



**astaro**  
internet security

[Astaro Firewall](#)

## Virus Protection Whitepaper

### **Desktop and gateway virus protection: why you need both**

Version: 1.00

Release date: January 27, 2004

Author: Alan Radding

Alan Radding, BA, MS, is an independent researcher/analyst specializing in technology and business.



## Desktop and gateway virus protection: why you need both

---

Astaro [www.astaro.com](http://www.astaro.com) [info@astaro.com](mailto:info@astaro.com)  
Pfinztalstrasse 90, 76227 Karlsruhe, Germany  
67 S. Bedford Street #400W, Burlington MA, 01803 USA

### Table of Contents

<b>Good news/bad news on the virus front</b> .....	<b>3</b>
<b>Approaches to virus protection</b> .....	<b>3</b>
<b>Why you need both</b> .....	<b>4</b>
Desktop advantages.....	4
Gateway advantages.....	4
<b>Recommendations</b> .....	<b>5</b>
<b>Selecting a virus protection gateway</b> .....	<b>6</b>
<b>Astaro Virus Protection Gateway</b> .....	<b>6</b>
<b>Conclusion</b> .....	<b>6</b>

## Good news/bad news on the virus front

Like the punch line of a bad joke, there is good news and bad news about the current state of computer viruses. The good news is that there was a slight decrease in the level of reported virus attacks, 82% of survey respondents reported virus attacks in 2003, down from 85% in 2002, according to the latest Computer Security Institute (CSI) data.

The bad news: any organization that got hit with the SoBig virus or any of the other viruses that wreaked havoc this past year saw how the virus wars continue to rage without letup. For managers on the front lines battling viruses, there has been no discernible decrease at all. If anything, from their standpoint, "the attacks are increasing," reports David Gillies, director of information services at Heating and Cooling Supply LLC, San Diego. And there is nothing to suggest any letup in the foreseeable future.

In 2003, companies reported that the cost of virus attacks alone exceeded \$27 million, more than 10% of the total value of losses from all security breaches combined.

The message from the data is clear: organizations must continue to battle viruses and bolster their anti-virus defenses. This certainly is Gillies' strategy at Heating and Cooling Supply, which now runs both desktop and gateway (perimeter) virus protection.

## Approaches to virus protection

Traditionally there have been two basic virus protection strategies, perimeter defense and desktop defense. In perimeter defense, the organization establishes an anti-virus gateway, which intercepts all traffic at the perimeter and scans it for viruses. The desktop defense, on the other hand, puts anti-virus capabilities on each desktop to protect against viruses locally. Typically, companies employ one or the other strategy.

Increasingly, however, companies like Heating and Cooling Supply, are combining the two strategies by implementing a virus protection gateway at the perimeter as well as putting anti-virus capabilities on all desktops or at least those most at risk of a virus attack.

The gateway runs on a single computer (or gateway appliance) that sits at the Internet's point of entry to your organization. It scans all inbound and outbound email for viruses using the most up-to-date list of virus signatures. Because gateways reside on a single computer, it is easy for administrators to maintain them, ensuring that the latest security updates are immediately deployed and that the gateway is available and operating properly 24/7.

Desktop defense relies on virus protection software on each desktop. Like the gateway, the desktop virus protection software scans all incoming and outgoing email and any other software on the system for viruses and takes appropriate actions when a virus is detected. Desktop defense, however, suffers from the problems that plague desktop system management in general—multiple configurations and difficulty controlling and enforcing proper user behavior. As a result, it is difficult to apply virus protection upgrades in a timely manner and user actions may unwittingly thwart the virus protection effort.

## Why you need both

Gateway and desktop virus protection bring their own advantages and disadvantages. For effective virus protection organizations need both gateway and desktop defense. This allows the organization to take advantage of the strengths of each while offsetting the weaknesses.

### *Desktop advantages*

The advantage of desktop virus protection is its ability to scan the entire desktop and protect everything there regardless of how it gets into the system. For example, workers might introduce viruses through floppy disks or CD ROMs. The growing use of portable USB storage and memory devices with desktops also opens another avenue in which viruses can be introduced. These avenues—floppies, CD ROMs, USB devices—bypass the gateway defense altogether.

In addition, some desktop systems actually are laptop or notebook systems sitting in a desktop docking station. When these systems are taken outside the organization and used on a network (e.g., using a hotel (Internet connection), they go beyond the protection of gateway virus defense. These systems especially need their own local protections.

The disadvantages of desktop virus protection have been identified above. To recap, they are difficult to deploy on a widespread basis, differences in configuration make them difficult and costly to maintain and slow to update. Finally, they can be thwarted by user behavior.

### *Gateway advantages*

Gateway virus protection prevents viruses from getting into the organization in the first place by stopping them at the perimeter. As noted above, gateway defense is easier and faster to set up since only one system, the gateway server or appliance, need be deployed. Similarly, it is easier, faster, and less costly to maintain the gateway and update virus protection because administrators are dealing with only one system. With a gateway, the organization is assured of the latest, most up-to-date virus protection. The gateway can be backed up to ensure reliable 24/7 protection. Finally, professional administrators are more accountable when it comes to security than are end users.

While the gateway is effective in defending against viruses coming in over the network, it cannot protect against viruses that enter in other ways. As noted, floppy disks, CD ROMs, and USB devices all bypass gateway defense, and systems that travel outside the organization are beyond the protection provided by the gateway.

By combining gateway and desktop virus protection, the organization is able to defend against viruses regardless of how they may enter the organization. The combined defense protects all the code, not just traffic coming across the network.

## Table: Approaches to Virus Defense—Advantages, Disadvantages

Defense Approach	Advantages	Disadvantages
<b>Desktop</b>	Protects all code on the system regardless of how it gets in Protects system when traveling outside the network	Difficult to deploy Difficult to maintain and update Easily thwarted by user action
<b>Gateway</b>	Provides most up-to-date protection Stops viruses before they enter the organization Easy to deploy, maintain, update	No protection against viruses entering in ways other than the network
<b>Combined</b>	Provides all the advantages of desktop and gateway defense	Increased cost

## Recommendations

As we have demonstrated, these two approaches to virus protection are complementary. According to International Data Corp. (IDC), a leading technology research firm based in Framingham, MA, "...there will be a strong push toward a layered security ... The layered security approach will combine solutions such as desktop anti-virus, server and gateway (perimeter) anti-virus, content filtering...and firewalls. " Clearly, deploying both gateway and desktop protection is the optimal strategy.

If budgets are limited the perimeter approach is easier to administer, more secure and more cost effective. According to the Yankee Group, a technology research firm based in Boston, "If you filter anti-virus as a network appliance (perimeter gateway), your risk gets shortened and you have less dependency to keep desktop anti-virus up-to-date."

You can, however, stretch your virus protection budget as Heating and Cooling Supply did by implementing gateway protection while providing desktop protection for selected desktops, those that are most at risk. At Heating and Cooling Supply, that meant protecting laptop systems that are periodically removed from their docking stations and taken beyond the network.

## Selecting a virus protection gateway

The following factors will help you find the right virus protection gateway:

- Integration with the other security applications—this simplifies security administration and lowers overall TCO
- Security track record—look for a gateway from a vendor with a proven track record in identifying viruses quickly
- Extremely current virus definition database—look for a comprehensive virus definition database that is continually updated and which offers a simple, fast update process

## Astaro Virus Protection Gateway

Although many vendors promise to provide effective gateway virus protection, Astaro has a proven track record of delivering. Two hundred and fifty engineers constantly monitor the Internet to identify and automatically download information on new viruses. Signatures of new viruses, which average 300 a week, are added to the existing database of 60,000 signatures as they are discovered and delivered to customers through frequent automatic updates. Astaro's same Up2Date service also provides updates for all other security applications in Astaro's comprehensive security solution, as well as enhancements to the basic virus detection engine.

In addition, Astaro integrates virus protection with a host of other security services, including firewall, VPN, spam filtering, and URL filtering, as part of its comprehensive solution. The availability of all these capabilities through a single, consistent interface will reduce the workload on the organizations system administrators, which will significantly reduce the TCO.

## Conclusion

Defending against viruses at both the perimeter and on the desktop provides a comprehensive defense against computer viruses, regardless of how they are carried into the organization. Given that today's Internet environment is increasingly hostile, every organization can expect to be subject to multiple virus attacks during the coming years. To protect against costly losses both gateway and desktop anti-virus solutions should be deployed.

In addition, Astaro complements virus protection with an integrated comprehensive security solution that delivers greater security, lower TCO, and simplified operation. A free 30-day evaluation version can be downloaded at <http://www.astaro.com/php/download.php> to verify operation in your environment.