



# Norton AntiVirus/IBM Solution Suite

## Highlights

**Detects and removes known, previously unknown and unidentified viruses**

**Works in the background to provide continuous, automatic protection**

**Provides broad coverage of clients, servers and gateways**

**Detects and disinfects 100% of in-the-wild viruses, including Microsoft Word macro viruses<sup>1</sup>**

**Analyzes viruses byte-for-byte before disinfection**

**Offers the same look-and-feel across multiple platforms**

**Automates and centralizes administration**

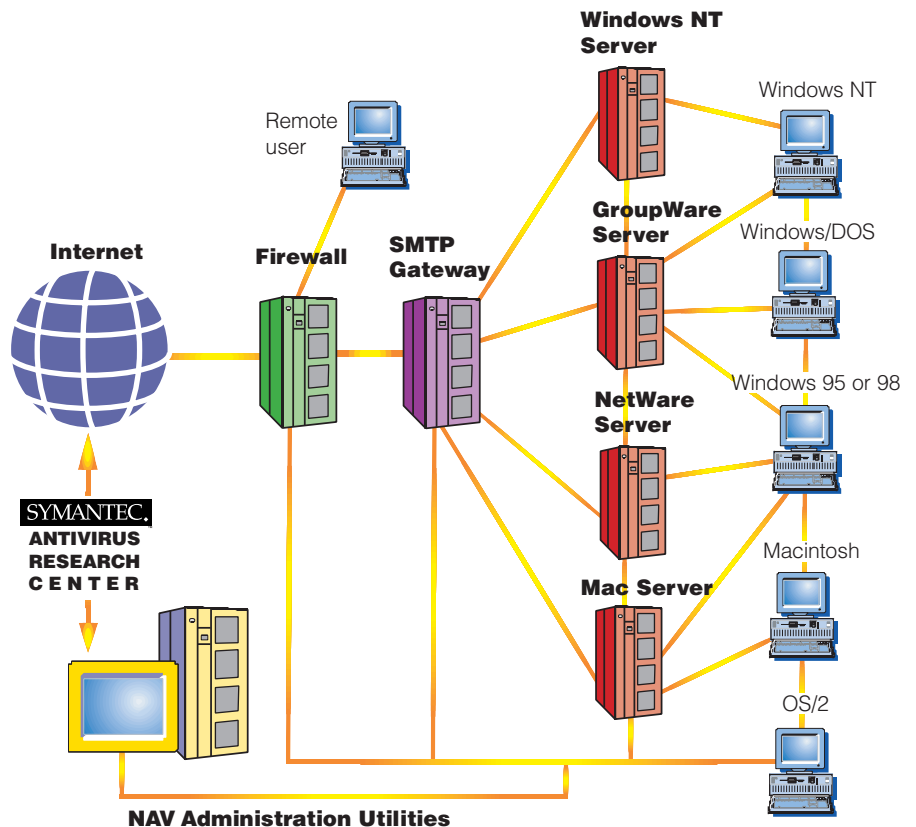
**Virtually eliminates false alarms**

**Delivers automated, server-based updates of the AntiVirus products**

Norton AntiVirus™ by Symantec™, one of the world's leading antivirus solutions, delivers advanced virus detection and elimination software to businesses of all sizes. This multiplatform solution provides easy-to-use, customizable, *install-and-forget* protection that begins guarding your workstations, servers and gateways as soon as it is installed.

## Safety first

Rare or previously unknown viruses don't have to be fatal. During installation, Norton AntiVirus/IBM Solution Suite provides a generic disinfection feature, a patent-pending technology that records information about your files for later use in disinfection. If a file is infected with a rare or previously unknown virus, generic



The Norton AntiVirus multi-tier solution

## *Powerful, integrated virus protection for your e-business*

disinfection attempts to use the recorded information to reconstruct the original uninfected file. If the reconstruction exactly matches the original file, the file will be safely disinfected.

Whatever type of virus is present, Norton AntiVirus (NAV) won't damage files or boot records to remove the virus. If it's unable to safely disinfect, you have the option to erase the infected files or replace the infected boot records. All actions are recorded in the ASCII log file where you can later access them to view or print. In September 1999, key Norton AntiVirus products achieved ICSCA Cleaning Certification. During certification testing, these key Norton AntiVirus products were shown to leave files intact while effectively removing viruses.<sup>2</sup>

### **Protection from the unknown**

Bloodhound™ technology protects your system from previously unknown viruses—including rapidly spreading macro viruses. It sets up a virtual computer to evaluate files, then scrutinizes a program's overall structure, programming logic, instructions, file data and other attributes to assess the likelihood of viral infection. Clean files pass through, but viral files are stopped before they can cause harm. It also eliminates new viruses that might arise between updates.

Norton AntiVirus also provides protection against malicious code. It can detect and remove Trojan horses and dangerous forms of ActiveX controls and Java™ applets. Symantec AntiVirus Research Center™ (SARC™) experts search the Web for malicious code and update Norton AntiVirus to protect against it.

### **Automatic updates**

With an average of 10 to 15 new viruses discovered every day, it's critical to keep your virus protection current. LiveUpdate™ enables automatic retrieval of new virus definitions from Symantec up to once a week. Run your first LiveUpdate session during installation and schedule future sessions to run automatically, helping ensure that your network is always protected against the latest virus threats without interrupting network activity.

### **24-hour, unobtrusive protection**

Norton AntiVirus can run automatically at prescheduled times to check all of your computers' hard disks for viruses. If your system becomes infected, Norton AntiVirus can disable the virus and allow the infected program to run as though it is not infected, without fear of spreading the infection or causing damage. The AutoProtect feature monitors your system in the background using realtime scanning, allowing you to focus on your work without interruption. Computers are guarded against viruses that might enter from networks or with e-mail attachments, Internet downloads, floppy diskettes and software CDs.

### **Efficient performance**

Exclusive Scan Caching technology provides fast scanning time and low bandwidth consumption. Once a file has been scanned and found to be virus-free, it will not be scanned again until changes are made, greatly improving day-to-day server performance. Norton AntiVirus scans all files in realtime as they are accessed or copied to and from the server. You can save even more time by scheduling automatic scans at regular intervals.

### **Reliable antivirus technologies**

Norton AntiVirus Quarantine technology provides a safe zone on a Quarantine server where you can isolate infected files and attachments for repair when network activity is lower. This quarantine area helps ensure that your other files stay clean and that you don't accidentally send infected files to anyone else. Quarantines, virus scans and removal can be managed from any location using a Web browser.

Striker™ technology detects and removes polymorphic viruses, which account for roughly 22 percent of today's viruses and often elude standard virus-detection methods. To detect these encrypted viruses, each time Norton AntiVirus scans the computer, it sets up a virtual PC or

*clean room* to safely execute potentially infected files. Once the virus has decrypted itself inside the Striker virtual PC, Norton AntiVirus can identify and repair the virus without endangering other files.

### **Minimize protection costs with NAVEX and SARA**

To minimize IT costs in the face of virus threats, Norton AntiVirus exploits a unique feature called NAVEX. With NAVEX, an extendible antivirus engine, Norton AntiVirus can be updated to include protection from new types of viruses without having to redeploy the product. Through Norton AntiVirus and NAVEX, the cost of keeping application and virus definitions up to date in the face of new and unknown viruses is low.

SARA, the Symantec AntiVirus Research Automation tool, automatically analyzes virus samples submitted to Symantec, creates virus definitions and repair schemes, and tests the newly-developed scheme—in less than five minutes. Scientists from IBM's T.J. Watson Research Center work in conjunction with Symantec to develop new technology for enhancing this tool. With SARA, you can help eradicate new viruses—which are appearing at a rapidly increasing rate—before they have the chance to spread widely and cause extensive damage.

### **Easy administration**

Norton AntiVirus enables maximum administrative control and flexibility with the following functions and features:

- Central distribution and administration
  - Remote configuration scanning
  - Continuous, automatic protection
  - Realtime, on-demand or scheduled scanning (for off-peak hours)
  - Ability to repair, quarantine or delete infected files
  - Comprehensive reporting and detailed logging capability
  - Customizable e-mail virus alerts sent to sender, receiver and administrator
  - Great control of your environment
  - Quick, easy configuration
  - Installation in minutes
  - Simple method for sending suspicious files to Symantec for evaluation with Scan and Deliver feature
- Norton AntiVirus offers the following family of products, plus the products in the chart on the next page:
- Desktop solutions: DOS, Microsoft® Windows® 3.1, Windows 95 and Windows 98, Windows NT® 3.51, Windows NT 4.0, Mac OS and IBM OS/2®
  - Server solutions: Windows NT 3.51, Windows NT 4.0, NetWare NLM, Lotus Notes® and Microsoft Exchange
  - Gateway solutions: Internet E-mail Gateways for Windows NT and Firewalls
  - Administration: NAV Plus for Tivoli® IT Director, NAV Plus for Tivoli Enterprise, Norton System Center, Macintosh Administrator and other administrative tools

### **Open for trusted e-business with IBM SecureWay FirstSecure**

IBM SecureWay® FirstSecure enables companies to build and operate secure and trusted environments to conduct e-business. FirstSecure offers an integrated, policy-driven solution for your IT security needs, including digital identities, network boundary protection, detection for viruses and intrusions, and tools for developing secure applications. Norton AntiVirus/IBM Solution Suite can be purchased as part of FirstSecure or separately through the IBM/Lotus Passport Advantage program.

### **For more information**

To learn more about the Norton AntiVirus/IBM Solution Suite, visit:

[www.ibm.com/software/security/antivirus](http://www.ibm.com/software/security/antivirus)

To learn more about IBM SecureWay FirstSecure, visit:

[www.ibm.com/software/security/firstsecure](http://www.ibm.com/software/security/firstsecure)

---

**Norton AntiVirus at a glance**

---

**Norton AntiVirus system requirements**

---

**OS/2**

- IBM PC or compatible system
- Intel® 80386 DX or higher (Intel 486 recommended)
- OS/2 2.11, Warp, Warp Connect or Warp 4
- 16MB of RAM (32MB recommended)
- 24MB of free hard disk space
- CD-ROM drive

**Windows NT**

- Windows NT Workstation 4.0
- 16MB of RAM (32MB or higher recommended)
- 24MB of free hard disk space
- 90MHz Pentium® or higher

**Windows 95 or Windows 98**

- 486 IBM PC or compatible system
- Windows 95 or Windows 98
- 8MB of RAM (16MB or higher recommended)
- 24MB of free hard disk space

**Windows 3.1 or DOS**

- 386 IBM PC or compatible system with 4MB of memory
- Windows 3.1
- DOS 5.0 or higher
- 10MB of free hard disk space to install Norton AntiVirus for Windows and DOS
- 5MB of free hard disk space to install only Norton AntiVirus for DOS

**Lotus Notes OS/2**

- OS/2 Warp 3 (Warp 4 recommended)
- Lotus Notes 4.5 (4.5.5 or higher recommended)
- 90MHz Pentium or higher
- 32MB RAM minimum (128MB recommended)
- 7MB of free hard disk space to install

**Lotus Notes Windows NT**

- Windows NT Server 3.51 with Service Pack 5 or Windows NT Server 4.0 with Service Pack 3
  - Lotus Notes Server 4.51 or higher (4.52 or higher is required to repair infected OLE objects embedded in documents)
  - 90MHz Pentium or higher
  - 32MB RAM minimum (64MB recommended)
  - 20MB of free hard disk space to install
  - 50MB minimum free hard disk space for processing (the location for temporary files is a Global Option that can be changed after install)
-

---

**Norton AntiVirus at a glance, continued**

---

**Norton AntiVirus system requirements**

---

**Firewall**

- Windows NT 3.51 or Windows NT 4.0
- 133MHz Pentium or higher
- 32MB of RAM minimum (64MB recommended)
- 500MB of free hard disk space (1GB recommended)

**Internet E-mail Gateways**

- Windows NT 3.51 or Windows NT 4.0
- 133MHz Pentium or higher
- 32MB of RAM minimum (64MB recommended)
- 150MB of free hard disk space (500MB recommended)

**Tivoli IT Director servers**

- Tivoli IT Director 1.2 or higher
- Windows NT 4.0 with Service Pack 3

**Tivoli IT Director clients**

- Tivoli IT Director 1.2 Endpoint software
- Windows NT: 16MB of RAM (32MB recommended);  
Windows 95 or Windows 98: 8MB of RAM  
(16MB recommended)
- 40MB of free hard disk space

**Microsoft Exchange**

- Windows NT Server 3.51 with Service Pack 5 or  
Windows NT Server 4.0 with Service Pack 3
- Microsoft Exchange 4.0 or higher
- 133MHz Pentium or higher
- 64MB of RAM
- 20MB of free hard disk space to install
- 50MB of free hard disk space for processing
- Netscape Navigator or Internet Explorer 3.x or higher;  
Java, JavaScript and cookies must be enabled
- Client for Microsoft Exchange or Microsoft Outlook

**NetWare NLM**

- 600KB of available RAM
- 4MB of free hard disk space
- Novell NetWare 3.11, 3.12, 4.1 or 4.11 (IntranetWare);  
Novell NetWare for OS/2 or SFT-III
- IPX protocol

**Macintosh**

- System 7.5 minimum
  - 68040 processor minimum (including Power Macintosh)
  - 8MB RAM
  - CD-ROM drive
-



© International Business Machines Corporation 1999

IBM Corporation  
Department VK4A  
3039 Cornwallis Road  
Research Triangle Park, NC 27709

Produced in the United States of America  
10-99  
All Rights Reserved

The e-business logo, IBM, OS/2 and SecureWay are trademarks of International Business Machines Corporation in the United States, other countries or both.

Lotus Notes is a trademark of Lotus Development Corporation in the United States, other countries or both.

Tivoli and Tivoli IT Director are trademarks of Tivoli Systems Inc. in the United States, other countries or both.

Intel and Pentium are trademarks of Intel Corporation in the United States, other countries or both.

Microsoft, Windows and Windows NT are trademarks of Microsoft Corporation in the United States, other countries or both.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries or both.

Norton AntiVirus and Symantec are U.S. registered trademarks of Symantec Corporation. Bloodhound, LiveUpdate, SARC, Striker and Symantec AntiVirus Research Center are trademarks of Symantec Corporation.

Other company, product and service names may be trademarks or service marks of others.

<sup>1</sup> Source: *Secure Computing* magazine's West Coast Labs Anti-Virus Checkmark Level 2 certification. For a product to be certified at this level, it must be able to detect and disinfect all viruses defined as those that appear at test time on The Wildlist Organisation's "In the Wild" list and which have been reported by more than one person. See [www.check-mark.com](http://www.check-mark.com) for more information on the West Coast Labs certification.

<sup>2</sup> ICSA certification is awarded only to products that have the ability to reliably clean and disinfect machines once they have become infected by a virus. The cleaning or disinfection capability checks to be certain that the software can effectively remove the virus from a file while leaving the file intact. NAV for Windows 3.1, Windows 95 and Windows 98, Windows NT workstation and server, and NetWare have been so certified. Further information is available at:  
[www.icsa.net/services/consortia/anti-virus](http://www.icsa.net/services/consortia/anti-virus)



Printed in the United States on recycled paper containing 10% recovered post-consumer fiber.



G325-3892-01