Managing Intelligent Tools Across the Corporation

A SYMANTEC CORPORATE SOLUTION

SYMANTEC.™

Table of Contents

Executive Summary 2

IT Professionals Face Many Problems 3

Current Tools Don't Provide a Complete Solution 4

New Tools Are Required to Manage Intelligent Tools Across the Corporation 5
- Best of Breed Intelligent Tools 5
- Proactive Solutions to Problems 5
- World-Class Support Organization 5
- Ongoing Utility Management 5
- Integration with Industry Standard Management Tools 5
- One Trusted Vendor Providing a Complete Solution 5

The Digital Immune System — A Proactive Approach to Keeping Systems Running Efficiently 6

The Digital Immune System Will Reduce Cost and Confusion With Central Management 8

The Digital Immune System — Solving Real-World Problems 10
- Policy Management 10
- Exterminate Malicious Code Before It Can Spread 10
- Keep Servers and Workstations Working at Peak Performance 12
- Solve Problems Remotely With pcAnywhere 13
- Mobile and Remote Users Are Part of the Corporation, Too 14
- Heading Off and Recovering From End-User Disasters 15
- System Stability 16

The Digital Immune System — Providing the Solutions You Need 17

About Symantec 18

Executive Summary

Information Technology (IT) departments are faced with challenges every day: problems that can threaten uptime, budgets, and the IT department's credibility.

> *"That problem with the email server's hard drive cost me half a day's work last week. And the solution turned out to be so simple."*
>
> *"We have users all over the country. It's breaking our budget sending technicians out to solve problems that could be handled remotely."*
>
> *"We just installed virus protection on everyone's workstation last month, and today the VP of Operations' system was hosed by a virus. That's embarrassing."*

Current solutions work well on individual servers and workstations, and there are means to distribute these solutions across the corporation, but there currently are no tools to insure that the solutions stay in place and function per IT and systems management policies.

Symantec is building the Digital Immune System™ to alleviate problems like these. The Digital Immune System will contain intelligent tools that keep systems running at peak performance and keep servers and workstations working at peak efficiency. It will protect corporations from virus attacks, while managing systems from a single central management console. The Digital Immune System will provide notification and proactive, solutions before problems cause lost productivity, while also providing on-going policy management to insure that IT specified policies and procedures are carried out.

This document explains:

- The problems faced by IT professionals
- That current tools don't provide a complete solution
- How new tools are required to manage intelligent tools across the network
- How the Digital Immune System is being designed to proactively keep system running efficiently
- How the Digital Immune System will reduce costs and confusion with central management
- How the Digital Immune System will solve real-world problems
- How the Digital Immune System is being built to provide the solutions you need

IT Professionals Face Many Problems

The IT community faces challenges every day keeping workstations and servers up and running. These challenges are accompanied by the demands of an increasingly complex IT environment and limited IT resources. In addition, IT professionals face a series of unknowns:

- Threats to systems uptime
- Threats to IT costs
- Threats to IT credibility

Threats to systems uptime take many forms. Mismatched software applications or incompatible DLLs on the same system, highly fragmented or corrupted hard drives, and viruses can cause workstations and servers to crash. Since many IT professionals are measured on fulfilling a Service Level Agreement (SLA) dealing with network availability, these threats are a significant issue for IT.

Every IT professional deals with threats to IT costs. Costs are incurred each time a system has problems and resources must be redirected to fix those problems. Given that IT time and money are limited, each time an end user or a server has a problem, resources are diverted from more strategic IT issues to problem solving.

Threats to credibility are perhaps the most serious for the IT organization. A high profile server goes down, perhaps one that provides email or network access. A senior executive encounters a serious virus on his PC, despite the anti-virus software deployed just weeks earlier. Problems like these can quickly erode the credibility of an IT organization. Decreased IT credibility within the organization can lead to IT management/organizational changes, outsourcing of IT functions, and diminished resource allocation. All of these diminish the ability of IT to be effective, to maintain SLAs, and to reach strategic goals.

Help desks respond to issues raised by end users. This means that they never start to solve a problem until it has negatively affected the end user's productivity. They do not have the tools to proactively identify and fix end user problems as they arise.

These problems come with the territory and IT organizations need strategies and robust tools to deal with them.

Current Tools Don't Provide a Complete Solution

Popular distribution management consoles provide a good means of distributing utility applications to workstations and servers across the corporation. But once they are installed, there is no guarantee that they will continue functioning as intended. It is very easy for users to turn off virus protection, for example, completely defeating the protection.

Current tools provide good solutions at the workstation and server level. Current anti-virus products provide virtually fool-proof protection, if they are running. Disk defragmentation tools can keep a hard drive at peak performance, if they are used. However, neither of these tools does any good if it is not used correctly.

Once installed on the desktop, these tools are out of the control of the IT department, and at the mercy of the users. There is no way to insure that the anti-virus program distributed to all workstations in a corporation is functioning properly, nor is there a practical way to insure that disk defragmentation tools are run at the appropriate times.

Anti-virus vendors make updated virus definitions available on a regular basis. They may even have a method to proactively deliver these files to client organizations. But distributing these files throughout a corporation remains a multi-step process that must be managed and carried out on a regular basis.

When a virus strikes, several things need to happen:

- The suspect file must be quarantined.
- The responsible IT professionals must be notified.
- The suspected file should be sent to the anti-virus vendor for analysis.
- The virus solution must be received from the anti-virus vendor.
- The virus solution must be distributed across the corporation.

There are tools that can assist with each of these procedures, but there are no current tools that manage the entire process.

New Tools Are Required to Manage Intelligent Tools Across the Corporation

What are the attributes of a set of tools that would solve these problems?

Best of Breed Intelligent Tools

A solution cannot be considered complete unless the components each solve the problems they are designed to solve. Each component must be at the top of its class.

Proactive Solutions to Problems

Solving problems after they affect productivity wastes time and money. Intelligent tools must recognize problems before they cause lost time, and must be able to propose effective solutions.

World-Class Support Organization

The solutions must be backed up by a support organization that can provide solutions to new problems, such as new virus strains, in a timely manner.

Ongoing Utility Management

There are many ways to distribute software throughout a corporation. What is needed is a way to insure that intelligent tools continue to work effectively. This requires on-going policy and systems management.

Integration with Industry Standard Management Tools

A good utility management solution should be able to integrate into the familiar operating environment of the corporation's current set of management tools. There should be no reason for users to have to implement and learn an entirely new set of management tools.

One Trusted Vendor Providing a Complete Solution

A complete suite of intelligent tools should be available from one trusted vendor, so they work together and leverage each other.

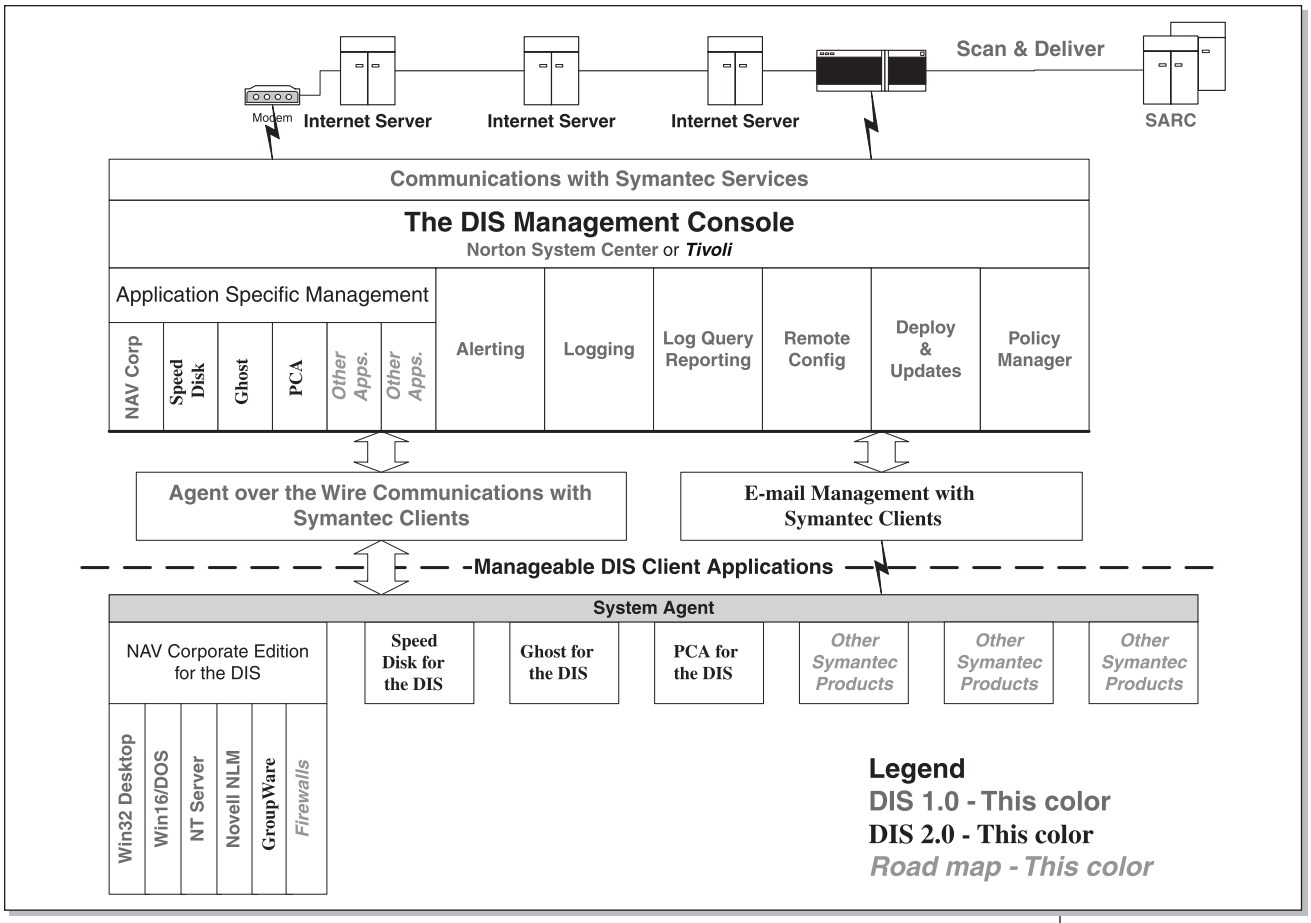
The Digital Immune System – A Proactive Approach to Keeping Systems Running Efficiently

Symantec is building the Digital Immune System to offer a suite of products that address many of the problems IT professionals face every day. The Digital Immune System will recognizes a variety of potential problems on systems and then be able to takes steps to solve the problems proactively, thus preventing a call to IT and possible downtime. Administrators will be able to control the level of the Digital Immune System's proactivity to suit the needs of their organization. The Digital Immune System is also being designed to provide the best solution to handle many of the help desk calls that occur.

The Digital Immune System management console will provide administrators with an easy way to install and manage these tools, so the solution does not create additional costs or resource demands. The first release of the Digital Immune System will feature the Norton AntiVirus family of products. As development continues, other Symantec best-of-breed products will be added. From one central management console, administrators will be able to configure domains, install and configure the Digital Immune System products, manage events with alerts and automated actions, and perform remote operations.

All the Digital Immune System products are being integrated so that they can be used individually or together, as they are needed. Every Digital Immune System product will be manageable from a common central console. IT professionals will be able to install, configure, manage, and maintain every component. Whether the products' automated features are on or off, Digital Immune System will provide the best set of tools for the corporation.

The following illustration shows Symantec's current architecture plan for the Digital Immune System. The client tools, or applications, such as Norton AntiVirus™ Corporate Edition and Norton Speed Disk™ will communicate with the Digital Immune System System Agent on the client computer. The System Agent will communicate with the Digital Immune System management console over the network, or in the case of mobile users, via email.



The Digital Immune System management console will provide specific interfaces for each managed tool for managing the configuration of those tools on the clients. The Digital Immune System management console will also provide alerting, logging, reporting, remote configuration, deployment, and updating services.

The Digital Immune System management console will contain the ability to communicate with Symantec to send potentially malicious code to the Symantec AntiVirus Research Center (SARC)™, to receive solutions from SARC, and to receive updates (via LiveUpdate™) to the Digital Immune System components.

The Digital Immune System Will Reduce Cost and Confusion With Central Management

The Digital Immune System is being designed to provide the system management capabilities that integrate with Microsoft® Management Console for a familiar look and feel. The Digital Immune System will also integrate with enterprise system management frameworks such as Tivoli® Enterprise Console so corporations can leverage the implementation and training investment made in these products.

The management console will provide discovery of connected systems, easy configuration of domains, and simple distribution and management of Digital Immune System components. The management console will be able to discover systems across Windows NT® and NetWare® networks. Discovered systems can be arranged in domains by location, server type, or other logical groupings.

Domain groupings will enable managing systems as groups. Client configuration can be done at the domain, server, multiple server, and individual client level. Both local and remote sites and domains can be managed from the Digital Immune System console.

The Digital Immune System is being designed as a cross-platform management tool. The Digital Immune System console will be able to manage and distribute Digital Immune System components to the following client operating systems:

- MS-DOS
- Windows 3.x
- Windows 95
- Windows 98
- Windows NT Workstation
- Windows NT Server
- NetWare

The Digital Immune System will use events, alerts and actions to provide proactive solutions to problems. The automation level will be configured at the Digital Immune System management console, for example, when a client workstation detects a possible virus, that event will trigger it to send an alert to the Digital Immune System console. An alert can trigger any or all of the following actions:

- The file with the suspected virus is quarantined.
- The event is recorded in the log.
- An email is sent to the responsible IT professionals to notify them of the problem.
- A page is sent to the responsible IT professionals to notify them of the problem.
- The file with the suspected virus is sent to the Digital Immune System console.
- The Digital Immune System console forwards the file with the suspected virus to SARC for analysis.

When the virus definition is received back from SARC, several things can automatically happen:

- The event is recorded in the log.
- An email is sent to the responsible IT professionals to notify them of the arrival of the solution.
- A page is sent to the responsible IT professionals to notify them of the arrival of the solution.
- The virus definition is automatically distributed to the client that experienced the problem.
- The virus definition is automatically distributed to all Digital Immune System clients.

The automation provided by the Digital Immune System can be tailored to the needs of the site. In some cases, where full-time monitoring is not available, more complete problem-solving automation may be desired. Sites that are monitored may prefer to have the Digital Immune System provide alerts when problems are detected, and have the responsible IT professional initiate corrective actions. Because the Digital Immune System will have the ability to send notifications in several ways, including Windows NT notifications, email, and paging, the management console will not require a full-time operator.

The Digital Immune System—Solving Real-World Problems

The Digital Immune System is being designed to solve the real-world problems experienced by IT professionals on a day-to-day basis. It will help reduce downtime, help reduce costs, and help maintain IT's credibility.

Policy Management

The International Computer Security Association (ICSA) study Virus Costs vs. Various Protection Strategies reports that implementing full-time virus protection versus periodic scanning can reduce virus-related costs by 88%.[1]

The Digital Immune System is being designed to provide the policy management and enforcement your corporation needs. The Digital Immune System tools will be able to be configured before and after deployment. Configuration settings can be locked down so users cannot change them. Alternately, client configuration settings can be monitored by the Digital Immune System, and actions initiated when changes are made. These actions can range from logging the change, alerting the Digital Immune System console monitor, or resetting the client configuration.

Client configuration will be able to be managed several ways. All client settings can be "locked down" so they cannot be changed by the user. Alternately, client systems can be configured by the management console and then monitored. If a user makes a change, for example, turning off real-time virus protection during installation of new software, an alert will be sent to the Digital Immune System management console. The alert can trigger an action of re-setting the virus protection during the following night to insure the workstation does not remain unprotected if the user forgets to re-enable the virus protection.

Client configuration can be audited at any time by the Digital Immune System management console to ensure that established policies are being followed. This provides an additional option for client management.

Exterminate Malicious Code Before It Can Spread

According to the ICSA 1998 Computer Virus Prevalence Survey, 99% of organizations encountered viruses in 1997, and 37% of organizations had a "virus disaster," defined as 25 or more computers infected by an outbreak of malicious code.[2]

The first version of Digital Immune System ready software will be the Norton AntiVirus™ family of products. Symantec's Norton AntiVirus Corporate Edition provides state-of-the-art protection from malicious code to your entire corporation. It can identify and disinfect viruses and other malicious code—even malicious code it has not previously been exposed to.

---

1. citations for this study, i.e., full author, date of publication, where published

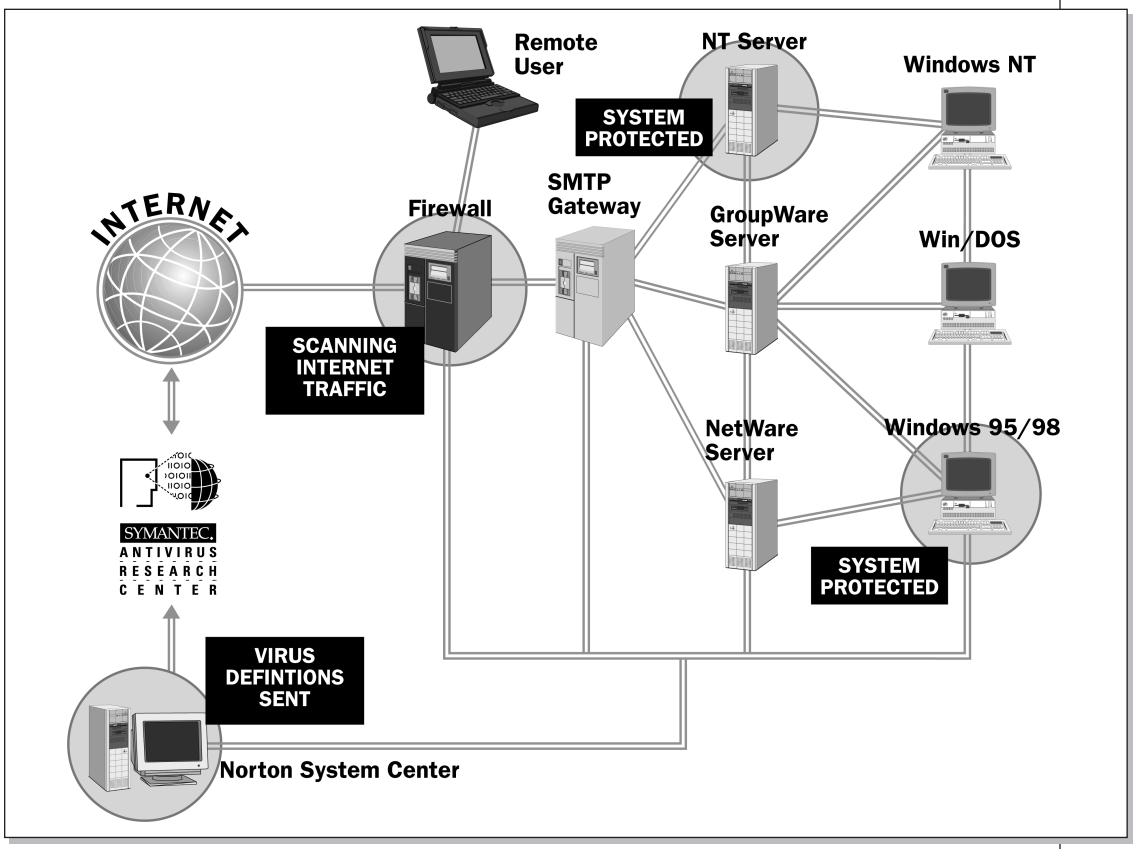
2. citations for this study, i.e., full author, date of publication, where published

Norton AntiVirus provides protection at all the points through which malicious code can enter your network, with the following products:

- Norton AntiVirus Corporate Edition 7.0
  - Windows® 95/98
  - NT Workstations
  - Windows NT® Server
  - NetWare®
  - Windows 3.x
  - DOS

- Norton AntiVirus, Microsoft® Exchange

- Norton AntiVirus, Lotus Notes®
  - Windows NT
  - Solaris®
  - AIX®
  - AS/400®
  - Os/390®



Norton AntiVirus protects the entire enterprise

- Norton AntiVirus Internet Gateways and Firewalls.

Note: Not all these products will be available with the first release of the Digital Immune System which is targeted for late 1999.

Symantec's Bloodhound™ technology identifies unknown malicious code using heuristics. When unknown malicious code is recognized, the file is quarantined, and an alert will be raised at the Digital Immune System management console. The Digital Immune System will also be able to initiate several different responses. For example, email or paging can notify the responsible parties. The malicious code can be forwarded to the management console, ready to send to SARC, or the malicious code can be sent automatically to SARC for analysis.

Once the SARC receives the suspected malicious code, it will analyze the code using technology licensed from IBM®, create a virus definition, and return it to the Digital Immune System management console. The Digital Immune System management console will then distribute the virus cure to all users automatically.

This proactive response to malicious code will prevent its spread across the network. Because the SARC response is so fast (between two and eight hours), malicious code will be controlled before it spreads.

When a new virus definition is not enough to stop a new type of malicious code, SARC will create a new NAVEX™, or Norton AntiVirus Extension. NAVEX is updated scanning code that is dynamically added to Norton AntiVirus. Because of the NAVEX technology, the Digital Immune System will be able to distribute updated scanning code without a complete reinstall of Norton AntiVirus. This means that improved scanning is available immediately without the cost and time delays of waiting for a new version of anti-virus software.

Keep Servers and Workstations Working at Peak Performance

Tests have shown that disk access time can double on a badly fragmented drive. Active servers' drives can become fragmented quickly due to the amount of data moving on and off. Fragmentation can degrade the performance of groupware applications, needlessly wasting users' time.

File fragmentation means that a file's data is distributed over scattered areas of the disk surface. Because fragmented files are stored on clusters scattered over the disk surface, reading and writing their data requires multiple passes of the disk's heads.

Disk fragmentation is the inevitable result of normal computer use. It slows file access and thus slows computer operation.

While slow disk performance can be an annoyance on a workstation, it can quickly become a crippling condition in a corporate environment. On servers performing thousands of file operations per minute and used simultaneously by many users, disk fragmentation can dramatically reduce system performance.

To regain maximum performance from computer disks, the files and free space must be defragmented. Norton Speed Disk™ optimizes disks by defragmenting files and free space.

Norton Speed Disk rearranges individual files on the disk so that they occupy contiguous clusters, optimizing access to the data. It consolidates the unused space on the disk so that there are fewer, larger areas of free space, thus allowing new data to be written to contiguous clusters.

Unfortunately, even after disk optimization, fragmentation can recur the moment files are modified. To maintain optimal disk performance, defragmentation with Speed Disk should be a regular part of system maintenance.

A Digital Immune System ready version of Norton Speed Disk is targeted for release in the first half of 2000. Managed from the Digital Immune System management console, Speed Disk will be able to monitor drives for fragmentation. When the fragmentation exceeds set limits, an alert can be sent to the Digital Immune System management console. The alert can trigger automated functions that notify responsible parties, or it can automatically schedule Speed Disk to defragment the drive during off-peak time. Speed Disk runs in the background without interfering with normal system operation.

The same Digital Immune System technology that will insure that servers stay at peak performance will also benefit end users by monitoring and automatically defragmenting their local workstation drives. Each action that the Digital Immune System takes will be logged and can alert the management console operator to identify growing problems before they cause a loss of productivity.

Solve Problems Remotely With pcAnywhere™

It can cost hundreds of dollars for an IT professional to make a site visit to fix a problem in an end user's system. The Digital Immune System is being designed to provide notification of impending problems before they cause lost time, as well as provide a means to fix problems on remote machines without a site visit. A Digital Immune System ready version of pcAnywhere is targeted for release in the first half of 2000. PcAnywhere provides the tools to remotely manage servers and workstations.

With pcAnywhere, the Digital Immune System will provide the ability to monitor, manage, and troubleshoot remote servers. pcAnywhere integrates with Windows NT security to provide secure management of remote servers. It enables access to data across LANs and WANs supporting a wide range of network connections including TCP/IP, NetWare IPX/SPX, NetBIOS, Banyan Vines, ISDN and NetWare Connect (ASI). It also supports a wide range of modems and devices including TAPI/Unimodem, as well as ASVD and DSVD.

PcAnywhere is the perfect solution for remote training and support requirements. It can solve user's problems remotely, and provides the ability to switch between voice, remote control and video conferencing at the touch of a button.

Besides the benefits that it provides to IT, pcAnywhere also provides benefits to end-users. Mobil users and telecommuters benefit from the following pcAnywhere features:

- ***Fastest, easiest access to an office PC from anywhere.*** Connect to an office PC from home or the road.
- ***Remote control.*** Manage an office PC from anywhere; over the phone, LAN or WAN or the Internet.
- ***File transfer.*** Quickly transfer and synchronize files between two computers.
- ***Drag-and-drop connections.*** Automatically establish a connection by dragging a program icon from your office PC to your remote PC.
- ***Plug-and-play support.*** pcAnywhere will know what kind of computer and model you are using.
- ***Support for the latest, fastest hardware.*** Users will minimize their online connection time.

Mobile and Remote Users are Part of the Corporation too.

A large and growing segment of users are mobile or remote. These users require the same level of support and access to the same information as users directly connected to the network. Through a combination of server-based delta technology and client-based update agent technology, Symantec Mobile Update™ technology adds intelligence to policy and configuration updates by automatically offering a seamless way of receiving changes to corporate documents.

Symantec Mobile Update technology serves mobile and telecommuting professionals, who rely on the most up-to-date information, but who are not always connected to the network to access changes. In addition, mobile and remote users are challenged with both slow connection speeds to the network (typically 28.8 Kb/sec modem), as well as the complexities of getting and staying connected. The Symantec Mobile Update solution comprises a server portion (for tracking files on the network and processing changes) and a client portion (for incorporating changes on the client).

The Symantec Mobile Update Server acts as an electronic assistant on the network, tracking configuration changes. When it detects a change, it checks the integrity of the file, then decides whether it needs to deliver the actual changes or simply send notice of a file change.

For mobile professionals, this means making one connection to the network to receive all messages and configuration updates. It also means that the size of the attachment is a fraction of the size of the full file, containing only the changes to be applied. By simply checking email—a task that is familiar, secure, and reliable, users receive all the information they need to stay current.

Heading Off and Recovering From End User Disasters

By definition, end user disasters cause lost time and productivity. An IT professional's first priority is to avoid these disasters, but when they occur, a quick solution will minimize lost time and the IT resources required to fix them.

Symantec's Norton Utilities™ is a set of intelligent tools that can help maintain system stability. Norton Utilities technology not only finds problems, it also suggests ways to fix them. This process can be run manually, or it can be scheduled to perform periodic maintenance. It provides extra protection by fixing unsuspected corruption in the Windows registry.

Norton Utilities technology will head off most end user disasters before they occur. But when disasters do occur, a quick recovery is in order. Help desk professionals can use disk cloning to correct a corrupted system, replacing the hard disk with a refreshed image or perhaps even using the opportunity to upgrade the user to a newer configuration.

Norton Ghost™ is a disk and/or partition-copying program that enables IT professionals to perform the following important tasks:

- Copy the entire contents of one hard drive to another.
- Create an image file of one drive, and use this image to create clones of the original.
- Copy the contents of one partition to another.
- Create an image file of a drive partition that can be used as a template to create other partitions.
- Reimage a remote drive to quickly recover from a disaster.
- Reimage a remote drive, then reapply the user's configuration.

Norton Ghost further lightens the burden by automatically taking care of the most time-consuming aspects of installing and configuring PCs, including dynamically resizing FAT12, FAT16, FAT32, and NTFS partitions as needed, and performing disk formatting on the fly. Manual procedures involving the FDISK and FORMAT commands are things of the past. Likewise, when the source and target disks are different sizes, Norton Ghost adjusts the position and size of the partitions automatically.

By using an advanced image compression system, Norton Ghost significantly reduces the amount of space required to store an image file. In fact, images may be compressed up to 70% depending on the compression method selected, as well as the contents of the partition or disk. Norton Ghost performs a Cyclic Redundancy Check (CRC) on the files to detect any corruption and is capable of verifying that a replicated disk contains the same files as the original. Image files can also be password protected for additional security.

Depending on the needs of the organization, image files can be easily saved to local or network drives, as well as removable storage devices such as JAZ® drives, ZIP® drives, CD-ROM, or other removable media. Norton Ghost permits a disk or partition image to be split across multiple volumes, prompting the user to insert another disk (or other media), or permitting the selection of an alternate location. Norton Ghost images can also be saved to, and loaded from, SCSI tape systems, providing an ideal means for implementing a robust disaster recovery solution.

Norton Ghost excels in its user interface, offering both a GUI interface for interactive operation and a powerful batch mode for automating repetitive tasks, such as when image files must be downloaded to a large number of workstations.

Norton Ghost excels in flexibility, featuring the ability to store an image on another hard drive, network drive, CD-ROM, or JAZ or ZIP drive. The software supports every important file system in use today, including FAT12, FAT16, FAT32, NTFS, HPFS, UNIX®, and Novell®. A Digital Immune System ready version of Norton Ghost is targeted for release in the first half of 2000.

System Stability

Every time an end user's computer crashes, time is lost. In many cases, a significant amount of unsaved work can be lost by a simple program crash.

PC crashes are inevitable, but Norton CrashGuard™ intercepts not only program crashes (the most common type of crash) but also many system freezes, "blue screens," and system crashes.

Norton CrashGuard will report program crashes to the Digital Immune System Console so problems that cause recurring crashes can be solved. A Digital Immune System ready version of Norton CrashGuard is targeted for release in the first half of 2000.

The Digital Immune System — Providing the Solutions You Need

The Digital Immune System is a growing technology, which Symantec is designing to provide anti-virus, disk performance, and remote control services for large-scale corporations. Digital Immune System tools will facilitate faster, even automated, problem solving for a variety of workstation and server issues. A central management console will make it easy to install and administer the Digital Immune System in a large organization, and across a variety of workstation and server platforms.

Because the Digital Immune System will provide a set of tools, and not a bundle, you will need to purchase only the tools you require. Other tools can be added and easily deployed whenever you need them.

The Digital Immune System will contain the following core tools:

- Norton AntiVirus provides desktop and server protection from viruses and other malicious code. (Digital Immune Ready Norton AntiVirus is targeted to release in late 1999.)

Because the Digital Immune System is modular, additional tools can be added as needed. In future revisions, the following tools will be added to the Digital Immune System:

- Norton Speed Disk for disk optimization. (Digital Immune Ready Norton Speed Disk is targeted to release in the first half of 2000.)

- PcAnywhere for remote control of servers and workstations. (Digital Immune Ready pcAnywhere is targeted to release in the first half of 2000.)

- Norton AntiVirus clients for Notes and Exchange Server, Norton CrashGuard for system stability. (Digital Immune Ready Norton CrashGuard is targeted to release in the first half of 2000.)

- Norton Utilities for identifying and solving Windows problems. (Digital Immune Ready Norton Utilities is targeted to release in the first half of 2000.)

- Norton Ghost for drive imaging and disaster recovery. (Digital Immune Ready Norton Ghost Disk is targeted to release in the first half of 2000.)

Simply stated, the Digital Immune System will provide "intelligent tools that keep systems running at peak performance" to ensure that systems stay up and running at optimal levels, allowing IT to focus on more strategic issues and reducing the costs associated with systems downtime. The Digital Immune System will provide a core set of tools that will grow as the needs of the IT community grow.

The Digital Immune System is being designed to keep your organization's workstations and servers up and running at peak performance. Whether it is finding and fixing a virus problem before it is noticed, optimizing a server's hard drive, or solving a crash problem in seconds by finding mismatched DLLs, the Digital Immune System will address threats to uptime, IT costs, and IT credibility.

About Symantec

Founded in 1982, Symantec Corporation is the world leader in utility and communications software for business and personal computing. More than 50 million people worldwide use Symantec products. And Symantec products occupy the number one or two position in every software category in which they compete – categories like Java™ development tools and utility and mobile worker software, that Symantec created with its innovative, first-to-market solutions.

Symantec is dedicated to providing its customers with the highest-quality, most cutting-edge software products available, and the superior service and support to back them up. With its charter to create products and solutions that maximize user productivity and minimize support from IT, Symantec is poised to build upon its 15 years of market excellence and leadership.

Notes

Notes

WORLD HEADQUARTERS
10201 Torre Avenue
Cupertino, CA 95014 USA
1 (800) 441-7234
1 (541) 334-6054
World Wide Web Sites Corporate:
http://www.symantec.com
Symantec Mobile Essentials
http://www.symantec.com/mobileessentials

Australia (Sydney): +61 3 9850 1000
Australia (Melbourne): +61 3 9823 6204
Brazil: +55 11 530 8869
Canada: 1(416) 441-3676
France: +33 1 41 38 5700
Germany: +49 n2102 7453 0
Hong Kong: +852 2528 6206
Italy: +39 2 69 5521
Ireland: +353 1 820 5060
Japan: +81 3 3476 1156
Korea: +82 2 3452 1600
Malaysia: +60 3 7567662
Mexico: +52 5 661 7978
New Zealand: +64 9 309 5620
Netherlands: +31 71 535 3111
Russia: +7095 238 3822
Singapore: +65 239 2000
Sweden: +46 8 457 3400
Switzerland: +41 71 626 20 40
South Africa: +27 11 804 4670
Taiwan: +886 2 729 9506
UK: +44 1628 592 222

We've described our current plans for our proposed Digital Immune System, however, plans and targeted release dates may change. We encourage you to contact us for the latest information. Call 1-800-745-6045 or visit www.digital-immune-system.com

SYMANTEC.™