The Symantec Enterprise Papers
Volume XXX

Understanding Symantec's Anti-virus Strategy for Internet Gateways

SYMANTEC.

Table of Contents

Introduction

The exponential increase in the use of the Internet brings with it a pandemic of computer virus attacks. As more of the world begins to operate on "Internet time," the click of a button may spread a computer virus around the globe in hours, if not sooner.

Consider a polymorphic virus, Hare.7610. It originated in New Zealand yet infected computers in South Africa and Canada within six days of its release via the Internet "into the wild" in July 1996.

Consider also macro viruses, the demon spawn of the Internet. Macro viruses infect documents, spreadsheets, and templates generated by Microsoft Word and Microsoft Excel. According to the Symantec AntiVirus Research Center™ (SARC), macro viruses have become the most prevalent type of computer virus since their first appearance in August 1995, spreading like wildfire when users share infected documents or distribute infected documents as attachments to electronic mail.

How bad is the macro virus problem? Email accounts for 23 percent of all virus incidents, according to a 1996 study by the National Computer Security Association (NCSA). By comparison, file downloads account for 11 percent of all virus incidents.

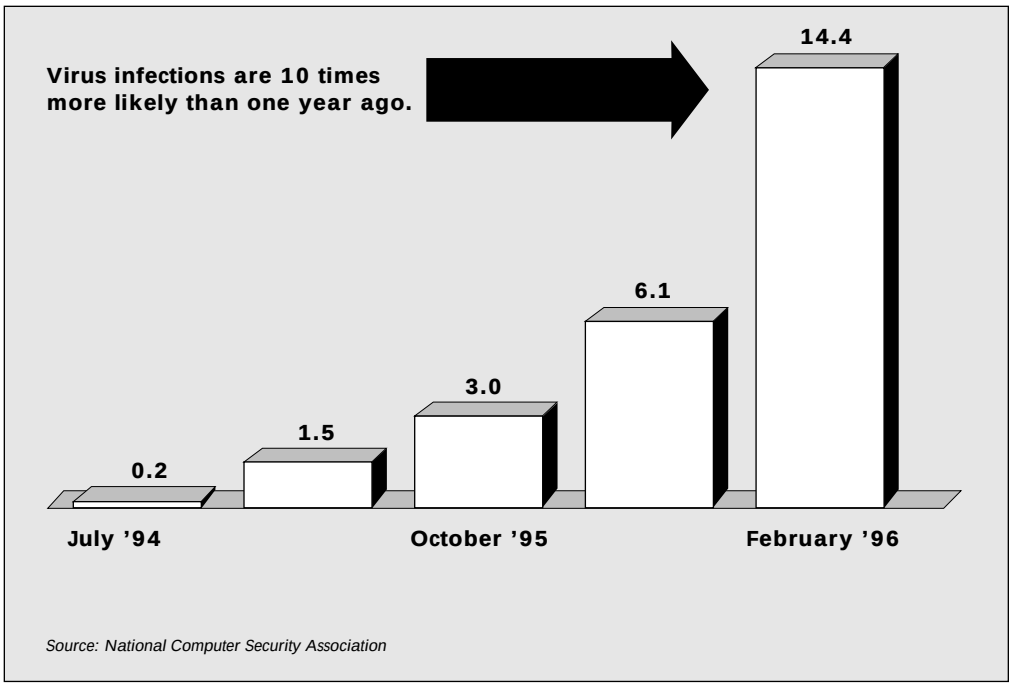

Figure 1. Number of Virus Encounters per 1,000 PCs per Month

In fact, it is now rare to find a corporate network that is not under attack. A remarkable 98 percent of all corporations experienced virus problems during the 14-month period addressed by the 1996 NCSA study, and virus infections are ten times more likely today than one year ago.

Each attack by a virus on a corporate site costs an average of $8,106, according to the NCSA. Even more costly is the amount of time spent recovering completely from a virus incident—more than 44 hours.

Simply, the accelerating use of the Internet has changed the demands on virus protection. Intranets—corporate networks that use Internet technology—bring similar change. More change is coming.

Each attack by a virus on a corporate site costs an average of $8,106, according to the NCSA.

This white paper provides an overview of what Symantec has done—and is doing—to protect Internet and intranet users. It also introduces two new products designed to defend Internet and intranet users: Norton AntiVirus™ for Firewalls and Norton AntiVirus for Internet Email Gateways.

The Evolution of Viruses

Consider the similarities of biologic and electronic viruses.

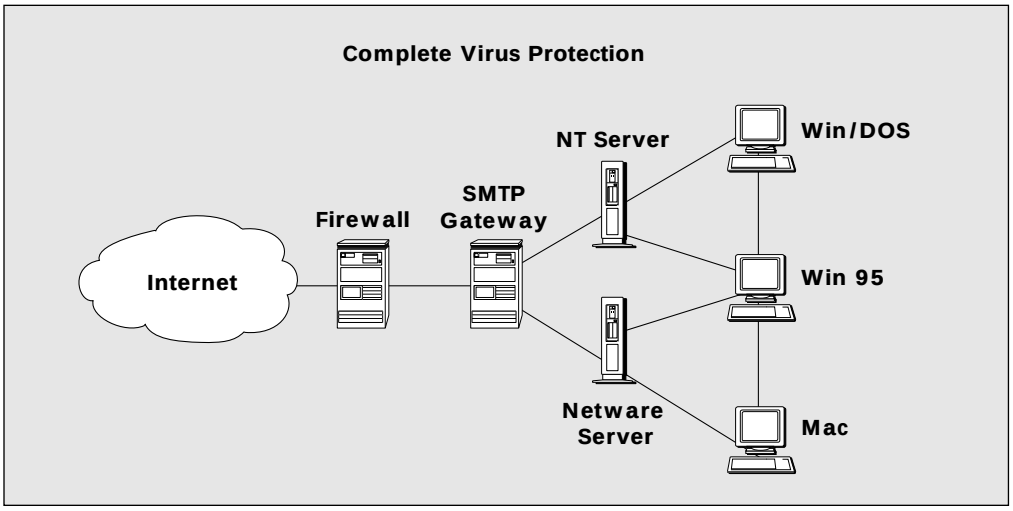

Figure 2. Virus protection is evolving to cover gateways, servers, and desktops.

Biologic viruses 500 years ago were transmitted from community to community by travelers on foot or on horse. A traveler reaching a city triggered a major outbreak. The Age of Discovery introduced a second level of threat as explorers set sail from continent to continent, introducing new diseases to native populations, bringing new diseases back to Europe. The Industrial Revolution began a third level of threat as steamships and trains compressed an entire era into months or weeks. Today, intercontinental flight means a virus can travel in hours from North Africa to the United States to Asia.

Similarly, the first electronic viruses traveled from personal computer to personal computer on shared floppy disks carried by users. This led to the introduction of such products as Norton AntiVirus for DOS/Windows, Norton AntiVirus for Windows 95, Norton AntiVirus for Windows NT Workstation, and Symantec AntiVirus™ for Macintosh.

These desktop protectors first kept a standalone computer free from viruses on shared floppy disks and boot-up system files. Over time, as the desktop environment evolved, desktop anti-virus programs added new technologies that protect against attacks from infected CD-ROMs, compressed files, files downloaded from bulletin boards and the Internet, and email attachments—all the ways a desktop can be infected by a computer virus.

Networks that connect desktops to servers introduced a second level of electronic threat. Norton AntiVirus for NetWare and Norton AntiVirus 2.0 for Windows NT extend desktop protection to the server, local area networks, and enterprisewide networks. These products protect the server from virus attack by detecting the virus before an infected file is copied to the server from a desktop workstation. They are effective against the transmission of viruses between workgroups and LANs.

The stampede to the Internet; the adoption of the Internet as a tool for commerce, communication, research, and entertainment; and the proliferating popularity of the World Wide Web introduce a third level of threat from electronic viruses. Simply, the Internet eliminates the boundary between the corporate network—and the rest of the electronic world. The ability to transmit and share information is instantaneous, just as intercontinental flight might seem to a long-ago traveler on foot or horse.

To guard the door to the outside world, corporations today deploy Internet firewalls and email gateways. Norton AntiVirus for Firewalls and Norton AntiVirus for Internet Email Gateways protect the internal network from unwanted invasions from the outside, yet permit internal users to search out and collect information, send and receive electronic mail, transact sales, or track and order inventory from suppliers, among other applications.

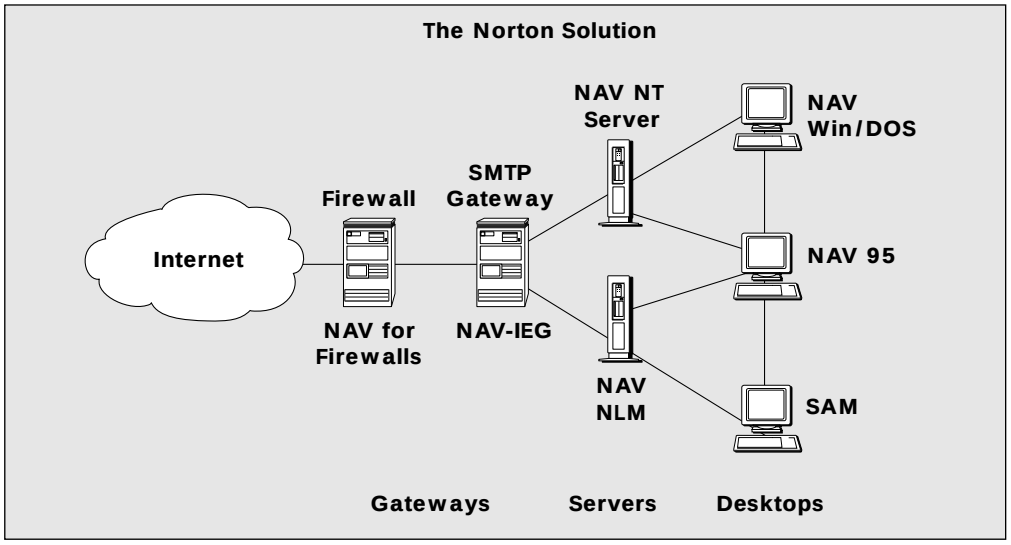

Figure 3. Symantec's anti-virus products are evolving to protect desktops, servers, and gateways.

The Internet eliminates the boundary between the corporate network—and the rest of the electronic world.

The ideal solution must integrate desktop, server, firewall, and gateway protection. Anti-virus products designed for the desktop alert the desktop user, but not the LAN administrator. In contrast, anti-virus products designed for use on a server, firewall, or gateway alert the sender, receiver, and LAN administrator.

Consider this all-too-common scenario. Joe, working at home, creates a document on a computer infected with a macro virus. The virus infects Joe's document. Joe copies the document to a floppy and, at work the next morning, attaches the infected document to email, which he sends to his workgroup and, via the Internet, to selected customers. Without a desktop anti-virus program installed, the macro virus spreads to Joe's desktop system at work. Without a server anti-virus program installed, the macro also spreads to Joe's workgroup. Without gateway and firewall anti-virus protection, Joe's customers are also at risk when they connect to the Internet via a network that is not protected against Joe's incoming infected message.

Firewall and Gateway Virus Scanning Architectures

In a survey by Symantec, 8 of 10 Fortune 500 companies called for multiple layers of anti-virus protection for firewalls and gateways. The most critical concern was the ability to stop viruses at the firewall or gateway without affecting system performance—a requirement met by only one of the three basic architectures for incorporating virus-scanning technologies into firewalls and gateways.

Classical Proxy Virus Scanners

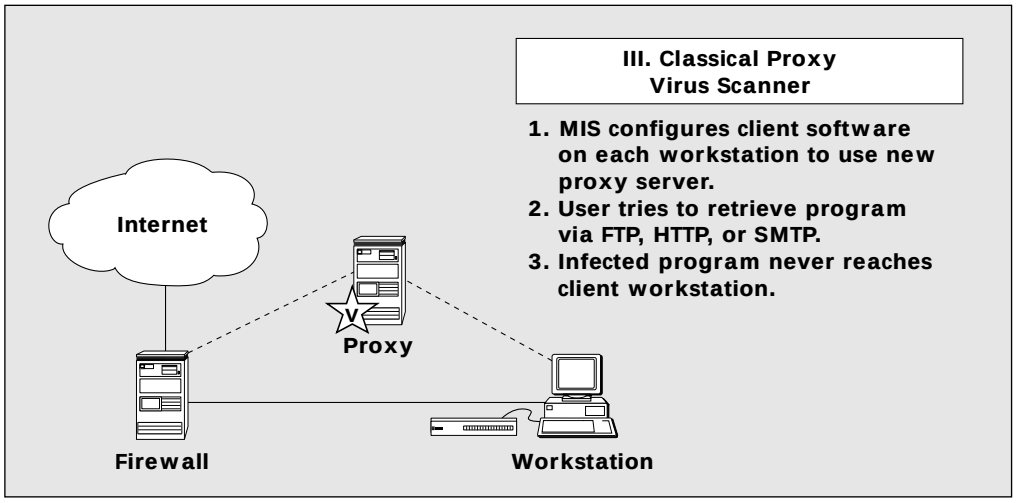

Figure 4.

The first of the three architectures is the classical proxy virus scanner. This architecture requires the installation by LAN administrators of client software at each workstation. LAN administrators must also configure that client software to use a proxy server—a second computer that processes all requests from the first. The server becomes a go-between to the outside network. It retrieves data for the client, scans it for viruses, and provides uninfected data to the workstation.

This is not a foolproof way to protect a firewall or gateway. It's easy to add a new machine to the network, but LAN administrators must configure every client to use the proxy. What's more, users can bypass the protection of the proxy server if the firewall is not properly configured.

Firewall with Onboard Virus Scanner

This second architecture integrates virus-scanning technologies with an existing firewall product. No additional server is required. LAN administrators do not have to install and configure each client.

In this approach, the firewall intercepts all data requests. It scans for viruses and provides the client workstation with uninfected data. However, the firewall can quickly become a bottleneck, bogging down as it scans all network and Internet traffic.

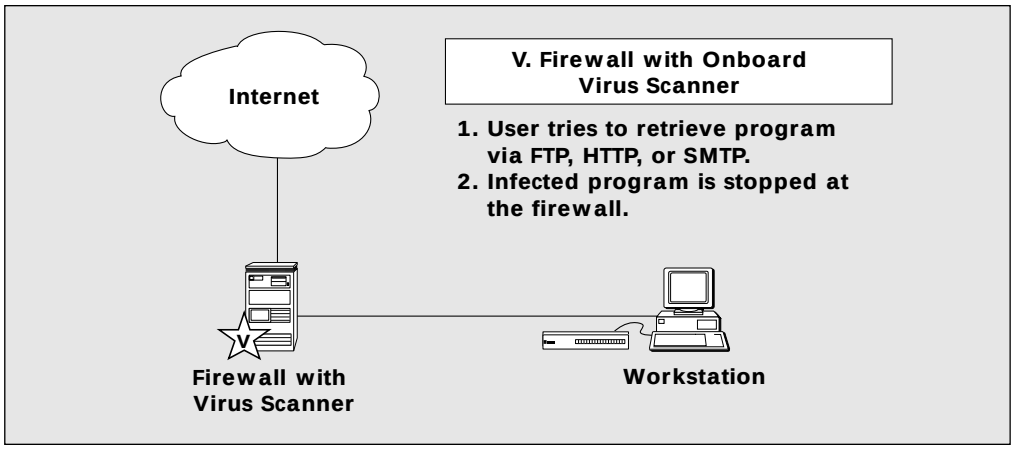

Figure 5.

Firewall with Intelligent Scanning Architecture (ISA)

This third architecture resolves the flaws inherent to the other approaches.

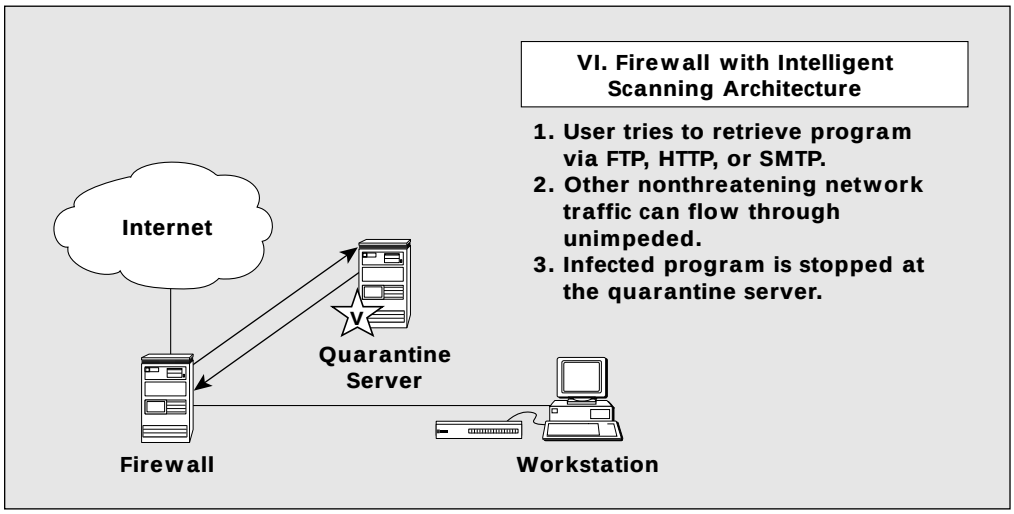

Figure 6.

The firewall and anti-virus server is flexible, supporting separate scanning policies for inbound and outbound traffic, and scanning only preselected files, which in turn helps maintain peak network performance.

A firewall with an intelligent scanner shifts virus scanning requests to a separate computer. The firewall directs only suspicious traffic to the anti-virus scanner—passing on GIF files, for example, that are almost never infected. This frees firewall resources, and firewall performance is not affected by virus scans.

This architecture scales well. LAN administrators can add multiple firewall or gateway scanners to help manage network traffic and improve performance. Each of the multiple scanners can be configured to scan specific file or protocol type or types, dividing the scanning workload and further improving performance.

Also, this architecture cannot be bypassed by users, and LAN administrators need not configure clients at each workstation. At the same time, the firewall and anti-virus server is flexible, supporting separate scanning policies for inbound and outbound traffic, and scanning only preselected files, which in turn helps maintain peak network performance.

This powerful, flexible architecture is used by Symantec in Norton AntiVirus for Firewalls.

Norton AntiVirus for Firewalls

Norton AntiVirus for Firewalls (NAV for Firewalls) is one of two products designed to extend Symantec's industry-leading virus protection "from the floppy to the wire."

NAV for Firewalls is a Windows NT–based virus-scanning server that uses Symantec's anti-virus detection and removal technologies to protect users with Internet gateways against viruses found in all types of Internet traffic.

The need for NAV for Firewalls is measurable. Market researcher IDC predicts the total number of firewall shipments will increase to 377,000 in 1988, up from 150,000 in 1997. IDC also predicts Windows NT–based firewalls will command 71 percent market share by 1999, up from 7 percent in 1996.

NAV for Firewalls is designed to plug into such market-leading firewalls as CheckPoint Firewall UNIX and Windows NT, Trusted Information Systems' Gauntlet Firewall for UNIX and Windows NT, Milkyway's Blackhole Firewall, and Microsoft Proxy Server, among others.

The most effective way to stop viruses before they reach the corporate LAN is to detect and eliminate them at the gateway.

Symantec built NAV for Firewalls using the Intelligent Scanning Architecture (ISA). With this approach:

- The firewall directs only suspicious traffic to the virus scanner—program files that may be infected with a polymorphic virus, for example, or .DOC files that may hide a macro virus. Seldom-infected .GIF files need not be scanned.
- The server requires no per-user configuration, and users cannot bypass the critical virus protection, such as in the case of a proxy server.
- A single firewall can be used for all-protocol or protocol-specific scans. This scalability permits LAN administrators to easily add more than one NAV for Firewalls server to the network—and each additional server can then be configured to scan a different file type, dividing the network traffic to eliminate potential bottlenecks.

Other customer benefits for NAV for Firewalls include:

- Comprehensive protection of all common Internet and Web-browsing traffic, as well as email attachments. NAV for Firewalls scans incoming and outgoing HTTP, FTP, and SMTP data—and system administrators can specify and add a fourth protocol.
- Robust scanning of and virus removal from a virtually unlimited number of file extensions, including ZIP, self-extracting ZIP, and MIME files, ensuring protection against potential future virus outbreaks.
- Support for different scanning policies for inbound and outbound traffic—flexibility that helps direct virus scanning to where it is most needed. Desktops and network servers that are protected, for example, permit LAN administrators to relax outbound scanning and target more network resources at traffic inbound from the Internet.
- No per-client configuration, easing the LAN administrator workload. All configuration is executed at the server. End users cannot bypass the full-time virus protection.
- Various options for treating infected files—repair, quarantine, and pass-through.
- Easy configuration using an HTML-based user interface that supports remote configuration with password protection.
- Complete command of system status via detailed logging and network statistics, displayed in HTML format—with customizable infection alerts via email to administrators and other recipients.

In addition, one-button virus-definition updates are built into NAV for Firewalls via Symantec's LiveUpdate™ feature. LiveUpdate obtains and installs new virus definitions and software updates, via the Internet, at administrator-specified frequency. It detects an Internet connection or modem, automatically dials and connects to file libraries residing on Symantec servers, then downloads and installs the latest virus definitions, which Symantec updates monthly. LiveUpdate also installs software patches and updates the virus scanning engine if a new type of virus appears. And the updates are free; no subscription is needed.

ISA was developed by Symantec and has received endorsement from several industry-leading firewall vendors. ISA provides unparalleled virus protection, with minimal impact on system performance. NAV for Firewalls is a powerful, flexible anti-virus solution for corporate firewalls, combining the functionality of ISA and Symantec's commitment to always provide the most up-to-date virus protection, free of charge, via LiveUpdate.

Norton AntiVirus for Internet Email Gateways

Norton AntiVirus for Internet Email Gateways (NAV for Internet Email Gateways) is the second of two new products designed to extend Symantec's industry-leading virus protection "from the floppy to the wire."

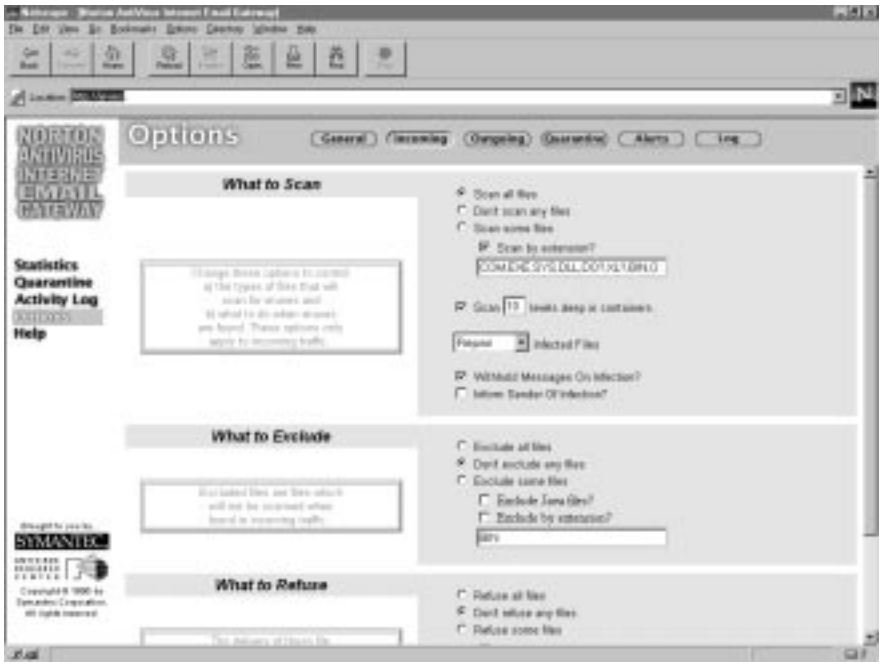

Figure 7. NAV for Internet Email Gateways screen capture.

While desktop and server anti-virus products protect workstations and LAN servers from viruses transmitted via floppy disk and file download, the most effective way to stop viruses before they reach the corporate LAN is to detect and eliminate them at the gateway.

Designed for companies that need virus protection on all incoming and outgoing email, NAV for Internet Email Gateways locks out viruses in Internet email attachments before they invade a corporate network that is not protected by a firewall. It protects gateways that send and receive Internet email using the Simple Mail Transfer Protocol (SMTP).

As with firewalls, the need for NAV for Internet Email Gateways can be measured. According to market researcher IDC, at least 72 percent of large corporations don't protect SMTP servers with a firewall. IDC further projects shipments of 55,000 new SMTP servers in 1997 and 121,000 new SMTP servers in 1998.

Benefits of NAV for Internet Email Gateways include:

- Scanning of any email going through the SMTP gateway, including compressed or encoded formats such as MIME, UUENCODE, and ZIP files. All email passing through the gateway must be certified before it can enter the corporate network.
- Support for different scanning policies for inbound and outbound traffic—flexibility that helps direct virus scanning to where it is most needed. Desktops and network servers that are protected, for example, permit LAN administrators to relax outbound scanning and target more network resources at traffic inbound from the Internet.
- Robust scanning of and virus removal from a virtually unlimited number of file extensions, including ZIP, self-extracting ZIP, and MIME files.
- Various options for treating infected files—repair, quarantine, and pass-through.
- Easy configuration using an HTML-based user interface that supports remote configuration with password protection.
- Complete command of system status via detailed logging and network statistics, displayed in HTML format, with customizable infection alerts via email to sender, receiver, and administrator.
- One-button, free virus-definition updates via LiveUpdate.
- Operation that is transparent to users, without affecting the performance of the network.

NAV for Internet Email Gateways also incorporates Striker™, Symantec's new, patent-pending system for detecting polymorphic viruses, the most complex and the hardest viruses to detect.

The ability to support different scanning policies for inbound and outbound traffic, add any number of new file extensions, and both detect and remove viruses makes NAV for Internet Email Gateways a must-have anti-virus solution for corporate gateways. The fact that virus-definition updates are free to users for the lifetime of the product makes Norton AntiVirus for Internet Email Gateways a even more cost-effective solution for today's small to medium-size businesses with higher-than-usual SMTP traffic load over other types of Internet traffic protocols.

The Symantec AntiVirus Research Center

SARC comprises of a dedicated team of virus experts whose mission is to provide swift, global responses to computer virus threats, proactively research and develop technologies that eliminate such threats, and educate the public on safe computing practices.

As new computer viruses appear, SARC develops identification and detection for these viruses, and provides either a repair or delete operation, thus keeping users protected against the latest virus threats. These virus-definition updates are available to users of Norton AntiVirus and are easily obtained by using LiveUpdate or Intelligent Updater. LiveUpdate provides one-button access to the latest virus-definition updates, free of charge (other than normal phone and Internet access charges) to registered users. Symantec is the only anti-virus company that provides its users virus definitions that are free of charge, easy to obtain and install, and updated monthly by SARC.

Conclusion

The stampede to the Internet and escalating use of the Internet for business requires multiple layers of virus protection for firewalls and gateways. However, of the three basic architectures for incorporating virus-scanning technologies into firewalls and gateways, only one is powerful and flexible enough to maximize virus protection without slowing network performance. It is this approach, the Intelligent Scanning Architecture, that is used by Symantec in its new product, Norton AntiVirus for Firewalls. For Internet email virus protection, Norton AntiVirus for Internet Email Gateways is the most cost-effective solution for small to medium-size corporations that have no firewall, but are constantly exchanging data via email attachments across the Internet.

Norton AntiVirus products are the protection of choice for many Fortune 500 companies and for more than 15 million users worldwide. Symantec's two new products give corporate users a set of integrated anti-virus tools that protect desktops, servers, and gateways.

Citations

- "NCSA virus study: Complete results and analysis," National Computer Security Association, 1996.
- "Internet commerce: The worldwide firewall market, 1995–2000," International Data Corp., February 1996.

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 and Controlling Viruses in 32-Bit Operating Environments*
- *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*
- *A Strategy for the Migration to Windows 95*
- *File Management and Windows 95*
- *Using the Object Windows Library 2.51 with Symantec C++*
- *Understanding Virus Behavior in the Windows NT Environment*
- *Integrating Remote Communications into Enterprise Computing*
- *Understanding the Benefits of Electronic Commerce Technologies*
- *Understanding and Managing Polymorphic Viruses*
- *Using Outsourcing to Reduce IT Labor Costs*

For copies of these papers or information about Symantec enterprise network products, call 1-800-453-1135 and ask for C321. Outside the United States contact the sales office nearest you (listed on the back cover).

Contacts for Media

Questions from the media should be directed to:

Lori Cross
Senior Public Relations Manager
Symantec Corp.
310-449-5258
lcross@symantec.com

About Symantec

Symantec Corporation is a leading software company with award-winning application and system software for Windows, DOS, Macintosh, and OS/2 computer systems. Founded in 1982, Symantec has grown rapidly through the success of its products and a series of 16 acquisitions resulting in a broad line of business and productivity solutions. The company has several enterprisewide products that have been introduced recently and others that are under development.

Symantec's acquisitions have strongly influenced the company's innovative organization. The company is organized into several product groups that are devoted to product marketing, engineering, technical support, quality assurance, and documentation. Finance, sales, and marketing are centralized at corporate headquarters in Cupertino, California.

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

Australia: +61 2 985 0 1000
Brazil: +55 11 530 8869
Canada: 1 (416) 446-8495
France: +33 1 34 63 07 02
Germany: +49 2191 991155
Italy: +39 2 22 478 033
Japan: +81 3 3498 0550
Mexico: +52 5 661 7978
New Zealand: +64 9 309 5620
The Netherlands: 06 0992277 *(freefone)*
Russia: +7 095 320 0733
Singapore: +65 321 8980
Sweden: +46 8 614 50 26
Switzerland: +41 72 22 80 20
Taiwan: +886 2 729 9506
UK: 0800 526459 *(freefone)*

07-71-00681