPLIERS BE LIABLE TO YOU OR TO ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR FOR ANY AND ALL OTHER DAMAGES OR LOSSES. IN NO EVENT WILL NETWORK ASSOCIATES BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE LIST PRICE NETWORK ASSOCIATES CHARGES FOR A LICENSE TO THE SOFTWARE, EVEN IF NETWORK ASSOCIATES SHALL HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY TO THE EXTENT THAT APPLICABLE LAW PROHIBITS SUCH LIMITATION. FURTHERMORE, SOME STATES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION AND EXCLUSION MAY NOT APPLY TO YOU. The foregoing provisions shall be enforceable to the maximum extent permitted by applicable law.
8. **United States Government.** The Software and accompanying Documentation are deemed to be “commercial computer software” and “commercial computer software documentation,” respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.
9. **Export Controls.** Neither the Software nor the Documentation and underlying information or technology may be downloaded or otherwise exported or re-exported (i) into (or to a national or resident of) Cuba, Iran, Iraq, Libya, North Korea, Sudan, Syria or any other country to which the United States has embargoed goods; or (ii) to anyone on the United States Treasury Department’s list of Specially Designated Nations or the United States Commerce Department’s Table of Denial Orders. By downloading or using the Software, you are agreeing to the foregoing provisions and you are certifying that you are not located in, under the control of, or a national or resident of any such country or on any such list.

IN ADDITION, YOU SHOULD BE AWARE THAT EXPORT OF THE SOFTWARE MAY BE SUBJECT TO COMPLIANCE WITH THE RULES AND REGULATIONS PROMULGATED FROM TIME TO TIME BY THE BUREAU OF EXPORT ADMINISTRATION, UNITED STATES DEPARTMENT OF COMMERCE, WHICH

RESTRICT THE EXPORT AND RE-EXPORT OF CERTAIN PRODUCTS AND TECHNICAL DATA. IF THE EXPORT OF THE SOFTWARE IS CONTROLLED UNDER SUCH RULES AND REGULATIONS, THEN THE SOFTWARE SHALL NOT BE EXPORTED OR RE-EXPORTED, DIRECTLY OR INDIRECTLY, (A) WITHOUT ALL EXPORT OR RE-EXPORT LICENSES AND UNITED STATES OR OTHER GOVERNMENTAL APPROVALS REQUIRED BY ANY APPLICABLE LAWS, OR (B) IN VIOLATION OF ANY APPLICABLE PROHIBITION AGAINST THE EXPORT OR RE-EXPORT OF ANY PART OF THE SOFTWARE. SOME COUNTRIES HAVE RESTRICTIONS ON THE USE OF ENCRYPTION WITHIN THEIR BORDERS, OR ON THE IMPORT OR EXPORT OF ENCRYPTION EVEN IF FOR ONLY TEMPORARY BUSINESS OR PERSONAL USE. YOU ACKNOWLEDGE THAT THE IMPLEMENTATION AND ENFORCEMENT OF THESE LAWS IS NOT ALWAYS CONSISTENT AS TO SPECIFIC COUNTRIES. ALTHOUGH THE FOLLOWING COUNTRIES ARE NOT AN EXHAUSTIVE LIST, THERE MAY EXIST RESTRICTIONS ON THE EXPORTATION OF ENCRYPTION TECHNOLOGY TO, OR IMPORTATION FROM: BELGIUM, CHINA (INCLUDING HONG KONG), FRANCE, INDIA, INDONESIA, ISRAEL, RUSSIA, SAUDI ARABIA, SINGAPORE, AND SOUTH KOREA. YOU ACKNOWLEDGE THAT IT IS YOUR RESPONSIBILITY TO COMPLY WITH ANY AND ALL GOVERNMENT EXPORT AND OTHER APPLICABLE LAWS, AND THAT NETWORK ASSOCIATES HAS NO FURTHER RESPONSIBILITY AFTER THE INITIAL SALE TO YOU WITHIN THE ORIGINAL COUNTRY OF SALE.

10. **High Risk Activities.** The Software is not fault-tolerant and is not designed or intended for use in hazardous environments requiring fail-safe performance, including without limitation, in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, weapons systems, direct life-support machines, or any other application in which the failure of the Software could lead directly to death, personal injury, or severe physical or property damage (collectively, "High Risk Activities"). Network Associates expressly disclaims any express or implied warranty of fitness for High Risk Activities.
11. **Miscellaneous.** This Agreement is governed by the laws of the United States and the State of California, without reference to conflict of laws principles. The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. The Agreement set forth here is advisory in nature and does not supersede the provisions of any Agreement set forth in the README.1ST, LICENSE.TXT, or other text file that accompanies the Software and purports to set forth the terms of your license agreement. Where the provisions of this Agreement conflict with the provisions of the README.1ST or the LICENSE.TXT document, the text document will constitute the terms of your license grant to use the Software. This Agreement may not be modified except by a written addendum issued by a duly authorized representative of Network Associates. No provision hereof shall be deemed waived unless such waiver shall be in writing and signed by Network Associates or a duly authorized representative of Network Associates. If any provision of this Agreement is held invalid, the remainder of this Agreement shall continue in full force and effect. The parties confirm that it is their wish that this Agreement has been written in the English language only.
12. **Network Associates Customer Contact.** If you have any questions concerning these terms and conditions, or if you would like to contact Network Associates for any other reason, please call (408) 988-3832, fax (408) 970-9727, write Network Associates, Inc. at 3965 Freedom Circle, Santa Clara, California 95054, or visit the Network Associates website at <http://www.nai.com>.

Table of Contents

Preface	xi
What happened?	xi
Why worry?	xi
Where do viruses come from?	xii
Virus prehistory	xii
Viruses and the PC revolution	xiii
On the frontier	xvi
How to protect yourself	xvi
How to contact Network Associates	xviii
Customer service	xviii
Technical support	xviii
Network Associates training	xix
Comments and feedback	xix
Reporting new items for anti-virus data file updates	xx
International contact information	xxi
 Chapter 1. Introducing VirusScan	1
What is VirusScan?	1
VirusScan components	2
Documentation included with VirusScan	3
 Chapter 2. Installing VirusScan	5
Before you start	5
System requirements	5
Installation instructions	5
Validating your files	6
How to validate your copy of VirusScan	7
Testing your installation with the Eicar Standard AntiVirus Test File	8
 Chapter 3. On-demand Scanning	11
What is on-demand scanning?	11

How VirusScan works	11
Basic scanning	12
Advanced scanning	15
Selecting scanning options	16
General options	16
Target options	17
Response and notification options	20
Report options	22
Creating a scanning profile	25
Running a scanning profile	26
Viewing the Virus List	27
Scanning your floppy disks	28
Chapter 4. On-access Scanning	31
What is on-access scanning?	31
Starting VShield	32
Optimizing VShield performance	32
Configuring VShield	32
VShield options	34
General options	34
Memory options	34
Target options	35
Notification options	35
Editing your AUTOEXEC.BAT file	36
Chapter 5. Removing Infections	
From Your System	37
If you suspect you have a virus	37
If VirusScan detects a virus	39
Removing a virus found in memory	39
Removing a virus found in a file	40
Additional virus cleaning tasks:	40
Understanding false alarms	41
Appendix A. Preventing Virus Infection	43
Keys to a secure system environment	43

Detecting new viruses	45
Updating your VirusScan data files	45
Validating the VirusScan program files	46
Creating an emergency disk	47
Write-protecting a disk	50
 Appendix B. Network Associates	
Support Services	51
PrimeSupport Options for corporate customers	51
PrimeSupport Basic	51
PrimeSupport Extended	52
PrimeSupport Anytime	52
Ordering PrimeSupport	54
Support services for retail customers	54
Network Associates consulting and training	55
Professional Consulting Services	55
Total Education Services	56
 Appendix C. Reference	57
VirusScan command-line options	57
VirusScan error levels	67
 Index	69

Preface

What happened?

If you've ever lost important files stored on your hard disk, watched in dismay as your computer ground to a halt only to display a prankster's juvenile greeting on your monitor, or found yourself having to apologize for abusive e-mail messages you never sent, you know first-hand how computer viruses and other harmful programs can disrupt your productivity. If you haven't yet suffered from a virus "infection," count yourself lucky. But with more than 16,000 known viruses in circulation capable of attacking Windows- and DOS-based computer systems, it really is only a matter of time before you do.

The good news is that of those thousands of circulating viruses, only a comparatively few have the means to do real damage to your data. In fact, the term "computer virus" identifies a broad array of programs that have only one feature in common: they "reproduce" themselves automatically by attaching themselves to host software or disk sectors on your computer, usually without your knowledge. Most viruses cause relatively trivial problems, ranging from the merely annoying to the downright insignificant. Often, the primary consequence of a virus infection is the costs you incur in time and effort to track down the source of the infection and eradicate all of its traces.

Why worry?

So why worry about virus infections, if most attacks do little harm? The problem is twofold: First, although relatively few viruses have destructive effects, that fact says nothing about how widespread the malicious viruses are. In many cases, viruses with the most debilitating effects are the hardest to detect—the virus programmer bent on causing harm will take extra steps to avoid discovery. Second, even relatively "benign" viruses can interfere with the normal operation of your computer and can cause unpredictable behavior in other software. Some viruses contain bugs, poorly written code, or other problems severe enough to cause crashes when they run. Other times, legitimate software has problems running when a virus has, intentionally or otherwise, altered system parameters or other aspects of the computing environment. Tracking down the source of resulting system freezes or crashes drains time and money from more productive activities.

Beyond these problems lies a problem of perception: once infected, your computer can serve as a source of infection for other computers. If you regularly exchange data with colleagues or customers, you could unwittingly pass on a virus that could do more damage to your reputation or your dealings with others than it does to your computer.

The threat from viruses and other malicious software is real, and it is growing worse. The International Computer Security Association has estimated the total worldwide cost in time and lost productivity simply of detecting and cleaning virus infections at \$1 billion per year, a figure that doesn't include the costs of data loss and recovery in the wake of attacks that destroyed data.

Where do viruses come from?

As you or one of your colleagues recovers from a virus attack or hears about new forms of malicious software appearing in commonly used programs, you've probably asked yourself a number of questions about how we as computer users got to this point. Where do viruses and other malicious programs come from? Who writes them? Why do those who write them seek to interrupt workflows, destroy data, or cost people the time and money necessary to eradicate them? What can stop them?

Why did this happen to me?

It probably doesn't console you much to hear that the programmer who wrote the virus that erased your hard disk's file allocation table didn't target you or your computer specifically. Nor will it cheer you up to learn that the virus problem will probably always be with us. But knowing a bit about the history of computer viruses and how they work can help you better protect yourself against them.

Virus prehistory

Historians have identified a number of programs that served as virus precursors, or that incorporated features now associated with virus software. Canadian researcher and educator Robert M. Slade traces virus lineage back to special-purpose utilities used to reclaim unused file space and perform other useful tasks in the earliest networked computers. Slade reports that computer scientists at a Xerox Corporation research facility called programs like these "worms," a term coined after the scientists noticed "holes" in printouts from computer memory maps that looked as though worms had eaten them. The term survives to this day to describe programs that make copies of themselves, but without altering host software.

A strong academic tradition of computer prank playing most likely contributed to the shift away from utility programs and toward more malicious uses of the programming techniques found in worm software. Computer science students, often to test their programming abilities, would construct rogue worm programs and unleash them to "fight" against each other, competing to see whose program could "survive" while shutting down rivals. Those same students also found uses for worm programs in practical jokes they played on unsuspecting colleagues.

Some of these students soon discovered that they could use certain features of the host computer's operating system to give them unauthorized access to computer resources. Others took advantage of users who had relatively little computer knowledge to substitute their own programs—written for their own purposes—in place of common or innocuous utilities. These unsophisticated users would run what they thought was their usual software only to find their files erased, to have their account passwords stolen, or to suffer other unpleasant consequences. Such “Trojan horse” programs or “trojans,” so dubbed for their metaphorical resemblance to the ancient Greek gift to the city of Troy, remain a significant threat to computer users today.

Viruses and the PC revolution

What we now think of as true computer viruses first appeared, according to Robert Slade, soon after the first personal computers reached the mass market in the early 1980s. Other researchers date the advent of virus programs to 1986, with the appearance of the “Brain” virus. Whichever date has the better claim, the link between the virus threat and the personal computer is not coincidental.

The new mass distribution of computers meant that viruses could spread to many more hosts than before, when a comparatively few, closely guarded mainframe systems dominated the computing world from their bastions in large corporations and universities. Nor did the individual users who bought PCs have much use for the sophisticated security measures needed to protect sensitive data in those environments. Most particularly, virus writers found it relatively easy to exploit some PC technologies to serve their own ends.

Boot-sector viruses

Early PCs, for example, “booted” or loaded their operating systems from floppy disks. The authors of the Brain virus discovered that they could substitute their own program for the executable code present on the boot sector of every floppy disk formatted with Microsoft's MS-DOS, whether or not it included system files. Users thereby loaded the virus into memory every time they started their computers with any formatted disk in their floppy drives. Once in memory, a virus can copy itself to boot sectors on other floppy or hard disks. Those who unintentionally loaded Brain from an infected floppy found themselves reading an ersatz “advertisement” for a computer consulting company in Pakistan.

With that advertisement, Brain pioneered another characteristic feature of modern viruses: the payload. The payload is the prank or malicious behavior that, if triggered, causes effects that range from annoying messages to data destruction. It's the virus characteristic that draws the most attention—many virus authors now write their viruses specifically to deliver their payloads to as many computers as possible.

For a time, sophisticated descendants of this first boot-sector virus represented the most serious virus threat to computer users. Variants of boot sector viruses also infect the Master Boot Record (MBR), which stores the partition information your computer needs to figure out where to find each of your hard disk partitions and the boot sector itself.

Realistically, nearly every step in the boot process, from reading the MBR to loading the operating system, is vulnerable to viral sabotage. Some of the most tenacious and destructive viruses still include the ability to infect your computer's boot sector or MBR among their repertoire of tricks. Among other advantages, loading at boot time can give a virus a chance to do its work before your anti-virus software has a chance to run.

But boot sector and MBR viruses have a particular weakness: they must spread by means of floppy disks or other removable media, riding concealed in that first track of disk space. As fewer users exchange floppy disks and as software distribution has come to rely on other media, such as CD-ROMs, other virus types have recently eclipsed the boot sector threat. The popularity of large-capacity floppy disks like the Iomega Zip disk and similar disks from Syquest and others, however, could cause a resurgence.

File infector viruses

At about the same time as the authors of the Brain virus found vulnerabilities in the DOS boot sector, other virus writers found out how to use existing software to help replicate their creations. An early example of this type of virus showed up in computers at Lehigh University in Pennsylvania. The virus infected part of the DOS command interpreter COMMAND.COM, which it used to load itself into memory. Once there, it spread to other uninfected COMMAND.COM files each time a user entered any standard DOS command that involved disk access. This limited its spread to floppy disks that contained, usually, a full operating system.

Later viruses quickly overcame this limitation, sometimes with fairly clever programming. Virus writers might, for instance, have their virus add its code to the beginning of an executable file, so that when users start a program, the virus code executes immediately, then transfers control back to the legitimate software, which runs as though nothing unusual has happened. Once it activates, the virus “hooks” or “traps” requests that legitimate software makes to the operating system and substitutes its own responses. Particularly clever viruses can even subvert attempts to clear them from memory by trapping the **CTRL+ALT+DEL** keyboard sequence for a warm reboot, then faking a restart. Sometimes the only outward indication that anything on your system is amiss—before any payload detonates, that is—might be a small change in the file size of infected legitimate software.

Stealth, mutating, encrypted, and polymorphic viruses

Unobtrusive as they might be, changes in file size and other scant evidence of a virus infection usually gives most anti-virus software enough of a scent to locate and remove the offending code. One of the virus writer's principal challenges, therefore, is to find ways to hide his or her handiwork. The earliest disguises were a mixture of innovative programming and obvious giveaways. The Brain virus, for instance, redirected requests to see a disk's boot sector away from the actual location of the infected sector to the new location of the boot files, which the virus had moved. This "stealth" capability enabled this and other viruses to hide from conventional search techniques.

Because viruses needed to avoid continuously reinfecting host systems—doing so would quickly balloon an infected file's size to easily detectable proportions or would consume enough system resources to point to an obvious culprit—their authors also needed to tell them to leave certain files alone. They addressed this problem by having the virus write a code "signature" that would flag infected files with the software equivalent of a "do not disturb" sign. Although that kept the virus from giving itself away immediately, it opened the way for anti-virus software to use the code signatures themselves to find the virus.

In response, virus writers found ways to conceal the code signatures. Some viruses would "mutate" or write different code signatures with each new infection. Others encrypted most of the code signature or the virus itself, leaving only a couple of bytes to use as a key for decryption. The most sophisticated new viruses employed stealth, mutation and encryption to appear in an almost undetectable variety of new forms. Finding these "polymorphic" viruses required software engineers to develop very elaborate programming techniques for anti-virus software.

Macro viruses

By 1995 or so, the virus war had come to something of a standstill. New viruses appeared continuously, prompted in part by the availability of ready-made virus "kits" that enabled even some non-programmers to whip up a new virus in no time. Most existing anti-virus software, however, could easily be updated to detect and dispose of the new virus variants, which consisted primarily of minor tweaks to well-known templates.

But 1995 marked the emergence of the Concept virus, which added a new and surprising twist to virus history. Before Concept, most virus researchers thought of data files—the text, spreadsheet, or drawing documents created by the software you use—as immune to infection. Viruses, after all, are programs and, as such, needed to be able to run in the same way executable software did in order to do their damage. Data files, on the other hand, simply stored information that you entered when you worked with your software.

That distinction melted away when Microsoft began adding macro capabilities to Word and Excel, its flagship applications in its Office suite. Using the stripped-down version of its Visual BASIC language included with the suite, users could create document templates that would automatically format and add other features to documents created with Word and Excel. Virus writers seized the opportunity that this presented to conceal and spread viruses in documents that you, the user, created yourself.

The exploding popularity of the Internet and of e-mail software that allowed users to attach files to messages ensured that macro viruses would spread very quickly and very widely. Within a year, macro viruses became the most potent virus threat ever.

On the frontier

Malicious software has even begun intruding into areas once thought completely out of bounds. Users of the mIRC Internet Relay Chat client, for example, have reported encountering viruses constructed from the mIRC scripting language. Script viruses get sent as plain text, which would ordinarily preclude them from getting infected, but older versions of the mIRC client software would interpret the instructions coded into the script and perform unwanted actions on the recipient's computer. The vendors moved quickly to disable this capability in updated versions of the software, but the mIRC incident illustrates the general rule that where a way exists to exploit a software security hole, someone will find it and use it.

Some virus writers do it for the thrill of it, some to gain notoriety in their own peer group. Still others do it to exact revenge against employers or others they believe have treated them badly. Whatever their motives, they continue to develop new ways to cause you trouble.

How to protect yourself

Network Associates anti-virus software already gives you an important bulwark against infection and damage to your data, but anti-virus software is only one part of the security measures you should take to protect yourself and your data. Most measures are common sense—checking disks you receive from unknown or questionable sources, either with anti-virus software or some kind of verification utility, is always a good idea. Malicious programmers have gone so far as to mimic the programs you trust to guard your computer, pasting a familiar face on software with a less-than-friendly purpose. Network Associates includes `VALIDATE.EXE`, a verification utility, with its distributions to prevent this type of manipulation, but neither it nor any anti-virus software can detect when someone substitutes a trojan or other malicious program for one of your favorite shareware or commercial utilities.

Web and Internet access poses its own risks. Having a top-notch firewall in place to protect your network and implementing other network security measures is a necessity when unscrupulous attackers can penetrate your network from nearly any point on the globe, whether to steal sensitive data or implant malicious code. You should also make sure that your network is not accessible to unauthorized users, and that you have an adequate training program in place to teach and enforce security standards.

To learn about the origin, behavior and other characteristics of particular viruses, consult the Virus Information Library maintained on the Network Associates website. Some Network Associates products also come with a Virus List that also catalogs all of the viruses that the program can detect and summarizes information about their sizes, the types of infections they attempt, and whether the product can remove them from your files.

Network Associates can provide you with other software in the Total Virus Defense (TVD) suite, the most comprehensive anti-virus solution available, and Total Network Security (TNS), the industry's most advanced network security suite. Network Associates backs them both with outstanding support, training and a worldwide network of research and development teams. Contact your Network Associates representative, or visit the Network Associates website at <http://www.nai.com>, to find out how to enlist the power of Total Virus Defense on your side.

How to contact Network Associates

Customer service

To order products or obtain product information, contact the Network Associates Customer Care department at (408) 988-3832 or write to the following address:

Network Associates, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
U.S.A.

Technical support

Network Associates is famous for its dedication to customer satisfaction. Network Associates continues this tradition by making our site on the World Wide Web a valuable resource for answers to technical support issues. Network Associates encourages you to make this your first stop for answers to frequently asked questions, for updates to Network Associates software, and for access to Network Associates news and virus information.

World Wide Web	http://support.nai.com
----------------	---

If you do not find what you need or do not have web access, try one of our automated services.

Automated Voice and Fax Response System	(408) 988-3034
Internet	support@nai.com
CompuServe	GO NAI
America Online	keyword MCAFEE

If the automated services do not have the answers you need, contact Network Associates at one of the following numbers Monday through Friday between 6:00 A.M. and 6:00 P.M. Pacific time.

For corporate-licensed customers:

Phone	(408) 988-3832
Fax	(408) 970-9727

For retail-licensed customers:

Phone	(972) 278-6100
Fax	(408) 970-9727

To provide the answers you need quickly and efficiently, the Network Associates technical support staff needs some information about your computer and your software. Please have this information ready before you call:

- Product name and version number
- Computer brand and model
- Any additional hardware or peripherals connected to your computer
- Operating system type and version numbers
- Network type and version, if applicable
- Contents of your AUTOEXEC.BAT, CONFIG.SYS, and system LOGIN script
- Specific steps to reproduce the problem

Network Associates training

For information about scheduling on-site training for any Network Associates product, call (800) 338-8754.

Comments and feedback

Network Associates appreciates your comments and reserves the right to use any information you supply in any way it believes appropriate without incurring any obligation whatsoever. Please address your comments about Network Associates documentation to: Network Associates, Inc., 3965 Freedom Circle, Santa Clara, CA 95054. You can also send faxed comments to (408) 970-9727 or e-mail to tvd_documentation@nai.com.

Reporting new items for anti-virus data file updates

Network Associates anti-virus software offers you the best available detection and removal capabilities, including advanced heuristic scanning that can detect new and unnamed viruses as they emerge. Occasionally, however, an entirely new type of virus that is not a variation on an older type can appear on your system and escape detection. Because Network Associates researchers are committed to providing you with effective and up-to-date tools you can use to protect your system, please tell them about any new viruses that your software does not now detect. Note that Network Associates reserves the right to use any information you supply as it deems appropriate, without incurring any obligations whatsoever. Send your suggestions to:

`virus_research@nai.com`

Use this address to report new virus strains.

To report items to our European research office, use this e-mail address:

`virus_research_europe@nai.com`

To report items to our Asia-Pacific research office, or our office in Japan, use one of these e-mail addresses:

`avert-jp@nai.com`

Use this address to report harmful items to our office in Japan.

`avert_apac@nai.com`

Use this address to report harmful items to our Asia-Pacific office.

International contact information

To contact Network Associates outside the United States, use the addresses and numbers below.

Network Associates Australia

500 Pacific Highway, Level 1
St. Leonards, NSW
Sydney, Australia 2065
Phone: 61-2-9437-5866
Fax: 61-2-9439-5166

Network Associates Austria

Pulvermuehlstrasse 17
Linz, Austria
Postal Code A-4040
Phone: 43-732-757-244
Fax: 43-732-757-244-20

Network Associates Belgium

Bessenveldtstraat 25a
Diegem
Belgium - 1831
Phone: 32-2-716-4070
Fax: 32-2-716-4770

Network Associates do Brasil

Rua Geraldo Flausino Gomez 78
Cj. - 51 Brooklin Novo - São Paulo
SP - 04575-060 - Brasil
Phone: (55 11) 5505 1009
Fax: (55 11) 5505 1006

Network Associates Canada

139 Main Street, Suite 201
Unionville, Ontario
Canada L3R 2G6
Phone: (905) 479-4189
Fax: (905) 479-4540

Network Associates People's Republic of China

New Century Office Tower, Room 1557
No. 6 Southern Road Capitol Gym
Beijing
People's Republic of China 100044
Phone: 8610-6849-2650
Fax: 8610-6849-2069

NA Network Associates Oy

Kielotie 14 B
01300 Vantaa
Finland
Phone: 358 9 836 2620
Fax: 358 9 836 26222

Network Associates France S.A.

50 Rue de Londres
75008 Paris
France
Phone: 33 1 44 908 737
Fax: 33 1 45 227 554

**Network Associates
Deutschland GmbH**

Industriestrasse 1
D-82110 Germering
Germany
Phone: 49 8989 43 5600
Fax: 49 8989 43 5699

Network Associates Srl

Centro Direzionale Summit
Palazzo D/1
Via Brescia, 28
20063 - Cernusco sul Naviglio (MI)
Italy
Phone: 39 (0)2 9214 1555
Fax: 39 (0)2 9214 1644

**Network Associates
Latin America**

150 South Pine Island Road, Suite 205
Plantation, Florida 33324
United States
Phone: (954) 452-1731
Fax: (954) 236-8031

**Network Associates
International B.V.**

Gatwickstraat 25
1043 GL Amsterdam
The Netherlands
Phone: 31 20 586 6100
Fax: 31 20 586 6101

Network Associates Hong Kong

19/F, Matheson Centre
3 Matheson Street
Causeway Bay
Hong Kong
Phone: 852-2832-9525
Fax: 852-2832-9530

Network Associates Japan, Inc.

Toranomon 33 Mori Bldg.
3-8-21 Toranomon Minato-Ku
Tokyo 105-0001 Japan
Phone: 81 3 5408 0700
Fax: 81 3 5408 0781

**Network Associates
de Mexico**

Andres Bello No. 10, 4 Piso
4th Floor
Col. Polanco
Mexico City, Mexico D.F. 11560
Phone: (525) 282-9180
Fax: (525) 282-9183

**Network Associates
Portugal**

Rua Gen. Ferreira Martins, 10-6ºc
1495 Algés
Portugal
Phone: 351 1 412 1077
Fax: 351 1 412 1488

**Net Tools Network Associates
South Africa**

Bardev House, St. Andrews
Meadowbrook Lane
Epson Downs, P.O. Box 7062
Bryanston, Johannesburg
South Africa 2021
Phone: 27 11 706-1629
Fax: 27 11 706-1569

**Network Associates
South East Asia**

7 Temasek Boulevard
The Penthouse
#44-01, Suntec Tower One
Singapore 038987
Phone: 65-430-6670
Fax: 65-430-6671

**Network Associates
Spain**

Orense 4, 4th Floor
Edificio Trieste
28020 Madrid
Spain
Phone: 34 91 598 18 00
Fax: 34 91 556 14 01

**Network Associates
Sweden**

Datavägen 3A
Box 596
S-175 26 Järfälla
Sweden
Phone: 46 (0) 8 580 100 00
Fax: 46 (0) 8 580 100 05

**Network Associates
AG**

Baeulerwisenstrasse 3
8152 Glattbrugg
Switzerland
Phone: 0041 1 808 99 66
Fax: 0041 1 808 99 77

**Network Associates
International Ltd.**

Minton Place, Victoria Street
Windsor, Berkshire
SL4 1EF
United Kingdom
Phone: 44 (0)1753 827 500
Fax: 44 (0)1753 827 520

What is VirusScan?

VirusScan Command Line is a collection of Network Associates' powerful command line products. From the DOS environment, you can direct VirusScan to search for viruses in any drive, volume, directory, folder, or file in your computer—"on demand" scans— as well as any time a file is opened—"on-access."

VirusScan's powerful array of options allow you to set decisive responses to any detected virus: moving the infected files to a quarantine location, cleaning, or deleting the infected files.

When a virus is detected, VirusScan will alert you to its presence. You can use VirusScan's alerting features to create an effective alerting system to ensure that not only the user, but *all* key personnel will be notified of a virus infection. You can customize the alert message to include the next steps an employee should take to best protect data and keep downtime at a minimum.

VirusScan, kept current with updated virus files from the McAfee research labs, can serve as a cornerstone for your comprehensive security program which should also include a variety of safety measures, such as regular backups, meaningful password protection, proper training, and awareness of security issues. Network Associates strongly urges you to set up a security program incorporating as many protective measures as possible.

Encourage all your employees to remain vigilant: awareness is your company's strongest defense against future infection. For additional information and resources, see [Appendix A, "Preventing Virus Infection."](#)

VirusScan features include:

- Code Trace, Code Poly, and Code Matrix scanning employ Network Associates proprietary technologies for pinpointing virus identification accuracy.
- For encrypted, mutated, and unknown macro viruses, VirusScan uses algorithms for detection that rely on statistical analysis, heuristics, and code disassembly.
- Files embedded within Microsoft Office files are scanned.
- Scans text files to detect mIRC script viruses.

Heuristic scanning for macro virus detection

In the 32-bit environment, VirusScan uses state-of-the-art heuristic scanning technology to detect possible macro viruses: one of the most crippling of all virus threats.

- VirusScan can remove macro viruses that have the ability to set their own passwords.
- It can also detect macro viruses in password-protected Microsoft Word 7.0 files (Word for Office 95) in all languages supported by Word.
- VirusScan's enhanced password sensitivity allows removal of macro viruses from password-protected Microsoft Excel 95 files without disturbing user passwords.

Virus data files

Regular updates to the virus signatures VirusScan uses are included with the purchase of a Network Associates subscription license to assure the best virus detection and removal rates. See [Appendix B, "Network Associates Support Services,"](#) for details.

VirusScan components

Scan

- Scan is the on-demand scanning component of VirusScan. Use the myriad options listed in [Chapter 3, "On-demand Scanning."](#) to configure the scan tasks you need.

VShield

- VShield, VirusScan's on-access scanner for DOS, will scan your system automatically every time you access a file, create a file, copy a file, rename a file, run a file, access a disk, or start up your system. For details on on-access scanning, see [Chapter 4, "On-access Scanning."](#)

DAT files

- Network Associates' current Virus Data files (DAT files) are a complete collection of virus signatures which VirusScan uses for virus detections. Your license agreement includes free monthly updates to these files. See [pages 45 to 46](#) for further details on these files.

Documentation included with VirusScan

The documentation you received with VirusScan includes:

- This user's guide, saved on the VirusScan CD-ROM or installed on your hard disk in Adobe Acrobat .PDF format. The *User's Guide* describes in detail how to use VirusScan Command Line, and includes other useful background information and advanced configuration options. Acrobat .PDF files are flexible online documents that contain hyperlinks, outlines and other aids for easy navigation and information retrieval.

☐ **NOTE:** For best results when opening and printing the *User's Guide*, Network Associates recommends using Acrobat Reader 3.0; Reader version 3.0.1 has difficulty correctly printing graphics included in the .PDF file.

- A WHATSNEW.TXT file. This file contains last-minute additions or changes to the documentation, lists any known behavior or other issues with the product release, and often describes new product features incorporated into incremental product updates. You'll find the WHATSNEW.TXT file at the root level of your VirusScan CD-ROM; you can open and print it from Windows Notepad, or from nearly any word-processing software.
- A README.1ST file. This file outlines the terms of your license to use VirusScan. Read it carefully: by installing VirusScan you agree to its terms.

Before you start


It's important to minimize the risk of spreading viruses that may already be present on your system before VirusScan is installed. Before installing VirusScan:

1. Review the system requirements below.
2. Ensure that your system is virus-free. If you suspect your system is infected, see [“If you suspect you have a virus ...” on page 37](#) before installing the software.
3. Confirm that your Date/Time settings are accurate.

System requirements

- A 386 or higher IBM-compatible personal computer running DOS version 5.0 or higher
- At least 4MB of memory and 4 MB of free hard drive space.

Installation instructions

 **NOTE:** If you suspect your system is already infected, see [“If you suspect you have a virus ...” on page 37](#) before installing VirusScan.

To install VirusScan:

1. Make a directory for VirusScan on your hard drive.
2. Complete either a or b, depending on the source of your VirusScan program files:
 - a. If you are installing from disk or compact disk, insert it into your floppy disk drive or CD-ROM drive, then copy the VirusScan files to the directory you created for them.
 - b. If you are installing from VirusScan files you downloaded from the Network Associates website, decompress the zipped files into the directory you created for them on your hard drive.

3. Add the VirusScan directory you created to the path statement in your AUTOEXEC.BAT file.
4. Make a clean start-up disk. See [“Creating an emergency disk” on page 47](#) for more information.

To run VirusScan from a NetWare login script without running out of memory, immediately after installation, follow these steps:

1. Rename LOGIN.EXE to LOGIN1.EXE, then remove any references to VirusScan from the file.
2. Create a batch file named LOGIN.BAT.
3. Use the first line of the batch file to run VirusScan with whatever options you want to include.
4. Use the second line of the batch file, to run LOGIN1.EXE.

These steps prevent LOGIN.EXE and SCAN.EXE from loading into memory at the same time. This allows VirusScan Command Line to run before your computer tries to get access to the network. Your login script should then run without complications.

Validating your files

Downloading or copying files from any outside source places your computer at risk of virus infection—even if the risk is small. Downloading anti-virus software is no exception. Network Associates uses strict, extensive security measures to ensure that the products you purchase and download from its website and its other electronic services are safe, reliable, and free from virus infections. But anti-virus software tends to attract the attention of virus- and Trojan horse-writers, some of whom find it amusing to post infected copies of commercial software, or use the same file names to camouflage their own work.

You can protect yourself from this possibility by ensuring that you

- Downloading your files only from the Network Associates website or other approved electronic source such as AOL or CompuServe; and
- Validating the files you download.

Network Associates includes a copy of VALIDATE.EXE, its validation software, with each VirusScan package.

How to validate your copy of VirusScan

To ensure that you have exactly the same files as did the engineers who packaged your copy of VirusScan, you need to compare the validation codes which VALIDATE.EXE generates against the packing list supplied with your copy of VirusScan. The packing list is a text file that contains the validation codes that Network Associates engineers generated from independent cyclical redundancy check (CRC) processes when they packaged VirusScan for delivery.

To validate your files, follow these steps:

1. Install VirusScan as described in [“Installation instructions” on page 5](#).
2. Click **Start** in the Windows taskbar, point to **Programs**, then choose **MS-DOS Prompt**.
3. In the window that appears, change your command prompt to point to the directory that contains the VirusScan files you installed. If you chose the default installation options, you'll find the files in this path:

C:\PROGRAM FILES\NETA\SCAN

4. Run VALIDATE.EXE. To do so, type `validate *.*` at the command prompt.

VALIDATE.EXE scans all of the files stored in your VirusScan program directory, then generates a file list that includes the file name, its size in bytes, its creation date and time, and two validation codes in separate columns. To use VALIDATE.EXE to examine individual files, simply follow `validate` with the name of the file you want to verify at the prompt, or use the DOS wildcards `?` and `*` to specify a range of files.

5. Network Associates recommends that you redirect the output from VALIDATE.EXE to your printer so that you can review it easily.

If you have set your printer to capture output from MS-DOS programs, type `validate >lpt1` at the MS-DOS prompt. (To learn how to set your printer to print from MS-DOS programs, please consult your Windows documentation.)

To finish the validation process, you will need to compare the output from VALIDATE.EXE that you just generated against the unique packing list codes included in your copy of VirusScan Command Line. Complete the sequence below to generate the packing list.

To generate the packing list and complete your comparison, follow these steps:

1. To display the packing list, type `type packing.lst` at the command-line prompt, then press **ENTER**.
2. Type `type packing.lst>lpt1` at the DOS prompt to redirect the output from PACKING.LST to your printer.
3. Compare the output from VALIDATE.EXE to that from PACKING.LST.


The sizes, creation dates and times, and validation codes for each file name should match *exactly*. If they do not, delete the file immediately: do not open the file or examine it with any other utility; doing so can risk virus infection.

Checking your VirusScan installation with VALIDATE.EXE does not guarantee that your copy is free from defects, copying errors, virus infections or tampering, but the program's security features make it extremely unlikely that anyone has tampered with files that have correct validation codes. See the files LICENSE.TXT or README.1ST included with your copy of VirusScan to learn the license terms that cover your use of the program.

Testing your installation with the Eicar Standard AntiVirus Test File

The Eicar Standard AntiVirus Test File is a combined effort by anti-virus vendors throughout the world to come up with one standard by which customers can verify their anti-virus installations. To test your installation of VirusScan, copy the following line into its own file, name it EICAR.COM, and save it as a text file.

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

 **NOTE:** The characters in this test file must all appear on one line.

When finished, you will have a 68- to 70-byte file.

When VirusScan is applied to this file, it will report finding the EICAR-STANDARD-AV-TEST-FILE virus.

It is important to know that THIS IS NOT A VIRUS. However, users often have the need to test that their installations function correctly. The anti-virus industry, through the European Institute for Computer Antivirus Research, has adopted this standard to facilitate this need.

Delete the file when installation testing is completed so unsuspecting users are not unnecessarily alarmed.

Because the Eicar Standard AntiVirus Test File is not a *true* virus infection, you will not be able to clean or repair this “infected” file.

What is on-demand scanning?

You can tell VirusScan to conduct a scan operation at any time, on any target drive, directory or file—with the scanning options you choose. This chapter explains how to use VirusScan's on-demand scan features to search specific files, directories, or drives for known boot, file, multi-partite, stealth, encrypted, polymorphic, and macro viruses.

When should you scan?

You should scan any file new to your system; any newly downloaded or installed files, and, depending on how susceptible your system is to virus infection, as frequently as once a day.

Remember, while you are learning how to configure basic scan tasks, and beginning to customize VirusScan, VirusScan is quietly running *on-access* protections through its VShield component, which runs with a default set of options at system startup. See [Chapter 4, page 31](#), for further details.

How VirusScan works

At the command line, configuring VirusScan's Scan component (see [page 2](#)) is all you need to do to initiate VirusScan's powerful scanning capabilities. Scan will dynamically respond to any environmental or limitation—such as restricted memory—and automatically call one of its “helper” programs to successfully run the scan tasks you have configured it to launch.

Should Scan use an additional component, such as Scan86 or ScanPM (protected memory), any change will be transparent to you. Only by viewing VirusScan's help file will you learn which particular on-demand scanning component VirusScan is running.

❏ **NOTE:** To view Scan's help file at any time, type `scan /?` at the command prompt.

Archived and compressed files recognized by VirusScan

32-BIT ENVIRONMENT:

Formats/utilities recognized:

.ARC, .ARI, .CAB, Diet, LZEXE, .LZH, PKLite, .TD0, .ZIP, ??_

16-BIT ENVIRONMENT:

VirusScan can not decompress files from within the 16-bit environment. Therefore, compressed and archived files cannot be scanned on-demand. Also, please note that .CAB files cannot be scanned in low-memory environments.

The switches /UNZIP and /NOCOMP can be used to help configure how VirusScan handles compressed files. Find these and other target-related scan options in the tables from [pages 17 to 20](#).

Basic scanning

To perform a basic scan:

1. Exit from Windows or any application programs, and reboot if necessary (**CTRL+ALT+DEL**) to get to the command prompt.
2. From the command prompt, use the `cd` command to change to the directory where VirusScan is installed. (For example, if VirusScan had been installed on the C: drive, in directory “Scan,” type `cd scan` at the C:\ prompt.)
3. The following examples are general scan options. See the tables in [pages 16 to 22](#) for a complete list of on-demand scan options at your disposal.

❏ **NOTE:** As you become more familiar with VirusScan’s capabilities, you can create “scanning profiles” which capture scan tasks for future use. See “[Creating a scanning profile](#)” on [page 25](#), for details.

- To scan every file on the C: and D: drives that are susceptible to infection, type:

```
scan c: d: /all
```
- To scan every file that is susceptible to infection in all system drives (including compressed drives and PC drives—but not disks), type:

```
scan /adl /all
```

where:

- /ADL specifies all local drives as the target of the scan.
- /ALL instructs VirusScan to scan all files that are susceptible to infection.

- To scan a floppy disk in the A: drive, type:

```
scan a:
```

4. VirusScan might take several minutes to check for viruses in memory and on drives, but will keep you informed of its progress. Read the information on the screen carefully. The following information is a sample of what VirusScan reports after scanning a floppy disk in the A: drive:

```
Scan engine v.4.0.01 for DOS/PM
Copyright (c) 1992-98 Network Associates, Inc. All rights
reserved.
(408) 988-3832 LICENSED COPY - Oct 21 1998.

Virus data file V4001 created 10/21/98
Checking memory for viruses ... is OK.
Scanning A:[]

Scanning A:\*.*

Summary report on A:\*.*:

Files(s)
    Total files: .....2
    Clean: .....1
    Not scanned: .....1
    Possibly Infected: ... 0

Master Boot Record(s):.....2
    Possibly Infected: ... 0

Boot Sector(s):.....1
    Possibly Infected: ... 0

Time: 00:00.04
```

In the example above, note that Scan, after ascertaining the system environment, automatically ran in protected mode (PM) to successfully complete the requested scan task. For more information on how Scan uses helper applications without user input, please see [“How VirusScan works” on page 11](#).

You may wish to redirect Scan's onscreen reports to a report file. See [“Report options” on page 22](#) for options.

Either of these results will occur:

If VirusScan reports No Viruses Found, your system is most likely virus-free. Copy important files to fresh disks or tape backup so your current and clean files are maintained should a virus later infect your system.

-
- ❏ **NOTE:** VirusScan's ability to detect viruses must be maintained through regular updates of the VirusScan data files. For more information about updating VirusScan, see [“Updating your VirusScan data files” on page 59.](#)
-

If VirusScan finds one or more viruses, a message similar to the following is displayed:

```
Scanning C:  
Scanning file C:\DOS\ATTRIB.EXE  
Found the Jerusalem Virus
```

-
- ❏ **NOTE:** VirusScan notes any unknown macro virus detected by heuristic scanning by reporting:

```
Could be a new virus!!!
```

Do not panic, even if the virus has infected many files. Do not run any other programs. Turn to [“If VirusScan detects a virus” on page 39](#) for details on how to manage a virus infection of your system.

Advanced scanning

By default, VirusScan runs with the most common scanning options enabled. Because a large number of custom scanning options are available, VirusScan can use a scanning profile, a text file that contains scanning options, to govern how it performs a scan.

- For information on selecting scanning options, see [“Selecting scanning options,”](#) below.
- For information on creating a scanning profile, see [“Creating a scanning profile”](#) on page 25.
- To run the scanning profile, see [“Running a scanning profile”](#) on page 26.

Selecting scanning options

Before creating a scanning profile, determine which parameters are necessary for your environment. In this section you will find tables of these various VirusScan options:

- Target options, see [page 17](#)
- Response and notification options, see [page 20](#)
- Report options, see [page 22](#)
- For a complete table of VirusScan command-line options, see [Appendix C, page 57](#).

❏ **NOTE:** For an onscreen list of scanning options and their usage, use the `cd` command to change to the directory where VirusScan is installed, then type `scan /?`


General options

The following table lists VirusScan's general scan options.

General Command Line Option	Limitations	Description
<code>/?</code> or <code>/HELP</code>	None.	Displays a list of VirusScan command-line options, each with a brief description.
<code>/ANALYZE</code>	Extended memory required.	Sets VirusScan to scan using its full heuristics, both program and macro. <i>Note:</i> <code>/MANALYZE</code> targets macro viruses only; <code>/PANALYZE</code> targets program viruses only.
<code>/FREQUENCY <n></code>	None.	Do not scan <code><n></code> hours after the previous scan. In environments where the risk of viral infection is very low, use this option to prevent unnecessary scans. Remember, the greater the scan frequency, the greater your protection against infection.
<code>/LOAD <filename></code>	None.	Load scanning options from the named file. Use this option to perform a scan you've already configured by loading custom settings saved in an ASCII-formatted file.
<code>/NOEXPIRE</code>	None.	Disables the "expiration date" message if the VirusScan data files are out of date.

Target options

The following table lists VirusScan's target-related scanning options.

 **NOTE:** To configure on-demand scans, you must note a target location for the scan (e.g. , C:\, A:\, /ADL, /ADN).

Target Command Line Option	Limitations	Description
/ADL	None.	<p>Scan all local drives—including compressed and PC drives, but not disks—in addition to any other drive specified on the command line.</p> <p>To scan both local and network drives, use the /ADL and /ADN commands together in the same command line.</p> <p>OS/2: /ADL includes the CD-ROM drive in the scan, when used with /NODDA</p>
/ADN	None.	<p>Scan all network drives—including CD-ROM—for viruses, in addition to any other drive(s) specified on the command line.</p> <p><i>Note:</i> To scan both local drives and network drives, use the /ADL and /ADN commands together in the same command line.</p>
/ALL	None.	<p>Overrides the default scan setting by scanning all infectable files—regardless of extension.</p> <p><i>Notes:</i></p> <p>Using the /ALL option substantially increases the scanning time required. Use it only if you find a virus or suspect you have one.</p> <p>By default, VirusScan only scans files with the following extensions: .EXE, .COM, .SYS, .BIN, .OVL, .DLL, .DOC, .DOT, .XLA, .XLS, .XLT, .RTF, and .VXD. These are the file types that are most susceptible to viruses.</p>
/ANALYZE	Extended memory required.	<p>Use /ANALYZE to set VirusScan to target both program and macro viruses.</p> <p><i>Note:</i> Use /MANALYZE to set VirusScan's heuristic scanning features to target macro viruses only; use /PANALYZE to set VirusScan's heuristic scanning to target only program viruses.</p>
/BOOT	None.	Scan boot sector and master boot record only.

Target Command Line Option	Limitations	Description
/EXCLUDE <filename>	None.	Do not scan or add validation codes to the files listed in <filename>. <p>Use this option to:</p> <ul style="list-style-type: none"> * Exclude specific files from a scan. List the complete path to each file that you want to exclude on its own line. You may use wildcards * and ?
/MANALYZE	Extended memory required.	Sets VirusScan's heuristic scanning features to target macro viruses only. <p><i>Note:</i> /PANALYZE targets program viruses only; /ANALYZE targets both program and macro viruses.</p>
/MANY	None.	Scans multiple disks consecutively in a single drive. VirusScan will prompt you for each disk. <p>Use this option to check multiple floppy disks quickly. You cannot use the /MANY option if you run VirusScan from a boot disk and you have only one floppy drive.</p>
/MAXFILESIZE <xxx.x>	None.	Scan only files no larger than <xxx.x> megabytes.
/MEMEXCL	Not available for Windows.	Excludes the memory address A0000:0000 from scanning.
/NOBREAK	None.	Disables CTRL-C and CTRL-BREAK during scans. Users will not be able to halt scans in progress with /NOBREAK in use.
/NOCOMP	Extended memory required.	Skips checking of compressed executables created with the LZEXE or PkLite file-compression programs. This reduces scanning time when a full scan is not needed. Otherwise, by default, VirusScan checks inside executable, or self-decompressing, files by decompressing each file in memory and checking for virus signatures. <p>VirusScan will still check for modifications to compressed executables if they contain VirusScan validation codes.</p>

Target Command Line Option	Limitations	Description
/NODDA	None.	<p>No direct disk access. This prevents VirusScan from accessing the boot record.</p> <p>This feature has been added to allow VirusScan to run under Windows NT.</p> <p>You might need to use this option on some device-driven drives.</p> <p>Using /NODDA with the /ADN or /ADL switches may generate errors when accessing empty CD-ROM drives or empty Zip drives. If this occurs, type F (for Fail) in response to the error messages to continue the scan.</p>
/NODOC	None.	Does not scan Microsoft Office files.
/NOMEM	None.	<p>Does not scan memory for viruses.</p> <p>This greatly reduces scan time.</p> <p>Use /NOMEM only when you are absolutely certain that your computer is virus-free.</p>
/PANALYZE	Extended memory required.	<p>Sets VirusScan to scan using program heuristics.</p> <p><i>Note:</i> /MANALYZE targets macro viruses only; /ANALYZE targets both program and macro viruses.</p>
/PLAD	None.	<p>Preserves the last access dates on Novell NetWare drives.</p> <p>Normally, proprietary network drives update the last access date when VirusScan opens and examines a file. However, some tape backup systems use this last access date to decide whether to back up the file. Use /PLAD to ensure that the last access date does not change as the result of scanning.</p>
/SUB	None.	<p>Scans subdirectories inside a directory.</p> <p>By default, when you specify a directory to scan rather than a drive, VirusScan will examine only the files it contains, not its subdirectories.</p> <p>Use /SUB to scan all subdirectories within any directories you have specified.</p> <p>It is not necessary to use /SUB if you are scanning an entire drive.</p>
/UNZIP	Extended memory required.	Scan inside compressed files.

Response and notification options

The following table lists VirusScan's response and notification options after a virus has been detected.

Response and Notification Command Line Option	Limitations	Description
/ALERTPATH <dir>	*Can only be used on networks whose servers are running the correct version of NetShield.	<p>Designates the directory <dir> as a network path to a remote NetWare volume or NT directory, monitored by Centralized Alerting.</p> <p>VirusScan will send an .ALR text file to the server when it detects an infected file.</p> <p>From this directory, NetShield will, through its Centralized Alerting feature broadcast or compile the alerts and reports according to its established configuration.</p> <p>Requirements:</p> <ul style="list-style-type: none"> • These remote NetWare or Windows NT servers running NetShield for Windows NT v2.5.3 and later, or NetShield for NetWare v2.3.3 and later. • You must have write access to the <directory> you specify. • <directory> must contain the NetShield-supplied CENTALRT.TXT file. <p>Add these variables to your AUTOEXEC.BAT file to ensure that the .ALR file VirusScan sends identifies the infected system and its user:</p> <p>Set COMPUTERNAME=<name of computer> Set USERNAME=<user name></p>
/CLEAN	None.	Clean viruses from all infected files and system areas.
/CLEANDOCALL	None.	<p>As a precautionary measure against macro viruses, /CLEANDOCALL cleans all macros from Microsoft Word and Office documents.</p> <p><i>Note:</i></p> <p>This option deletes all macros, including macros not infected by a virus.</p>

Response and Notification Command Line Option	Limitations	Description
/CONTACTFILE <filename>	None.	<p>Display the contents of <filename> when a virus is found. It is an opportunity to provide contact information and instructions to the user when a virus is encountered.</p> <p>This option is especially useful in network environments, because you can easily maintain the message text in a central file rather than on each workstation.</p> <p><i>Note:</i></p> <p>Any character is valid in a contact message except a backslash (\). Messages beginning with a slash (/) or a hyphen (-) should be placed in quotation marks.</p>
/DEL	None.	Deletes infected files permanently.
/LOCK	Not available in low-memory environments.	<p>With this /LOCK option enabled, VirusScan will halt and lock your system if it finds a virus.</p> <p>/LOCK is appropriate in highly vulnerable network environments, such as open-use computer labs.</p> <p>Network Associates recommends using /LOCK with the /CONTACTFILE option to tell users what to do or whom to contact if VirusScan locks the system.</p>
/MOVE <dir> or *.???	None.	<p><i>/MOVE <directory>:</i></p> <p>Moves all infected files found during a scan to the specified directory, preserving drive letter and directory structure. <i>Note:</i> This option has no effect if the Master Boot Record or boot sector is infected, since these are not actually files.</p> <p><i>/MOVE*.???:</i></p> <p>VirusScan will change the extension of infected files, but not move them. For example, using the /MOVE*.BAD option will result in any infected files being simply renamed with the extension .BAD but not physically moved.</p>
/NOBEEP	None.	Disables the tone that sounds whenever VirusScan finds a virus.

Report options

The following table lists the available options available to configure how VirusScan displays the results of scanning activity.

- **To view the results of a scan task onscreen**, none of the options below are necessary to add to the command line. (Including /PAUSE on the command line will make reading a long report easier.)

For example,

```
scan a: /ONLY WEEKLY
```

will result in the scan results of a floppy disks' directory "Weekly" appearing onscreen.

- **To capture a VirusScan report to a text file**, /REPORT must be used, along with any additional switches as needed.

In the following example, the results of the above scan will not appear onscreen; they are instead redirected to a text file named, "rpt1.txt" in the C: drive directory, "Scans."

```
scan a: /ONLY WEEKLY /REPORT> c:\scans\rpt1.txt
```

The resultant text file can be viewed with any text editor.

Report Command Line Option	Limitations	Description
/ALERTPATH <dir>	None.	Designates the directory <dir> as a network path monitored by Centralized Alerting.
/APPEND	None.	Used with /REPORT to append report message text to the specified report file instead of overwriting it.
/PAUSE	None.	<p>Enables screen pause.</p> <p>The "Press any key to continue" prompt will appear when VirusScan fills a screen with messages. Otherwise, by default, VirusScan fills and scrolls a screen continuously without stopping, which allows VirusScan to run on PCs with multiple drives or that have severe infections without needing your input.</p> <p>Network Associates recommends omitting /PAUSE when using the report options (/REPORT, /RPTCOR, and /RPTERR).</p>

Report Command Line Option	Limitations	Description
/REPORT <filename>	None.	<p>Creates a report of infected files and system errors, and saves the data to <filename> in ASCII text file format.</p> <p>If <filename> already exists, /REPORT will overwrite it. To avoid overwriting, use the /APPEND option with /REPORT: VirusScan will instead add report information to the end of the file, instead of overwriting it.</p> <p>You can also use /RPTALL, /RPTCOR, and /RPTERR to add scanned files, corrupted files, modified files, and system errors to the report.</p> <p>You can include the destination drive and directory (such as D:\VSREPRT\ALL.TXT), but if the destination is a network drive, you must have rights to create and delete files on that drive.</p> <p>Network Associates recommends omitting /PAUSE when using any report option.</p>
/RPTALL	None.	<p>Include all scanned files in the /REPORT file.</p> <p>When used with /REPORT, this option adds the names of corrupted files to the report file.</p> <p>You can use /RPTCOR with /RPTERR on the same command line.</p> <p>Network Associates recommends omitting /PAUSE when using any report option.</p>
/RPTCOR	None.	<p>Include corrupted files in /REPORT file.</p> <p>When used with /REPORT, this option adds the names of corrupted files to the report file. Corrupted files which VirusScan finds may have been damaged by a virus.</p> <p>You can use /RPTCOR with /RPTERR on the same command line.</p> <p>There may be false readings in some files that require an overlay or another executable to run properly (that is, a file that is not executable on its own).</p> <p>Network Associates recommends omitting /PAUSE when using any report option.</p>

Report Command Line Option	Limitations	Description
/RPTERR	None.	<p>Include errors in /REPORT file.</p> <p>When used with /REPORT, this option adds a list of system errors to the report file.</p> <p>/LOCK is appropriate in highly vulnerable network environments, such as open-use computer labs.</p> <p>You can use /RPTERR with /RPTCOR on the same command line.</p> <p>System errors can include problems reading or writing to a disk or hard disk, file system or network problems, problems creating reports, and other system-related problems.</p> <p>Network Associates recommends omitting /PAUSE when using any report option.</p>
/VIRLIST	None.	<p>Displays the name and a brief description of each virus that VirusScan detects.</p> <p>You may use the /PAUSE option on the same command line as /VIRLIST to read the virus list one screen at a time.</p> <p><i>To redirect the /VIRLIST output to a text file:</i></p> <p>At the command prompt, type:</p> <pre>scan /VIRLIST> filename.txt</pre> <p>Because VirusScan can detect many viruses, this file will be over 250 pages long. This is too large for the MS-DOS "Edit" program to open; Network Associates recommends using Notepad or another text editor to open the virus list.</p>

Creating a scanning profile

Before creating a scanning profile, select the scanning options best suited to your computing environment and needs. See [“Selecting scanning options” on page 16](#) for a complete options list. Once you have made your choices, you are ready to construct a “scanning profile,” a text file of instructions and options VirusScan will use to execute a specific scan task.

Like other text files, you may update these scan profiles at any time, and create as many specialized scan tasks as you need.

To create a scanning profile, follow these steps:

1. Using the `cd` command, change to the VirusScan directory.
(For example, if VirusScan was installed on directory, “Scan” on your C: drive, type `cd \scan` at the command prompt.)
2. Type the following:

```
edit profile.txt
```

☐ **NOTE:** You may choose any filename for your scanning profile, and you may use any text editor to create the profile.

The MS-DOS program Edit opens.

3. Enter a scanning option (e.g. `/ADL`, `/ADN`, etc.).
4. Press **ENTER**.
The cursor is moved to the next line.
5. Repeat steps 3 and 4 until all options are entered, one per line.
6. To save the file, press **ALT+F** to access the File menu then press **S** to save.
7. To exit and return to the command prompt, press **ALT+F** to access the File menu, then press **X** to exit.

The file is created. To run the file, see [“Running a scanning profile,”](#) below.

Running a scanning profile

To run a scanning profile, complete the following procedure.

1. Using the `cd` command, change to the VirusScan directory.
2. Type the following:

```
scan /load <filename>
```

where *<filename>* is the name of the scanning profile that contains the instructions for the scan task of your choice.

VirusScan will execute the scan as detailed in the scanning profile you've just loaded.

To add a scanning profile to run at system startup, complete the following steps:

1. Change to the root directory by typing `cd c:\`
2. Type the following:

```
edit autoexec.bat
```

The Edit program starts.

3. Locate the first VShield line. Insert one space between VShield and the first option.
4. After the single space, type:

```
/load <filename>
```

where *<filename>* is the name of the scanning profile you'd like VirusScan to run at system startup. To add additional scanning profiles to VirusScan's startup, continue with Steps 5 and 6. If you are finished editing your AUTOEXEC.BAT, please skip to Step 7 below.

5. Type a single space.
6. Repeat Steps 4 and 5 until you have entered all the scanning profiles you want VirusScan to load at startup.
7. To save your changes to the AUTOEXEC.BAT, type **ALT+F** to open the File menu, **ALT + S** to save, then type **X** to exit.

Viewing the Virus List

The Virus List is a comprehensive list of viruses detected by VirusScan. The list provides information for each known virus VirusScan can detect, including what type of virus it is, its characteristics, size, and whether or not it is able to be “cleaned,” leaving the infected file intact.

Monthly updates to this list are available from Network Associates, and should be updated monthly; please see [“Updating your VirusScan data files” on page 45](#) for details.

To view the list of viruses detected by VirusScan onscreen:

1. Using the `cd` command, change to the VirusScan directory.
2. Type the following command:

```
scan /virlist > <filename>.txt
```

where *<filename>* is the name you have chosen for the text file. You may use any name you wish. This will redirect the output of the current Virus List to *<filename>.txt*.

3. Since the Virus List is over 250 pages long, it is too large a file for Edit to open. To view this file, open it in Notepad or another text editor of your choice. For instructions on printing the file, see directly below.


To print the list of viruses detected by VirusScan, complete the following:

1. Using the `cd` command, change to the VirusScan directory.
2. Type the following command:

```
scan /virlist > filename.txt
```

where *<filename>* is the name you have chosen for the text file. You may use any name you wish. This will redirect the output of the current Virus List to *<filename>.txt*.

3. If you have set your printer to capture output from MS-DOS programs, type `<filename>.txt>lpt1` at the MS-DOS prompt to redirect the output of *<filename>.txt* to your printer.

 **NOTE:** To learn how to set your printer to print from MS-DOS programs, please consult your Windows documentation.

Scanning your floppy disks

Why floppy disks pose a threat

Since over 90% of viruses invade systems when systems boot from an infected disk, or when users copy, run, or install programs or files that are infected, scanning all new floppy disks *before first use* will go a long way toward stopping the introduction of new viruses into any computing environment.

You should always take the proactive precaution of scanning all floppy disks you use. Even disks received from friends, co-workers, and other people you know should not be assumed to be virus-free.

Though it may be hard to believe, floppy disks pose a threat even if they are not bootable. To help address this threat, Network Associates recommends that you get in the habit of checking to make sure that your disk drives are empty before you turn on your computer: that way, your system will not pick up a boot sector virus from an infected floppy disk that is lying in one of your disk drives.

Preparing your system

VirusScan needs to run from your hard drive in order to scan floppy disks inserted into the A: drive. This means that if you have VirusScan running from floppy disks, and you have only one floppy drive on your computer, you will have to install and run VirusScan from your hard drive in order to scan floppy disks from the A: drive. (See [Chapter 2, “Installing VirusScan.”](#) for installation instructions.)


How to scan floppy disks

To scan floppy disks:

1. Using the `cd` command, change to the directory where VirusScan was installed.
2. Type:

```
scan a: /many
```
3. Insert the first disk to scan into the A: drive, and press **ENTER**.

The disk is scanned and the names of any infected files are displayed.

 **NOTE:** If VirusScan detects a virus on this disk, it will carry out the command-line option you chose for dealing with the virus. See [“Removing a virus found in a file” on page 40](#) for details on virus removal.

4. Remove the scanned floppy disk from the A: drive.
5. Insert the next disk and press **ENTER**. Repeat Steps 3 - 4 for all floppy disks needing to be scanned.

What is on-access scanning?

VShield, VirusScan's on-access scanner for DOS, automatically scans any file on your system as it's opened, or any executable as it's launched. Once you install VShield, it starts protecting you immediately with a default set of options, providing a strong defense against new virus threats. You can further customize on-access scanning by using the options listed in the tables from [pages 34 to 35](#) of this chapter.

You can easily configure VShield to launch at system startup to ensure continuous on-access protection: see [“Editing your AUTOEXEC.BAT file” on page 36](#) for instructions. VShield will then launch and run silently in the background, terminating when you end your DOS session.

On-access scanning in the Windows NT environment:

On-access scanning is not available for the Windows NT command line environment. To perform on-access scanning in a Windows NT environment, Network Associates recommends the graphical user interface version of VirusScan for Windows NT. See [“How to contact Network Associates” on page xviii](#) for further details.

On-access scanning in the OS/2 environment:

Network Associates recommends the new VirusScan for OS/2 for users needing on-access scanning protection in the OS/2 environment.

Users of earlier versions of VirusScan Command Line may wish to continue using VShield in the OS/2 environment. Limitations of VShield in OS/2 include:

- VShield does not run directly in the OS/2 environment. You can, however, use VShield features to scan DOS or FAT partitions on your hard disk by starting a DOS or WINOS2 session in OS/2.
- Some configuration options do not function in an OS/2 environment—this manual notes these exceptions in the descriptions of each option. See the command tables in [“Configuring VShield” on page 32](#), and in the [Appendix C, page 57](#), for details.
- VShield will detect only those viruses that can propagate in the OS/2-DOS environment; a virus in a file with a long filename, for example, will not be detected.

Starting VShield

If you have configured VirusScan to load VShield at startup, it will load and remain active in the background when you start your system.

Is VShield active? Follow either of these steps to find out:

- Type `chkvshld` at the DOS prompt in the VirusScan directory. You will receive a message that tells you whether VShield is running and which VShield options you have selected.
- Check your AUTOEXEC.BAT file for the VShield command line. (See [“Editing your AUTOEXEC.BAT file” on page 36](#) for instructions.)

Optimizing VShield performance

VShield is a Terminate-and-Stay-Resident (TSR) program, which remains in memory while you run other programs. VShield tries to optimize memory usage and minimize conflicts with other TSRs.

If, however, you do encounter problems using on-access scanning, it may be due to conflicts with other TSR programs in your system, or with other programs that monitor disk access. VShield minimizes the use of conventional memory by attempting to load into extended, expanded, upper memory, or a combination thereof, before using conventional memory. If you have more than 640 KB, VShield tries to load as much of itself as possible above conventional memory, first into expanded memory (EMS), into extended memory (XMS), then into upper memory blocks (640 KB to 1024 KB, or UMB).

Configuring VShield

VShield runs with the most common configuration options enabled by default. Unless you disable the program, or stop it entirely, you never have to worry about starting VShield or scheduling tasks for it.

As you become more familiar with how on-access scanning can best help guard your system, you can edit your AUTOEXEC.BAT to tailor VShield to best meet your needs.

To customize VShield, follow these steps:

1. Choose the VShield options most suitable for your work environment.

For an on-screen list of scanning options and their usage, use the `cd` command to change to the VirusScan directory, then type `vshield /?` at the command prompt.

A complete list of VShield options will appear. This list is also reprinted in the tables at the bottom of [page 34](#).

2. When you've chosen your VShield options, continue with the instructions on [page 36](#) to add these options to the VShield line in your AUTOEXEC.BAT file.

VShield options

General options

Command-line Option	Limitations	Description
/? or /HELP	None.	Displays a list of VirusScan command-line options, each with a brief description.
/NOREMOVE	None.	Prevents VShield from being removed from memory with the /REMOVE switch.
/RECONNECT	None.	Restores VShield after it has been disabled by certain drivers or memory-resident programs.
/REMOVE	None.	Unloads VShield from memory.
/SAVE	None.	Saves the command-line options to the VSHIELD.INI file.

Memory options

Memory Command-line Option	Limitations	Description
/MEMEXCL	Not available for Windows.	Excludes the memory address A0000:0000 from scanning.
/NOEMS	None.	Keeps VShield from using expanded memory (EMS).
/NOMEM	None.	Does not scan memory for viruses. This greatly reduces scan time. Use /NOMEM only when you are absolutely certain that your computer is virus-free.
/XMSDATA	None.	Loads VShield data files into XMS memory.

Target options

Target Command-line Option	Limitations	Description
/ANYACCESS	None.	Scans: <ul style="list-style-type: none"> the boot sector whenever a disk is either read or written to executables any newly created files.
/BOOTACCESS	None.	Scans a disk's boot sector for viruses whenever the disk is accessed (including read/write operations).
/FILEACCESS	None.	Scans executable files on access as well as execution. <i>Note:</i> This scan will <i>not</i> check the boot sector.
/IGNORE <drive(s)>	None.	Does not check any files loaded from the specified drive(s).
/NODISK	None.	Does not scan boot sector while loading VShield.
/NOWARMBOOT	None.	Does not check the disk boot sector of the floppy disk in drive A: for viruses during warm boot (system reset or CTRL+ALT+DEL).
/ONLY <drive(s)>	None.	Checks only files loaded from the specified drive(s).

Notification options

Notification Command-line Option	Limitations	Description
/CONTACT <message>	None.	Displays the specified message when a virus is detected. This message cannot exceed 255 characters.
/CONTACTFILE <filename>	None.	Displays the contents of <filename> if a virus is detected.
/LOCK	Not available in low-memory environments.	With this /LOCK option enabled, VirusScan will halt and lock your system if it finds a virus. /LOCK is appropriate in highly vulnerable network environments, such as open-use computer labs. Network Associates recommends using /LOCK with the /CONTACTFILE option to tell users what to do or whom to contact if VirusScan locks the system.

Editing your AUTOEXEC.BAT file

After you have chosen the VShield configuration options best suited to your environment and operating system (see “[Configuring VShield](#)” on page 32 for a list of options), you are ready to edit your AUTOEXEC.BAT file.

To edit your AUTOEXEC.BAT file, follow these steps:

1. Change to the root directory by typing `cd c:\`
2. Type:

`edit autoexec.bat`

The Edit program starts.
3. Locate the first VSHIELD line. Insert one space between VShield and the first option.
4. Type a scanning option (e.g., `/ANYACCESS`, `/BOOTACCESS`, etc.).

 **NOTE: For DOS sessions in OS/2:**

- The `/BOOTACCESS` option, *is not valid* since VShield will scan only files stored on floppy disks, but will not scan the boot sectors of floppy disks.
 - The `/ANYACCESS` option, while functional, will scan only floppy disk files.
-

5. Type a single space.
6. Repeat steps 4 and 5 until you have entered all of your chosen options.
7. To save your revisions, press **ALT+F**. The File menu will appear; press **S** to save.
8. To exit and return to the DOS prompt, press **ALT+F** to open the File menu, then press **X** to exit.

Removing Infections From Your System

5


If you suspect you have a virus ...

First of all, don't panic! Although far from harmless, *most* viruses that infect your machine will not destroy data, play pranks, or render your computer unusable. Even the comparatively rare viruses that do carry a destructive payload usually produce their nasty effects in response to a trigger event. In most cases, unless you actually see evidence of a payload that has activated, you will have time to deal with the infection properly. The very presence of these small snippets of unwanted computer code can, however, interfere with your computer's normal operation, consume system resources and have other undesirable effects, so you should take them seriously and be sure to remove them when you encounter them.

A second idea to keep in mind is that odd computer behavior, unexplained system crashes, or other unpredictable events might have causes other than virus infections. If you believe you have a virus on your computer because of occurrences such as these, scanning for viruses might not produce the results you expect, but it will help eliminate one potential cause for your computer problems.

If you have or suspect you have a virus, and you haven't yet installed VirusScan, follow these steps to clean your system:

1. Turn off your computer.

 **WARNING:** Do not reboot using the reset button or **CTRL+ALT+DELETE**; if you do, some viruses might remain intact or drop destructive payloads.

2. Place a clean start-up disk into the floppy disk drive. If you do not have a clean start-up disk, see [“Creating an emergency disk” on page 47](#).
3. Turn on your computer.
4. At the command prompt, type `scan /ADL /ALL /CLEAN`.

5. If viruses were removed:

Shut down your computer and remove the disk. Begin the installation procedure described in [Chapter 2, “Installing VirusScan.”](#)

To find and eliminate the source of infection, scan your disks immediately after installation. For information on scanning your disks, see [“Scanning your floppy disks” on page 28.](#)

If viruses were not removed:

If VirusScan cannot remove a virus, you will receive one of the following messages:

```
Virus could not be removed.
```

```
There is no remover currently available for the  
virus.
```

If VirusScan finds a virus in a file and cannot remove it, your only choice is to delete the infected file and restore from backups. If the virus was found in the Master Boot Record, refer to documents on the Network Associates website related to manually removing viruses.

If VirusScan detects a virus

Viruses attack computer systems by infecting files—usually executable program files or Microsoft Word documents and templates. VirusScan can safely remove most common viruses from infected files and repair any damage they may have caused.

Some viruses, however, are designed to damage your files beyond repair. These irreparably damaged files, called “corrupted” files, can be moved by VirusScan to a quarantine directory or deleted permanently to prevent further infection of your system.

Removing a virus found in memory

If VirusScan discovers a memory-resident virus, complete the following steps to remove it:

1. Turn off your computer.

NOTE: Do not reboot using the reset button or **CTRL+ALT+DELETE**; if you do, some viruses might remain intact or drop their destructive payloads.

2. Place a clean start-up disk into the floppy disk drive. If you do not have a clean start-up disk see [“Creating an emergency disk” on page 47](#).
3. Turn on your computer.
4. At the command prompt, type `scan /ADL /ALL /CLEAN`
5. **If viruses were removed:**

If VirusScan successfully removes all the viruses, shut down your computer and remove the clean start-up disk. Begin the installation procedure again, as described in [Chapter 2, “Installing VirusScan.”](#)

To find and eliminate the source of infection, scan your disks immediately after installation. For information on scanning your disks, see [“Scanning your floppy disks” on page 28](#).

If viruses were not removed:

If VirusScan cannot remove a virus, you will receive the message:

```
Virus could not be removed.
```

```
There is no remover currently available for the virus.
```

If the virus was found in a file and cannot be removed by VirusScan, you should delete the file and repeat the steps described in [“If you suspect you have a virus...” on page 37](#). If the virus was found in the Master Boot Record, refer to documents on the Network Associates website related to manually removing viruses. For more information, see [“How to contact Network Associates” on page xviii](#).


Removing a virus found in a file

If VirusScan detects a virus in a file, it will display the path/names of infected files and take the action specified in the scanning profile or command-line options. (See [“Advanced scanning” on page 15](#).) For example:

- If you selected /MOVE, VirusScan will automatically move the infected files to the specified quarantine directory.
- If you selected /CLEAN, VirusScan will attempt to repair the file.
- If you selected /DEL, VirusScan will delete and permanently overwrite the infected file.

Additional virus cleaning tasks:

Cleaning macro viruses from password-protected files

 **NOTE:** VirusScan detects macro virus infections in password-protected Microsoft Word 95 (Word 7.0) files in at least six languages.

VirusScan is designed to respect users' passwords and leave them intact as often as possible. For example, in password-protected Microsoft Excel 95 files, VirusScan removes macro viruses without disturbing users' passwords.

Macro viruses that infect Microsoft Word files, however, sometimes plant their own passwords. Depending on the capabilities of the particular virus, VirusScan will take one of the following actions when it is instructed to clean a password-protected file:

- **If the macro virus cannot plant its own password:** VirusScan notes the infection but does not clean it.
- **If the macro virus can plant its own password:** VirusScan cleans the file, removing the planted password along with the virus itself.

Windows NT hard disks:

To clean the Master Boot Record (MBR) on a hard disk formatted with the Windows NT file system (NTFS), follow these steps:

1. Start the computer that has the NTFS partition from a virus-free DOS boot disk.
2. Start VirusScan Command Line with the options, /BOOT /CLEAN. Be sure to run VirusScan from a floppy disk you know is free from viruses.

This will clean the NTFS Master Boot Record, but VirusScan Command Line cannot read the rest of the NTFS partition when you boot into a DOS environment.

3. To scan the rest of the NTFS partition, reboot into Windows NT, then run VirusScan Command Line again.

Understanding false alarms

A false alarm is a report of a virus found in a file or in memory when a virus does not actually exist. You are more likely to see false alarms if you are using more than one brand of virus protection software, because some anti-virus programs store their virus signature strings unprotected in memory. As a result, VirusScan may “detect” these unprotected strings falsely as a virus.

It is safest to assume that any virus reported by VirusScan is a genuine virus threat, and take steps to remove it from your system. If, however, you have reason to believe that VirusScan is generating a false alarm—for example, flagging a file as infected when you have been using it safely for years—review these potential sources for the false detection before contacting Network Associates.


- **You may have more than one anti-virus program running.** If so, VirusScan might think that unprotected virus signatures that the other product uses in its own detection efforts are viruses. To solve this problem, configure your system to run only one virus program. When you’ve completed reconfiguring your system, shut down your computer, and turn off the power. Wait a few seconds before turning it on again so that your system can clear the other program’s virus signatures from its memory.
- **You have a BIOS chip with anti-virus features.** Some BIOS chips include an anti-virus feature that could be the source of false alarms. Refer to your computer’s reference manual for details on how its anti-virus features work, and how to disable them if necessary.

- **You have an older Hewlett-Packard or Zenith PC.** Some older models from these manufacturers modify the boot sector each time the system is booted. VirusScan may detect these modifications as a possible infection. Check your computer's reference manual to determine if your PC has self-modifying boot code.
- **You have copy-protected software.** There are types of copy protection which may trigger VirusScan to report viruses in the boot sector or Master Boot Record on some floppy disks or other media.
- **Operating system security issues may be limiting how you can scan for viruses.** Because of operating system security, when VirusScan scans PAGEFILE.SYS, registry hive files, or user profiles, the system may beep, and a "Read Access Denied" non-critical error message may be displayed.
- **You do not have the correct administrative rights to scan correctly.** Within the Windows NT environment, VirusScan will not be able to access the boot sectors and the Master Boot Record unless you have administrative rights.

If none of these situations apply, contact Network Associates technical support (see [page xviii](#) for contact information), or e-mail AVresearch@nai.com with a detailed explanation of your situation.

Keys to a secure system environment

VirusScan is a powerful tool for preventing, detecting, and recovering from virus infection. It is most effective, however, as the cornerstone of a comprehensive computing security program that includes a variety of safety measures, such as regular backups, meaningful password protection, user training, and awareness.

 **NOTE:** If you suspect you have a virus, take steps to clean your system before installing VirusScan. See [“If you suspect you have a virus ...” on page 37.](#)

To help minimize your chance of infection:

- Follow the installation procedures described in [Chapter 2, “Installing VirusScan.”](#)
- Create a start-up disk containing VirusScan by following the instructions outlined in [“Creating an emergency disk” on page 47.](#) Make sure to write-protect this disk so that it cannot become infected.
- Make frequent backups of important files. Even with VirusScan’s abilities to contain and clean most viruses, there are certain malicious viruses (as well as fire, theft, vandalism, or ordinary disk failure) which can render infected files unrecoverable. Without recent backups, you will not be able to recover your data.
- Scan all disks that you use. See [“Scanning your floppy disks” on page 28.](#)
- Never start your computer from an unscanned disk.
- Always make sure your disk drives are empty before starting your computer.
- Always scan programs which are new to your computer. Before running the software for the first time, be sure to scan the directory containing the new program files.

Outlining a full security program is beyond the scope of this manual. However, by following the steps provided in this appendix and reading the information provided in the Preface, [“Where do viruses come from?” on page xii](#), you can gain a clearer understanding of what viruses are, how they affect your system, and what you can do to prevent an infection.

Detecting new viruses

There are two ways for you to proactively guard against new virus threats to your system:

- Validate your VirusScan program files as soon as you receive your software.
- Update your VirusScan data files regularly. These are the files with information on current viruses that VirusScan uses for detection and cleaning.

Updating your VirusScan data files

To offer the best virus protection possible, Network Associates continually updates the files VirusScan uses to detect viruses. After a certain time period, VirusScan will notify you about updating its virus definition database. Network Associates recommends that you update these data files on a regular basis for maximum protection.

What is a data file?

The files CLEAN.DAT, NAMES.DAT, and SCAN.DAT all provide virus information to your VirusScan software. These are the data files we're referring to in this user's guide.

Why would I need a new data file?

New viruses are discovered at a rate of more than 200 per month. Often, these new viruses are not detected by software using older data files. The data files that came with your copy of VirusScan might not be able to help VirusScan detect a virus discovered months after you first bought the product.

❏ **NOTE:** Network Associates cannot guarantee the backward compatibility of new data files with a previous version of VirusScan. By subscribing to a maintenance plan and upgrading your VirusScan software, you ensure complete virus protection for at least one year after your VirusScan purchase.

Updating the data file

To update your Network Associates data file, follow these steps:

1. Download the data file (for example, DAT-4001.ZIP) from one of the Network Associates electronic services. On most services, such as AOL or CompuServe, you can find Network Associates downloads in the anti-virus area.

You can also download data files from the Network Associates' website, <http://www.nai.com>.

☐ **NOTE:** Please note that your ability to access these updates is legally restricted by the maintenance terms outlined in the README.1ST file accompanying VirusScan, and detailed in the software license agreement. See [“Network Associates Support Services” on page 51](#) for more information.

2. Copy the file to a new directory.
3. The file is in a compressed format. Decompress the file using any PKUNZIP-compatible decompression software. If you don't have the decompression software, you can download PKUNZIP (shareware) from any of Network Associates' electronic sites.
4. Locate the directories on your hard drive where your VirusScan software is currently loaded. Typically, the files are stored in C:\NETA\VIRUSCAN.
5. Copy the new files into the directory or directories, overwriting the old data files.

☐ **NOTE:** There might be part of the software in more than one directory. If so, place the updated files in each directory.

6. Reboot your computer so that changes take place immediately.

Validating the VirusScan program files


When you download a file from any source other than the Network Associates bulletin board or other Network Associates service, it is important to verify that it is authentic, unaltered, and uninfected. To facilitate this, VirusScan includes a utility program called Validate that you can use to ensure that your version of VirusScan is authentic. When you receive a new version of VirusScan, run Validate on all of its program files and .DAT files.

For detailed instructions, see [“How to validate your copy of VirusScan” on page 7.](#)

Creating an emergency disk

In case your system becomes infected, you should have a clean start-up (also called boot, or emergency) disk. This section describes how to create that emergency disk. Since any virus residing in your system could be transferred to your emergency disk and reinfect your system, your system *must* be virus-free to create it. If your computer is infected, go to another computer and scan it. If it is virus-free, create your boot disk at this alternate workstation.

This emergency disk is for scanning the boot sector only; it is not intended for normal scanning.


 **IMPORTANT:** Because of limitations of how floppy disks are formatted within Windows NT, an emergency disk cannot be created from within Windows NT.

To create a boot disk:

1. Exit from Windows or any applications to get the command prompt (C:\>).
2. Insert a blank, *unformatted* disk into the A: drive.
3. Format the disk by typing the following command at the command prompt:

```
format a: /s /u
```

This will overwrite any information already on the disk.

 **NOTE:** If you are using DOS 5.0 or earlier, do not type the /u. To check which version you are using, type `ver` at the command prompt to display the DOS version number.

4. Locate HIMEM.SYS on your hard drive.
 - DOS users: by default, this can be found in the \DOS directory.
 - Windows users: by default, this file can be found in the \WINDOWS\COMMAND directory.
5. Copy HIMEM.SYS to your A: drive by typing the following at the command prompt:

```
copy himem.sys a:\
```

6. Create a file called CONFIG.SYS.

You can do this from within DOS, or by using Notepad or any other text editor of your choice.

- To create CONFIG.SYS at the command prompt:

a. Type:

```
Edit
```

The DOS editing program will start.

b. Type the following lines:

```
[CONFIG.SYS]  
DEVICE=HIMEM.SYS  
DOS=HIGH
```

c. Select **File, Save As ...** and enter the name CONFIG.SYS.

d. Click **OK** to save the file.

e. Select **File, Exit** to close Edit and return to the command prompt.

- To create CONFIG.SYS using Notepad or any other text editor of your choice:

a. Launch the editing program, and open a new file.

b. Complete steps b.> through e.> above.

7. When the system prompts you for a volume label, enter an appropriate name for your start-up disk. Remember to limit the length of this name to no more than eleven characters.

8. Change to the VirusScan directory. By default, this is C:\NETA\SCAN.

9. Copy the command-line version of VirusScan to the disk by typing the following commands at the prompt:

```
copy bootscan.exe a:\  
copy emscan.dat a:\scan.dat  
copy emclean.dat a:\clean.dat  
copy emnames.dat a:\names.dat  
copy license.dat a:\  
copy messages.dat a:\
```

You have now copied, and renamed where necessary, all the files VirusScan will need to scan the boot sector of an infected computer.

10. Copy any other DOS utilities you may need to start your computer, debug your system software, manage any extended or expanded memory you have, or perform other tasks at startup. If you use a disk compression utility, be sure to copy the drivers you need to uncompress your files.
11. You have now completed copying all necessary programs for rebooting your system on to this boot disk
12. You may want to copy these additional useful command-line programs to a *second* disk:

❏ **NOTE:** Do not attempt to copy these programs to the clean boot disk you are making. Conventional disks do not have enough storage space to accommodate both VirusScan and these programs.

- debug.*
- diskcopy.*
- fdisk.*
- format.*
- label.*
- mem.*
- sys.*
- xcopy.*

❏ **NOTE:** If you use a disk compression utility or a password encryption utility, be sure to copy the drivers required to access your drives onto the clean boot disk. See the documentation for those utilities for more information about those drivers.

13. Label and write-protect these disks, then store it in a secure place. See [“Write-protecting a disk” on page 50](#) for more information.

Write-protecting a disk

Floppy disks are convenient, portable devices for storage and retrieval of computer data. They are also the most common vehicle viruses use to invade your computer's system.

One way to help avoid infection via floppy disk is to *write-protect* the disks you are using for read-only data. If your system becomes infected with a virus, the write-protection feature will keep these disks from becoming infected as well, preventing reinfection after your system is cleaned.

-
- ❏ **NOTE:** Any disks that are not write-protected should be scanned and cleaned before you write-protect them.
-

To write-protect 3.5" floppy disks:

1. Position the disk face down with the metal slide facing you.
2. Examine the small rectangular hole on the upper left side. There should be a square, plastic tab that you can slide up and down across the hole.

To write-protect the disk, slide the plastic tab upward toward the edge of the disk so that the hole is open. This stops you from accidentally changing data on the disk. It also prevents viruses from infecting the disk.

-
- ❏ **NOTE:** If there is no tab and the hole is open, the disk is permanently write-protected.
-

Network Associates Support Services

B

Choosing Network Associates anti-virus and security software helps to ensure that the critical information technology you rely on functions smoothly and effectively. Taking advantage of a Network Associates support plan extends the protection you get from your software by giving you access to the expertise you need to install, monitor, maintain and upgrade your system with the latest Network Associates technology. With a support plan tailored to your needs, you can keep your system or your network working dependably in your computing environment for months or years to come.

Network Associates support plans come under two general headings. If you are a corporate customer, you can choose from three levels of extended support under the Network Associates PrimeSupport program. If you purchased a retail version of a Network Associates product, you can choose a plan geared toward your needs from the Personal Support program.

PrimeSupport Options for corporate customers

The Network Associates PrimeSupport program offers a choice of Basic, Extended, or Anytime options. Each option has a range of features that provide you with cost-effective and timely support geared to meet your needs.

PrimeSupport Basic

PrimeSupport Basic gives you telephone access to essential product assistance from experienced Network Associates technical support staff members. If you purchased your Network Associates product with a subscription license, you will receive PrimeSupport Basic as part of the package for two years from your date of purchase. If you purchased your Network Associates product with a perpetual license, you can renew your PrimeSupport Basic plan for an annual fee.

PrimeSupport Basic includes these features:

- Telephone access to technical support from Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time.
- Unrestricted access 24 hours per day to Network Associates technical support information via the Network Associates website.
- Updates to data files and product upgrades via the Network Associates website.

PrimeSupport Extended

PrimeSupport Extended gives you personalized, proactive support from an assigned technical support engineer. You'll enjoy a relationship with a support professional who is familiar with your Network Associates product deployment and support history, and who will call you at an interval you designate to verify that you have the knowledge you need to use and maintain Network Associates products. By calling in advance, your PrimeSupport Extended representative can help to prevent problems before they occur. If, however, an emergency arises, PrimeSupport Extended gives you a committed response time that assures you that help is on the way. You may purchase PrimeSupport Extended on an annual basis when you purchase a Network Associates product either with a subscription license or a perpetual license.

PrimeSupport Extended includes these features:

- Access to an assigned technical support engineer
- Proactive support contacts via telephone or e-mail from your assigned support engineer, at an interval you designate
- Committed response times: your support engineer will respond within one hour to pages, within four hours to voice mail, and within 12 hours to e-mail
- Telephone access to technical support from Monday through Friday, 7:00 a.m. to 7:00 p.m., Central time
- Unrestricted access 24 hours per day to Network Associates technical support information via the Network Associates website
- Updates to data files and product upgrades via the Network Associates website
- Ability to designate up to five people in your organization as customer contacts.

PrimeSupport Anytime

PrimeSupport Anytime offers round-the-clock, personalized, proactive support for Network Associates products deployed in the most business-critical information systems. PrimeSupport Anytime delivers the features of PrimeSupport Extended 24 hours a day, seven days a week, with shorter response time commitments. You may purchase PrimeSupport Anytime on an annual basis when you purchase a Network Associates product either with a subscription license or a perpetual license.

PrimeSupport Anytime includes these features:

- Access to an assigned technical support engineer
- Proactive support contacts via telephone or e-mail from your assigned support engineer, at an interval you designate
- Committed response times: your support engineer will respond within half an hour to pages, within one hour to voice mail, and within four hours to e-mail
- Telephone access to technical support 24 hours a day, seven days a week
- Unrestricted access 24 hours per day to Network Associates technical support information via the Network Associates website
- Updates to data files and product upgrades via the Network Associates website
- Ability to designate up to 10 people in your organization as contacts.

Feature	Basic	Extended	Anytime
Technical support via telephone	Monday–Friday 8:00 a.m.–8:00 p.m.	Monday–Friday 7:00 a.m.–7:00 p.m.	24 hours a day, 7 days a week
Technical support via website	Yes	Yes	Yes
Software updates	Yes	Yes	Yes
Assigned support engineer	—	Yes	Yes
Proactive support contact	—	Yes	Yes
Designated customer contacts	—	5	10
Committed response time	—	Pager: 1 hour Voicemail: 4 hours E-mail: 12 hours	Pager: 30 mins. Voicemail: 1 hour E-mail: 4 hours

Ordering PrimeSupport

To order PrimeSupport Basic, PrimeSupport Extended or PrimeSupport Anytime for your Network Associates products:

- Contact your sales representative; or
- Call Network Associates Support Services at 1-800-988-5737 or 1-650-473-2000 from 6:00 a.m. to 5:00 p.m. Pacific Time, Monday through Friday.

❏ **NOTE:** The PrimeSupport program described in this guide is available in North America only. To learn about PrimeSupport options available outside North America, contact your regional sales office. Contact information appears near the front of this guide.

Support services for retail customers

If you purchased your Network Associates product through a retail vendor or from the Network Associates website, you also receive some support services as part of your purchase. The specific level of included support depends on the product that you purchased. Examples of the services you receive include:

- Free data (.DAT) file updates for the life of your product via the Network Associates website, your product's AutoUpdate feature, or the SecureCast service (see [“Updating your VirusScan data files” on page 45](#) for details). You can also update your data files by using your web browser to visit <http://www.nai.com/download/updates/updates.asp>.
- Free program (executable file) upgrades for one year via the Network Associates website, your product's AutoUpdate feature, or the SecureCast service (see [“Updating your VirusScan data files” on page 45](#) for details). If you purchased a deluxe version of a Network Associates product, you receive free program upgrades for two years. You can also upgrade your software by visiting:

<http://www.nai.com/download/upgrades/upgrades.asp>.

- Free access 24 hours a day, seven days a week to online or electronic support through the Network Associates voice and fax system, the Network Associate's website, and through such other electronic services as America Online and CompuServe.

To contact Network Associates electronic services, choose one of these options:

- Automated voice and fax system: (408) 988-3034
- Network Associates website: <http://support.nai.com>
- CompuServe: GO NAI
- America Online: keyword MCAFEE
- Ninety days of complimentary technical support from a Network Associates support technician during regular business hours, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time.

After your complimentary support period expires, you can take advantage of a variety of personal support options geared toward your needs. Contact Network Associates Customer Care at (972) 278-6100 to learn more about the options available, or visit the Network Associates website at:

<http://www.nai.com/services/support/support.asp>.

Network Associates consulting and training

Network Associates provides expert consulting and comprehensive education that can help you maximize the security and performance of your network investments through the Network Associates Total Service Solutions program.

Professional Consulting Services

Network Associates Professional Consulting Services is ready to assist during all stages of your network growth, from planning and design, through implementation, and with ongoing management. Network Associates consultants provide an expert supplemental resource and independent perspective to resolve your problems. You'll get help integrating Network Associates products into your environment, along with troubleshooting assistance or help in establishing baselines for network performance. Network Associates consultants also develop and deliver custom solutions to help accomplish your project goals—from lengthy, large-scale implementations to brief problem-solving assignments.

Total Education Services

Network Associates Total Education Services builds and enhances the skills of all network professionals through practical, hands-on instruction that you can take right back to your job. The Total Education Services technology curriculum focuses on network fault and performance management and covers problem solving at all levels. Network Associates also offers modular product training so that you understand the features and functionality of your new software.

You can enroll in Total Education Services courses year-round at Network Associates educational centers, or you can learn from customized courses conducted at your location. All courses follow educational steps along a learning path that takes you to the highest levels of expertise. Network Associates is a founding member of the Certified Network Expert (CNX) consortium.

To learn more about these programs, contact your sales representative or call Total Service Solutions at 1-800-395-3151.

VirusScan command-line options

The following table lists all of the VirusScan options. When typing commands, remember that if you name a file which resides *outside* the directory where VirusScan is installed, you must include the full path to that file.

Command-Line Option	Limitations	Description
<i>All the options listed below can be used to configure both on-demand and on-access scans, unless otherwise noted.</i>		
/? or /HELP	None.	Displays a list of VirusScan command-line options, each with a brief description.
/ADL	On-demand scanning option only.	<p>Scan all local drives—including compressed drives and PC cards, but not disks—in addition to any other drive(s) specified on the command line.</p> <p>To scan both local and network drives, use the /ADL and /ADN commands together in the same command line.</p> <p>OS/2: /ADL includes the CD-ROM drive in the scan, when used with /NODDA.</p>
/ADN	On-demand scanning option only.	<p>Scan all network drives—including CD-ROM—for viruses, in addition to any other drive(s) specified on the command line.</p> <p><i>Note:</i> To scan both local drives and network drives, use the /ADL and /ADN commands together in the same command line.</p>

Command-Line Option	Limitations	Description
/ALERTPATH <dir>	On-demand scanning option only. Can only be used on networks whose servers are running the correct version of NetShield.	Designates the directory <dir> as a network path to a remote NetWare volume or NT directory, monitored by Centralized Alerting. VirusScan will send an .ALR text file to the server when it detects an infected file. From this directory, NetShield will, through its Centralized Alerting feature broadcast or compile the alerts and reports according to its established configuration. Requirements: --These remote NetWare or Windows NT servers running NetShield for Windows NT v2.5.3 and later, or NetShield for NetWare v2.3.3 and later. --You must have write access to the <directory> you specify. --<directory> must contain the NetShield-supplied CENTALRT.TXT file. Add these variables to your AUTOEXEC.BAT file to ensure that the .ALR file VirusScan sends identifies the infected system and its user: Set COMPUTERTNAME=<name of computer> Set USERNAME=<user name>
/ALL	On-demand scanning option only.	Overrides the default scan setting by scanning all infectable files—regardless of extension. <i>Notes:</i> Using the /ALL option substantially increases the scanning time required. Use it only if you find a virus or suspect that you have one. By default, VirusScan only scans files with the following extensions: .EXE, .COM, .SYS, .BIN, .OVL, .DLL, .DOC, .DOT, .XLA, .XLS, .XLT, .RTF, and .VXD. These are the file types that are most susceptible to viruses.
/ANALYZE	On-demand scanning option only. Extended memory required.	Sets VirusScan to scan using its full heuristics, both program and macro. <i>Note:</i> /MANALYZE targets macro viruses only; /PANALYZE targets program viruses only.

Command-Line Option	Limitations	Description
/ANYACCESS	On-access scanning option only.	Scans: * the boot sector whenever a disk is either read or written to * executables * any newly created files.
/APPEND	On-demand scanning option only.	Used with /REPORT to append report message text to the specified report file instead of overwriting it.
/BOOT	On-demand scanning option only.	Scan boot sector and master boot record only.
/BOOTACCESS	On-access scanning option only.	Scans a disk's boot sector for viruses whenever the disk is accessed (including read/write operations).
/CLEAN	On-demand scanning option only.	Clean viruses from all infected files and system areas.
/CLEANDOCALL	On-demand scanning option only.	As a precautionary measure against macro viruses, /CLEANDOCALL cleans all macros from Microsoft Word and Office documents. <i>Note:</i> This option deletes all macros, including macros not infected by a virus.
/CONTACT <message>	On-access scanning option only.	Displays specified message when a virus is detected. This message cannot exceed 255 characters.
/CONTACTFILE <filename>	None.	Display the contents of <filename> when a virus is found. It is an opportunity to provide contact information and instructions to the user when a virus is encountered. This option is especially useful in network environments, because you can easily maintain the message text in a central file rather than on each workstation. <i>Note:</i> Any character is valid in a contact message except a backslash (\). Messages beginning with a slash (/) or a hyphen (-) should be placed in quotation marks.
/DEL	On-demand scanning option only.	Deletes infected files permanently.

Command-Line Option	Limitations	Description
/EXCLUDE <filename>	On-demand scanning option only.	Do not scan or add validation codes to the files listed in <filename>. Use this option to: * Exclude specific files from a scan. List the complete path to each file that you want to exclude on its own line. You may use wildcards * and ?
/FILEACCESS	On-access scanning option only.	Scans executable files on access as well as execution. <i>Note:</i> This scan will <i>not</i> check the boot sector.
/FREQUENCY <n>	On-demand scanning option only.	Do not scan <n> hours after the previous scan. In environments where the risk of viral infection is very low, use this option to prevent unnecessary scans. Remember, the greater the scan frequency, the greater your protection against infection.
/HELP or /?	None.	Displays a list of VirusScan command-line options, each with a brief description.
/IGNORE <drive(s)>	On-access scanning option only.	Does not check any files loaded from the specified drive(s).
/LOAD <filename>	On-demand scanning option only.	Load scanning options from the named file. Use this option to perform a scan you've already configured by loading custom settings saved in an ASCII-formatted file.
/LOCK	Not available in low-memory environments	With this /LOCK option enabled, VirusScan will halt and lock your system if it finds a virus. /LOCK is appropriate in highly vulnerable network environments, such as open-use computer labs. Network Associates recommends using /LOCK with the /CONTACTFILE option to tell users what to do or whom to contact if VirusScan locks the system.
/MANALYZE	On-demand scanning option only. Extended memory required.	Sets VirusScan's heuristic scanning features to target macro viruses only. <i>Note:</i> /PANALYZE targets program viruses only; /ANALYZE targets both program and macro viruses.

Command-Line Option	Limitations	Description
/MANY	On-demand scanning option only.	Scans multiple disks consecutively in a single drive. VirusScan will prompt you for each disk. Use this option to check multiple floppy disks quickly. You cannot use the /MANY option if you run VirusScan from a boot disk and you have only one floppy drive.
/MAXFILESIZE <xxx.x>	On-demand scanning option only.	Scan only files no larger than <xxx.x> megabytes.
/MEMEXCL		Excludes the memory address A0000:0000 from scanning.
/MOVE <dir> or *.???	On-demand scanning option only.	<i>/MOVE <directory>:</i> Moves all infected files found during a scan to the specified directory, preserving drive letter and directory structure. <i>Note:</i> This option has no effect if the Master Boot Record or boot sector is infected, since these are not actually files. <i>/MOVE*.???:</i> VirusScan will change the extension of infected files, but not move them. For example, using the /MOVE*.BAD option will result in any infected files being simply renamed with the extension .BAD but not physically moved.
/NOBEEP	On-demand scanning option only.	Disables the tone that sounds whenever VirusScan finds a virus.
/NOBREAK	On-demand scanning option only.	Disables CTRL-C and CTRL-BREAK during scans. Users will not be able to halt scans in progress with /NOBREAK in use.
/NOCOMP	On-demand scanning option only. Extended memory required.	Skips checking of compressed executables created with the LZEXE or PkLite file-compression programs. This reduces scanning time when a full scan is not needed. Otherwise, by default, VirusScan checks inside executable, or self-decompressing, files by decompressing each file in memory and checking for virus signatures. VirusScan will still check for modifications to compressed executables if they contain VirusScan validation codes.

Command-Line Option	Limitations	Description
/NODDA	On-demand scanning option only.	<p>No direct disk access. This prevents VirusScan from accessing the boot record.</p> <p>This feature has been added to allow VirusScan to run under Windows NT.</p> <p>You might need to use this option on some device-driven drives.</p> <p>Using /NODDA with the /ADN or /ADL switches may generate errors when accessing empty CD-ROM drives or empty Zip drives. If this occurs, type F (for Fail) in response to the error messages to continue the scan.</p>
/NODISK	On-access scanning option only.	Does not scan boot sector while loading VShield.
/NODOC	On-demand scanning option only.	Does not scan Microsoft Office files.
/NOEMS	On-access scanning option only.	Keeps VShield from using expanded memory (EMS).
/NOEXPIRE	On-demand scanning option only.	Disables the "expiration date" message if the VirusScan data files are out of date.
/NOMEM	None.	<p>Does not scan memory for viruses.</p> <p>This greatly reduces scan time.</p> <p>Use /NOMEM only when you are absolutely certain that your computer is virus-free.</p>
/NOREMOVE	On-access scanning option only.	Prevents VShield from being removed from memory with the /REMOVE switch.
/NOWARMBOOT	On-access scanning option only.	Does not check the disk boot sector of the floppy disk in the A: drive for viruses during warm boot (system reset or CTRL+ALT+DEL).
/NOXMS	On-access scanning option only.	Does not use extended memory (XMS).
/ONLY <drive(s)>	On-access scanning option only.	Checks only files loaded from the specified drive(s).

Command-Line Option	Limitations	Description
/PANALYZE	On-demand scanning option only. Extended memory required.	Sets VirusScan to scan using program heuristics. <i>Note:</i> /MANALYZE targets macro viruses only; /ANALYZE targets both program and macro viruses.
/PAUSE	On-demand scanning option only.	Enables screen pause. The “Press any key to continue” prompt will appear when VirusScan fills a screen with messages. Otherwise, by default, VirusScan fills and scrolls a screen continuously without stopping, which allows VirusScan to run on PCs with multiple drives or that have severe infections without needing your input. Network Associates recommends omitting /PAUSE when using the report options (/REPORT, /RPTCOR, and /RPTERR).
/PLAD	On-demand scanning option only.	Preserves the last access dates on Novell NetWare drives. Normally, proprietary network drives update the last access date when VirusScan opens and examines a file. However, some tape backup systems use this last access date to decide whether to back up the file. Use /PLAD to ensure that the last access date does not change as the result of scanning.
/RECONNECT	On-access scanning option only.	Restores VShield after it has been disabled by certain drivers or memory-resident programs.
/REMOVE	On-access scanning option only.	Unloads VShield from memory.


Command-Line Option	Limitations	Description
/REPORT <filename>	On-demand scanning option only.	<p>Creates a report of infected files and system errors, and saves the data to <filename> in ASCII text file format.</p> <p>If <filename> already exists, /REPORT will overwrite it. To avoid overwriting, use the /APPEND option with /REPORT: VirusScan will instead add report information to the end of the file, instead of overwriting it.</p> <p>You can also use /RPTALL, /RPTCOR, and /RPTERR to add scanned files, corrupted files, modified files, and system errors to the report.</p> <p>You can include the destination drive and directory (such as D:\VSREPRT\ALL.TXT), but if the destination is a network drive, you must have rights to create and delete files on that drive.</p> <p>Network Associates recommends omitting /PAUSE when using any report option.</p>
/RPTALL	On-demand scanning option only.	<p>Include all scanned files in the /REPORT file.</p> <p>When used with /REPORT, this option adds the names of corrupted files to the report file.</p> <p>You can use /RPTCOR with /RPTERR on the same command line.</p> <p>Network Associates recommends omitting /PAUSE when using any report option.</p>
/RPTCOR	On-demand scanning option only.	<p>Include corrupted files in /REPORT file.</p> <p>When used with /REPORT, this option adds the names of corrupted files to the report file. Corrupted files that VirusScan finds may have been damaged by a virus.</p> <p>You can use /RPTCOR with /RPTERR on the same command line.</p> <p>There may be false readings in some files that require an overlay or another executable to run properly (that is, a file that is not executable on its own).</p> <p>Network Associates recommends omitting /PAUSE when using any report option.</p>

Command-Line Option	Limitations	Description
/RPTERR	On-demand scanning option only.	<p>Include errors in /REPORT file.</p> <p>When used with /REPORT, this option adds a list of system errors to the report file.</p> <p>/LOCK is appropriate in highly vulnerable network environments, such as open-use computer labs.</p> <p>You can use /RPTERR with /RPTCOR on the same command line.</p> <p>System errors can include problems reading or writing to a disk or hard disk, file system or network problems, problems creating reports, and other system-related problems.</p> <p>Network Associates recommends omitting /PAUSE when using any report option.</p>
/SAVE	On-access scanning option only.	Saves the command-line options to the VSHIELD.INI file.
/SUB	On-demand scanning option only.	<p>Scans subdirectories inside a directory.</p> <p>By default, when you specify a directory to scan rather than a drive, VirusScan will examine only the files it contains, not its subdirectories.</p> <p>Use /SUB to scan all subdirectories within any directories you have specified.</p> <p>It is not necessary to use /SUB if you are scanning an entire drive.</p>
/UNZIP	On-demand scanning option only. Extended memory required.	Scan inside compressed files.

Command-Line Option	Limitations	Description
/VIRLIST	On-demand scanning option only.	<p>Displays the name and a brief description of each virus that VirusScan detects.</p> <p>You may use the /PAUSE option on the same command line as /VIRLIST to read the virus list one screen at a time.</p> <p><i>To redirect the /VIRLIST output to a text file:</i></p> <p>At the command prompt, type:</p> <pre>scan /VIRLIST> filename.txt</pre> <p>Because VirusScan can detect many viruses, this file will be over 250 pages long. This is too large for the MS-DOS "Edit" program to open; Network Associates recommends using Notepad or another text editor to open the virus list.</p>
/XMSDATA	On-access scanning option only.	Loads VShield data files into XMS memory.

VirusScan error levels

When you run VirusScan in the DOS environment, a DOS error level is set. You can use the ERRORLEVEL in batch files to take different actions based on the results of the scan.

 **NOTE:** See your DOS operating system documentation for more information.

VirusScan can return the following error levels:

Errorlevel	Description
0	No errors occurred; no viruses were found.
2	Driver integrity check failed.
6	A general problem.
8	Could not find a driver.
10	A virus was found in memory.
13	One or more viruses or hostile objects were found.
15	VirusScan self-check failed; it may be infected or damaged.
20	Scanning prevented due to the /FREQUENCY switch.
102	User quit via ESC-X, ^C or Exit button. <i>Note:</i> This can be disabled with the /NOBREAK command line option.

Index

A

America Online, technical support via, [xviii](#), [55](#)

anti-virus software

 problems from using multiple programs from different vendors, [41](#)

 reporting new viruses not detected by to Network Associates, [xx](#)

 use of code signatures for virus detection, [xv](#)

archived files

see compressed files

AUTOEXEC.BAT

 editing, [26](#)

B

Basic, as macro virus programming language, [xvi](#)

BIOS chips

 anti-virus features in, [41](#)

boot record

 preventing VirusScan from accessing, [19](#), [62](#)

boot sector

 command to scan on-access, [35](#), [59](#)

 limiting scan to, [17](#), [59](#)

 omitting from scanning during a warm boot, [35](#), [62](#)

 PCs which self-modify., [42](#)

 to not include in on-access scanning, [35](#), [62](#)

boot-sector viruses, definition and behavior of, [xiii](#) to [xiv](#)

Brain virus, [xiii](#)

C

CAB files

 limitations on scanning, [12](#)

Centralized Alerting

 setting VirusScan to send to, [20](#), [58](#)

clean

 all infected files, [20](#), [59](#)

 all macros from Microsoft Word and Office files, [20](#), [59](#)

code signatures, use of by viruses, [xv](#)

command to scan on-access in OS/2, [35](#), [59](#)

COMMAND.COM files, virus infections in, [xiv](#)

compressed files

 setting VirusScan to scan inside of, [19](#), [65](#)

 skipping during virus scans, [18](#), [61](#)

 types recognized by VirusScan

CompuServe, technical support via, [xviii](#), [55](#)

computer problems, attributing to viruses, [37](#)

Concept virus, introduction of, [xv](#) to [xvi](#)

consulting services, [55](#)

copy-protected software, possibly triggering false alarms, [42](#)

corrupted files, [39](#)

costs from virus damage, [xi](#) to [xii](#)

CTRL+ALT+DEL

 setting VirusScan to not scan the boot sector during, [35](#), [62](#)

CTRL+ALT+DEL, caution against using to clear viruses, [xiv](#)

CTRL+BREAK

 disabling during scans, [18](#), [61](#)

CTRL+C

 disabling during scans, [18](#), [61](#)

Customer Care

contacting, [xviii](#)

D

damage from viruses, [xi](#)

payloads, [xiii](#)

.DAT file updates, reporting new items for, [xx](#)

data files

updating, [45](#)

default settings

creating multiple configuration files, [16](#),
[60](#)

DEFAULT.CFG

using a different configuration file, [16](#),
[60](#)

definition of virus, [xi](#) to [xii](#)

detected, error level for, [67](#)

detection of viruses, use of code signatures for,
[xv](#)

direct drive access

disabling with VirusScan, [19](#), [62](#)

directories

scanning, [19](#), [65](#)

disguising virus infections, [xv](#)

disks

scanning, [28](#)

scanning multiple, [18](#), [61](#)

write protecting, [50](#)

disks, floppy, as medium for virus

transmission, [xiii](#) to [xiv](#)

displaying list of detected viruses

with VirusScan, [24](#), [66](#)

document files, as agents for virus

transmission, [xv](#) to [xvi](#)

documentation

VirusScan, [3](#)

DOS error levels

VirusScan, [67](#)

driver

missing, error level for, [67](#)

drives

scan only files loaded from a specific
drive, [35](#), [62](#)

scanning local, [17](#), [57](#)

scanning network, [17](#), [57](#)

specifying a drive to ignore in scanning,
[35](#), [60](#)

E

educational services, description of, [56](#)

electronic services, contacting for technical
support, [55](#)

e-mail

addresses for reporting new viruses to
Network Associates, [xx](#)

as agent for virus transmission, [xvi](#)

emergency disk

making a, [47](#)

enabling full heuristic scanning, [16](#) to [17](#), [58](#)

encrypted viruses, [xv](#)

Excel files, as agents for virus transmission,
[xvi](#)

excluding files

during virus scans, [18](#), [60](#)

executable files, as agents for virus

transmission, [xiv](#)

executables, [35](#), [59](#)

expiration date message

disabling, [16](#), [62](#)

extended memory, setting VirusScan not to
use, [34](#), [62](#)

F

false alarms, [41](#)

file types

scanning all, [17](#), [58](#)

file-infector viruses, definition and behavior
of, [xiv](#)

files

corrupted, [39](#)

deleting infected files, [21](#), [59](#)

moving infected files, [21, 61](#)

floppy disks

- role in spreading viruses, [xiii to xiv](#)
- scanning multiple, [18, 61](#)
- scanning on access in OS/2, [35, 59](#)

frequency

- determining for VirusScan, [16, 60](#)
- error level for frequency settings
- preventing scanning, [67](#)

H

help

- displaying, [16, 34, 57, 60](#)

heuristic scanning

- enabling VirusScan's full capabilities, [16 to 17, 58](#)
- to target macro viruses only, [18, 60](#)
- to target program viruses only, [19, 63](#)

Hewlett-Packard PCs, self-modifying boot sectors in, [42](#)

hiding

- virus infections, [xv](#)

history of viruses, [xii to xvi](#)

I

infected files

- deleting permanently, [21, 59](#)
- moving, [21, 61](#)
- removing viruses from, [37](#)

Internet

- spread of viruses via, [xvi](#)

Internet Relay Chat

- as agent for virus transmission, [xvi](#)

L

last access dates

- preserving on Novell NetWare drives, [19, 63](#)

local drives

- scanning, [17, 57](#)

locking the system

- if a virus is found, [21, 35, 60](#)

LZEXE

- and VirusScan, [18, 61](#)

M

macro viruses

- cleaning, [40](#)
- cleaning from Microsoft Office files, [20, 59](#)
- Concept virus, [xv to xvi](#)
- definition and behavior of, [xv to xvi](#)
- setting heuristic scanning to target, [18, 60](#)

malicious software

- payload, [xiii](#)
- script viruses, [xvi](#)
- types
 - Trojan horses, [xiii](#)
 - worms, [xii](#)

master boot record (MBR)

- command to scan on-access, [35, 59](#)
- formatted with Windows NT
- how to clean, [41](#)
- susceptibility to virus infection, [xiv](#)

memory

- excluding area from scans, [18, 34, 61](#)
- extended memory
 - setting VirusScan not to use, [62](#)
- false alarms of a virus found in memory, [41](#)
- omitting from scans, [19, 34, 62](#)
- preventing VShield from being removed from, [34, 62](#)
- to load VShield files into XMS memory, [34, 66](#)
- unloading VShield from, [34, 63](#)
- virus infections in, [xiii to xiv](#)
- virus infections in, error level for, [67](#)

messages

- displaying when a virus is found, [21, 59](#)
- pausing when displaying, [22, 63](#)

Microsoft Office

- command to clean all macros from, [20](#), [59](#)

- omitting files from scans, [19](#), [62](#)

Microsoft Visual Basic, as macro virus programming language, [xvi](#)

Microsoft Word and Excel files, as agents for virus transmission, [xvi](#)

mIRC script virus, [xvi](#)

moving

- infected files, [21](#), [61](#)

mutating viruses, definition of, [xv](#)

N

Network Associates

- consulting services from, [55](#)

contacting

- Customer Care, [xviii](#)

- outside the United States, [xxi](#)

- via America Online, [xviii](#)

- via CompuServe, [xviii](#)

- within the United States, [xix](#)

- educational services, [56](#)

- support services, [51](#)

- training, [xix](#), [55](#)

- website address for software updates and upgrades, [54](#)

network drives

- scanning, [17](#), [57](#)

new viruses, reporting to Network Associates, [xx](#)

Novell NetWare

- running VirusScan from login script, [6](#)

Novell NetWare drives

- preserving last access dates on, [19](#), [63](#)

O

Office, Microsoft

- command to clean all macros from, [20](#), [59](#)

- files as agents for virus transmission, [xvi](#)

- omitting files from scans, [19](#), [62](#)

on-access scanning, [31](#)

- configuring, [32](#)

- restoring, [34](#), [63](#)

on-demand scanning

- definition of, [11](#)

origin of viruses, [xiii](#) to [xvi](#)

P

panic, avoiding when your system is infected, [37](#)

password-protected files, [40](#)

pausing

- when displaying VirusScan messages, [22](#), [63](#)

payload, definition of, [xiii](#)

PC viruses, origins of, [xiii](#)

PKLITE

- and VirusScan, [18](#), [61](#)

plain text, use of to transmit viruses, [xvi](#)

polymorphic viruses, definition of, [xv](#)

pranks, as virus payloads, [xiii](#)

preventing infection, [43](#)

PrimeSupport

- Anytime, options, [52](#)

- availability, [54](#)

- Basic, options, [51](#)

- Extended, options, [52](#)

- ordering, [54](#)

Professional Consulting Services

- description of, [55](#)

Q

quarantine, 39

R

RAM, virus infections in, [xiii to xiv](#)

reference, 57

reporting viruses not detected to Network Associates, [xx](#)

reports

adding names of corrupted files to, [23, 64](#)

adding names of scanned files to, [23, 64](#)

adding system errors to, [24, 65](#)

generating with VirusScan, [22 to 23, 59, 64](#)

requirements

system, 5

responses, default, when infected by viruses, [37](#)

restarting with CTRL+ALT+DEL, caution against using to clear viruses, [xiv](#)

retail customers, support features included with purchase, 54

S

Scanning disks, 28

scanning profile

to run at system startup, 26

script viruses, [xvi](#)

self-check, error level if fails, 67

signatures, use of for virus detection, [xv](#)

software updates and upgrades, website address for obtaining, 54

spreadsheet files, virus infections in, [xv to xvi](#)

stealth viruses, definition of, [xv](#)

subdirectories

scanning, [19, 65](#)

support

for retail customers, options, 54

hours of availability, 55

PrimeSupport

Anytime, 52

availability, 54

Basic, 51

Extended, 52

ordering, 54

via electronic services, 55

system crashes, attributing to viruses, 37

system files, as agents for virus transmission, [xiv](#)

system requirements, 5

T

technical support

e-mail address for, [xviii](#)

features included with retail purchase, 54

hours of availability, 55

information needed from user, [xix](#)

online, [xviii](#)

PrimeSupport

Anytime, 52

availability, 54

Basic, 51

Extended, 52

ordering, 54

via electronic services, 55

text messages, use of to transmit viruses, [xvi](#)

Total Education Services

description of, 55

Total Service Solutions

contacting, 55

training for Network Associates products, [xix, 55](#)

scheduling, [xix](#)

Trojan horse, definition of, [xiii](#)

U

updates and upgrades, website address for obtaining, [54](#)

V

validate, [46](#)

VALIDATE.EXE, use of to verify Network Associates software, [xvi](#)

validating VirusScan, [46](#)

virus

- new and unknown, [45](#)
- preventing infection, [43](#)
- updating data files, [45](#)

virus scanning

- excluding files, [18, 60](#)
- excluding the memory area, [18, 34, 61](#)
- including subdirectories, [19, 65](#)
- moving infected files, [21, 61](#)
- multiple disks, [18, 61](#)
- network drives, [17, 57](#)
- preventing users from halting, [18, 61](#)
- scanning all file types, [17, 58](#)
- skipping compressed files, [18, 61](#)
- system memory, [19, 34, 62](#)

viruses, [67](#)

- boot-sector infectors, [xiii to xiv](#)
- Brain virus, [xiii](#)
- Concept, [xv to xvi](#)
- costs of, [xi to xii](#)
- current numbers of, [xi](#)
- definition, [xii](#)
- definition of, [xi](#)
- disguising infections of, [xv](#)
- displaying list of detected, [24, 66](#)
- effects of, [xi, 37](#)
- encrypted, definition of, [xv](#)
- file infectors, [xiv](#)
- history of, [xii to xvi](#)
- locking the system if found, [21, 35, 60](#)

macro, [xv to xvi](#)

mutating, definition of, [xv](#)

origins of, [xii to xvi](#)

payload, [xiii](#)

polymorphic, definition of, [xv](#)

programs similar to

 Trojan horses, [xiii](#)

 worms, [xii](#)

removing

 from infected files, [37](#)

reporting new strains to Network Associates, [xx](#)

role of PCs in spread of, [xiii](#)

script language, [xvi](#)

spread of via e-mail and Internet, [xvi](#)

stealth, definition of, [xv](#)

use of code signatures by, [xv](#)

why worry?, [xi to xii](#)

VirusScan, [16 to 17, 58, 67](#)

command-line examples, [57](#)

command-line options, [57](#)

disabling expiration date message, [16, 62](#)

disabling sound VirusScan generates upon virus detection, [21, 61](#)

displaying a message when a virus is found, [21, 59](#)

displaying list of detected viruses, [24, 66](#)

documentation, [3](#)

error levels, [67](#)

excluding files, [18, 60](#)

excluding memory area from scans, [18, 34, 61](#)

generating a report file, [22 to 24, 59, 64 to 65](#)

installation

 as best protection against infection, [37](#)

limiting scans to files under a certain size, [18, 61](#)

locking the system, [21, 35, 60](#)

multiple disks, [18, 61](#)

preventing users from halting, [18, 61](#)

scanning only the boot sector, [17, 59](#)

setting the scan frequency, [16, 60](#)

VirusScan command-line options

/? or /HELP, 16, 34, 57, 60
 /ADL, 17, 57
 /ADN, 17, 57
 /ALERTPATH, 20, 22, 58
 /ALL, 17, 58
 /ANALYZE, 16 to 17, 58
 /ANYACCESS, 35, 59
 /APPEND, 22, 59
 /BOOT, 17, 59
 /BOOTACCESS, 35, 59
 /CLEAN, 20, 40, 59
 /CLEANDOCALL, 20, 59
 /CONTACT, 59
 /CONTACTFILE, 21, 59
 /DEL, 21, 40, 59
 /EXCLUDE, 18, 60
 /FILEACCESS, 60
 /FREQUENCY, 16, 60
 /HELP, 16, 34, 57, 60
 /IGNORE, 35, 60
 /LOAD, 16, 60
 /LOCK, 21, 35, 60
 /MANALYZE, 18, 60
 /MANY, 18, 61
 /MAXFILESIZE, 18, 61
 /MEMEXCL, 18, 34, 61
 /MOVE, 21, 40, 61
 /NOBEEP, 21, 61
 /NOBREAK, 18, 61
 /NOCOMP, 18, 61
 /NODDA, 19, 62
 /NODISK, 35, 62
 /NODOC, 19, 62
 /NOEMS, 34, 62
 /NOEXPIRE, 16, 62
 /NOMEM, 19, 34, 62
 /NOREMOVE, 34, 62
 /NOWARMBOOT, 35, 62
 /NOXMS, 62
 /ONLY, 35, 62
 /PANALYZE, 19, 63

/PAUSE, 22, 63
 /PLAD, 19, 63
 /RECONNECT, 34, 63
 /REMOVE, 34, 63
 /REPORT, 23, 64
 /RPTALL, 23, 64
 /RPTCOR, 23, 64
 /RPTERR, 24, 65
 /SAVE, 34, 65
 /SUB, 19, 65
 /UNZIP, 19, 65
 /VIRLIST, 24, 66
 /XMSDATA, 34, 66

Visual Basic, as macro virus programming language, xvi

VShield

configuring, 32
 starting, 32
 using, 31

W

warm boot, caution against using to clear viruses, xiv

website, Network Associates technical support via, 55

why worry about viruses?, xi to xii

Windows NT

administrative rights and scanning, 42
 possible error messages when scanning, 42

Windows NT File System (NTFS)

how to clean the MBR of, 41

Word files, as agents for virus transmission, xvi

worms, definition of, xii

write-protecting disks, 50

Z

Zenith PCs, self-modifying boot sectors in, 42

