Managing the Virus Threat on the Enterprise

A Strategic Briefing for Enterprise Network Decision Makers

intel.

Executive Summary

Computer viruses – they have existed for less than a decade, yet they have come to significantly impact network management. Protection against viruses is now a vital task in many enterprises.

Network decision makers may have received mixed information regarding the virus threat. Since the first virus attack was detected in 1987, reports of the virus threat have ranged from hype to more reasoned cautions. Viruses, which are pieces of renegade and damaging code that attach to files, are easily introduced into a network, but they may or may not do damage. In fact, many of the 5,000 viruses known today have been discovered, submitted, and analyzed by anti-virus vendors, and do not exist "in the wild" on real networks.

But this does not diminish the threat. One virus – not 5,000 – is all it takes to corrupt data, freeze workstations, or impact critical networked tasks. Some of these 5,000 viruses are in fact very common viruses and spread quite easily, often using the server as the breeding ground and central distribution point. Thus, network managers need to be concerned about viruses – not because of their number, but because they affect system performance and take up valuable disk space. Most important, viruses can damage files, data, or even the integrity of the entire network system.

Contents

Executive Summary 2

How a Single Virus Can Threaten Your Enterprise 3

But is it Real, or Just Hype? 3

What is a Virus? 4

Common Virus Types 4

- Another Breed: Stealth Viruses
- Shape Shifters: Polymorphic viruses
- Other destructive code

Which Viruses Pose the Greatest Threat? 6

How Do Viruses Spread? 6

The Evolution of Anti-Virus Technologies 7

The Next Generation – Virus Firewall Protection 8

- Clean Room Certification
- The Integrity Shield
- What does this mean to the administrator?

Developing an Enterprise-Wide Virus Protection Strategy 9

The LANDesk® Virus Protect Solution 9

- Protection at the server
- Protection at the workstation
- Companion technologies

Centralized Management 11

Intel Product Support Numbers 12

As vendors became aware of the virus threat, technologies were developed that attacked the problem from several angles. For example, virus protection may include pattern scanning to detect known virus code strings, traps that look for virus-like activity to identify renegade code intrusions, and checksumming to detect any change in a file. (These approaches will be discussed in greater detail below.)

A single tool, such as a virus scanner, is usually not enough to provide robust protection across the enterprise. Different platforms (servers and workstations) have different vulnerabilities. In addition, the enterprise itself has its own vulnerabilities and restrictions.

As a result, most virus protection software combines some or all of these technologies, and it resides on the server as well as the individual workstation to further ensure enterprise-wide protection. Intel led the market for overlapping technology, server-based virus protection with its LANDesk® Virus Protect product, introduced in 1992.

Recently, network managers have recognized that simply detecting viruses on the network is not enough. As the number of potential viruses patterns has grown, the process of identifying errant code strings becomes a performance and management burden in itself. Worse, it does nothing to prevent infection of the network in the first place.

What managers require is advanced virus technologies that actually prevent viruses from propagating. Ideally, virus protection software should also be efficient and well-integrated with centralized management functions.

In 1995, Intel introduced LANDesk Virus Protect 3.0, a unique combination of technologies that creates an impenetrable virus firewall – it actually prevents the server from acting as a source of virus infection and spread.

The remainder of this document provides in-depth background on the enterprise virus, leading to a close-up examination of Intel LANDesk Virus Protect's virus firewall solution.

How a Single Virus Can Threaten Your Enterprise

One virus incident may be all it takes to seriously affect the productivity of your enterprise. Consider this potential scenario: You are the administrator of a large enterprise with thousands of nodes covering the entire country. Your system is interconnected to enterprises in Europe and Asia. The many subnets on your enterprise are managed by individual subnet administrators. Your system spans virtually every time zone in the world.

At 8 a.m., your Eastern European field office begins its workday. A particularly nasty stealth virus, written perhaps by Dark Avenger, one of the most notorious of the virus writers in the Bulgarian "virus factories," is on a user's workstation. It infects a file that is about to be sent to your main office in San Francisco.

The infected file arrives attached to an electronic mail message in California. The recipient reads e-mail, retrieves the file and sets it aside for later. After a full day of meetings, the recipient finally gets back the office and executes the file, which immediately infects the logout executable on the workstation. Finished with the file, the recipient logs off the network, in the process infecting the login executable on the network's login directory on the file server.

The next day, arriving early for a meeting, the recipient logs into the network. During the login process the user places the virus, which was hidden in the login executable on the file server, on the workstation where it begins to infect every file executed. Meanwhile, other workers on the network begin to log in using the infected login file. Within an hour, every workstation on the San Francisco network is infected, and every executable file that has been executed at the infected workstations is infected. Unknowingly, an engineer transfers an executable file, infected by the virus, to the New York office.

The same process that infected San Francisco now begins in New York. The logout executable infects the login executable. When the New York employees return from lunch and log back onto the network for an afternoon's work, every workstation in New York becomes infected.

The virus soon destroys boot sectors, partition tables and file allocation tables. Workstations in New York and San Francisco go down. Worse, infected

files have now been transferred to the company's offices in Chicago, Dallas, Atlanta, Rome, Paris, London, Tokyo and Singapore. By the time three hours have passed, all of the American offices have workstations down. At the start of work the next day, the scenario repeats in the newly infected offices.

But is it Real, or Just Hype?

The earliest computer viruses came out of Eastern Europe in the late 1980s. Since that time, the number of viruses and virus authors has grown dramatically, giving rise to a fair amount of press coverage and user concern. In 1990, the Michelangelo virus in particular elicited much media hype and prognostication. When nothing much happened on the dreaded date (March 6, Michelangelo's birthday), the credibility of the virus threat, and products designed to protect against it, was questioned.

However, research suggests that data loss from virus attacks remains a possibility in unprotected networks. Information Week, a respected trade publication, explored the virus threat in its July 19, 1993 issue. In a reader poll the publication found that 58% had experienced at least some direct effect from viruses in the preceding 12 months, and 5% of the respondents said viruses had affected more than 50% of their PCs. 87% believed that networks had either caused an increase in the threat or, at least, kept it constant with non-networked systems.

The potential loss from virus infection is significant. Even relatively innocuous viruses that don't bring down entire networks still take their toll: corrupted files, lost administrator time, wasted disk space, lowered productivity of workers who rely on the network.

Therefore, managers and administrators still need to take viruses seriously. For a good understanding of virus protection strategies, it is important to first understand the basics about what viruses are and how they spread.

What is a Virus?

A computer virus is a piece of malicious code that attaches to key vectors: executable files and boot areas of floppy diskettes and hard drives. Once in memory, it can infect other executable files or disk boot areas.

The majority of viruses are written for DOS-based PCs and the numbers continue to grow rapidly. A handful of Macintosh* viruses exist, but there has been very little activity in this area in recent years. There are currently no known native OS/2* or Windows NT* viruses in the wild. However, operating systems that use the FAT file system, such as OS/2 and Windows NT, are vulnerable to boot viruses. From these files, viruses can execute and spread to DOS boxes or Virtual DOS Machines.

By definition, a virus must replicate or infect other host files or disks. The virus accomplishes this by loading into memory as its host file is executed or the computer boots from an infected drive. Besides replication, a computer virus typically performs some other function, usually intended to do damage or spread a message. Typically, a virus will replicate but otherwise remain dormant until some trigger event occurs such as a system date or other system events.

The more complex the virus is, the more dangerous it becomes. For example, many viruses employ stealth techniques to evade detection by scanners. One of the more dangerous effects of stealth memory-resident viruses is that they resist detection and then attempt to infect the detection mechanism itself. Other dangerous viruses are polymorphic, those that change their signatures to avoid detection.

Other kinds of destructive code exist which are not called viruses, because they do not replicate. Such destructive codes, including Trojan horses, worms, and logic bombs (see definitions below), may not replicate but are still dangerous because they steal system resources or corrupt data.

Common Virus Types

Viruses can be classified by what they infect. Three basic "target" virus classifications exist:

- File viruses
- Boot viruses
- Multi-partite viruses

File viruses. File viruses attach them-

selves to executable files by inserting instructions into the execution sequence and then launch virus code which has been attached somewhere in the file. When the file is executed, the virus launches its code and then returns to the normal execution sequence. This typically happens so quickly that the user is not even aware that the virus executed.

There are three sub classifications of file viruses: memory resident, direct action, and companion. Memory resident viruses stay in memory as a TSR (terminate-stay-resident) program and typically infect other files as they are executed or opened. Direct action viruses simply execute, infect other files, and unload. A companion virus associates itself with an executable file without modifying it. For example the virus might create a WORD.COM that may be flagged or hidden as a companion file to the WORD.EXE file. When the WORD program is launched, the infected WORD.COM file will execute, perform the virus activities, and then spawn the WORD. EXE file.

Boot viruses. Boot viruses insert instructions into boot sectors of floppy diskettes or the boot sector or master boot record (partition sector) of a fixed hard drive. When the computer boots from an infected floppy, the virus infects the boot hard drive and loads its code into memory. The floppy does not have to be bootable for the virus to spread. The virus remains memory resident and infects any floppy disks that are accessed. Typically the trigger for a boot virus is the system date or time. The Michelangelo virus is a boot virus that wipes out the hard drive of its host.

A floppy or hard drive with an infected boot sector will not infect any files, unless it is a multi-partite virus. A true boot sector virus cannot spread to the server or over the network.

Multi-partite viruses. Multi-partite viruses are hybrids of file and boot viruses. For example, the Junkie virus can infect executable files and therefore travel over the network. It can also infect the boot areas and floppies, similar to a boot virus.

Another breed: stealth viruses

Stealth viruses hide their modifications or presence by hooking interrupts so when certain system functions are called, the virus "forges" the results, making everything look normal. Stealth viruses corrupt files by:

- Forging file sizes and dates.
- Hiding changes the virus has made to the boot sector.
- Redirecting most read attempts.

Stealth viruses can be disabled by booting from a clean floppy. This makes certain that the virus is no longer in memory.

Shape shifters: polymorphic viruses

Mutation or "polymorphic" viruses change form every time they infect, making traditional pattern scanning ineffective, and rampant infection is possible. Each generation of infection changes the way the virus appears in the file, making traditional pattern matching difficult. Mutation engines can be added to existing viruses to make the viruses polymorphic.

Other destructive code

There are other types of code that are destructive but not classified as viruses. It is important to note that virus protection programs may not protect against these.

Trojan horses are programs that contain hidden, destructive code but don't replicate. They may act like viruses with this one exception.

Worms replicate, but instead of being pieces of code which attach to and infect another file, worms are stand-alone programs. They usually steal system resources such as memory, disk space, or CPU cycles.

Logic bombs are pieces of code implanted in a program at the time of creation or modification, triggering destructive actions at a later time. Often, a given condition is set to trigger the action. A payroll program may, for example, erase all records a couple of months after it fails to read the name of a disgruntled, terminated employee. Logic bombs are a form of revenge or code sabotage.

Which Viruses Pose the Greatest Threat?

Among the most dangerous are the boot and master boot record infectors, because they can enter the system on floppy disks whether or not the disk carries executable files.

Boot viruses cannot spread from a PC to a file server over the network. However, the DOS partition of a NetWare* server can become infected by a boot virus from a floppy diskette and can potentially damage the drive, even though it cannot spread to the NetWare file system.

The danger posed by a virus can also depend on the kind of file it infects. For example, a virus that infects executable files may be far more dangerous on stand-alone PCs as a .COM file infector than as an .EXE file infector, because it could infect command.com and spread rapidly with each new bootup of the PC. A virus that infects .EXE files, on the other hand, might be dangerous in networks, such as NetWare LANs, that use a login.exe file. Every new login could pose a new opportunity for the virus to infect. (See How do Viruses Spread, below).

Once inside the system, memory-resident viruses become the most dangerous. Memory-resident viruses can enter via executable files, and from there they infect every target file (.COM and/or .EXE) that executes. A few memory resident viruses simply require that the file be opened. Some will infect with as little as the execution of the DIR command.

In addition, the more complex the virus is, the more dangerous it becomes. For example, many viruses employ stealth techniques to evade detection by scanners. One of the more dangerous effects of stealth memory-resident viruses is that they resist detection and then attempt to infect the detection mechanism. Other dangerous viruses are polymorphic, those that change their signatures to avoid detection.

It is also important to know the mutation skill of the local virus writers. There are some areas of the country where virus writers are very skilled at turning out modifications of unusual viruses. This makes pattern matching, a standard tool in identifying viruses, difficult and unreliable.

Considering threat by virus type, however, is only one method of determining the real danger from viruses to your system. One must also consider how viruses spread.

How Do Viruses Spread?

A virus infects a system by entering it at some intrusion point. The obvious ones are floppy drives on user workstations. On a network, these expand to include e-mail (including the downloadable files from the Internet, BBBs, WWW), modem pools, and bridges and routers to other networks (Figure 1). Your network may have others.

Once in the system, viruses can spread in two ways: through critical disk areas and in

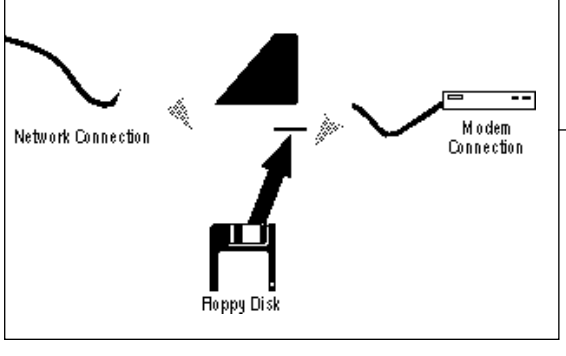


Figure 1.
The primary intrusion points for viruses are diskettes, network connections and modems.

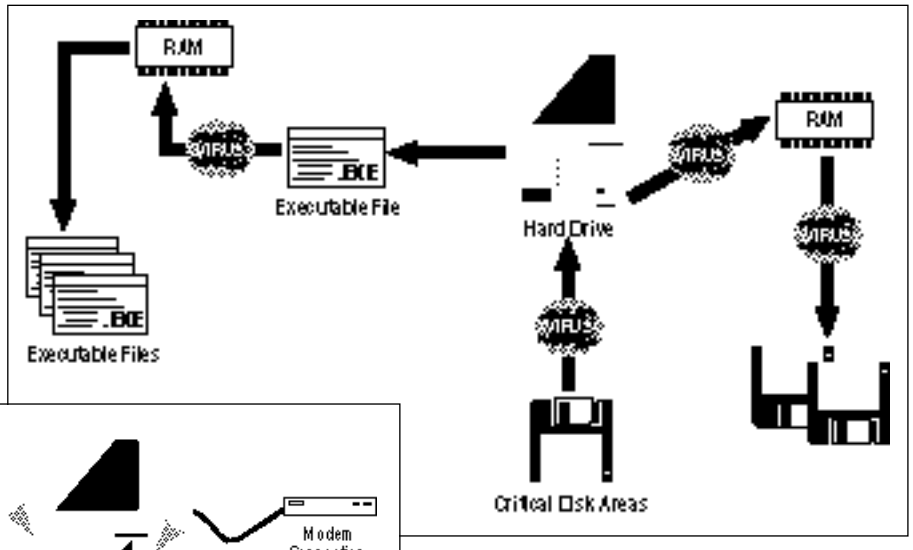


Figure 2.
Viruses spread by loading into memory and infecting other executable files or diskette boot sectors.

executable files (Figure 2). The first affects individual workstations, the second is a major trigger for server-based spread.

For example, a boot virus on a floppy disk can enter the system when a computer attempts to boot from an infected floppy. The boot virus then infects the critical disk areas (boot sector, partition table or master boot record) of the computer's hard drive. Once the boot sector of the hard drive is infected,
the virus installs itself in memory and infects the boot sector of any other floppy disk that is accessed by this computer – a great way to infect workstation after workstation as
users exchange floppy disks.

A more recently created type of virus called a "multi-partite" (see definition above) can travel as a file virus and then infect a boot sector. It also can be transmitted through floppy disks.

Executable files are a common source of spread from servers. Though there are currently no known viruses native to the Novell NetWare network operating system, NetWare servers pose a significant virus threat because they become a central distribution point –
an infection vector – for other workstations on the network.

Viruses can get onto the server in two ways:

1. New virus-infected files are copied onto a file server volume.
2. A virus in the memory of an attached PC infects a file already on the server.

When a virus-infected file is executed by an attached PC, the virus becomes active in the memory of this PC and can spread to other files on the server and the desktop system. A virus on a file server becomes especially dangerous if it has infected a critical file used by all or most users, such as LOGIN.EXE.

Here's a potential scenario for this kind of spread: A user is having trouble with his system and asks you to take a look at his machine. You need to get access to a diagnostic utility off of the server and log in as supervisor. Harmless scenario right? What you aren't aware of is that a virus had infected the user's PC and is resident in memory. When you logged in to the server as supervisor, you gave the virus full access to the
file server and allowed the virus to infect LOGIN.EXE (a file typically protected from normal users).

With conventional anti-virus solutions in place, this story has two possible endings:
1. The virus was new and unknown to the scan engine and the infection was undetected. The next morning, every station that logs in is infected by the virus.
2. The virus infection was detected and LOGIN.EXE was deleted or placed in a quarantine area. The next morning, users cannot login because LOGIN.EXE is gone.

This real-life scenario points out a fundamental weakness in anti-virus technologies up until now. These technologies focus on detecting a virus after it has already infected a file, which at best requires eradication and restoration of the infected file – time-consuming and a drain on administrator resources. As we shall see below, Intel's LANDesk Virus Protect virus firewall actually prevents infections from reaching, and being spread by, the NetWare server.
It's the next step in the evolution of anti-virus technologies.

The Evolution of Anti-Virus Technologies

Since the late 1980s, a series of anti-virus (AV) technologies have been developed and marketed.

First Generation. Pattern matching scanners, including those that recognize wildcards in scan strings, are first-generation AV products. Typically, these products were for stand-alone workstations, and were time-consuming to install across an entire network. In addition, no scanner can provide 100% protection, making it necessary to use multiple overlapping techniques.

Second Generation. Second-generation scanners go beyond simple pattern scanning, using heuristics to identify likely virus mechanisms rather than looking for complete strings of code. These products also moved protection to the server, a concept pioneered by Intel in its 1992 LANProtect product, now called

LANDesk Virus Protect. Server-based virus protection uses Novell's Netware Loadable Module (NLM) concept to protect the files on the server.

Third Generation. Third-generation AV products are virus "traps." These products wait for the virus to attempt to infect and, by observing its activity, trap and isolate the virus before it can complete its action. Third-generation products also enable integration with centralized network management consoles.

A combination of these technologies provides excellent virus protection. Scanning gives a static view of virus infection in both workstations and servers, while trapping detects unknown or mutated viruses missed by the scanner. When these tools are combined with strong enterprise management, the threat of virus infection can practically be eliminated.

The Next Generation – Virus Firewall Protection

Intel LANDesk Virus Protect v3.0 creates a new level in the evolution of AV technologies. It combines the most advanced virus detection technologies with powerful new Integrity Shield and Clean Room technologies – a virus firewall for the enterprise.

Clean Room Certification

LANDesk Virus Protect v3.0 creatively combines continuous "clean room" file certification technology with innovative Integrity Shield protection to keep server viruses from infecting executable files and spreading across the enterprise. Here's how it works.

LANDesk Virus Protect 3.0 continually certifies the server environment as virus-free. The certification scanning process consists of three automated steps:

1. Files are scanned for known viruses. If they pass the scan they are given a stamp of approval and issued two baseline integrity snapshots that are used to verify the integrity of the file at a later time.

2. The integrity of files is periodically checked for any changes from the baseline snapshots and changes characteristic of a virus infection.

3. Any time the virus pattern file is updated, each file is automatically scanned and re-certified.

Virus Protect uses a comprehensive integrity checking technology to track any changes in the environment. The integrity checking eliminates the need for redundant scanning and speeds the performance of real-time checking. The only files that need to be re-scanned are those that change and those that were scanned with an old pattern file. In addition, this method is a highly accurate means for detecting unknown virus infections.

Before LANDesk Virus Protect 3.0, integrity checking technology was impractical to implement for several reasons. Because traditional integrity checking simply looks for any change in a file, it can cause false alarms on files that change legitimately. Conventional integrity checking solutions also require a separate database of checksum values which easily becomes invalid if files are moved from their original location. Finally, many integrity checking algorithms use a simple CRC check that can be fooled by some viruses.

LANDesk Virus Protect addresses two problems of conventional integrity checking:

- Two integrity checking technologies are used – one that detects any change in a file, and one that detects changes in certain regions of a file which are most vulnerable to a virus infection. This significantly reduces annoying and time-wasting false positive alerts.
- A separate database to store checksum values is no longer needed. Each checksum value is associated with the file in NetWare. This method is faster, more secure, and checksum values go with a file when it is moved properly.

Virus protect uses two highly secure algorithms, the Message Digest Algorithm* (MD5) from RSA Data Security Inc., and a proprietary Critical Data Snapshot (CDS) which captures key regions of a file. These two algorithms cannot be fooled by viruses or other malicious attempts.

The Integrity Shield

LANDesk Virus Protect's Integrity Shield prevents spread of viruses from an infected station to the server. The Integrity Shield goes beyond detection, it actually stops virus infection and spread from .EXE, .COM and other executable files by protecting them from modification. The

Integrity Shield prevents virus spread by both privileged and non-privileged users.

The logic behind the Integrity Shield is simple. The primary targets of file viruses are executables files such as .EXE and .COM. Rarely does an administrator or anyone else need to modify or write to an executable file. Therefore, if we write-protect selected files, extensions or directories, we can prevent virus infections without getting in the way of normal administrative processes. Supervisors or users with administrative rights can work on the file server, with no danger of placing critical files at risk.

What does this mean to the administrator?

With the Integrity Shield in place, the administrator can confidently work on the file server without exposing it to viruses. Protected files on the server become immune to unknown viruses even though scanners cannot identify them. The Integrity Shield also prevents file corruption and eradication efforts related to known virus infections. In contrast, conventional anti-virus software can only detect known viruses after they have infected and corrupted a file.

LANDesk Virus Protect proves that an ounce of prevention is worth more than a pound of cure.

Developing an Enterprise-Wide Virus Protection Strategy

There are three primary issues that network administrators must face when deciding on a virus protection strategy: effectiveness, cost, and ease of management. Effectiveness of protection requires multiple countermeasures throughout the network to provide full distributed protection. That means protecting the server as well as the workstation. It also means protecting against both known and unknown viruses.

From a financial standpoint, using combinations of stand-alone products may be burdensome, no matter how much protection is offered. Likewise, requiring endless hours of support and updating by network administrators is not a particularly efficient use of their valuable time.

The other important issue, ease of management, is unique to the enterprise. If it takes a significant amount of administrator time to keep protection current, it will be a burden on the network. If users are expected to keep their protection up to date, it simply won't get done. Centrally managed, enterprise-wide protection assures that cost per workstation is very reasonable, while enabling consistent deployment and management across the enterprise.

Enterprise-wide virus protection and management strategy should also provide the following:

- Scaleability for different network sizes, OSs, and configurations
- Simple, server-domain installation and easy or automatic maintenance
- Comprehensive protection at all intrusion points
- Transparent performance with little or no user intrusiveness
- Liberal licensing across the enterprise, including servers, workstations, stand-alone PCs, and home users
- Free virus pattern upgrades, easily downloadable and distributable

Once a strategy is defined, decision makers need to select the appropriate tools to implement it. These tools must be network-centric rather than PC-centric. In other words, they must first and foremost meet the requirements of the network in terms of technology, protection, management and cost. They must be designed to work together. A hodgepodge of different products from subnet to subnet offers no consistent protection at all. The solution should also be scalable to provide future protection as your network grows and the nature and number of intrusion points increases. Finally, the solution must be easy to manage. You want to be able to manage your virus protection resources centrally.

The LANDesk Virus Protect Solution

LANDesk Virus Protect is designed to combine virus firewall protection with centralized enterprise management.

Centralized management means simple, server-domain based deployment and configuration, server-based alerting and reporting, and the ability to generate custom graphical reports that integrate data from across the network. Comprehensive and compatible, LANDesk Virus Protect works with all Novell NetWare platforms and management consoles, and fully integrates with Intel's LANDesk Management Suite 2.0.

This integration means administrators have more time to do what they're there for: managing the network. They spend less time putting out fires caused by virus infections or distributing scan pattern files to hundreds or thousands of workstations.

Protection at the server

The Integrity Shield and Clean Room certification technologies are the primary line of server defense.

Intel pioneered server-based virus protection with the LANDesk Virus Protect NLM, which continuously scans all incoming and outgoing files including DOS, Windows,* OS/2, UNIX* and Macintosh.

The Integrity Shield expands this protection by preventing modification of key server files, while Clean Room technology prevents infected files from being placed onto the server or copied to a client. The result is a proactive virus firewall around the server that stops viruses from spreading.

In addition, The NLM rules-based traps stop known and unknown virus activity by detecting virus-like behavior on a server. The NLM can also be prescheduled to scan entire network volumes at convenient times or scan manually on demand.

Intel also invented real-time server based scanning in the original LANProtect product, and LANDesk Virus Protect 3.0 continues to provide leading technology. In the 3.0 release, the scan engine has been enhanced with the ability to decrypt mutation viruses and detect multiple strains and variations of a virus with fewer virus patterns.

Protection at the workstation

The virus threat on the workstation can be twofold: boot sector infectors residing on a floppy, and file infectors hidden in executables accessed from floppies, the network, modems and other intrusion points. Complete workstation protection needs to take into account both types of virus threats.

Intel provides software and hardware-based solutions to protect the workstation. LANDesk Virus Protect includes workstation software that protects against boot and file viruses after the PC has booted. It backs up the boot area at installation and checks for virus infections each time the PC is booted. LANDesk Virus Protect also offers on-demand scanning tools for DOS and Windows and two optional TSRs to provide real-time protection. One TSR (8.5 KB) uses a pattern-based scanning technique to identify files or floppy boot sectors carrying known viruses before DOS accesses them. Another TSR (14k) uses rules-based technology to trap known and unknown viruses as they are attacking a file or boot sector.

LANDesk Virus Protect includes a program called LDVPDOCK, which can be configured to automatically distribute desktop protection components and keep them up to date. Mobile users are protected with a stand-alone solution on the road and when they return to the network, LDVPDOCK automatically updates their virus pattern file, the scanner modules, and uploads any reports of virus activity.

WINProtect, a program for attached or stand-alone machines, includes a pattern-based scanner and a rules-based virus behavior trap. WINProtect uses the same powerful scan engine as the NLM to scan for known viruses on the desktop. Scans can be launched automatically from the system login script, the AUTOEXEC.BAT, or from Windows and can be scheduled to scan on a periodic basis.

In addition, Virus Protect licensing allows individual users to install workstation protection software on any networked or stand-alone PC, including portables and home systems. Additional workstation software is available to run pattern scans, protect boot areas, and watch for and stop virus-like activity.

Companion technologies

Because boot viruses load before DOS, booting from an infected floppy will infect the hard drive before any anti-virus drivers or TSRs can be loaded. In other words, if a PC is booted from an infected diskette and becomes infected with a boot virus, a software-only method would at best detect the known virus after

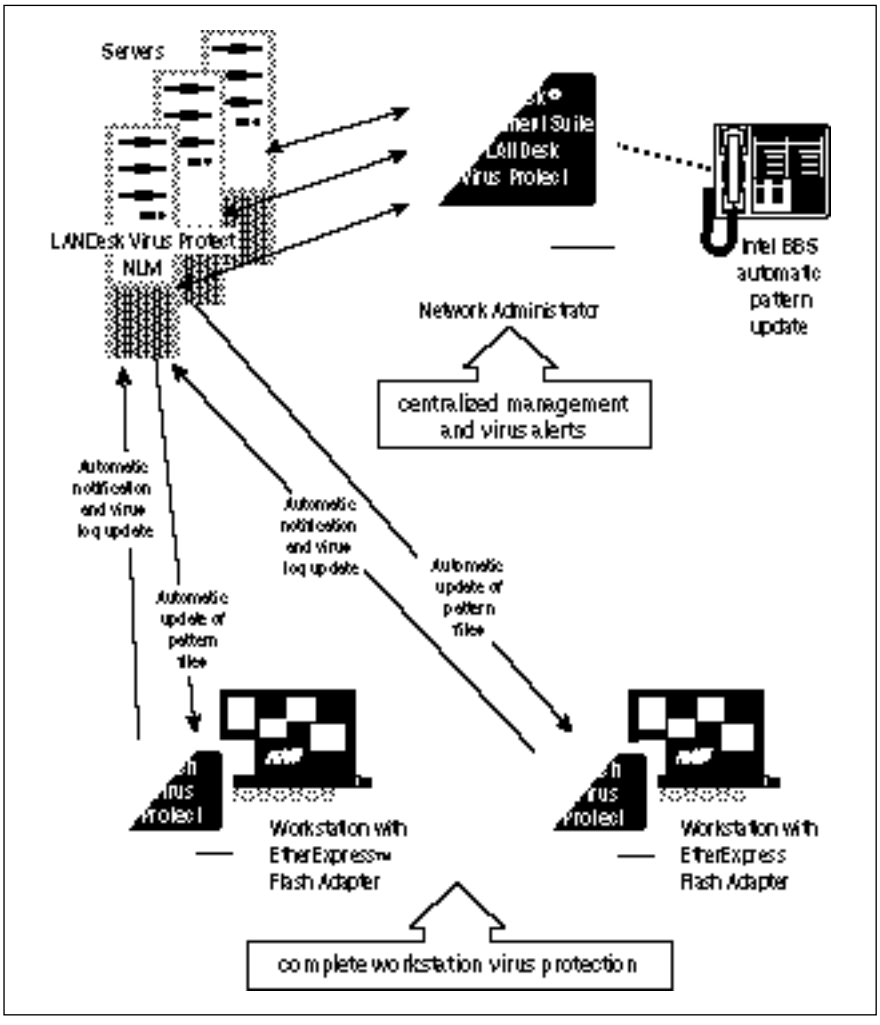
the infection had occurred. Thus, a hardware, pre-boot scanning approach, such as Intel's EtherExpress™ Flash adapter, is needed to provide protection from the workstation's hard drive.

The EtherExpress Flash adapter provides pre-boot protection by booting the PC from the flash memory on the adapter rather than booting from a diskette or hard drive that may contain a virus. Once the PC is booted from flash memory, Flash VirusProtect (a piece of code residing in the card's flash memory) scans the boot area and the entire contents of all local drives. The first time Flash VirusProtect is run, it backs up the hard drive's boot area and the system's CMOS information into flash memory. If a boot virus manages to corrupt the boot area (a condition which normally causes data loss), Flash VirusProtect can automatically restore the boot area and continue the boot process. This way, Flash VirusProtect prevents booting from an infected hard drive or floppy.

Intel LANDesk Virus Protect and Flash VirusProtect thus work in conjunction to provide the most comprehensive protection available at the workstation.

Centralized Management

Virus protection should be centrally managed, easy to update and, wherever possible, automatically manage themselves. LANDesk Virus Protect provides such centralized management with its simplified configuration and maintenance,



LANDesk® Virus Protect

- *Continuous virus firewall protection of file servers and workstations.*
- *Automated updates of virus pattern files from the Intel BBS to all file servers and workstations.*
- *Centralized configuration of virus protection, and enterprise-wide reports and audit logs of virus activity on servers and workstations, including Flash VirusProtect scan reports.*
- *Integrated tracking and reporting of virus alerts and event driven notification via beeper, pager, fax and e-mail.*

EtherExpress™ Flash Adapter

- *Flash VirusProtect provides pre-boot scanning of local drives; prevents booting from an infected hard drive or floppy.*

LANDesk Management Suite

- *Remote control of workstations to facilitate virus diagnosis and eradication.*
- *Shares common alert management system and reporting with LANDesk Virus Protect.*
- *Complete software inventory of file servers, DOS/Windows PCs and Macintosh computers to track anti-virus software installations.*

Figure 3. Intel products work together to provide comprehensive, enterprise-wide virus protection.

single-point control, and efficient use of the administrator's time and resources.

With LANDesk Virus Protect, entire server domains can be configured in a single step, and free virus pattern updates are automatically distributed across the enterprise from Intel's BBS. Centralized server-based alerting notifies administrators of virus activity via numerous alerting options, while centralized, graphical reporting integrates data from across the network.

LANDesk Virus Protect also integrates with Intel's LANDesk Management Suite 2.0, a set of applications that work together to enable task-level management of the entire network. LANDesk Management Suite provides a common task-oriented interface, strong data links between applications, common data bases and shared alert handling and reporting.

When combined with the LANDesk Management Suite, LANDesk Virus Protect gives administrators unmatched centralized management of enterprise-wide virus protection. LANDesk Virus Protect also snaps into Novell's NetWare Management System* (NMS) and ManageWise* for single-point control across the network.

In summary, mission-critical data resides on your company's networks today. Intel LANDesk Virus Protect gives you a robust enterprise-wide virus protection scheme that protects this data at an acceptable cost in both hard dollars and management time. By providing the dual elements of multiple overlapping protection and centralized management (Figure 3). Intel products work together to provide comprehensive, enterprise-wide virus protection – it's a virus firewall of protection.

Product	**Order Number**
Intel LANDesk® Virus Protect Single Server	SLAN1218
Intel LANDesk Virus Protect 4-Server Pack	SLAN1218-4
Intel LANDesk Virus Protect 20-Server Pack	SLAN1218-20
Single Server Upgrade	SLAN1218-U
4-Server Pack Upgrade	SLAN1218-4U
20-Server Pack Upgrade	SLAN1218-20U
FaxBack* Document	**Document Number**
Intel LANDesk® Virus Protect v3.0 Data Sheet	9558
Intel LANDesk Virus Protect v3.0 White Paper, "Virus Firewall"	5516

Intel Product Support Numbers

	U.S. & Canada	Europe	Asia-Pacific
Product Information	(800) 538-3373 or (503) 264-7354	+44-1793-431155	Singapore: +65-735-3811 Australia: +61-2-975-3300
Technical Support			
FaxBack*	(800) 525-3019 or (503) 264-6835	+44-1793-432509	Singapore: +65-256-5350 Australia: +61-2-975-3922
Intel Bulletin Board	(503) 264-7999	+44-1793-432955	Singapore: +65-256-4776 Australia: +61-2-975-3066
CompuServe*†	GO INTEL	GO INTEL	GO INTEL
Technician Support	(503) 629-7000	+44-1793-431144 (English) +44-1793 421777 (French) +44-1793-421333 (German)	Contact local dealer or distributor**

**In Singapore and Australia, request FaxBack document 9000 for a list of dealers and distributors

† Modem settings: 7-E-1, up to 14.4Kbps

Support files on the Internet

Intel FTP Server hostname: ftp.intel.com
Intel FTP Server IP address: 143.185.65.2
File directory location: /pub/PCandNetworkSupport
World Wide Web address (URL):
http://www.intel.com

Intel Corporation
5200 N.E. Elam Young Parkway
Hillsboro, Oregon 97124-6497

Printed on Recycled Paper

Part #C445.01