

How can I maintain optimum security on Linux workstations?

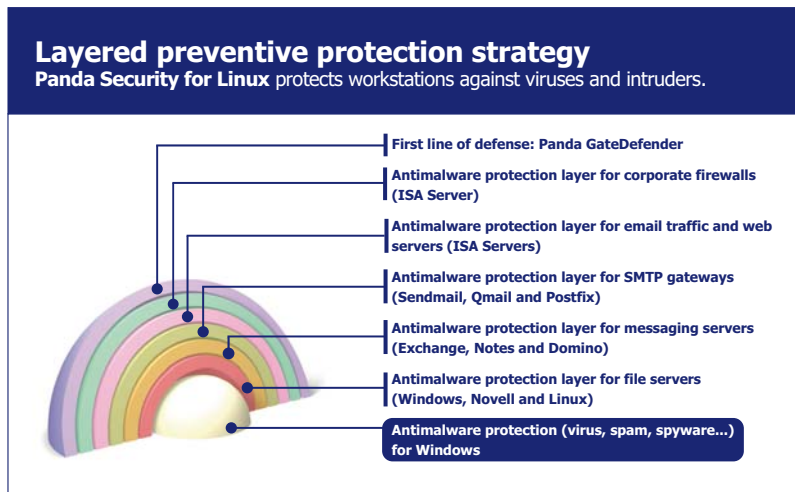
Many corporate IT environments are made up of a variety of platforms to adapt to the specific needs of different areas. These often include Linux systems that could store or email infected Windows files.

The mistaken belief that Linux does not have any **vulnerabilities** or that it is not the target of attacks, along with the difficulties involved in installing Linux on workstations means that these computers are sometimes left unprotected. This decision puts the **security** of the entire company at risk, as it opens an entry-point for malware.

Protection designed exclusively for Linux workstations

Panda Security for Linux, the ideal solution for companies with Linux distributions installed on their workstations. It is designed to respond to the **specific demands** of desktop computers running this operating system.

This powerful solution incorporates, in an intuitive graphic interface, antivirus technologies, heuristic technologies and a firewall aimed at protecting Linux computers from malware, and preventing these computers from being used as a gateway to spread infections across the Windows workstations in the local network.



Main benefits

- **Prevents loss of data** caused by hacker attacks and all types of malware that infiltrate workstations.
- **Protects your external communications**, whether by email, Internet or other applications.
- **Improves productivity**, thanks to its ease-of-use and automatic updates.

Key features

- **Antimalware protection** against both Windows and Linux threats, including dialers and spyware.
- **Mail protection.** Resident mail protection that scans and disinfects mailboxes in the most widely used mail clients, such as Ximian or Mozilla.
- **Ease of use.** Designed to optimize your time, allowing you to see the protection status at a glance, using the system's self-diagnosis feature.
- **Powerful firewall.** From the X-Windows interface, you can configure the connections, detect intruders and assign access permissions to programs.
- **Flexible updates.** The automatic update mechanism protects the user transparently.
- **Customized service.** Get advice about installation and responses to your queries and incidents within 24 hours.



Anti-malware protection

Panda for Linux uses a signature file to detect viruses, worms, Trojans, **spyware** and dialers, neutralizing all types of malware regardless of its origin: Windows or Linux.

Panda for Linux also incorporates a latest generation and highly effective heuristic engine that can detect potential threats and block them until the disinfection routine is available.

Permanent mail protection

Email is the main means of propagation used by malware. It is essential to ensure that you have **permanent protection** that monitors the email messages sent to users' mailboxes in order to disinfect malware before it infects the file system.

Panda for Linux scans mail traffic in the most widely used clients, such as Ximian Evolution, Kmail, Mozilla Mail and Thunderbird; and clients compatible with "standard Unix mailbox" format.

Ease of use

To ease implementation of the solution, **Panda for Linux** provides an intuitive graphic interface based on **X-Window**, which is fully compatible with most distributions and desktops on the market, including **Gnome and KDE**.

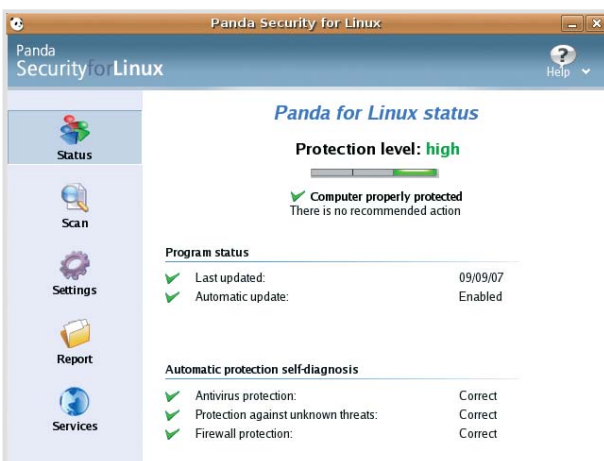
Panda for Linux also offers local warnings displayed in a pop-up window, as well as a **self-diagnosis** system. This allows you to see the current situation at a glance or get reports and statistics for more detailed information about virus incidents.

Powerful firewall

Panda for Linux includes firewall technology.

The **application rules** in **Panda for Linux** let you control the connection permissions assigned to the applications installed on a computer, as if it were a personal firewall.

This firewall can also be configured using **system rules** to administer external connections.



Flexible updates

Panda for Linux is updated automatically via the Internet and therefore does not require additional files to be deployed.

The scans can be scheduled and the daily malware signature file updates can be configured, significantly **reducing the impact on communications**. These updates are incremental in order to reduce bandwidth consumption.

Finally, **Panda for Linux** includes a cache of files scanned. This system improves the **performance** of the permanent protection so that it is almost imperceptible to the user.

Customized service

Clients of **Panda for Linux** licenses can access a wide range of complementary services that allow the product to adapt to the precise needs of the client.

As well as the software upgrades and malware signature file updates, the solution also includes, at no extra charge, **24h-365d** telephone and email **Tech Support, SOS** service to analyze suspicious files and provide a solution within 24 hours.

Technical requirements

Minimum requirements:

CPU: Pentium II 400+ MHz (or equivalent AMD).
RAM: 128 MB
Disk space: 20150 MB free space.

Recommended:

CPU: Pentium III 800+ MHz (or equivalent AMD).
RAM: 256 MB.
Disk space: 200 MB Free space.

Distributions supported:

Ubuntu: 6.06, 6.10, 7.04; OpenSuse: 10.1 y 10.2; Fedora Core: 6; Debian: 3.1 (sarge) y 4.0 (etch); Red Hat Enterprise: 4 (Desktop, Workstation, Server) y 5 (Client); SUSE Enterprise: 10; Mandriva: 2007, 2007.1.



Remember **Panda Security for Linux** can be bought independently or as part of **Panda Security for Business** or **Panda Security for Enterprise**.



Get your evaluation of Panda Security for Linux.
www.pandasecurity.com

PANDA
SECURITY