



# Securing Instant Messaging

**INSIDE** INSIDE

- > Instant messaging primer
- > Securing instant messaging in your corporation
- > Instant messaging best practices

# Contents

Executive summary . . . . .	3
Instant messaging primer . . . . .	4
Instant messaging and client-server communications . . . . .	4
Instant messaging and peer-to-peer communications . . . . .	5
Instant messaging and encryption . . . . .	5
Instant messaging and file transfers . . . . .	6
Instant messaging and scripting . . . . .	6
Instant messaging and other features . . . . .	6
Instant messaging vulnerabilities and exploits . . . . .	7
Eavesdropping . . . . .	7
Account hijacking . . . . .	7
Data access and modification . . . . .	7
Worms and blended threats . . . . .	8
Scripting instant messaging threats . . . . .	8
Instant messaging threats that exploit vulnerabilities . . . . .	9
Denial of service . . . . .	9
Instant messaging server vulnerabilities . . . . .	9
Securing instant messaging in your corporation . . . . .	10
Understanding instant messaging and corporate firewalls . . . . .	10
Understanding instant messaging file transfers and corporate firewalls . . . . .	11
Instant messaging best practices . . . . .	12
The future . . . . .	14
Conclusion . . . . .	14

## > Executive summary

From its beginnings as a simple buddy-to-buddy chatting service, instant messaging has blossomed to become a staple mode of communication for tens of millions of Internet users. Popular systems such as America Online's Instant Messenger, Microsoft's MSN Messenger, ICQ, and Internet Relay Chat (IRC) have changed the way we communicate with friends, acquaintances, and business colleagues. Once limited to desktops, popular instant messaging systems are finding their way onto handheld devices and cell phones, allowing users to chat from virtually anywhere. According to IDC, the number of corporate instant messaging users is expected to grow to over 200 million by 2005 with an additional 300 million home computer users having IM systems by that time<sup>1</sup>

Like the Palm®Pilot, instant messaging has quietly worked its way into corporate America. IM systems, while not supported by many IT departments, are quickly gaining popularity with knowledgeable workers who find these systems faster and more convenient than email or telephone. Unfortunately, while IM systems have the ability to fundamentally change the way we communicate and do business, many of today's implementations pose security challenges.

Most IM systems presently in use were designed with scalability rather than security in mind. Virtually all freeware IM programs lack encryption capabilities and most have features that bypass traditional corporate firewalls, making it difficult for administrators to control instant messaging usage inside an organization. Many of these systems have insecure password management and are vulnerable to account spoofing and denial-of-service (DoS) attacks. Finally, IM systems meet all the criteria required to make them an ideal platform for rapidly spreading computer worms and blended threats:<sup>2</sup> they are ubiquitous; they provide a communications infrastructure; they have integrated directories (buddy lists) that can be used to locate new targets; and they can, in many cases, be controlled by easily written scripts. Even worse, no firewall on the market today can scan instant messaging transmissions for viruses.

This paper details the security risks of using instant messaging systems and provides guidelines to help enterprises make informed decisions about how to properly implement such systems within a corporate environment.

<sup>1</sup> <http://www.computerworld.com/softwaretopics/os/windows/story/0,10801,61141,00.html>

<sup>2</sup> Blended threats combine virus and/or worm-like propagation, hacking, and denial-of-service techniques to rapidly spread, often without human interaction. Recent blended threats, such as Nimda and CodeRed, were able to spread to hundreds of thousands or millions of machines in just hours, causing billions of dollars in damage.

## > Instant messaging primer

While instant messaging may seem like a new technology, it is actually decades old. The first system, IRC, was developed in 1988 by Jarkko Oikarinen<sup>3</sup>. Still in use, this system allows users to form ad-hoc discussion groups, chat with one another, and exchange files. Since the introduction of IRC, many new IM systems have been launched; for example, ICQ, AOL Instant Messenger, MSN Messenger, and Yahoo Messenger. While each of these offers different features, they all provide the same basic service: peer-to-peer real-time chatting and file transfer capabilities.

### INSTANT MESSAGING AND CLIENT-SERVER COMMUNICATIONS

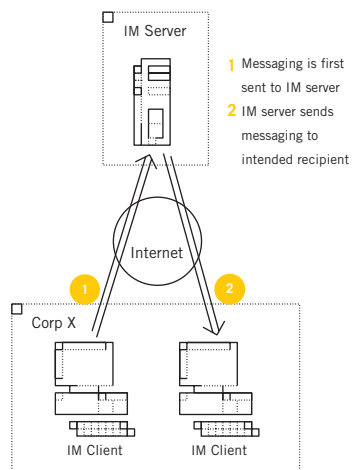


Figure 1. Client-server instant messaging

Virtually all IM systems employ the same basic client-server architecture. Users install instant messaging clients on their client machines—desktop computers, wireless devices, or PDAs, for example—and these clients communicate with an IM server in the messaging provider’s infrastructure to locate other users and exchange messages. In most instances, messages are not sent directly from the initiating user’s computer to the recipient’s computer, but are sent first to an IM server, and then from the IM server to the intended recipient. (See Figure 1.)

In the majority of client-server instant messaging systems, data exchanged between users is plainly visible, making it susceptible to eavesdropping.

<sup>3</sup> [http://www.irc.org/history\\_docs/jarkko.html](http://www.irc.org/history_docs/jarkko.html)

## INSTANT MESSAGING AND PEER-TO-PEER COMMUNICATIONS

While most instant messaging systems use centralized servers to transmit all messages, some systems do offer peer-to-peer messaging. In such a model, clients contact the IM server to locate other clients. Once the client chat program has located its peer, it contacts the peer directly. (See Figure 2.)

The peer-to-peer scheme offers better security than the client-server-client scheme (shown in Figure 1) when both users are on the same local area network because messages do not travel over the Internet. However, if one user is located outside the corporate network, messages sent between machines are exposed to potential eavesdroppers, just as in the client-server-client scheme.

## INSTANT MESSAGING AND ENCRYPTION

Today few, if any, public instant messaging systems encrypt messages as they travel from the client to the server and back to the second client. This data is potentially visible to eavesdroppers anywhere along its Internet path or within the IM provider's network. Also, popular IM systems do not encrypt peer-to-peer traffic. As shown in Figure 1, even if two users are sitting in adjacent cubicles, their messages travel over the Internet, potentially revealing sensitive information.

Corporations should consider the confidentiality of instant messaging to be only as safe as sending all internal and external company email using a public email service. For client-server-client systems, traffic sent between two users can be assumed to travel unencrypted over the Internet. For peer-to-peer systems, if either client is outside the corporate firewall, all traffic again flows unencrypted over the Internet. In both cases, content can be intercepted by attackers with the proper tools.

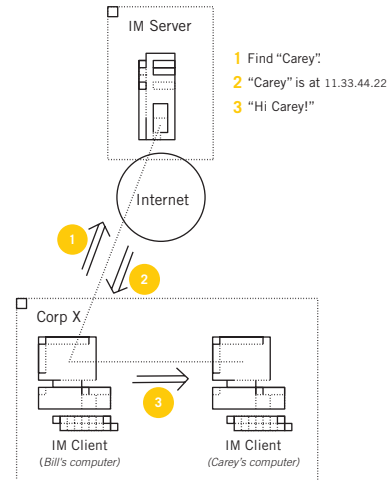


Figure 2. PEER-TO-PEER instant messaging

#### INSTANT MESSAGING AND FILE TRANSFERS

In addition to sending messages between users, instant messaging systems allow users to exchange files. Current systems transfer files directly between peers rather than through the server, as with text messaging. In other words, the technique shown in Figure 2 is always used for file transfers. This peer-to-peer scheme is used to eliminate the high bandwidth demands that server-centric file transfers would place on the provider's network.

Currently, none of the major instant messaging systems encrypt files transferred between instant messaging clients. While the files do not directly flow through instant messaging servers, they may flow over the Internet, over a corporate LAN or WAN, or over both. If both users are on the same company network, file transfers will likely remain on the corporate network; however, if one of the users is outside the network, files will be sent unencrypted over the Internet.

#### INSTANT MESSAGING AND SCRIPTING

A handful of instant messaging platforms offer scripting capabilities, enabling users to write Visual Basic, JavaScript, proprietary script code, and other complex programs to control various features in the messaging client. This functionality, while convenient, provides mechanisms that enable the spread of computer worms and blended threats. Scripts such as these are able to instruct the instant messaging client to do any number of things: contact other users, send files, change program settings, and/or execute potentially malicious actions. A more detailed discussion surrounding these kinds of security issues is provided in the following section on instant messaging vulnerabilities and exploits.

#### INSTANT MESSAGING AND OTHER FEATURES

Finally, in response to a highly competitive instant messaging market, some instant messaging companies have added additional functionality to messaging clients to gain customers. For example, ICQ contains a mini-Web server that allows users to run small Web sites directly from a desktop computer. As with any Web-enabled software feature, such functionality creates the security risk that the site could be hacked to break into a system.

## > Instant messaging vulnerabilities and exploits

This section describes significant vulnerabilities that are present in common instant messaging systems and the types of attacks that can exploit them. A discussion on safeguarding corporations from these threats immediately follows in the next section entitled “Securing instant messaging in your corporation.”

### EAVESDROPPING

Given that most IM systems do not encrypt network traffic, a determined third-party can eavesdrop on conversations between two IM users using a packet sniffer or similar technology. As discussed previously, this holds true for both client-server and peer-to-peer messaging models.

### ACCOUNT HIJACKING

Many instant messaging systems are vulnerable to account hijacking or spoofing, allowing an attacker to hijack another user’s instant messaging account and impersonate that user in conversations with others. A number of Web sites provide do-it-yourself tools or describe techniques for launching such an attack.

Password protection is very limited in most instant messaging systems. Some IM systems store user passwords in data files on the client’s PC. In some cases, these passwords are encrypted; in other cases, they are plainly visible. There currently exists at least one Web site that gives detailed instructions on how to crack the password encryption scheme for one popular IM system.

### DATA ACCESS AND MODIFICATION

Like all Internet-enabled software, IM programs could have bugs that may be exploited by attackers over the Web. Using attacks such as buffer overflows or malformed data packets, an attacker could gain access to a PC on which a vulnerable IM client is installed. Given the large number of ancillary features present in many IM products, there are numerous potential areas for attack.

As an example, in May 2002, a hacking group known as w00w00 identified a vulnerable piece of computer code in a popular instant messaging program. This vulnerability could have been exploited by an attacker to gain full access to targeted systems. From there, the attacker could have installed computer viruses, stolen or deleted data, and even grabbed passwords. Fortunately, the IM vendor moved quickly in this situation and issued a fix for the vulnerability to protect their customers.

## WORMS AND BLENDED THREATS

Like email systems, instant messaging platforms provide the enabling technologies that are needed for spreading worms and blended threats (such as CodeRed).

First, the instant messaging software provides a robust communications channel between system users. Second, virtually all IM software products maintain a list of buddies with whom the user frequently interacts. Like email address books, buddy lists can be leveraged as hit lists to spread a worm rapidly through the IM user base. Lastly, some of the instant messaging systems are scriptable or programmable, providing malicious programs targeted at these systems with a mechanism by which to spread.

Given the ubiquity of popular instant messaging systems, a blended threat targeted at such a system could potentially spread to tens of millions of personal and business computers in just a few hours. Once in each system, a worm could delete data, install back doors, and possibly export critical data. Symantec™ experts predict that such an attack will more than likely happen within the next decade, if not sooner. The fast growth of broadband Internet connections will only exacerbate these security problems.

Blended threats and computer worms can spread through instant messaging systems in two ways: by leveraging IM scripting and by exploiting a buffer overflow or other vulnerability in an instant messaging system.

### *Scripting instant messaging threats*

As described earlier, IM systems provide scripting capabilities that let other programs or script files (e.g., Visual Basic or JavaScript) control the client IM software via simple programming commands. By taking advantage of such commands, malicious code can use the IM system as a communications platform to send itself into other members of the system, change program settings, steal confidential information, and perform other potentially malicious actions. Similar functionality in traditional email clients has been exploited in the past by malicious worms such as LoveLetter and SirCam.

There are dozens of real-world worms that propagate using IRC as a communications platform. These worms are written in a scripting language provided by popular IRC client software and typically work as follows: a user with a computer that has been infected by a worm joins a discussion group and begins chatting. As subsequent (and still as yet uninfected) users join the same chat group, the worm detects the new users and sends a copy of itself to them in the form of a script file. In some instances, the receiving user is prompted to open the file; in others, the user receives no notification. Once the worm infects the new computer, the cycle begins anew.

In addition to IRC worms there now exist a number of Windows®-based worms targeted at certain IM systems. These worms use scripting techniques similar to those used by the Nimda and LoveLetter and SirCam threats, to send themselves from user-to-user via instant messaging software. Fortunately, none of these worms have been widespread so far, but they clearly demonstrate that instant messaging platforms are susceptible to such attacks.



#### INSTANT MESSAGING THREATS THAT EXPLOIT VULNERABILITIES

As we have seen with CodeRed and Nimda, it is possible to construct a blended threat that spreads without user interaction by exploiting vulnerabilities in an Internet-enabled software platform such as a Web server. In the future, we could see similar worms or blended threats that exploit bugs or other vulnerabilities in client-side IM software. Such a threat could, for instance, use a buffer overflow attack on an IM client program to gain access to a new system. Once in the system, it could access the user's buddy list to gain a new set of targets.

This is an area of great concern, given the speed at which such a threat could possibly spread and the large number of machines the threat could affect. While CodeRed was able to attack several hundred thousand Internet servers in hours, a well-crafted IM-based worm would have the potential to hit millions or even tens of millions of home computers or wireless devices in the same amount of time.

##### *Denial-of-Service*

Like other communications systems, instant messaging platforms are susceptible to denial-of-service attacks. For example, an attacker could send large numbers of specially crafted TCP/IP packets to IM servers residing in the IM provider's infrastructure to prevent legitimate messages from flowing through the system. This would be similar to the denial-of-service attacks launched on major Internet properties in the last few years. Alternatively, an attacker could send large numbers of packets to a specific user or set of users to flood them with chat or file transfer requests.

##### *Instant messaging server vulnerabilities*

While many security experts have focused on the vulnerabilities of IM clients, it is also important to consider potential IM server vulnerabilities. If attackers gained access to these servers, they could also eavesdrop on all conversations, impersonate any user, launch denial-of-service attacks, or spread malicious threats with little effort. Recall that little, if any, IM traffic is encrypted, meaning that an attacker in control of an IM server can gain access to the contents of every transmission.

## > Securing instant messaging in your corporation

Instant messaging may soon become an indispensable business tool; however, the risks of using an unsecured IM platform in corporations are high. This section explores the security issues introduced with the use of corporate instant messaging and offers best practices that can help in deploying a secure IM platform.

### UNDERSTANDING INSTANT MESSAGING AND CORPORATE FIREWALLS

Many corporate customers may wish to use their network firewall to block users from communicating over insecure instant messaging systems. Unfortunately, out-of-the-box firewall configurations are often not sufficient enough to block access to the latest generation of popular IM systems. These IM systems were designed with firewalls in mind and employ a number of techniques to sneak past corporate firewalls to reach their servers.

All IM clients are preconfigured with one or more TCP/IP network addresses that allow them to connect to their IM server(s). Once connected, the clients can exchange messages with other IM clients. Because many companies configure perimeter firewalls to block all Internet services except for a small critical set (e.g., SMTP email, HTTP Web surfing, and DNS), IM providers have designed their clients to tunnel over these commonly allowed Internet services, if required, and slip past the corporate firewall.<sup>4</sup>

For instance, if they initially encounter trouble connecting to their servers, many IM programs attempt to contact these servers using network port number 80, the port used by browsers to surf the Web. Given that most corporate firewalls are configured to allow any PC on the company network to surf the Web, the firewall will pass transmissions through port number 80, including transmissions sent by an IM client to contact its server. To the firewall, the IM client looks just like any other Web browser. However unbeknownst to the firewall, the IM client sends messaging commands rather than Web surfing (HTTP) commands to its server.<sup>5</sup>

Imagine that an instant messaging client is a fugitive on the run from the authorities. The fugitive wants to cross a police roadblock (a firewall) on the main highway to reach his safe house (the instant messaging server) and hide. Because the fugitive knows that the police are blocking traffic on all lanes of the highway, he decides to take the bike path next to the highway (HTTP, port 80). Since the police assume that only legitimate cyclists (Web surfers) will use the bike path, the fugitive can safely slip by the roadblocks and reach the safe house. This analogy illustrates at a basic level how instant messaging systems avoid detection by corporate firewalls.

<sup>4</sup> Most popular instant messaging clients also support Socks proxies for companies running this proxy. This provides the client with an official way to talk through the firewall but affords no additional security.  
<sup>5</sup> Some application firewalls, such as the Symantec Enterprise Firewall, can prevent this type of tunneling over standard ports if the chat program uses a nonconforming protocol when communicating

In summary, to block instant messaging clients in a corporation, they must be prevented from reaching their IM servers. To do this, the firewall administrator must add either the server address name(s) (e.g., instantmessageserver.chatservice.com) or the server IP addresses (e.g., 11.22.33.44, 11.22.33.45) to the firewall block list for every instant messaging service to be blocked. Given that some IM systems (such as IRC) can connect to multiple independent servers, blocking these systems may require a fair amount of research; however, this is the only way to achieve the desired results with any certainty.

#### UNDERSTANDING INSTANT MESSAGING FILE TRANSFERS AND CORPORATE FIREWALLS

Because existing instant messaging systems use peer-to-peer communications to send files between users (rather than communicating through a central server that can be tweaked to allow access), it is much easier to configure perimeter firewalls to block file transfers than to block simple message exchanges.

The best way to block file transfers at the corporate firewall is to add rules to block the port number(s) used by popular IM products for peer-to-peer file transfers. This ensures that any attempt to transfer files through the firewall using one of these IM systems will be stopped. However, transfers between two users within the corporation will not be blocked by this technique. Furthermore, at least one existing commercial instant messaging system provides file transfer mechanisms that allow users to sneak past corporate firewalls. For this reason, and because no current commercial corporate firewalls scan instant messaging file transfers for viruses, organizations should deploy antivirus software on all desktops to detect any infections entering through IM services.

In the future, we will likely see the commercial release of new firewall products and other types of proxies that can scan IM file transmissions traveling between the corporation and the Internet. Symantec is currently investigating various solutions in this space.

## INSTANT MESSAGING BEST PRACTICES

Symantec recommends the following best practices for securely deploying instant messaging systems within an enterprise:

### *Establish a corporate instant messaging usage policy*

Given the risks involved in using public instant messaging systems, corporations should consider prohibiting the use of public instant messaging systems entirely, or ask employees to refrain from using public instant messaging systems for business communications.

### *Properly configure corporate perimeter firewalls*

System administrators should configure perimeter firewalls to block all non-approved instant messaging systems. Given that the firewall must block both messaging and file transfers, adding firewall rules for both cases is also a good practice.

To block messaging, an administrator may add rules to their firewall to block access to all popular IM servers. If this is not feasible, administrators can configure firewalls to block commonly used IM port numbers from all clients on the network. Note, however, that this still permits properly configured IM clients to tunnel through the firewall.

To block file transfers, system administrators can identify the port number(s) used for peer-to-peer file transfers by each IM product and configure the firewall to block all communications over those port(s).

### *Deploy desktop antivirus software*

Because current corporate firewalls are unable to scan IM file transfers for computer viruses, worms, and Trojan horses, it is imperative for an enterprise to roll out up-to-date antivirus protection on all desktops. Desktop antivirus is currently the last—and only—line of defense against IM-delivered malicious code.

### *Employ personal firewalls to ensure policy compliance*

Personal firewalls like the Symantec™ Desktop Firewall (SDF) can be configured to prevent uncertified and unapproved programs, including unapproved IM products, from communicating over the Internet. A desktop firewall can provide far more granular protection than a perimeter firewall because the desktop firewall can be configured to permit or deny communications on a per-program basis (e.g., Chat Program A can use the Internet, but Chat Program B cannot use the Internet), whereas the perimeter firewall can provide only a blanket policy for the entire machine.

*Deploy corporate instant messaging servers*

If at all possible, a corporation should deploy a secure instant messaging server on the company network and configure all IM clients to connect to this server.

A number of private companies offer IM products for sale to corporations. In addition, systems such as IRC can be obtained for very reasonable prices (or for free). Deploying one or more IM servers within the corporate network to ensure that all internal IM communications are kept behind the corporate firewall is a valuable practice.

*Recommended instant messaging client settings*

If a corporation chooses to use an external instant messaging system—one whose servers are operated by the instant messaging provider—the following security practices should be kept in mind:

1. For the best security, do not use any external IM system that does not employ a certified encryption system.
2. Configure all IM clients so that they will accept chat requests only from users specified in employees' buddy lists. This prevents attackers from connecting to computers on the network and sending malicious code. Only those users explicitly specified by employees should be able to contact them.
3. Configure the IM system to either block file transfers or allow such transfers only from users specified on the buddy list. If this is not feasible, configure the IM software to prompt the employee before all file transfers.
4. Configure the IM system to use antivirus software to scan file transfers, if supported.
5. Configure IM accounts so they are not listed on public servers. This further prevents unsolicited chat requests.

*Install all instant messaging patches as soon as possible*

System administrators should roll out new fixes as soon as possible when security holes or bugs are found in corporate instant messaging systems. CodeRed, Nimda, and even the Internet Worm of 1988 all used known vulnerabilities to spread to new systems. It is likely there will be future attacks on instant messaging systems employing similar techniques.

*Use vulnerability management solutions to ensure policy compliance*

Corporations should consider using vulnerability management (VM) tools, such as the Symantec Enterprise Security Manager (ESM), to ensure that users don't change IM client settings in a manner that violates company policy. Such tools can provide system administrators with an overall view of IM policy compliance and facilitate the process of updating machines that violate policy. VM tools also help administrators determine whether IM software is up-to-date, whether users are running versions with security holes or buffer-overflow vulnerabilities, and whether users are running company-required antivirus and personal firewall packages.

## > The future

Instant messaging usage is expected to explode through the next decade—in the home, in the enterprise, and even “over the air.” Ideally, the use of such services will bring people closer together and dramatically increase business efficiency; instant messaging may soon be as indispensable as email and the telephone. However, this growing dependence on instant messaging will place a heavy burden on the underlying IM infrastructure. Even small vulnerabilities within these communications frameworks may have huge societal and economic repercussions.

According to some estimates, over 500 million computers will have IM capabilities by 2005.<sup>6</sup> In such a world, IM systems will have the ubiquity of email, coupled with the instant-communications capabilities characteristic of IM systems. Furthermore, the growth of high-speed, always-on broadband connections in the home will increase the number of potential targets. A computer worm or blended threat directed at such an infrastructure could potentially spread at CodeRed speeds through the IM network, hitting tens or hundreds of millions of computers. If such a threat were to delete, corrupt, or encrypt the data on just of a fraction of these infected machines, it could materially affect our economy.

Another area of concern is wireless space. Consider the growing number of wireless phones already supporting IM services. Vulnerabilities in such systems could expose countless phones to a fast-spreading worm or blended threat—a wireless CodeRed or Nimda. In addition to spreading through the network, such a threat could wipe out phone lists, cause a denial-of-service to wireless Internet access or to emergency services, or cut off voice communications from compromised phones. Clearly, such an attack would be devastating.

Given the increasing penetration of instant messaging systems into our homes and offices, we must consider their security implications now, before a major attack occurs.

## > Conclusion

Due to the efficiency and convenience of their communications, instant messaging systems are rapidly becoming very important tools within corporations. Unfortunately, many of the current instant messaging systems are inadequately secured and in turn are exposing some enterprises to serious security and economic breaches.

Ideally, corporations looking to leverage instant messaging should deploy a secure, corporate-focused IM solution within the company network, and then layer suitable security systems on top of this solution (firewalls, vulnerability management, antivirus, etc.) However, many companies continue to permit employees to use popular free IM services. These organizations need to understand the associated security risks and plan accordingly.

Clearly, the growth of instant messaging systems will bring greater efficiencies to the global workplace. Only by appropriately securing these systems will businesses be able to reap their full economic benefits.

<sup>6</sup> [http://www.computerworld.com/cwi/story/0,1199,NAV47\\_ST061141,00.html](http://www.computerworld.com/cwi/story/0,1199,NAV47_ST061141,00.html)

**SYMANTEC, THE WORLD LEADER IN INTERNET SECURITY TECHNOLOGY, PROVIDES A BROAD RANGE OF CONTENT AND NETWORK SECURITY SOLUTIONS TO INDIVIDUALS AND ENTERPRISES. THE COMPANY IS A LEADING PROVIDER OF VIRUS PROTECTION, FIREWALL AND VIRTUAL PRIVATE NETWORK, VULNERABILITY MANAGEMENT, INTRUSION DETECTION, INTERNET CONTENT AND EMAIL FILTERING, REMOTE MANAGEMENT TECHNOLOGIES, AND SECURITY SERVICES TO ENTERPRISES AROUND THE WORLD. SYMANTEC'S NORTON BRAND OF CONSUMER SECURITY PRODUCTS LEADS THE MARKET IN WORLDWIDE RETAIL SALES AND INDUSTRY AWARDS. HEADQUARTERED IN CUPERTINO, CALIF., SYMANTEC HAS WORLDWIDE OPERATIONS IN 38 COUNTRIES.**

**FOR MORE INFORMATION, PLEASE VISIT [WWW.SYMANTEC.COM](http://WWW.SYMANTEC.COM).**

**WORLD HEADQUARTERS**

**20330 Stevens Creek Blvd.  
Cupertino, CA 95014 U.S.A.  
408.517.8000  
800.721.3934**

**[www.symantec.com](http://www.symantec.com)**

**For Product information  
in the U.S., call toll-free  
800-745-6054.**

**Symantec has worldwide  
operations in 38 countries.  
For specific country  
offices and contact numbers  
please visit our Web site.**