

Understanding Virus Behavior under Windows NT

- [Introduction](#)
- [Master Boot Record \(MBR\) Viruses Under Windows NT](#)
- [Boot Record Viruses Under Windows NT](#)
- [MBR and Boot Record Viruses—The Bottom Line](#)
- [DOS File Viruses Under a Windows NT DOS Box](#)
- [File Virus Infections Under Windows NT—Outside of a DOS Box](#)
- [DOS File Viruses Under Windows NT—System Susceptibility During Boot-up](#)
- [DOS File Viruses—The Bottom Line](#)
- [Windows 3.1 Viruses Under Windows NT](#)
- [Macro Viruses Under Windows NT](#)
- [Native Windows NT Viruses](#)
- [Conclusion](#)
- [Further Reading](#)
- [About Symantec](#)

Introduction

The Windows NT operating system introduces a paradigm shift from other Microsoft operating systems. It differs from other current PC operating systems in several ways:

- Windows NT does not rely upon a resident DOS kernel for system services.
- Windows NT currently supports four different file systems: a FAT-based file system, the OS/2 HPFS, the new NTFS file system, and the MAC file system (on NT servers). A new OLE file system is also under development.
- Windows NT does not rely upon the computer's ROM BIOS disk drivers and comes with NT-specific software drivers to perform all low-level disk-access functions.
- Windows NT automatically prevents all DOS programs executed in DOS boxes from directly writing to hard drives.

This paper describes how each of the major types of viruses encountered today will function under Windows NT given the differences between it and previous Microsoft operating systems. The following virus classes are detailed: MBR viruses (on floppy diskette and hard drive), boot record viruses (on floppy diskette and hard drive), direct-action file viruses, memory-resident file viruses, multipartite viruses (which have both file and boot infection capabilities), macro viruses, and Windows 3.1 viruses. Finally, the paper describes native Windows NT viruses.

Master Boot Record (MBR) Viruses Under Windows NT

MBR viruses are typically acquired in two different ways. The first method involves booting off of an infected floppy diskette. The second method involves running a "dropper" program from a DOS session, which directly "drops" the virus onto the MBR of the hard drive; multipartite computer viruses sometimes attempt this type of infection.

MBR Infection by Booting Off an Infected Floppy Diskette

The Windows NT operating system is still susceptible to this type of infection. Since NT does not have control of the computer during system boot-up, booting from an infected floppy diskette allows the virus to infect the MBR of any of the physical drives on the system using the usual techniques. This vector of infection is quite common, and we can expect to see more of the same.

MBR Infection by Running a Dropper Program or Multipartite Virus

Dropper programs and multipartite viruses infect the MBR of the hard drive by using BIOS or DOS services to write directly to the hard drive. Since Windows NT prevents all such writes from within Windows NT DOS box, this type of infection will be completely prevented while NT is running. However, if the computer in question also has the ability to boot to DOS or Windows 95, then the user could boot to one of these operating systems and execute the dropper program or multipartite virus normally.

The NT Boot-up Process with MBR Infection

Once a virus is present in the MBR, future system reboots will allow the virus to become memory-resident in the usual fashion. In addition, if the virus contains any type of payload that is triggered during boot-up, this trigger mechanism will function just as it would under a DOS or Windows 95 system. Thus, viruses such as Michelangelo and One-half can still cause significant damage to Windows NT systems.

Upon boot-up, once the virus has installed itself in memory, it passes control to the original system MBR, which then transfers control to the Windows NT boot record. This boot record then loads the Windows NT loader, which loads the rest of the operating system. During this loading process, NT switches into protected mode and installs its own protected-mode disk drivers. These protected-mode drivers are used for all further disk operations; consequently, the original BIOS disk drivers and any virus that "hooked" into these drivers are never activated or used in any way.

Once Windows NT starts using its own drivers, the resident MBR virus is effectively stopped in its tracks. Furthermore, unlike Windows 95, Windows NT does not support a compatibility mode, which allows disk requests to be sent to the original disk drivers (and potentially a virus). These Windows NT characteristics have the following implications:

- MBR viruses will be unable to infect other diskettes after Windows NT has loaded.
- Under DOS and Windows 95 systems, some viruses (such as the Ripper virus) can "hook into" direct disk services (provided by the computer's BIOS) and maliciously alter data during disk accesses. Under Windows NT, the virus will still be able to alter bytes retrieved or stored to the disk while the original BIOS disk drivers are used during boot-up. Thus, all components of the operating system that are read from disk before the protected-mode disk drivers are employed may become corrupted. However, as soon as the operating system starts using the protected-mode disk drivers, the virus is disabled and can do no further damage.
- During boot-up, the One-half virus encrypts information on the hard drive (on DOS, Windows 95, or Windows NT). On DOS and Windows 95 systems, the One-half virus dynamically decrypts these sectors as they are accessed by the operating system. Since Windows NT cuts the virus off entirely once its protected-mode drivers are loaded, all encrypted sectors remain encrypted and are not dynamically decrypted by the virus. This results in data loss.
- Stealth viruses are unable to function properly once Windows NT has loaded since the virus routines are never given control. This makes these viruses easy to detect but can cause other problems (see next item).
- MBR viruses such as Monkey (which do not maintain a partition table in the infected MBR sector) will cause infected drives to be inaccessible to Windows NT. This occurs because Windows NT reads the

partition table from the MBR to determine what logical drives are present on the system using protected-mode disk drivers. Since the protected-mode drivers are used, the virus stealth mechanism is bypassed and the virus is unable to present the original, decrypted partition table. Hence, Windows NT reads a garbled partition table and is unable to identify the logical drives on the system. Under DOS and Windows 95 systems, the active stealth capabilities of the virus allow it to provide the operating system with the original partition table information, avoiding this problem. Contrast with the next point.

- If the virus does not modify the partition table of the MBR, then Windows NT should behave normally, assuming the virus has no payloads that trigger during system boot-up.

Boot Record Viruses Under Windows NT

Boot record viruses are typically acquired in two different ways. The first method involves booting off of an infected floppy diskette. The second method involves running a dropper program from a DOS session, which directly "drops" the virus onto the boot record of the active partition; multipartite computer viruses sometimes attempt this type of infection.

Boot Record Infection by Booting Off an Infected Floppy Diskette

The Windows NT operating system is still susceptible to this type of infection. Since the NT does not have control of the computer during system boot-up, booting from an infected floppy allows the virus to infect the boot record of any of the active partitions on the system using the usual techniques. This vector of infection is quite common, and we can expect to see more of the same.

Boot Record Infection by Running a Dropper Program or Multipartite Virus

Dropper programs and multipartite viruses infect the boot record of the hard drive by using BIOS or DOS services to write directly to the hard drive. Since Windows NT prevents all such writes from within an NT DOS box, this type of infection will be completely prevented while NT is running. However, if the computer in question also has the ability to boot to DOS or Windows 95, then the user could boot to one of these operating systems and execute the dropper program or multipartite virus normally.

Possible Damage from Boot Record Virus Infection

As described, hard drives can still become infected with boot record viruses by booting off of an infected floppy diskette. Boot record viruses infect hard drive boot records by relocating the original boot record to a new (and hopefully unused) location of the drive and then replacing the original boot record with the viral boot record. Usually, boot record viruses place the original, uninfected boot record at the end of the infected drive. Depending on what type of file system is being used on the Windows NT boot partition, different problems may arise.

Damage Due to Boot Record Virus Infection on FAT Systems

- If the virus places the original boot record at the end of the drive and does not take steps to protect this sector, then Windows NT may inadvertently overwrite the saved boot record. This will cause the system to crash during boot-up. The same behavior can also be observed under DOS and Windows 95.
- If the virus does not maintain the BPB (BIOS Parameter Block) section of the boot record and relies upon stealth functionality to properly provide this information to DOS, Windows NT will have difficulty accessing the drive once the protected-mode disk drivers are utilized.

Damage Due to Boot Record Virus Infection on NTFS or HPFS Systems

On bootable NTFS partitions, Windows NT places a "boot-strap" operating system loader program on the sectors immediately following the NTFS boot record. When the Windows NT boot record is loaded and executed by the MBR during system boot-up, it immediately rereads itself and these additional "boot-strap" sectors into memory and transfers control to them. The NTFS boot sector and these additional sectors comprise a "boot-strap" program which is capable of loading and launching the bulk of the Windows NT operating system.

If a boot record virus infects the NTFS boot record, it effectively overwrites the first sector of the multi-sector "boot-strap" program, causing important routines and data to be lost. Consider the NTFS boot-up process with a boot record infection: During the NTFS boot-up, the uninfected MBR loads and transfers control to the viral boot record of the active NTFS partition. The virus then installs itself in memory and transfers control to the original NTFS boot record, which is retrieved from the end of the logical or physical drive where the virus stored it. At this point, a small routine in the NTFS boot record attempts to load the entire NTFS "boot-strap" program (which is comprised of what should be the original NTFS boot record and the following sectors). However, the first sector of the boot strap program has been overwritten by the body of the virus. Thus, a corrupted copy of the "boot-strap" program is loaded and executed. This will result in a system crash and Windows NT will fail to start up.

The bottom line is that most boot record viruses will cause an NTFS-based, Windows NT system to crash during boot-up. However, if the boot record virus has stealthing capabilities, Windows NT may be able to properly load. The boot-up process takes place before Windows NT loads and utilizes its own protected mode disk drivers; in other words, the standard BIOS disk services (and any resident computer virus which has "hooked" into these services) are used by the NTFS boot record to load the "boot-strap" program from the hard drive. If the virus has stealth capabilities, when the Windows NT boot record uses these BIOS/virus services to load the NTFS "boot-strap" program, the virus can hide the infected boot record and correctly load the original NTFS boot record along with the other "boot-strap" sectors. Once the proper "boot-strap" program has been loaded, Windows NT can boot-up normally.

The NT Boot-up Process with a Boot Record Infection

During the boot-up process, the uninfected MBR loads and transfers control to the viral boot record of the active NTFS, HPFS, or FAT partition. The virus then installs itself in memory and drops any pay-loads. Finally, the virus boot record loads and transfers control to the original boot record and the boot process continues normally. Once again, Windows NT switches into protected mode and installs its own protected-mode disk drivers. These protected-mode drivers are used for all further disk operations; consequently, the original BIOS disk drivers and any virus that "hooked" into these drivers are never activated or used in any way. Thus, boot record viruses are disabled in the same fashion as MBR viruses.

Windows NT Installation with Existing Boot Record Infection

Windows NT can be installed within an existing DOS/Windows 95 FAT-based partition and gives the user the option of booting either into Windows NT or into the old DOS or Windows 95 operating system. Windows NT provides this "dual-boot" service by making a backup copy of the DOS/Windows 95 boot record during its installation, and saving this backup copy to a file called BOOTSEC.DOS. Windows NT then replaces the boot sector of the FAT-based drive with the Windows NT boot sector. Each time the user reboots the system, the Windows NT loader asks the user which operating system to start. If the user requests a boot-up into DOS or Windows 95, then the Windows NT loader loads and executes the original boot record contained in the BOOTSEC.DOS file and boots the computer into a standard DOS/Windows session. Unfortunately, if the boot record of the DOS/Windows 95 partition is infected with a virus before Windows NT was installed, a copy of this virus is placed within the BOOTSEC.DOS file during installation. Consequently, each time the user boots the system into DOS or Windows 95, the virus gains control of the system. In addition, since the virus is not located within the boot record of the drive, it will not be detected by antivirus tools that are unaware of Windows NT.

MBR and Boot Record Viruses - The Bottom Line

Viruses such as Michelangelo and One-half are capable of doing damage during the boot-up process but are completely disabled once Windows NT starts using its protected mode disk drivers. Thus, infection of floppy diskettes or files (in the case of a multipartite virus) will be prevented in all instances (i.e. in DOS boxes, etc.). Viruses which do not save the boot record's BPB information or the MBR's partition table may prevent NT from booting or make certain drives inaccessible. Furthermore, all non-stealth boot record viruses (such as the Form virus) that infect bootable NTFS partitions will corrupt the operating system "boot-strap" loader and cause Windows NT to crash during boot-up. When booting from an infected floppy diskette, buggy virus infection mechanisms may also cause data loss under all file systems supported by NT.

DOS File Viruses Under a Windows NT DOS Box

Most DOS file viruses function correctly under a Windows NT DOS box. File viruses typically come in two flavors: direct-action viruses and memory-resident viruses. Direct-action viruses attempt to infect other files on the system as soon as an infected file is executed. Memory-resident viruses attempt to hook into the DOS system services and infect files on a per-access basis.

Direct-Action File Viruses Under a Windows NT DOS Box

Direct-action-file viruses will function in exactly the same manner under Windows NT as they would under a standard DOS or Windows 95 system. These viruses typically use the standard DOS system services, which are thoroughly emulated in Windows NT DOS boxes.

Memory-Resident File Viruses Under a Windows NT DOS Box

In most cases, memory-resident file viruses will stay memory-resident within the confines of a Windows NT DOS box. Once the virus is resident within a given DOS box, it can infect any programs accessed or executed within that DOS box, assuming the user who launched the virus has write access to the target program. The virus will be unable to spread to other DOS boxes as each DOS box has its own protected memory space. However, nothing prevents a user from executing infected programs in several DOS boxes. Thus, several independent copies of the virus can be active and infectious at once. Furthermore, if the virus in question has infected the command shell (for example, CMD.EXE or NDOS.COM) used in Windows NT DOS boxes, then every time users open a new DOS box, they automatically launch the memory-resident virus into the box's memory space. This implies that memory scanning should be performed on a per-DOS box basis.

Windows NT faithfully emulates most DOS functionality within its DOS boxes, and in some ways provides more compatible support than Windows 95 DOS boxes. Memory-resident viruses that "hook into" the DOS system services within a DOS box can gain control and infect files any time the system services are used by DOS or other programs.

For example, when a user executes a DOS program on a standard DOS machine (that is, one that does not run Windows NT or Windows 95), the command shell (for example, COMMAND.COM or NDOS.COM) generates an "EXECUTE PROGRAM" system service request to the DOS kernel. Many viruses intercept this system service to infect program files as they are executed by the user. Windows NT faithfully provides the same functionality in its DOS boxes and allows viruses to intercept this system service and infect at will.

Furthermore, Windows NT allows users to launch native Windows applications directly from the DOS box's command line. Under the NDOS command shell, any Windows program that is launched from a DOS box's command line will cause the NDOS command interpreter to generate an "EXECUTE PROGRAM" system service request. Thus, if a memory-resident virus were to hook into the EXECUTE system service, it could potentially infect these Windows programs as they are executed. However, most DOS viruses are incapable of correctly infecting

native Windows executable programs. Interestingly, the default command shell (CMD.EXE) that ships with Windows NT does not generate the "EXECUTE" system service request when Windows executables are launched from a DOS box; thus, memory-resident computer viruses will be unable to infect native Windows programs launched from a "CMD.EXE" based NT DOS box.

Damage by File Viruses Under a Windows NT DOS Box

Windows NT does provide file-level access control that will prevent protected files from becoming modified by DOS-based file viruses. The access control provided by Windows NT is significantly more robust than DOS's simple read-only attribute and cannot be bypassed by DOS programs. However, if an infected program is run by a system operator with root privileges or the Windows NT system is set up without access control, the virus can modify all files to which the operator has access.

If we assume that the typical Windows NT configuration does not employ Windows NT's security features, then viruses will be able to damage files just as they did on a standard MS-DOS system. For instance, viruses that corrupt program files unintentionally during the infection process will still be able to do so under Windows NT DOS boxes. However, file viruses that attempt to "trash" the hard drive using direct disk access will be thwarted under Windows NT since all direct access to hard drives is prevented by Windows NT.

While Windows NT does prevent DOS programs from writing directly to hard drives, it does not prevent DOS programs from directly writing to floppy diskettes. Thus, multipartite DOS viruses launched from within a DOS box may infect or damage floppy diskettes. However, most multipartite viruses, when launched from an infected DOS program, attempt to infect the hard drive's MBR or boot record to gain control during boot-up. Since Windows NT will prevent these direct disk writes from within a DOS box, these viruses will likely be neutered.

File Virus Infections Under Windows NT—Outside of a DOS Box

DOS-based file viruses will function properly only within a DOS box under Windows NT. Under all other circumstances, these viruses will fail to function correctly and will be non-viral in nature.

DOS File Viruses Under Windows NT - System Susceptibility During Boot-up

Should one of the files responsible for Windows NT boot-up become infected with a DOS-based computer virus, Windows NT will most likely be unable to load properly. This is because DOS-based viruses require the DOS kernel and other "real-mode" data structures to function, and these data structures are necessarily absent during Windows NT boot-up (since NT does not use DOS in its operation). The absence of the DOS kernel during the boot-up process will probably cause any infected executable to crash once the virus begins executing.

DOS File Viruses - The Bottom Line

Most DOS file viruses should propagate under Windows NT DOS boxes just as they do on standard DOS systems. The built-in Windows NT file and directory protection will prevent infection of protected files; however, the system must be explicitly configured to provide this protection. Unfortunately, many users may be unaware of or inconvenienced by this protection and disable it.

Multipartite viruses (viruses that infect both files and boot sectors) will no longer be able to infect hard drive boot records or master boot records from within DOS boxes. If the virus relies upon this behavior for propagation, it will be neutered by Windows NT's direct-disk access restrictions. However, multipartite file viruses will still be able to infect floppy diskette boot records if they are so inclined (although this behavior is rare).

DOS file viruses will function only within DOS boxes. While it is possible that native Windows NT system files may become infected (by direct-action viruses that go searching for files all over the hard drive), the infected system files will most likely fail to function properly and crash the machine during Windows NT boot-up.

If a resident DOS file virus is launched from within a DOS box, only files referenced from within the infected DOS box can potentially become infected. Thus, any Windows NT antivirus product that executes outside of a DOS box (such as a 32-bit Windows application) can safely scan the computer without the possibility of infecting clean files; memory scanning is not necessary to properly detect and repair virus infections.

Windows 3.1 Viruses Under Windows NT

Most of the native Windows 3.1 viruses will function under Windows NT as they do under Windows 3.1.

At least one Windows 3.1 virus uses DPMI (DOS Protected Mode Interface) to hook into the standard Windows system services and establish itself as a memory-resident Windows TSR. The "Ph33r" virus hooks into the Windows 3.1 "EXECUTE PROGRAM" system service and is notified every time a program is executed by the user or another Windows 3.1 process. Upon notification, the "Ph33r" virus can infect the Windows 3.1 executable file before it is executed.

Viruses that hook into these services will also function under Windows NT as they do under Windows 3.1. However, under Windows NT, the Windows 3.1 TSR virus described above will only be notified about the execution of standard Windows 3.1 executables. For instance, if a user launches a native 32-bit Windows NT or Windows 95 application, the Windows 3.1 subsystem under Windows NT (and any Windows 3.1 TSRs hooked into its system services) will not be made aware of the 32-bit program's execution. Consequently, only Windows 3.1 executables executed on the Windows NT system will be susceptible to infection by Windows 3.1 viruses.

Furthermore, Windows NT allows the user to specify whether each Windows 3.1 application is launched in a common memory area or in its own separate memory area. This functionality was provided so that users could prevent misbehaved Windows 3.1 applications from interfering with each other. If the user loads an infected Windows 3.1 application in its own memory area, then the resident virus will not receive notification of system service requests from other Windows 3.1 applications.

Macro Viruses Under Windows NT

All macro viruses written for applications that run on Windows 3.1 or Windows 95 will function correctly under Windows NT if the host application works correctly under Windows NT. For example, since Word for Windows version 6.0+ works both on Windows 95 and Windows NT, the Concept virus works correctly under both platforms as well. The file-level protection provided by Windows NT can be used to prevent unauthorized use of documents (limiting potential infection); however, these macro viruses can still be spread through electronic mail or publicly accessible files. The bottom line is that macro viruses will continue to propagate under Windows NT systems. Given the necessity of information-sharing in the enterprise environment, the macro viruses may surpass their DOS cousins as the most common viral threat.

Native Windows NT Viruses

Windows NT presents a much greater challenge for virus writers. First, the basic Windows NT operating system requires at least 12 megabytes of conventional RAM, a high-speed microprocessor and tens of megabytes of hard drive space. Most machines sold today are not powerful enough to provide a bare-bones Windows NT setup for software development. In other words, virus writers (who are often teenagers) may not be able to afford the appropriate hardware to develop native Windows NT viruses.

In addition to the Windows NT hardware requirements, the native Windows NT and Windows 95 executable file formats are also more complex than those found in DOS. Windows 3.1 also employs similar executable file formats that may account for the lower number of native Windows viruses. Furthermore, far less documentation is available on these file formats, requiring virus writers to spend time reverse-engineering their file structure.

Finally, the Windows 3.1 architecture permitted Windows applications to call standard DOS system services directly just as if they were DOS applications. This permitted virus writers with only a superficial understanding of the Windows 3.1 operating system to create viruses using standard DOS-based virus algorithms. The Windows NT and Windows 95 operating systems do not allow 32-bit applications to use the DOS system services, although Windows 3.1 programs running in these environments are allowed to use these services. Therefore, virus writers will have to gain a fairly detailed understanding of the Windows 32-bit API to create native Windows NT or Windows 95 viruses. This will probably reduce the number of native Windows NT and Windows 95 viruses encountered in the short term. However, as more detailed documentation is published in popular books and magazines, we will undoubtedly see an increasing number of native Windows viruses.

Conclusion

The Windows NT operating system is definitely susceptible to DOS-based computer viruses. In many instances, Windows NT will prevent viruses from spreading as they would under DOS or Windows 95; however, these same viruses can still intentionally or unintentionally cause significant damage to the Windows NT operating system, its programs, and data. As described above, DOS-based viruses can be split into two categories: boot record viruses and file viruses.

The Windows NT architecture severely limits the functionality of boot viruses, should the MBR or boot record of the hard drive become infected. If Windows NT is able to start up on an infected system, the infecting boot virus is never activated because the Windows NT protected-mode disk drivers are used instead of the viral disk drivers. Thus, standard boot viruses will be unable to propagate under the Windows NT operating system. Unfortunately, these viruses can still cause serious damage to NT systems:

- They can affect the boot-up process, causing Windows NT to crash.
- They can inadvertently damage data within the Windows NT partition.
- They can still trigger and intentionally cause damage during the boot-up process, before Windows NT gains control of the computer.

In addition, if Windows NT is installed on top of a DOS or Windows 95 partition, it provides the user with a special mechanism for "dual booting" between between the Windows NT and DOS/Windows 95. To provide this "dual boot" functionality, Windows NT maintains a copy of the original DOS/Windows 95 boot record (present on the drive before Windows NT installation) and uses this copy in the DOS/Windows 95 boot-up process. Unfortunately, if the boot record of the DOS/Windows 95 partition was infected before Windows NT installation, the copy of the boot record maintained by Windows NT will also contain this infection. Furthermore, the copy of the boot record is stored within a file and not in the traditional boot area of the hard drive; thus, antivirus tools that are unaware of Windows NT will be unable to detect and repair this infection, leaving the system vulnerable to any boot record virus present on the system at the time Windows NT was installed.

If Windows 95 and Windows NT do become the predominant operating systems on PCs, we can expect to see a reduction in the number of boot virus infections, since these operating systems sub-vert their primary method of infection. However, for the time being, these viruses can still cause serious damage to Windows NT systems and traditional tools may not be able to recover from infection.

Most of the DOS-based and Windows 3.1-based file viruses will function properly under Windows NT. Under the NTFS file system, Windows NT does allow the user to protect files on a per-file or per-directory basis; however, this security feature may have little effect on DOS/Windows 3.1-based file viruses:

Symantec AntiVirus Research Center

- FAT-based partitions cannot be safeguarded by this type of protection.
- The typical end user will have no reason to enable this protection.
- A virus executed in a user's account can still infect all files owned by that user, even though those files may be protected and inaccessible to other users of the Windows NT system.

Currently, DOS/Windows 3.1 file viruses are unable to infect native Windows NT executable files, although they may unknowingly try to do so and cause damage. In addition, there is no reason why a hybrid file virus could not be written to infect both DOS and Windows NT executable files. In fact, this basic concept has already been observed: The recently released "Ph33r" virus can infect both DOS and Windows 3.1 executable files.

The new macro viruses will also function properly under Windows NT. These viruses do not rely upon the underlying operating system to propagate and therefore have no difficulty infecting on any Windows NT machine that supports macro-capable products.

Finally, while there are no native Windows NT viruses today, their future appearance is unquestioned. Even though Windows NT provides a significant amount of memory and file protection, native VDD-based (Virtual Device Driver) viruses will have the ability to modify memory, infect or damage files, and directly access both hard drives and floppy diskettes. They will be able to intercept any system service and infect programs or floppy diskettes at will. In short, they will have the same abilities as their DOS cousins on an unprotected DOS machine.

Further Reading

This document is one of a series of papers on Symantec's enterprise network strategy and its network management product offerings. Additional papers include:

- The Truth About Virus Outbreaks in a Networked Environment
- Addressing Today's Access to the Enterprise Network
- Workstation Access Control: A Key Element in Securing Enterprise Network
- Reducing Network Administration Costs with Remote Workstation Recovery Tools
- Using Backup Products for Enterprise-wide Storage Management
- Enterprise Developer: Creating Client/Server Applications in an Enterprise Environment
- Managing Distributed Networks with the Norton Enterprise Framework Architecture
- Improving the Bottom Line with Project Management Software
- Trends in Project Management Software: Open Connectivity and Client/Server Architecture
- Using Remote Control Software to Gain Access to the Enterprise Network
- Building the Ecosystem: Enabling the Next Generation of Client/Server Computing
- Understanding Virus Behavior in a 32-Bit Environment
- Why Norton Utilities is a Natural Complement to the Windows 95 Environment
- Reducing the Cost of Enterprise Computing with Inventory, Distribution, and Metering Tools
- Managing Desktop Interfaces Across the Enterprise
- Understanding File Management and Windows 95
- A Strategy for the Migration to Windows 95

Symantec AntiVirus Research Center

For copies of these papers or information about Symantec enterprise network products, call 1-800-488-9914 and ask for C193. Outside the United States contact [the sales office nearest you](#).