

VirusScan for UNIX

User's Guide

4.0

COPYRIGHT

Copyright © 1999 Networks Associates Technology, Inc. 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 Networks Associates Technology, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

** ActiveHelp, Bomb Shelter, Building a World of Trust, CipherLink, Clean-Up, Cloaking, Compass 7, CNX, CyberCop, CyberMedia, Data Security Letter, Discover, Distributed Sniffer System, Dr Solomon's, Enterprise Secure Cast, First Aid, ForceField, Gauntlet, GMT, Hunter, ISDN Tel/Scope, LM 1, LANGuru, Leading Help Desk Technology, Magic Solutions, MagicSpy, MagicTree, Magic University, MagicWin, MagicWord, McAfee Associates, McAfee, MoneyMagic, More Power To You, Multimedia Cloaking, NetCrypto, NetRoom, NetScan, Net Shield, NetShield, Net Tools, NetOctopus, NetStalker, Network Associates, Network General, Network Uptime!, NetXRay, Nuts & Bolts, PC Medic, PCNotary, PGP, PGP (Pretty Good Privacy), PocketScope, PowerTelnet, Pretty Good Privacy, PrimeSupport, RecoverKey, RecoverKey-International, ReportMagic, RingFence, Router PM, Safe & Sound, SalesMagic, SecureCast, Service Level Manager, ServiceMagic, Site Meter, Sniffer, SniffMaster, SniffNet, Stalker, Statistical Information Retrieval (SIR), SupportMagic, T-POD, TeleSniffer, TIS, TMach, TMeg, Trusted Mach, Trusted Mail, Total Network Visibility, Total Virus Defense, Uninstaller, Virex, Virex-PC, Virus Forum, ViruScan, VirusScan, VShield, WebScan, WebShield, WebSniffer, WebStalker WebWall, and ZAC 2000* are registered trademarks of Network Associates and/or its affiliates in the US and/or other countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners.

LICENSE AGREEMENT

NOTICE TO ALL USERS: FOR THE SPECIFIC TERMS OF YOUR LICENSE TO USE THE SOFTWARE THAT THIS DOCUMENTATION DESCRIBES, 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.

Table of Contents

Preface	v
What happened?	v
Why worry?	v
Where do viruses come from?	vi
Virus prehistory	vi
Viruses and the PC revolution	vii
Where next?	x
How to protect yourself	x
How to contact Network Associates	xi
Customer service	xi
Technical support	xii
Network Associates training	xiii
Comments and feedback	xiii
Reporting new items for anti-virus data file updates	xiii
International contact information	xiv
 Chapter 1. Introducing VirusScan for UNIX	19
Welcome	19
Why use VirusScan for UNIX?	19
 Chapter 2. Installing VirusScan for UNIX	21
Before you begin	21
About the distributions	21
Installation Requirements	21
Installing VirusScan for UNIX	22
Troubleshooting	24
Testing your installation	24
Uninstalling VirusScan for UNIX	25

Chapter 3. Using VirusScan for UNIX	27
Overview	27
Syntax	27
Performing on-demand scanning	28
Preconfiguring scan operations	30
Scheduling scan operations	31
What to do if VirusScan detects a virus	33
Exit codes	34
The VirusScan program report features	35
Options tables	36
Appendix A. Preventing Virus Infection	45
Keys to a secure system environment	45
Detecting new and unidentified viruses	45
Why would I need a new .DAT file?	46
Updating your .DAT files	46
Appendix B. Network Associates Support Services	51
PrimeSupport Options for Corporate Customers	51
PrimeSupport KnowledgeCenter	51
PrimeSupport Connect	52
PrimeSupport Connect 24-By-7	52
PrimeSupport Enterprise	53
Ordering Corporate PrimeSupport	54
PrimeSupport Options for Retail Customers	56
Ordering Retail PrimeSupport	57
Network Associates Consulting and Training	58
Professional Consulting Services	58
Total Education Services	59
Index	61

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 45,000 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 small proportion 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 cost 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 "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. Some estimates have placed the total worldwide cost in time and lost productivity for merely 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 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. As further catalyst, 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 virus 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. Many Network Associates anti-virus products anticipate this possibility by allowing you to create an emergency disk you can use to boot your computer and remove infections.

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 other vendors, 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. But most existing anti-virus software easily kept pace with updates that detected and disposed 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, the 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.

Where next?

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. The chat client sends script viruses as plain text, which would ordinarily preclude them from infecting systems, 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. Anti-virus software, moreover, is only as good as its latest update. Because as many as 200 to 300 viruses and variants appear each month, the data (.DAT) files that enable Network Associates software to detect and remove viruses can get quickly outdated. If you have not updated the files that originally came with your software, you could risk infection from newly emerging viruses. Network Associates has, however, assembled the world's largest and most experienced anti-virus research staff within its Anti-Virus Emergency Response Team (A.V.E.R.T)* division. This means that the files you need to combat new viruses appear as soon as—and often before—you need them.

Most other security 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.

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.

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, 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.
McCandless Towers
3965 Freedom Circle
Santa Clara, CA 95054-1203
U.S.A.

Technical support

Network Associates is famous for its dedication to customer satisfaction. We have continued this tradition by making our site on the World Wide Web a valuable resource for answers to technical support issues. We encourage 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 anti-virus product documentation to: Network Associates, Inc., 15220 NW Greenbrier Parkway, Suite 100, Beaverton, OR 97006-5762, U.S.A. You can also send faxed comments to (503) 531-7655 or e-mail to tv_d_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 Java classes, ActiveX controls, dangerous websites, or 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 questions or virus samples to:

virus_research@nai.com

Use this address to send questions or virus samples to our North America and South America offices

vsample@nai.com

Use this address to send questions or virus samples gathered with Dr Solomon's Anti-Virus Toolkit* software to our offices in the United Kingdom

To report items to our European research offices, use these e-mail addresses:

virus_research_europe@nai.com	Use this address to send questions or virus samples to our offices in Western Europe
virus_research_de@nai.com	Use this address to send questions or virus samples gathered with Dr Solomon's Anti-Virus Toolkit software to our offices in Germany

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

virus_research_japan@nai.com	Use this address to send questions or virus samples to our offices in Japan and East Asia
virus_research_apac@nai.com	Use this address to send questions or virus samples to our offices in Australia and South East Asia

International contact information

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

Network Associates Australia

Level 1, 500 Pacific Highway
St. Leonards, NSW
Sydney, Australia 2065
Phone: 61-2-8425-4200
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

**NA Network Associates
Oy**

Sinikalliontie 9, 3rd Floor
02630 Espoo
Finland
Phone: 358 9 5270 70
Fax: 358 9 5270 7100

**Network Associates
Deutschland GmbH**

Ohmstraße 1
D-85716 Unterschleißheim
Deutschland
Phone: 49 (0)89/3707-0
Fax: 49 (0)89/3707-1199

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
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

**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 Hong Kong

19th Floor, Matheson Centre
3 Matheson Way
Causeway Bay
Hong Kong 63225
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 0780

**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
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
International B.V.**

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

**Network Associates
Portugal**

Av. da Liberdade, 114
1269-046 Lisboa
Portugal
Phone: 351 1 340 4543
Fax: 351 1 340 4575

**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**

78 Shenton Way
#29-02
Singapore 079120
Phone: 65-222-7555
Fax: 65-220-7255

**Network Associates
Spain**

Orense 4, 4ª Planta.
Edificio Trieste
28020 Madrid
Spain
Phone: 34 91 598 18 00
Fax: 34 91 556 14 04

**Network Associates
Sweden**

Datavägen 3A
Box 596
S-175 26 Järfälla
Sweden
Phone: 46 (0) 8 580 88 400
Fax: 46 (0) 8 580 88 405

**Network Associates
AG**

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

**Network Associates
Taiwan**

Suite 6, 11F, No. 188, Sec. 5
Nan King E. Rd.
Taipei, Taiwan, Republic of China
Phone: 886-2-27-474-8800
Fax: 886-2-27-635-5864

**Network Associates
International Ltd.**

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

Introducing VirusScan for UNIX

1

Welcome

Thank you for purchasing VirusScan for UNIX* — the Network Associates virus detection and removal solution for UNIX-based systems.

Network Associates anti-virus researchers provide fast, responsive coverage for new viruses and other malicious software. New-generation VirusScan for UNIX scanning technology has the ability to detect and remove more than 42,000 known boot, file, macro, multi-partite, stealth, encrypted, and polymorphic viruses.

A pre-eminent, worldwide staff made up of the former McAfee Associates and Dr Solomon's Software teams develops and backs each new scan engine update and virus definition file release.

Network Associates worldwide virus research team develops weekly updates for the VirusScan virus definition files, leaving you confident that your network is well protected from attack.

Why use VirusScan for UNIX?

The UNIX operating system is a secure environment, relatively unaffected by computer viruses. The DOS and Windows world, however, is different. DOS computers have no security and are very susceptible to virus infections. Since DOS system viruses don't affect UNIX systems, you might be asking: "Why should I be concerned?"

One reason for concern is that DOS- and Windows-based computers are a rapidly expanding presence on the Internet — and most of these computers use the Internet for file transfer. A UNIX server may still harbor DOS system viruses and, while not itself affected, pass them on to numerous DOS- and Windows-based clients. Rather than trying to block viruses at each DOS- and Windows-based computer connected to a UNIX system, you can install the VirusScan for UNIX software and use it as an efficient centralized solution. In order to protect yourself and your users, it is more important than ever to maintain anti-virus security.

VirusScan software provides the best available anti-virus security, but is only one important element of a comprehensive security program that includes a variety of safety measures such as regular backups, meaningful password protection, and training and awareness programs about virus issues.

Before you begin

Network Associates distributes the VirusScan for UNIX software in two ways: as an archived file that you can download from the Network Associates website or from other electronic services; and on CD-ROM disk. Once you have downloaded a VirusScan software archive or placed your VirusScan software installation disk in your CD-ROM drive, the installation steps you follow after that are the same for each type of distribution. Review the system requirements shown below to verify that the VirusScan software will run on your system, then follow the installation steps on

About the distributions

The VirusScan for UNIX program comes in five distribution versions, one for each supported operating system. If you install the VirusScan program from CD-ROM, you will find each version is in its own directory. Each distribution also includes its own installation script.

- Solaris SPARC 2.5.1 or later
- HP-UX version 10.20 or later
- AIX 4.2.1 or later
- Linux 2.x kernels
- SCO OpenServer release 5

Installation Requirements

To install and run VirusScan for UNIX, you need:

- 4MB of free hard disk space for a full installation.
- A CD-ROM drive. If you downloaded the VirusScan software from the Network Associates FTP site, this is an optional item.

Other recommendations

To take full advantage of the regular .DAT file updates that Network Associates offers from its FTP site, you should have an Internet connection, either through your local area network, or via a high speed modem and an Internet service provider.

- ❏ **NOTE:** Network Associates does **not** provide Internet connections. Contact a local service provider to learn about rates and terms of service, or see your system administrator to learn about connecting to the Internet through your office network.
-

Installing VirusScan for UNIX

The following example installs the VirusScan for Solaris distribution. To install other versions, substitute the correct filename where the example specifies `vsun4031.tar.Z`.

To start a VirusScan software installation script, follow these steps:

1. Create a directory on your hard disk where you want to install the VirusScan program.

To do so, you must have Write and Execute permissions on the target computer.

- ❏ **NOTE:** Installing to a directory is optional. If you do not specify a directory, the installation script copies the VirusScan program to `/usr/local/bin`. If the installation directory that you specify does not exist, you must create it.
-

2. Copy the file `vsun4031.tar.Z` to a directory on your system.

- ❏ **NOTE:** Network Associates recommends that you do not copy this file to the directory in which you plan to install the VirusScan program.
-

3. Type this line at the command prompt:

```
uncompress vsun4031.tar.Z
```

This decompresses the file to your hard disk.

4. Type:

```
tar -xf vsun4031.tar
```

This extracts the VirusScan for UNIX program files.

5. Type this line at the command prompt to execute the installation script:

```
./install-uvscan
```

or to install the VirusScan program to a directory you've created, type this line:

```
./install-uvscan <dir>
```

Here <dir> represents the path to your target directory.

6. Press the RETURN or ENTER key on your keyboard to start the installation.

The installation script asks you whether you want to place a link to uvscan in the directory /usr/local/bin.

7. Type **y** to create the link or type **n** to skip this step.

Network Associates recommends that you include the link in your search path.

The installation script asks you whether you want to place a link to libsufv.so in the directory /usr/local/lib.

8. Type **y** to create the link or type **n** to skip this step.

Network Associates recommends that you create this link or you will need to set these environment variables:

- LD_LIBRARY_PATH for the Solaris 2.x distribution or the SCO OpenServer Release 5 distribution; or
- SHLIB_PATH for the HP-UX distribution.

☐ **NOTE:** The VirusScan for UNIX program also looks in the /usr/lib or /lib directory or the current directory for the shared library.

9. The installation program copies the VirusScan files to your hard disk, then scans your default home directory.

If the installation does not complete correctly, see the [“Troubleshooting”](#) section below to learn which errors can occur and to see suggested courses of action that you can take.

Troubleshooting

The table below lists the error messages most likely to occur after an unsuccessful installation together with their likely cause and any recommended solutions.

Error	Cause or action
Failed to create install_dir	Verify that you have permission to create install_dir
Cannot write to install_dir	Verify that you have permission to create install_dir
The install_dir exists, but is not a subdirectory	Choose another installation directory
<file> is missing	The file might not exist.


Testing your installation

Once installed, the VirusScan program is ready to scan your system for infected files. You can test whether the program has installed correctly and verify that it can properly scan for viruses by implementing a test developed by Eicar, a coalition of anti-virus vendors headquartered in Europe, as a method for their customers to test any anti-virus software installation.


To test your installation, follow these steps:

1. Open a standard text editor, then type the following line:

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

 **NOTE:** The line shown above should appear as *one line* in your text editor window. If you are reading this manual on your computer, you can copy the line directly from the Adobe Acrobat .pdf file to your text editor by choosing **Select Text** from the **Tools** menu in Acrobat.

2. Save the file with the name EICAR.COM. The file size will be 69 or 70 bytes.
3. Start the VirusScan program and allow it to scan the directory that contains EICAR.COM. When VirusScan examines this file, it will report finding the Eicar test file, but you will not be able to clean or repair it.


 **IMPORTANT:** The Eicar test file *does not contain a virus*—it cannot spread or infect other files, or otherwise harm your system. Delete the file when you have finished testing your installation to avoid alarming other users.

Uninstalling VirusScan for UNIX

To remove the VirusScan program from your system quickly, you can:

- Run the uninstallation script which you'll find in the VirusScan program directory; or
- Delete the VirusScan program files from the command line.

You will not be able to uninstall the VirusScan program unless you have the necessary permissions to do so. Administrators should take precautions to ensure that users cannot accidentally uninstall their VirusScan software.

 **IMPORTANT:** Uninstalling the VirusScan for UNIX program leaves your computer defenseless against virus attack. Uninstall the product only when you are sure that you can upgrade quickly to a new version.

To run the uninstall script:

1. Type this line at the command prompt:

```
./uninstall-uvscan
```

The uninstall script is installed when the VirusScan program is installed and enables you to uninstall the product quickly and easily.

2. If you created your own links during the installation process, you will need to remove those yourself.
3. When the VirusScan software has been removed, you must manually delete the uninstall script to remove the program completely from your system.

To delete VirusScan program files:

1. Go to the directory where you installed the VirusScan program.
2. To remove each file in the directory, type on the command line:

```
rm <filename>
```

3. If you created your own links during the installation process, you must also remove them separately.

Overview

The VirusScan for UNIX program is a command-line driven software package designed to offer sophisticated virus scanning without sacrificing flexibility. In this chapter, you will learn how to use its powerful features and functions, and customize the program to meet your specific needs.

The following VirusScan features offer optimum protection for you and your network:

- Powerful on-demand scan modules let you start a scan operation immediately or schedule automatic scan operations to suit your work flow.
- Advanced heuristic scanning technology detects previously unidentified or unclassified macro and program viruses.
- Virus definition file updates and program component upgrades can ensure that the VirusScan software has up-to-the-minute scanning technology to deal with viruses as they emerge from the field.


Later sections in this guide describe each of these features in detail.

Syntax

A summary of the command line and its associated options appears on [page 28](#). A full description of each command appears in the “[Options tables](#)” later in this guide.

-
- ❏ **NOTE:** Some of the options in the syntax summary consists of a verbose form and an abbreviated form. The abbreviated form appears first, then the verbose form appears after the | symbol. You may use either form to add an option to the command line
-

```
uvscan [--analyze,--analyse] [-c |--clean] [--cleandocall]
[--config file] [--dam] [-d |--data-directory directory]
[--exclude file] [-e |--exit-on-error] [--extra file]
[--extensions EXT1,[EXT2]] [--fam] [-f |--file file]
[-h |--help] [--ignore-compressed] [--ignore-links]
[--load file] [--manalyze,--manalyse,--macro-heuristics]
[--maxfilesize X] [-m |--move directory] [--noboot]
[--nodecrypt] [--nodoc] [--noexpire] [--one-file-system]
[-p|--atime-preserve] [-r |--recursive,--sub] [--secure]
[-s |--selected][--summary][--unzip][-v|--verbose]
[--version] [--virus-list] {file / directory}
```

 **NOTE:** Do not type the square brackets [] or the | symbol when you type your options in the command line.

Performing on-demand scanning

You can scan any drive, directory, or file on your computer or network from the command line by adding one or a combination of options to the basic commands.

The VirusScan program includes three groups of options:

- **Scanning and targeting options.** These options govern how and where the VirusScan program looks for infected files.
- **Response options.** These options tell the VirusScan program how to respond to any infected files it detects.
- **General options.** These options tell the VirusScan program to report its scanning activities.

Each group of options appears in its own table with a full description of its function. See [“Options tables” on page 36](#) for details.

Command line conventions

Use these conventions to add options to the command line:

- Type each option in lower case and separate each with spaces.
- Do not use any option more than once on the command line.
- Follow the syntax correctly. The UNIX operating system is case-sensitive.

- Type single consecutive switches as one switch for your convenience. For example, instead of:

```
-c -r --one-file-system,
```

you can type:

```
-cr --one-file-system
```

To start the VirusScan for UNIX program and run a basic scan operation:

To target a specific file, directory, or text list of file names follow your list of options with the name of the file that you want the VirusScan program to examine, or the directory that contains files you want scanned.

1. To start running the VirusScan software, at the UNIX command prompts, type:

```
uvscan
```

By default, the VirusScan software will look for viruses in an entire directory tree. To have it examine a specific file or list of files, add the target files to the command line. You may also create a text file that lists your target files, then simply add the name of the text file to the command line.

-
- ❑ **NOTE:** By default, the VirusScan software examines all files, no matter what their extensions. You may limit your scan operation by adding only those extensions you want to examine to the command line after the `--extensions` option, or you may exclude certain files from scan operations with the `--exclude` option. See [“Options tables” on page 36](#) for details
-

General Hints and Tips:

To display a list of commonly used options, each with a short description of their features, type:

```
uvscan --help
```

To display a list of all the viruses that VirusScan detects, type:

```
uvscan --virus-list
```

To ensure your VirusScan software gives you maximum protection from virus attack, you must regularly update your .DAT files. See [Appendix A, “Preventing Virus Infection”](#) for details.

To display information about the version of the VirusScan software, type:

```
uvscan --version
```

Preconfiguring scan operations

Instead of running each scan operation with all of its attendant options directly from the command line, you can configure a scan operation with the options you choose, then save it in a text file as a scan task.

That way, you can run complete scan operations with ease, and at any time.

The scan task can specify targets for the VirusScan program to examine and the actions it should take when it detects a virus.

To preconfigure a scan operation:

1. Choose the command options you want to use.

See [“Options tables” on page 36](#) for a description of available options.

2. Type the command options into a text editor just as you would on the command line.
3. Save your text in a file. You may name the file any way you wish.
4. Start the VirusScan for UNIX program, then type either of these lines at the command prompt.

```
uvscan --load <file> OR uvscan --config <file>
```

Here <file> is the name of the text file you created.

5. Press the RETURN or ENTER key on your keyboard to run the scan operation.

If the VirusScan program does not find a virus, it displays no output.

❑ **NOTE:** To learn how to specify the options you want to use, see [“Command line conventions” on page 28](#).

2. To append a new entry to the named file and specify what type of scan operation you want to perform, type:

```
echo "<minute> <hour> <day> <month> <day of the week>  
uvscan --options" >> <file>
```

where 'minute | hour | day' and so on indicates the time and date that you want to perform the scan operation, according to the guidelines given earlier in this section.

The double quotes must be typed as you see them in the example but do not type the angled brackets.

3. Then, to resubmit all the jobs to cron, type:

```
crontab <file>
```

Cron will carry out the scan automatically as instructed by the command line.

If a crontab file does not already exist, the message "can't open your crontab file" appears. To set up a new crontab file, ignore step 1 above, create a text file, and then continue with step 2.

For more detailed information on how to set up a crontab file, see the UNIX man page for crontab. Type this line at the command prompt:

```
man crontab
```

To schedule a scan operation for a specific date and at a specific time:

1. Type this line at the command prompt:

```
crontab -l > <file>
```

Here <file> is the name of the text file that lists your crontab entries.

2. Specify the type of scan operation you want to perform. To do so, type this line at the command prompt:

```
echo '0 0 13 10 * uvscan --selected' >> <file>
```

3. Then, to run the scan, type:

```
crontab <file>
```


What to do if VirusScan detects a virus

If the VirusScan program discovers a virus, it generates an exit code when it finishes the scan operation. See [“Exit codes” on page 34](#) for a full description of each code.

To clean infected files or directories, or move them to a “clean” area of your network, run your scan operations with one or more of these options:

- `-c | --clean`

This option tells the VirusScan program to try automatically to remove any viruses from infected files. Network Associates recommends you perform another scan operation after using this option to ensure that the program cannot detect any virus remnants in files it has cleaned.

This option tells the VirusScan program to remove all macros from any file that the program’s heuristic scanning has identified as potentially infected.

- `-m <directory> | --move <directory>`

The VirusScan program moves any infected files it detects to a quarantine directory that you specify.

- `--delete`

The VirusScan program deletes any infected files it finds automatically.

Detailed descriptions of these options appear in the [“Response options” table on page 41](#).

The following scenarios list some of the ways in which you can use these options to respond to a virus attack. They assume that the `uvscan` executable is available in your search path.

Scenario No. 1

To tell the VirusScan program to scan and clean all files in the `/usr/dos` directory and all of its subdirectories, type:

```
uvscan -cr /usr/dos
```

The VirusScan program scans `/usr/dos` and its subdirectories automatically, and cleans any infected files it encounters.

Scenario No. 2

To tell the VirusScan program to scan and clean all files in `/usr/dos` and its subdirectories, but to ignore any other file systems that are mounted as volumes, type:

```
uvscan -cr --one-file-system /usr/dos
```

The VirusScan program scans /usr/dos and its subdirectories automatically without moving across file systems. It cleans any infected files it encounters.

Scenario No. 3

To tell the VirusScan program to scan all files, except compressed files, in /usr/dos and its subdirectories and to move any infected files to /usr/local/viruses, type:

```
uvscan -m /usr/local/viruses -r --ignore-compressed
--exit-on-error /usr/dos
```

The VirusScan program scans /usr/dos and its subdirectories automatically. It ignores any compressed files. It moves any viruses it encounters to /usr/local/viruses. If it encounters any errors, it automatically exits.

Exit codes

The VirusScan program returns an informational code when it exits. These codes identify any viruses or problems that are found during a scan operation.

Exit code description

0	The VirusScan program found no viruses and returned no errors.
2	Driver integrity check failed.
6	A general problem occurred.
8	Could not find a driver.
13	One or more viruses or hostile objects were found.
15	The VirusScan program self-check failed; it may be infected or damaged.
102	User quit using the --exit-on-error option.

Exit code 102 occurs when the scan operation encounters an unexpected condition; for example, if it can't get access to a file or runs out of available memory. On these occasions, the program exits immediately and does not finish the scan operation. Exit code 102 occurs only if you specified the --exit-on-error option when you started the VirusScan program. If you did not specify this option, Exit Code 6 is returned.

The VirusScan program report features

The VirusScan program may take some time to complete a scan operation, particularly if it scans a lot of drives, directories and files. It will, however, keep you informed of its progress and any viruses it finds together with the actions it took to respond to them.

The VirusScan program will display this information on your screen provided that you add the `--summary` or `--verbose` options to the command line. To learn more about each option, see [“Response options” on page 41](#).

A sample of the VirusScan report information appears below where both the `--summary` and `--verbose` options have been used to perform a scan operation on files located in the `/usr/data` directory.

The `--verbose` option tells you which files the VirusScan program is examining. When the scan operation finishes, the `--summary` option identifies how many files the program scanned, how many files it cleaned, how many files it did not scan, and how many infected files it found.

```
$ uvscan --summary -v .
Scanning /usr/data/*
Scanning file /usr/data/command.com
Scanning file /usr/data/grep.com
Summary report on /usr/data/*
File(s)
      Total files: ..... 2
      Clean: ..... 2
      Not scanned: ..... 0
      Possibly Infected: ..... 0
```

Options tables

The following tables describe the options you can use to target your scan operations.

The descriptions use these conventions to identify the options or required variables:

- Short versions of each command line appear after a single dash (-).
- Long versions of each command option, if any, appear after two dashes (--).
- Variables, such as filenames or paths, appear in *italic* within brackets < >.

To learn how to add these options to the command line, see [“Command line conventions”](#) on [page 28](#).

Scanning options

Scanning options describe how and where each scan operation will look for infected files.

You may use a combination of these options to shape the scan operation to suit your needs. If the UVSCAN default column entry for that options is “on”, the option automatically runs without your needing to add it to the command line. You may override some of these default options with other options.

Option	Description	UVSCAN default
--analyze, --analyse	This option tells uvscan to use heuristics to look for possible viruses in “clean” files. This step would occur after the software has checked for other viruses.	Off
--config <file>, --load <file>	This option causes uvscan to run these options specified in <file>. You may not nest configuration files within other configuration files.	Off
-d <directory>, --dat <directory> --data-directory <directory>,	This option tells uvscan where to find scan.dat, names.dat, and clean.dat.	If uvscan cannot find these data files, the program issues exit code 6.

Option	Description	UVSCAN default
--exclude <file>	This option excludes the files you specify within <file> from the scan operation.	Off
-e, --exit-on-error	This option tells uvscan to quit and display an error message if it encounters an error. The error message indicates the severity of the error. See page 34 for an explanation of exit codes.	Off
--extensions <EXT1,EXT2>	This option directs uvscan to examine these files that have the extension that you specify. You can specify as many extensions as you wish, provided you separate each with a comma, but without a space.	Off
--fam	This option tells uvscan to locate all files that have macros. Use this option with caution if you use it in conjunction with the “ --cleandocall , --dam ” options.	Off
-f <file>, --file <file>	This option tells uvscan to scan the files you specify within <file>. Save your list of target files as a text file and specify its path in the command line.	Off

Option	Description	UVSCAN default
--ignore-compressed, --nocomp	This option tells uvscan to ignore compressed files. By default, the program scans files saved in these compression formats: ICE, LZEXE, PKLITE, Cryptcom, COM2EXE, Diet, Teledisk, Microsoft Expand and GZIP. This option reduces the time it takes to complete a scan, but also reduces file security.	By default, VirusScan scans compressed files.
--ignore-links	This option tells uvscan not to resolve any symbolic links it finds and not to scan the link targets.	Off
--manalyze, --manalyse --macro-heuristics	This option tells uvscan to use heuristic detection to identify potential macro viruses. This is a subset of "--analyze, --analyse" .	Off
--maxfilesize X	This option tells uvscan to examine only those files smaller than X size. Here, X is a file size measured in megabytes.	Off
--noboot	This option tells uvscan to turn off boot sector scanning on startup.	Off
--nodecrypt	This option tells uvscan not to decrypt encrypted files in order to scan them.	Off
--noexpire	This option tells uvscan not to warn you your .DAT files are out of date.	Off
--nodoc	This option tells uvscan not examine .DOC files.	Off

Option	Description	UVSCAN default
--one-file-system	<p>This option allows you to scan an entire directory tree without scanning attached file systems, if you use it in conjunction with the “-r, --recursive, -sub” option.</p> <p>Use this option to prevent uvscan from scanning attached file systems.</p>	Off. Normally, VirusScan treats a mount point as a subdirectory and scans that file system.
--panalyze, --panalyse	<p>This option tells uvscan to use heuristic detection to identify potential program viruses. This is a subset of “--analyze, --analyse”.</p>	Off
-p, --atime-preserve, --plad	<p>This option tells uvscan to reset the time that the file was last accessed to what it was before the scan operation started. This enables you to correctly schedule file backups and their operations keyed to this value. If uvscan finds a virus in, or removes a virus from, a file or, if the person who starts the scan operation does not own the file, the program will not reset the access time.</p>	Off
-r, --recursive, -sub	<p>This option tells uvscan to examine any target directories you specify and all of its subdirectories.</p>	Off

Option	Description	UVSCAN default
--secure	This option activates the --analyze and --unzip options and deactivates the --selected and --extensions options at the same time. Use this option to tell uvscan to examine all files.	Off
-s, --selected	<p>This option tells uvscan to look for viruses for any file that has execute permissions and all files that have any of these extensions:</p> <p>.EXE, .COM, .BAT, .SMM, .DOT, .BIN, .APP, .CMD, .OVL, .DLL, .DEV, .001, .002, .QLB, .XTP, .XLB, .SCR, .SYS, .OLE, .VXD, .386, .HTM, .INI, .VBS, .MD?, .BO?, .IM?, .MB?, .OV?, .XL?, .DO?.</p> <p>VirusScan scans only those files susceptible to virus infection. Because VirusScan scans a smaller set of files, it can scan a target directory faster.</p>	On
--unzip	This option tells uvscan to examine files saved in .zip , LHA, PKarc, ARJ, TAR and RAR formats.	Off

Response options

These options determine how your scan operation responds to a virus infection. You may use a combination of these options

You may use a combination of these options to shape the scan operation to suit your needs. If the UVSCAN default column entry for that options is “on”, the option automatically runs without your needing to add it to the command line. You may override some of these default options with other options.

Option	Description	UVSCAN default
-c, --clean	This option tells uvscan to try automatically to remove any viruses from infected files. If the program cannot close, it displays a warning message. If you use this option, you should run another scan operation to ensure that the program cannot detect any virus remnants in files it has cleaned.	Off
--cleandocall, --dam	The scan operation will delete all macros in infected files that have them. Use these options with caution if you use them in conjunction with the “--fam” option.	Off

Option	Description	UVSCAN default
--delete	This option tells uvscan to automatically delete any infected files that it finds.	Off
-m <directory>, --move <directory>	<p>This option tells uvscan to move any infected files it finds to a quarantine directory that you specify.</p> <p>When the program moves an infected file, it replicates the full directory path for the infected file inside the quarantine directory so that you can determine the infected file's original location.</p>	Off

General options

These options give you additional information that you can use as you run your scan operations or get further help

You may use a combination of these options to shape the scan operation to suit your needs. If the UVSCAN default column entry for that options is “on”, the option automatically runs without your needing to add it to the command line. You may override some of these default options with other options.

Option	Description	UVSCAN default
-h, --help	This option lists all of the uvscan options available, together with a short description. To get help on specific UNIX commands and functions, type <code>man</code> on the command line.	Off
--summary	This option summarizes the results of your scan operation. The summary includes: <ul style="list-style-type: none"> • How many files uvscan examined. • How many infected files uvscan found. • How many viruses uvscan removed from infected files. 	Off
-v, --verbose	This option tells uvscan to display a progress summary as it conducts a scan operation.	Off

Keys to a secure system environment

VirusScan anti-virus software is an effective tool for preventing virus infections, but it is most effective when used in conjunction with a comprehensive computing security program that includes a variety of safety measures, such as regular backups, meaningful password protection, user training, and awareness of virus threats.

To create a secure system environment and minimize your chance of infection, Network Associates recommends that you:

- Install VirusScan software and other Network Associates anti-virus software.
- Include the uvscan command line and all appropriate options in a cron file.
- Make frequent backups of important files. Even if you have VirusScan software available to prevent attacks from viruses, damage from fire, theft, or vandalism can render data unrecoverable without a recent backup.

Detecting new and unidentified viruses

The best way for you to deal with new or unidentified viruses that might affect your system is to update your VirusScan virus signature (.DAT) files.

To offer the best virus protection possible, Network Associates continually updates the .DAT files that VirusScan uses to detect viruses. For maximum protection, you should update these files on a regular basis.

-
- ❏ **NOTE:** The term “update” refers only to the .DAT files; the term “upgrade” refers to product version revisions, executables, and definition files. Network Associates offers free online .DAT file updates for the life of your product but cannot guarantee their backward compatibility with previous versions’ executable files. By upgrading your software to the latest product version and updating regularly to the latest .DAT files, you ensure complete virus protection for the term of your software subscription or maintenance plan
-

Why would I need a new .DAT file?

More than 200 new viruses appear each month. Often, older .DAT files cannot assist the VirusScan software in detecting these new variations. For example, the .DAT files that came with your copy of VirusScan, may not detect a virus that was discovered after you bought the product.

If you suspect you may have found a new virus, see [“Reporting new items for anti-virus data file updates” on page xiii](#) for instructions on contacting Network Associates.

Updating your .DAT files

Download the new files from either of these sources:

- **The Network Associates FTP server.** Open a connection to ftp.nai.com.
Use `anonymous` as your user name and your e-mail address as your password to gain access. Look for VirusScan .DAT files in the directory `pub/antivirus/datfiles/4.x`.
- **The Network Associates Web Site.** Start your browser, then go to `http://www.nai.com/download` to download the latest data files.

Next, follow these steps to unpack the update and use the new .DAT files:

1. Create a download directory.
2. Change to the download directory and download the new .DAT file from the source you have chosen.

The number given to the .DAT file will change on a regular basis. A higher number indicates a later version of the .DAT file.

3. To unpack the .DAT file, type:

```
tar -xf <file>
```

Here `<file>` is the name of the file you downloaded.

4. Type this line at the command prompt to move the .DAT files to the directory where your software is installed:

```
mv *.dat /usr/local/uvscan
```

Your system overwrites the old .DAT files with the new files.

 **IMPORTANT:** The name given to the file must be in lower case.

Your software will now use the new .DAT files to scan for viruses.

Update script example

To follow is an example of an update script to update your .DAT files from the Network Associates FTP site.

This entry must appear in the .netrc file for this script to work:

```
machine ftp.nai.com
login anonymous
password <e-mail address>
macdef init
cd pub/antivirus/datfiles/4.x
bin
prompt
mget dat-*.tar
close
bye
```

where *<e-mail address>* is the address of the user who is logging in to the FTP server

```
#!/bin/sh

# Assume uvscan is installed in the same directory as
# this script.
install_directory=`dirname $0`

# Create a download directory
mkdir /tmp/dat-updates
cd /tmp/dat-updates

# Get the version of the currently installed dats from the info
# given by the --version switch
current_version=`
    $install_directory/uvscan --version |
    grep "Virus data file" |
    awk '{ print substr($4,2,4) }'`

# Get the new dats.
```

```
# The entry in your .netrc file should take care of the
# downloading.
ftp ftp.nai.com

# Get the version of the new dats from the filename.
new_version=`echo dat-*.tar | awk '{ print substr($1,5,4) }'`

# If they are the same age or older than the current ones,
# don't install them
if [ "$current_version" -ge "$new_version" ]
then
    echo "No new dats available at this time"
    echo "Currently installed version:  $current_version"
    echo "Version on FTP site:          $new_version"
else
    tar -xf dat-*.tar

    # Move them to the install directory, making sure the
    # filename is lower case.
    for file in `tar -tf dat-*.tar`
    do
        newfile=`echo $file | tr [A-Z] [a-z]`
        mv ./ $file "$install_directory/$newfile"
    done

    # Get the current version again and make sure the new dats
    # installed correctly.
    current_version=`
        $install_directory/uvscan --version |
        grep "Virus data file" |
        awk '{ print substr($4,2,4) }'`

    if [ ! "$current_version" -eq "$new_version" ]
    then
        echo "Dat file updates did not work correctly."
        echo "Please try manually."
    fi
fi
```



```
fi
# Delete the directory that you created.
cd /
rm -fr /tmp/dat-updates
```


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 four levels of extended support under the Network Associates Corporate PrimeSupport program. If you purchased a retail version of a Network Associates product, you can choose a plan geared toward your needs from the Retail PrimeSupport program.

PrimeSupport Options for Corporate Customers

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

PrimeSupport KnowledgeCenter

PrimeSupport KnowledgeCenter gives you access to technical support assistance via a Network Associates online knowledge base, in addition to product upgrades via the Network Associates website. If you purchased your Network Associates product with a subscription license, you receive PrimeSupport KnowledgeCenter as part of the package for either one or two years from your date of purchase, depending on the length of your subscription. If you purchased your Network Associates product with a one-year license, you can renew your PrimeSupport KnowledgeCenter plan for an annual fee.

To receive your KnowledgeCenter password or to register your PrimeSupport agreement with Network Associates, visit:

<http://knowledge.nai.com/>

Your completed form will go to the Network Associates Customer Care Center. You must complete this form before you connect to the PrimeSupport KnowledgeCenter or before you call Network Associates PrimeSupport.

PrimeSupport KnowledgeCenter features:

- Online access to technical solutions from a searchable knowledge base, electronic incident submission, and technical documents such as user's guides, FAQs, and release notes
- Unrestricted, 24-hour-per-day access to Network Associates technical support information via the Network Associates website
- Updates to data files and product upgrades via the Network Associates website

PrimeSupport Connect

PrimeSupport Connect gives you telephone access to essential product assistance from experienced Network Associates technical support staff members.

PrimeSupport Connect features:

- Unlimited toll-free telephone access to technical support from Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time
- Online access to technical solutions from a searchable knowledge base, electronic incident submission, and technical documents such as user's guides, FAQs, and release notes
- Unrestricted, 24-hour-per-day access to Network Associates technical support information via the Network Associates website
- Updates to data files and product upgrades via the Network Associates website

PrimeSupport Connect 24-By-7

PrimeSupport Connect 24-By-7 gives you round-the-clock telephone access to essential product assistance from experienced Network Associates technical support staff members. You can purchase PrimeSupport Connect 24-By-7 on an annual basis when you purchase a Network Associates product, either with a subscription license or a one-year license.

PrimeSupport Connect 24-By-7 features:

- Unlimited toll-free telephone access to technical support from Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time
- Priority call handling during business hours
- After-hours responses for urgent issues within one hour, including weekends and local holidays
- Online access to technical solutions from a searchable knowledge base, electronic incident submission, and technical documents such as user's guides, FAQs, and release notes
- Unrestricted, 24-hour-per-day access to Network Associates technical support information via the Network Associates website
- Updates to data files and product upgrades via the Network Associates website

PrimeSupport Enterprise

PrimeSupport Enterprise gives you round-the-clock, 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 Enterprise representative can help to prevent problems before they occur. If, however, an emergency arises, PrimeSupport Enterprise gives you a committed response time that assures you that help is on the way. You may purchase PrimeSupport Enterprise on an annual basis when you purchase a Network Associates product either with a subscription license or a one-year license.

PrimeSupport Enterprise features:

- Unlimited, toll-free telephone access to an assigned technical support engineer on a 24-hour-per-day, seven-day-per-week basis, including on weekends and local holidays
- Proactive support contacts via telephone or e-mail from your assigned support engineer, at an interval you designate
- Committed response times from your support engineer, who will respond to pages within half an hour, to voice mail within one hour, and to e-mail within four hours

- Ability to designate at least five people in your organization as customer contacts
- The option to be a beta site for new Network Associates products
- Online access to technical solutions from a searchable knowledge base, electronic incident submission, and technical documents such as user's guides, FAQs, and release notes
- Unrestricted, 24-hour-per-day access to Network Associates technical support information via the Network Associates website
- Updates to data files and product upgrades via the Network Associates website

Ordering Corporate PrimeSupport

To order PrimeSupport KnowledgeCenter, PrimeSupport Connect, PrimeSupport Connect 24-By-7, or PrimeSupport Enterprise for your Network Associates products:

- Contact your sales representative; or
- In North America, call Network Associates Support Services at (800) 988-5737 or (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.

Table B-1. Corporate PrimeSupport at a Glance

Feature	Knowledge Center	Connect	Connect 24-By-7	Enterprise
Technical support via website	Yes	Yes	Yes	Yes
Software updates	Yes	Yes	Yes	Yes
Technical support via telephone	—	Monday–Friday 8:00 am–8:00 pm Central Time	Monday–Friday 8:00 am–8:00 pm Central Time After-hours emergency response	24-hour-per-day access to your assigned support engineer (24 hours per day, 7 days per week)
Priority call handling	—	—	Yes	Yes
After hours support	—	—	Yes	Yes
Assigned support engineer	—	—	—	Yes
Proactive support contact	—	—	—	Yes
Designated customer contacts	—	—	—	At least 5
Committed response time	—	—	Within 1 hour for urgent issues	After hours pager: 30 minutes Voicemail: 1 hour E-mail: 4 hours

PrimeSupport Options 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 the chapter or appendix about software updating in your anti-virus software *User's Guide* 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 the chapter or appendix about software updating in your anti-virus software *User's Guide* 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 using your web browser to visit:

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

- Free 24-hour-per-day, seven-days-per-week access to online or electronic support through the Network Associates voice and fax system, the Network Associates 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) 346-3414
 - Network Associates website: <http://support.nai.com>
 - CompuServe: GO NAI
 - America Online: keyword MCAFEE
- Free access to the PrimeSupport KnowledgeBase: online access to technical solutions from a searchable knowledge base, electronic incident submission, and technical documents such as user's guides, FAQs, and release notes. Visit the KnowledgeBase at:

<http://knowledge.nai.com>

- 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.

You can also take advantage of a variety of additional support options geared toward your needs. You can purchase these options either with your Network Associates product or after your complimentary 90-day support period expires:

- **Small Office/Home Office Annual Plan.** This plan gives you unlimited toll-free access to technical support during regular business hours, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time.
- **Pay-Per-Minute Plan.** This plan gives you support only when you need it: 900-number access to technical support features priority call handling to minimize your hold time and the first two minutes of support free.
- **Online Upgrades Plan.** This plan gives you the convenience of automatic access to product upgrades via Network Associates online or electronic services.
- **Quarterly Disk/CD Plan.** This plan gives you automatic quarterly delivery of upgrade disks or CDs if you cannot access product upgrades online. This service is available for VirusScan and NetShield only.

Ordering Retail PrimeSupport

To order the PrimeSupport Small Office/Home Office Annual Plan, Pay-Per-Minute Plan, Online Upgrades Plan, or Quarterly Disk/CD Plan for your Network Associates products:

- In North America, call Network Associates Customer Care at (972) 278-6100; or
- Visit the Network Associates website at:

http://www.nai.com/services/support/add_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 Global Professional 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.

Jumpstart Services

You can take advantage of a variety of Jumpstart Services to help you implement your new Network Associates product:

- **Basic and Advanced.** This service installs, configures, and optimizes your new Network Associates product, and gives basic operational product knowledge to your team.
- **Selfstart.** This service helps prepare you to perform your new product implementation on your own and, in some cases, installs the product.
- **Proposal Development.** This service evaluates processes and procedures as well as hardware and software requirements prior to a new product implementation, enabling a consultant to prepare your custom proposal.

Network Consulting

Network Associates consultants provide expertise in protocol analysis and a vendor-independent perspective that creates unbiased solutions for troubleshooting and optimizing your network. Also, their broad understanding of network management best practices and industry relationships speeds escalation of problems through vendor support.

You can order a custom consultation to help with planning, design, implementation, and ongoing management of your network. With it, you can assess the impact of rolling out new applications, network operating systems, or internetworking devices.

Contact Network Associates Consulting Services at 1-800-395-3151 to learn more about the options available, or visit the Network Associates website at:

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

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 offer 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.

Contact your sales representative to learn more about these programs, or call Network Associates Total Education Services at 1-800-395-3151. You can also visit the Network Associates website at:

<http://www.nai.com/services/education/>

Index

Symbols

.DAT file updates, [45](#)

A

America Online

technical support via, [xii](#)

America Online, technical support via, [56](#)

anti-virus software

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

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

automatic scan operations, [31](#)

B

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

boot-sector viruses, definition and behavior
of, [vii](#) to [viii](#)

"Brain" virus, [vii](#)

C

cleaning infected files, [41](#)

code signatures

use of by viruses, [ix](#)

command line

typing options, [28](#)

command syntax

variables, [36](#)

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

compressed files, ignoring during scans, [38](#)

CompuServe, technical support via, [xii](#), [56](#)

Concept virus, introduction of, [ix](#) to [x](#)

configuration file, option for loading
saved, [36](#)

consulting services, [58](#)

conventions

typing options, [28](#)

costs from virus damage, [v](#) to [vi](#)

Cron, [31](#)

crontab files

using to scan automatically, [31](#)

CTRL+ALT+DEL, ineffective use of to clear
viruses, [viii](#)

Customer Care

contacting, [xi](#)

D

damage from viruses, [v](#)

payloads, [vii](#)

.DAT file updates

reporting new items for, [xiii](#)

.DAT files

option for not showing expiration
notice, [38](#)

option for setting location of, [36](#)

.DAT file updates, [46](#)

definitions

virus, [v](#)

disguising virus infections, [ix](#)

disks

floppy

as medium for virus
transmission, [vii](#) to [viii](#)

distributions

versions of VirusScan, [21](#)

document files, as agents for virus

transmission, [ix](#) to [x](#)

E

educational services, description of, [59](#)

electronic services, contacting for technical support, [56](#)

e-mail

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

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

encrypted viruses, [ix](#)

error messages, [24](#)

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

executable programs

as agents for virus transmission, [viii](#)

exit codes, [34](#)

exit on error, setting for scan operations, [37](#)

F

file-infecting viruses

definition and behavior of, [viii](#)

floppy disks

role in spreading viruses, [vii](#) to [viii](#)

H

help

UNIX man page on crontab files, [32](#)

heuristics

options, [36](#)

heuristics, options, [39](#), [41](#)

heuristics, options, [38](#)

history of viruses, [v](#) to [x](#)

I

infected files

cleaning, [41](#)

installation requirements, [21](#)

installing VirusScan, [21](#)

Internet

spread of viruses via, [x](#)

Internet Relay Chat

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

L

last access date of files, preserving, [39](#)

library paths, [23](#)

logging on, [29](#)

M

macro viruses

Concept virus, [ix](#) to [x](#)

definition and behavior of, [ix](#) to [x](#)

macros, [41](#)

malicious software

payload, [vii](#)

script viruses as, [x](#)

types

Trojan horses, [vii](#)

worms, [vi](#)

manually installing VirusScan, [25](#)

manually uninstalling VirusScan, [25](#)

master boot record (MBR), susceptibility to virus infection, [viii](#)

memory

virus infections in, [vii](#) to [viii](#)

Microsoft

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

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

Microsoft Word files, options for not including in scans, [38](#)

mIRC script virus, [x](#)

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

N

Network Associates

- consulting services from, [58](#)
- contacting
 - Customer Care, [xi](#)
 - outside the United States, [xiv](#)
 - via America Online, [xii](#)
 - via CompuServe, [xii](#)
 - within the United States, [xii](#)
- educational services, [59](#)
- training, [xiii](#), [58](#)
- website address for software updates and upgrades, [56](#)

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

no decrypt, [38](#)

O

Office, Microsoft, files as agents for virus transmission, [x](#)

on demand scanning, [28](#)

option for deleting from files, [41](#)

origin of viruses, [v](#) to [x](#)

P

payload, definition of, [vii](#)

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

performing a scan operation, [28](#)

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

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

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

preventing virus infection, [45](#)

PrimeSupport

corporate

- at a glance, [55](#)
- Connect, [52](#)
- Connect 24-By-7, [52](#)
- Enterprise, [53](#)
- KnowledgeCenter, [51](#)
- ordering, [54](#)

retail

- Online Upgrades Plan, [57](#)
- ordering, [57](#)
- Pay-Per-Minute Plan, [57](#)
- Quarterly Disk/CD Plan, [57](#)
- Small Office/Home Office Annual Plan, [57](#)

Professional Consulting Services

description of, [58](#)

Q

quarantine

- option for moving infected files to, [42](#)

R

RAM

virus infections in, [vii](#) to [viii](#)

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

restarting

- with CTRL+ALT+DEL, ineffective use of to clear viruses, [viii](#)

S

- scan results, displaying, [43](#)
- scheduling a scan, [31](#)
- script viruses, [x](#)
- signatures, use of for virus detection, [ix](#)
- software updates and upgrades, website address for obtaining, [56](#)
- spreadsheet files, virus infections in, [ix](#) to [x](#)
- standard input, using to set scan targets, [37](#)
- starting VirusScan, [29](#)
- stealth viruses, definition of, [ix](#)
- summary of scan results, displaying, [43](#)
- support
 - corporate PrimeSupport
 - at a glance, [55](#)
 - Connect, [52](#)
 - Connect 24-By-7, [52](#)
 - Enterprise, [53](#)
 - KnowledgeCenter, [51](#)
 - ordering, [54](#)
 - for retail customers, [56](#)
 - hours of availability, [57](#)
 - retail PrimeSupport
 - Online Upgrades Plan, [57](#)
 - ordering, [57](#)
 - Pay-Per-Minute Plan, [57](#)
 - Quarterly Disk/CD Plan, [57](#)
 - Small Office/Home Office Annual Plan, [57](#)
 - via electronic services, [56](#)
- syntax
 - summary of options, [27](#)
 - using variables in, [36](#)
- system files, as agents for virus transmission, [viii](#)

T

- technical support
 - corporate PrimeSupport
 - at a glance, [55](#)
 - Connect, [52](#)
 - Connect 24-By-7, [52](#)
 - Enterprise, [53](#)
 - KnowledgeCenter, [51](#)
 - ordering, [54](#)
 - e-mail address for, [xii](#)
 - hours of availability, [57](#)
 - information needed from user, [xii](#)
 - online, [xii](#)
 - phone numbers for, [xii](#)
 - retail PrimeSupport
 - Online Upgrades Plan, [57](#)
 - ordering, [57](#)
 - Pay-Per-Minute Plan, [57](#)
 - Quarterly Disk/CD Plan, [57](#)
 - Small Office/Home Office Annual Plan, [57](#)
 - via electronic services, [56](#)
- text
 - messages, use of to transmit viruses, [x](#)
- Total Education Services
 - description of, [58](#)
- Total Service Solutions
 - contacting, [58](#)
- training for Network Associates products, [xiii](#), [58](#)
 - scheduling, [xiii](#)
- Trojan horse, definition of, [vii](#)
- troubleshooting installation, [24](#)

U

uninstalling VirusScan
 using the uninstall script, [25](#)
 unzip, [40](#)
 updates, [27](#)
 updates and upgrades, website address for
 obtaining, [56](#)
 updating VirusScan
 methods, [46](#)
 using a file to supply scan targets, [37](#)

V

variables, use of in command line, [36](#)
 verbose scan reports, setting, [43](#)
 viruses
 "Brain" virus, [vii](#)
 boot-sector infectors, [vii](#) to [viii](#)
 cleaning out of infected files, [41](#)
 code signatures, use of by, [ix](#)
 Concept, [ix](#) to [x](#)
 costs of, [v](#) to [vi](#)
 current numbers of, [v](#)
 definition of, [v](#)
 disguising infections of, [ix](#)
 effects of, [v](#)
 encrypted, definition of, [ix](#)
 file infectors, [viii](#)
 history of, [v](#) to [x](#)
 macro, [ix](#) to [x](#)
 mutating, definition of, [ix](#)
 origins of, [v](#) to [x](#)
 payload, [vii](#)
 polymorphic, definition of, [ix](#)
 programs similar to
 Trojan horses, [vii](#)

 worms, [vi](#)
 reporting new strains to Network
 Associates, [xiii](#)
 role of PCs in spread of, [vii](#)
 script language, [x](#)
 spread of via e-mail and Internet, [x](#)
 stealth, definition of, [ix](#)
 why worry?, [v](#) to [vi](#)
 VirusScan
 installing, [21](#)
 introducing, [19](#)
 options
 -analyze, [36](#)
 -c, --clean, [41](#)
 --cleandocall, --dam, [41](#)
 --config, [36](#)
 -d, --data-directory, [36](#)
 --delete, [42](#)
 -e, --exit on error, [37](#)
 --exclude, [37](#)
 -f, --file, [37](#)
 --fam, [37](#)
 -h, --help, [43](#)
 --ignore-compressed, --nocomp, [38](#)
 --ignore-links, [38](#)
 --load, [36](#)
 -m, --move DIR, [42](#)
 --manalyze, [38](#)
 -maxfilesize X, [38](#)
 --noboot, [38](#)
 --nocomp, --ignore-compressed, [38](#)
 --nodecrypt, [38](#)
 --nodoc, [38](#)
 --noexpire, [38](#)
 --one-file-system, [39](#)

- p, --atime-preserve, --plad, [39](#)
- panalyze, [39](#)
- s, --selected, [40](#)
- summary, [43](#)
- v, --verbose, [43](#)
- overview of features, [19](#)
- system requirements, [21](#)
- updating
 - methods, [46](#)

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

W

warm boot, ineffective use of to clear viruses, [viii](#)

website, Network Associates technical support via, [56](#)

why use VirusScan?, [19](#)

why worry about viruses?, [v](#) to [vi](#)

Word files, as agents for virus transmission, [x](#)

worms, definition of, [vi](#)

Z

zipped files, ignoring during scans, [38](#)