

## Protect employee productivity and corporate data from the most frequent form of electronic attack

[Astaro Firewall](#)

E-mail has become one of the most frequent means of communicating with customers, suppliers and employees. Widespread adoption has also made it the number one vehicle for launching electronic attacks, using malicious code embedded in e-mails or attachments. Astaro Security Linux is a complete, integrated suite of security software. It is installed on standard PC hardware and placed at the point where the Internet connects to an organization's network. It provides the capability to scan and eliminate inbound and outbound e-mails containing viruses and other dangerous content.

### Approaches to Virus Protection

There are two common forms of virus protection available:

1. Host-based scanners: These are software applications installed on every computer in the organization, including mail servers and desktop PC's. They scan each file received or sent from that system. While they are valuable, they suffer several weaknesses:
  - Configuration problems or being powered down (disconnected) from the network can keep the software from getting the updates needed to catch current viruses. Due to the volume of computers, administrators cannot keep them all configured correctly.
  - Employees are known to turn off their desktop scanners to eliminate the processing slow downs and delays e-mail desktop scanners can cause while in "receiving" mode.
  - A pure host-based approach to virus protection causes service calls to be generated across the organization. Whether it is a user asking for guidance when a virus is identified, the need to disinfect due to configuration issues, or the need to manually screen a rapidly spreading new virus before updates are downloaded to the computers, a host-only virus strategy is labor intensive.
  - Host-based systems typically act only on files written to the disk, leaving the system vulnerable to memory resident viruses.
2. Perimeter-based scanners: These are virus scanning programs, like Astaro's, which reside on a single computer (or gateway appliance) that sits at the Internet's point of entry to your organization, scanning all inbound and outbound e-mail. Benefits of this approach include:
  - Single point of administration, meaning this first line of defense can easily be maintained. In the case of new, rapidly spreading viruses, the administrator can create filters at a single point to catch the virus before automatic updates are available.
  - Viruses are stopped at the edge of the network, before they spread to numerous hosts. This eliminates the risk of infection due to mis-configuration, memory resident viruses, local host clean-up calls, and so forth.
  - Perimeter systems are specialized secure computers, while host-based systems run on standard computers that the viruses could attack to circumvent the scanners.

### Recommendations

In fact these two approaches to virus protection are complementary. According to IDC, a firm that studies the security industry, "...there will be a strong push toward a "layered security" ... The layered security approach will combine solutions such as desktop antivirus, server and gateway (perimeter) anti-virus, content filtering...and firewalls. " However, if budgets are limited, the perimeter approach is easier to administer, more secure and more cost effective. According to the Yankee Group, another security specialist, " 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."

### Astaro Security Linux's Virus Protection Option

The Virus Protection option provides unsurpassed accuracy in the identification of malicious code embedded in e-mail bodies and attachments by using a combination of detection mechanisms including virus signatures, heuristics and emulation. A staff of 250 people constantly monitors the Internet to identify and automatically download information on new viruses to your local Virus Protection option. Messages containing specific file types or text strings can also be blocked, providing extra security and fast response to new threats.