



## Virus Protection for Small to Medium Networks

### 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.

### THE VIRUS PROBLEM

Today there are over 50,000 known viruses with another 200-800 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 6<sup>th</sup> 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.

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).



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 Viruses, Boot Sector Viruses, and Parasitic Viruses.

### 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 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.

## SOLUTIONS:

**Single-User Anti-Virus Software:** Single-user desktop anti-virus software is installed and maintained on each computer on a network. Desktop anti-virus software combat viruses received from email, Internet downloads, and portable media such as floppy disks. However, there is no centralized management and the systems are dependent upon users to access updates routinely.

**Managed Anti-Virus Service:** Management of the anti-virus software is handled by an Application Service Provider (ASP). Virus updates are automatically sent to each computer on the network from the ASP anti-virus server.

**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 email, downloads and portable media with client software automatically installed from the Internet security appliance.

**Server-based Anti-Virus:** Server-based anti-virus protection adds the virus scanner software to the server acting as the Internet gateway or an email server on the local network. 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 system.

## YOUR OPTIONS

- Look beyond the cost of the product itself.
- Implement an anti-virus solution that incorporates desktop protection.
- Use desktop scanning with real-time enforcement and updates for every computer on the network.
- Add email server protection only after the desktop is secured.

## USER EDUCATION

Here are some common sense guidelines that can help minimize the virus threat to your network.

1. Do not open unexpected attachments.
2. Make sure your anti-virus software updates itself regularly.
3. Install patches for software you use.
4. Always scan floppy disks and CDs for viruses before using them.
5. Block executables file attachments.
6. Be careful with downloaded software.
7. Back up your data on a regular basis.
8. Create a virus-free start-up disk for your computer.

Summarized from *Virus Protection for Small to Medium Networks: A White Paper* by SonicWALL, Inc. 2001.

