

Versatile management of the protection against viruses, spam and spyware for all users

Postfix servers never have the same configuration, not even those within the same company, as they need to be adapted to the function they carry out (mail gateway or server), the profiles of the users whose mailboxes they manage and the characteristics of the computers running them.

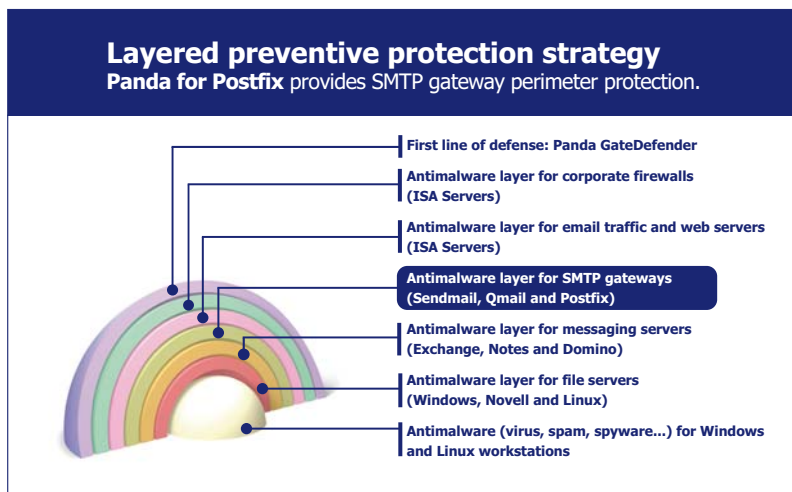
The **mail service offered by these servers must be protected** from the threat of hackers and intruders that try to penetrate the corporate network perimeter in order to steal information, distribute junk mail or interrupt the service on users' computers.

This situation requires the application of a **coherent and customized security policy** for each type of malware that adapts to the needs of each Postfix server.

An easy-to-manage customized solution offering complete protection for SMTP mail

Panda Security for Postfix provides specific anti-malware protection for messages received **via SMTP** in the Postfix mail systems used by companies and ISPs.

Panda Security for Postfix integrates seamlessly **with Postfix**, when acting as an independent gateway (channeling traffic to other servers) or as a mailbox server (delivering emails to their final destinations).



Main benefits

- Customizable security policies help protect **corporate image**, avoid fines for failure to comply with regulations, prevent industrial espionage, data theft, etc.
- Boosts administrator and end-user productivity.
- **Maximizes email communication security**, preventing the spread of infections.
- Gets the **most out of mail server**

Key features

- **Complete protection for email traffic. Detects all malware** (viruses, hoaxes, spyware, etc.). The whole message is deleted in the event of denial of service attacks.
- **Complete and accurate antispam protection** - easy to configure and set up.
- **Blocks new threats** with ultra-reliable heuristic techniques.
- **Optimized performance and detection ratios** based on in-memory scanning.
- **Seamless integration with Postfix technology.**
- **Centralized and remote administration** through a web-based console or with the Windows management and deployment tool AdminSecure.
- **Hourly updates** of the malware signature file.



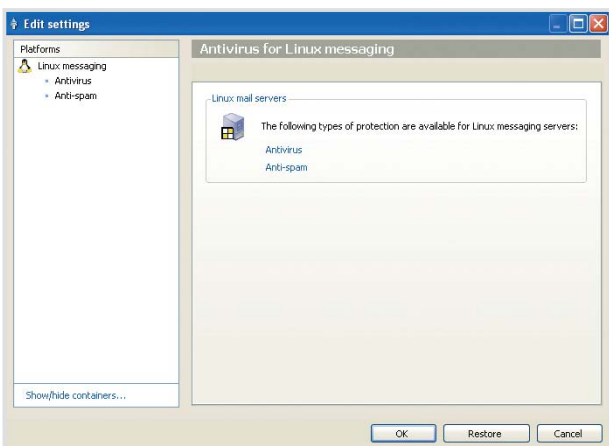
Complete mail protection

Panda for Postfix stands out for its ability to scan and disinfect malware in the body of messages in any format: plain text or HTML. It can also check attached files, compressed files, nested messages and even embedded OLE objects, for all types of malware, such as spyware, adware, phishing, worms, Trojans, dialers, jokes, hoaxes, security risk and hacking tools.

Panda for Postfix scans all messages, both those sent to Postfix server mailboxes and those sent to other servers using the Postfix content filter.

Complete and accurate antispam protection

Panda for Postfix incorporates an advanced anti-spam engine based on **rules, lists, patterns, Bayesian algorithms and remote learning** in order to optimize the accuracy of the spam classification process. **Panda for Postfix** detects hoaxes and junk mail that use false NDR messages. It offers several levels of sensitivity and includes senders and domains in white lists and blacklists and identifies spam in the subject of the message to improve user experience.



Blocking of new threats

The advanced *Genetic Heuristic Engine* (GHE) in **Panda for Postfix** detects new threats and isolates suspicious code. It also automatically requests analysis from Panda in order to disinfect threats and notify the sender or recipient of the message in just a few hours.

Optimized performance and detection ratios

Panda for Postfix adapts to your precise needs, allowing you to configure and select the domains and email addresses to scan or exclude from scanning, allowing the protection to be prioritized if the server becomes saturated.

Its innovative technology scans all types of compressed file in memory much faster than antivirus products that need to copy them to hard disk, resulting in optimum scan performance and faster message processing.

Maximum integration with Postfix

In addition to the latest generation scan engine, **Panda for Postfix** uses the latest technologies recommended for integration with Postfix and the Linux distributions it works with to obtain maximum performance in multi-thread environments with multiple processors. This makes it the perfect solution for these platforms.

Remote, centralized administration

Panda for Postfix can be managed from two administration consoles in order to facilitate installation and monitoring of incidents and updates across the network.

As well as using the traditional web console, **Panda for Postfix** can now be administered from Windows with **Panda AdminSecure**. This tool remotely controls the protection level of each mail server and of the rest of Panda's solutions through different view options, graphic reports, warnings, etc. in order to provide a global, real-time view of the protection status of the company.

Hourly automatic updates

Panda for Postfix can be configured to check hourly whether new signatures are available, and if so, update automatically. The incremental updates of the malware and spam signature file help reduce bandwidth use and mitigate communication traffic peaks.

Technical requirements

Pentium processor 200 MHz, 64 MB RAM and 90 MB free hard disk space.

Operating system to integrate with AdminSecure or independent installation: Red Hat 7.2 or 9, Red Hat Enterprise 2.1, 3 AS/ES or 4 AS/ES, Debian 3.0 or 3.1, Mandrake 9.0, 9.1 or 10, Mandrake Corporate Server 4.0, Suse 8.1, 8.2, 9.0, 9.1 Professional, 9.2 Professional, 9 Enterprise Server or 10 Enterprise Server.

Web console: Internet Explorer 4.0 (or later), Netscape Navigator 4.6 (or later).

Panda AdminSecure: Pentium III 800 MHz, 512 MB RAM, 512 MB hard disk.



Powered by:



Remember **Panda for Postfix** can be bought separately or as part of **Panda Security for Enterprise**.

Get your evaluation version of Panda Security for Postfix.
www.pandasecurity.com

PANDA
SECURITY