

Virus Protection for Small to Medium Networks

A White Paper

by SonicWALL, Inc.



Overview

Computer viruses are a leading security threat to Internet-connected networks. As more and more businesses have increased their productivity by using networks and high-speed Internet connections, viruses have become the most prolific and costly security issue facing small and medium organizations. And the problem appears to be getting worse each year, both in terms of the number of virus infections and the cost of cleanup.

Destructive viral programs can infect networked computers through e-mail attachments, Web content or infected files. Once a virus infects computers on your network, users can quickly damage entire networks by unknowingly downloading and launching dangerous computer viruses. Viruses can also be used as delivery mechanisms for hacking tools, putting the security of the organization in doubt, even if a firewall is installed.

This paper explains the virus threat, available anti-virus solutions, and how you can implement an effective anti-virus strategy to protect your network.

The Virus Problem

Today, there are over 50,000 known viruses with another 200 to 800 discovered each month. Virus infections have increased steadily from 1 per 100 computers in 1996 to 9 per 100 computers this year, according to the International Computer Security Association (ICSA) Labs 6th Annual Computer Virus Prevalence Survey 2000. ICSA also reports that over 99% of all companies have been infected with at least one virus in the past 12 months, and over half have experienced a virus disaster.

These virus infections come at a significant cost to companies, including resources required for cleanup, lost productivity, and damage to your company's reputation by unknowingly spreading the virus to customers. Two recent viruses alone, Melissa and LoveLetter, resulted in clean-up costs of \$385 Million and \$10 Billion respectively. Melissa took only four days to gather steam and do its damage. LoveLetter, in an order of magnitude shift, passed up Melissa's damage totals in a mere four hours.

How Virus Infections Spread

A virus is a program, which attaches itself to, overwrites, or otherwise replaces another program in order to reproduce itself. It must attach itself to a host program, usually an executable file, to replicate. E-mail is increasingly becoming the most common method of transmitting viruses. In the ICSA survey, respondents reported that 87% of viruses were spread through e-mail. According to MessageLabs, a firm that scans electronic communications for viruses, one in 700 e-mails are infected.

The LoveLetter virus took advantage of Microsoft Outlook to replicate and send itself as an e-mail attachment to everybody in the address book. The ease with which a user can click on an attachment and launch an application is a significant factor in the spread of e-mail borne viruses. To help viruses spread via e-mail, virus authors use psychology to tempt users to open e-mail attachments. For example, a virus used the header, "A great Shockwave flash movie," to entice the e-mail recipient to open the attachment.

Many businesses have virus protection, but are still vulnerable because of the challenge of keeping virus protection up to date. Anti-virus scanners rely on a database of all known viruses in order to be effective in detecting the latest viruses. Because many anti-virus scanners rely on users to keep these updates current, a serious gap exists in maintaining network wide anti-virus protection. A recent survey showed that 25% of all users neglect to install or update their anti-virus software (June 2000 Central Commands survey).

Types of Viruses

The way in which a virus becomes active depends on how the virus has been designed. Different types of viruses infect computers in particular ways; the most widespread types are Macro, Boot and Parasitic viruses.

- **Macro Viruses.** Most popular applications like Microsoft Word, Excel and PowerPoint use macros. A macro is an instruction that carries out program commands automatically. If you access a document containing a viral macro and unwittingly execute the macro virus, it can then copy itself into that application's startup files. Any document on that computer using the same application is then infected. If the infected computer is on a network, the infection is likely to spread rapidly to other computers on the network as files are sent to others.
- **Boot Sector Viruses.** When a computer is switched on, the hardware automatically locates and runs the boot sector program. This program typically resides on your hard disk and is the first software loaded onto your computer. This program then loads the rest of the operating system into memory. Without a boot sector, a computer cannot run software. A boot sector virus infects computers by modifying the contents of the boot sector program by replacing the legitimate contents with its own infected version. The result is you can't get access to your computer's operating system and data.
- **Parasitic Viruses.** Parasitic viruses attach themselves to programs, also known as executables. When a user launches a program that has a parasitic virus, the virus is given the same rights as the program that the virus is attached because the operating system understands it to be part of the program. These rights allow the virus

to replicate itself into memory. An infamous parasitic virus called Jerusalem deletes every program a user launches.

Protecting Your Network

Protecting your network from viruses requires a two-pronged strategy. The foundation of your anti-virus strategy is an anti-virus scanner designed to keep viruses from infecting computers on your network. Supporting the deployment of virus scanning technology is educating network users with common sense guidelines to further minimize the virus threat to your network.

Anti-Virus Scanners

Anti-virus scanners are at the front line of preventing virus attacks. Scanners, which scan files for viruses, are by far the most popular type of anti-virus software used today. Information about all known viruses is stored in a central database, so anti-virus scanners need to be kept updated in order to be effective. In addition, when a new virus is discovered, all anti-virus software deployed within an organization must be quickly updated with the latest virus definition files.

The widespread outbreak of viruses illustrates the problematic nature of virus defense for small and medium businesses. Users without the most current virus definition files allow these viruses to multiply and infect many other users and networks. Many small to medium businesses don't have adequate IT staff to maintain their anti-virus software. The resulting gaps in virus defenses can easily lead to data loss and decreased employee productivity.

There are a variety of anti-virus solutions available today. These anti-virus solutions fall into four categories: single-user desktop software, managed virus protection service, enforced virus protection, and server-based virus protection.

Single-User Anti-Virus Software

Single-user desktop anti-virus software is installed and maintained on each computer on a network. These widely available products typically cost around \$35 per user. Desktop anti-virus software combat viruses received from email, Internet downloads, and portable media such as floppy disks. The downside of single-user anti-virus software is it lacks any centralized management to ensure uniform and consistent anti-virus protection across a network. Desktop anti-virus software users can easily remove or disable the software if they feel the performance of their system is being adversely affected.

The use of single-user anti-virus software also means there is no unified enforcement of updates. A recent survey showed that 25% of all users neglect to install or update their anti-virus software (June 2000 Central

Commands survey). The desktop-by-desktop anti-virus approach requires network administrators to spend considerable resources to maintain network wide anti-virus protection.

Managed Anti-Virus Service

A managed anti-virus service solution frees up your organization from the hassles of managing a desktop-by-desktop anti-virus solution. Instead, an Application Service Provider (ASP) provides the anti-virus software agent for each computer on your network. Virus updates are automatically sent to each computer on the network from the ASP's anti-virus server. The managed anti-virus service provides network administrators with tools to manage virus protection including virus activity reports and centralized software license management. On the downside, ASP delivered anti-virus doesn't provide any enforcement of anti-virus on the local network and can be expensive.

Enforced Network Anti-Virus

Enforced virus protection is a hybrid anti-virus solution that adds centralized enforcement and management to the complete protection of desktop anti-virus software. Networked computers are secure against viruses in e-mail, downloads and portable media with client software automatically installed from the Internet security appliance. When users attempt to access the Internet, the Internet security appliance checks to verify each user's PC has the latest version of the virus-scanning software installed and active. In the event of out-of-date or deactivated anti-virus software, the Internet security appliance automatically updates and activates the virus protection. Anti-virus scanner updates are maintained on each desktop by the network Internet security appliance. The enforced network anti-virus solution also provides tools for management of anti-virus, such as e-mail attachment filtering and virus alerts.



Enforced virus protection is a hybrid anti-virus solution that adds centralized enforcement and management to the complete protection of desktop anti-virus software along with automatic virus updates.

Server-Based Anti-Virus

Server-based anti-virus protection adds the virus scanner software to the server acting as the Internet gateway or an e-mail server on the local network. An e-mail anti-virus solution resides on the e-mail server and scans all e-mail attachments for viruses. The gateway anti-virus solution resides on the server being used as the Internet gateway and scans all Internet data traffic for viruses. Server-based anti-virus provides robust virus protection designed to scan all traffic traveling across the network, but it comes with an expensive price tag because it requires intensive IT resources to manage the anti-virus system. And while these server-based approaches provide virus protection for Internet-borne viruses, they don't provide protection for portable media borne viruses.

Combining e-mail server anti-virus with an enforced network anti-virus solution provides the highest level of protection currently available. However, the incremental benefit provided by stopping all viruses before they get to the user must be weighed against the expense and resources required to implement and maintain this type of solution.

Evaluating Your Virus Protection Options

Choosing the right anti-virus solution requires evaluating what are your risk tolerances, IT resources, and budget constraints. Each virus protection method has benefits and drawbacks. The question comes down to the reasonable level of risk that you are willing to take and the amount of money you are willing to pay to alleviate that risk level. Here are guidelines to help you evaluate the best anti-virus solution for your organization.

- **Look beyond the cost of the product itself.** Take into account the total cost of ownership over the life of the product. Your budget for any anti-virus solution should include the costs of required IT resources and the often hidden costs of software upgrades required to keep the product up-to-date.
- **Implement an anti-virus solution that incorporates desktop protection.** Anti-virus protection at the desktop level is the most effective way to combat viruses from all sources including e-mail, Internet downloads, and portable media. However, single user desktop anti-virus software without centralized network enforcement leaves a big virus protection hole open: the user.
- **Use desktop scanning with real-time enforcement and updates for every computer on the network.** This hybrid approach

combines desktop anti-virus protection with enforced network anti-virus protection to provide the most effective anti-virus method, according to the International Computer Security Association (ICSA).

- **Add e-mail server protection only after the desktop is secured.** However, the incremental benefit provided by adding anti-virus protection at the e-mail server must be weighed against the cost and complexity required to implement and maintain this anti-virus solution. Least in importance is file and print server protection.

Virus Prevention User Education

To effectively supplement your anti-virus scanning products, network users need to be vigilant about viruses. User education plays an important role in preventing infections by keeping users from installing software or opening email attachments without considering the consequences. Combining virus scanner protection with the following common sense guidelines can minimize the virus threat to your network.

1. **Do not open unexpected attachments.** Most viruses are sent as e-mail attachments. Virus transmission via e-mail is insidious because users often will open attachments thinking it was sent by acquaintances, co-workers or friends, only to find the attachment is in fact a virus. Don't execute any attachment until your anti-virus scanner has processed it or be sure the attachment has been knowingly sent by a trusted source. If you didn't expect the attachment, take a moment to confirm with the sender that they did in fact send the attachment.
2. **Make sure your anti-virus software updates itself regularly.** Anti-virus software scanners are only able to detect and delete a computer virus that is found in its anti-virus database. This is why it's very important that anti-virus scanner get updated regularly. The more often the database is updated, the more viruses the anti-virus scanner will be equipped to detect and destroy.
3. **Install patches for software you use.** There are viruses that exploit "holes" or vulnerabilities in operating systems and applications. Anti-virus programs are generally able to protect you from this kind of viruses even if you have not installed the appropriate patch for that vulnerability. However, installing security patches adds another layer of protection against viruses.
4. **Always scan floppy disks and CDs for viruses before using them.** While e-mail is the most common form of virus distribution, don't ignore the traditional transport mechanism for viruses: floppy disks, CDs or any portable storage media. You should always check these external media for viruses before using it.

5. **Block Executables.** The blocking of executable programs as e-mail attachments, such as EXE and VBS files keeps these virus carriers at bay. Don't use self-extracting ZIP files to send or receive files. Instead use statically compressed ZIP files that need to be unzipped before they can be executed so they can be scanned for viruses.
6. **Be careful with downloaded software.** Software is widely available on the Internet and it can be infectious. Not only pirated software, but also software from well-established, credible vendors can contain viruses. Always scan any software you download from the Internet for viruses before you install it.
7. **Back up your data on a regular basis.** While backing up your data won't protect you against a virus infection, it will allow you to protect your valuable data in case your computer becomes infected. Back up your most valuable data using external media storage devices.
8. **Create a virus-free start-up disk for your computer.** An infected computer can be made inoperable by preventing the operating system from being loaded. To solve this problem, you should create a start-up disk for your operating system that will help you start your computer and delete any viruses in your operating system.

SonicWALL's Network Anti-Virus Solution

SonicWALL Network Anti-Virus delivers industry-leading, proactive virus protection with zero administration. Developed in partnership with McAfee, the market leader in business anti-virus solutions, SonicWALL Network Anti-Virus dramatically reduces time-to-protection with advanced heuristics and automatic alerts to provide the most reliable anti-virus solution on the market today.

SonicWALL Network Anti-Virus is also the only zero administration solution that automatically manages all aspects of virus protection including client auto-installation, virus definition updates, and network-wide policy enforcement to significantly reduce support costs.

SonicWALL's Network Anti-Virus is a subscription-based service for SonicWALL's family of Internet Security Appliances that transparently monitors virus definition files, and automatically triggers new virus definition file downloads and installations for each PC on the network. Acting as an auto enforcer of virus policy, the SonicWALL Internet Security Appliance with SonicWALL Network Anti-Virus ensures every PC accessing the Internet has the most up-to-date anti-virus software installed and active, preventing the spread of new viruses or a rogue user from exposing the entire organization to an outbreak.

SonicWALL Network Anti-Virus Features

SonicWALL Network Anti-Virus includes these features:

- **Auto Anti-Virus Policy Enforcement.** SonicWALL Network Anti-Virus verifies every PC accessing the Internet has the most up-to-date version of anti-virus software installed and active to guarantee enforcement of your organization's virus protection policy to prevent the spread of viruses or a rogue user from exposing the entire organization to an outbreak.
- **Advanced Anti-Virus Technology.** SonicWALL Network Anti-Virus, based on McAfee anti-virus technology, dramatically reduces time to protection with advanced heuristic technologies and automatic alerts backed up by McAfee's Anti-Virus Emergency Response Team (AVERT) with than 90 researchers worldwide.
- **Zero Administration to Reduce Support Costs.** SonicWALL Network Anti-Virus automatically manages all aspects of virus protection including client auto-installation, virus definition updates, and enforcement of virus protection to significantly reduce the time and costs of managing virus protection.
- **Early Warning Virus Alerts.** With SonicWALL Network Anti-Virus, the administrator is kept abreast of newly discovered serious viruses. When virus alerts are issued, the information is logged in the SonicWALL Internet security appliance and an e-mail alert is sent to the administrator with detailed information on the virus.
- **Network-Wide Virus Protection.** SonicWALL Network Anti-Virus ensures all the PCs on a network are protected by automatically and transparently updating the virus software on every computer on the network.
- **Efficient License Sharing.** SonicWALL Network Anti-Virus enables organizations with distributed security networks of multiple SonicWALL Internet security appliances to efficiently allocate Anti-Virus licenses to meet changing conditions.
- **E-Mail (SMTP) Attachment Filtering.** SonicWALL Network Anti-Virus enables custom rule configuration for filtering potential virus carrying e-mail (SMTP) attachments. A network administrator can either delete or disable e-mail attachments based on a centralized list of file extensions.

How SonicWALL Network Anti-Virus Works

The key to the SonicWALL Network Anti-Virus enforcement process is based on a series of communications between the McAfee VirusScan agent, which resides on the desktop and the SonicWALL Internet Security

Appliance. Whenever a desktop computer attempts to send traffic across the SonicWALL, a request for the version of the VirusScan files is automatically returned to the desktop. If the desktop does not respond, or if it responds with an outdated version, the SonicWALL triggers a transparent, automatic update to ensure that all users are updated on a regular basis before they use the Internet.

SonicWALL provides real-time virus information and alerting to SonicWALL Network Anti-Virus subscribers. When a fast moving, dangerous virus is discovered, we will notify you immediately and provide as much detailed information as possible. This allows you to take immediate action with your users, warning them of the characteristics of the new virus. Additionally, you can add the new virus to the list of e-mail attachments to be filtered, immediately providing a base level of protection against the new threat.

When the fix is available, in the form of updated McAfee VirusScan virus files, an alert is sent to your SonicWALL Internet Security Appliance, which automatically triggers immediate enforcement of the new files for all users as they attempt to access the Internet. This automatic enforcement in the event of alerts ensures that you have the latest protection as soon as it is available. And it is fully automated, so once you have enabled the virus-alerting feature, SonicWALL will take actions to protect your network from the next virus outbreak whether or not you are available.

Be Vigilant About Viruses

Viruses are everywhere on the Internet, and you need to protect your LAN from the havoc they can create. Integrating a virus protection strategy into your overall Internet security plan is essential. Any effective anti-virus strategy requires a careful balance between the amount of acceptable risk and the total cost of ownership for any anti-virus solution. For small to medium businesses, an anti-virus strategy requires an affordable and easy to manage virus scanner solution to ensure your network is protected. SonicWALL Network Anti-Virus blends desktop anti-virus with centralized and enforced management to create a complete, easy-to-use and affordable anti-virus solution.

To learn more information on how SonicWALL can help you protect your business, call 1-888-557-6642 or visit us at www.sonicwall.com.



SonicWALL, Inc

E-mail: info@sonicwall.com

Web: www.sonicwall.com

©2001 SonicWALL is a registered trademark of SonicWALL, Inc. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.