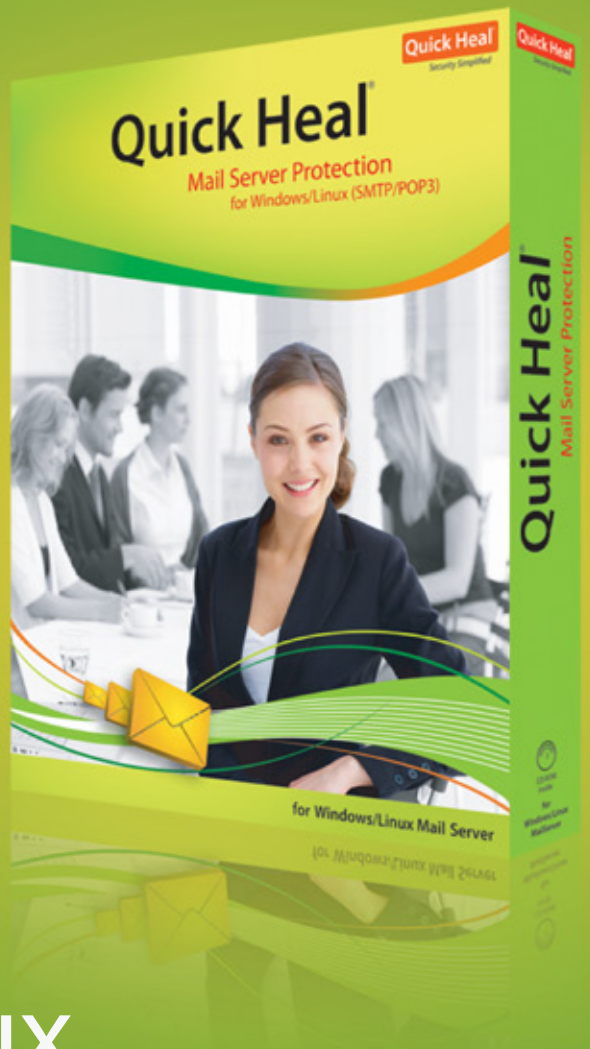
Quick Heal®

Security Simplified



Quick Heal
Mail Protection for Linux

Scan. Prevent. Monitor.

Feature List

Anti-spam technology removes the vast majority of unsolicited emails before they get to the mail server. Robust solution prevents virtually all known malicious codes from entering and propagating across the network.

- Prevents internal threats from utilizing your resources to spread viruses or spam.
- Inbuilt proactive techniques that allow seamless control of web traffic.
- Black list and white list facility for spam control.

Powerful platform independent scan engine

The advanced scan engine resolves all compatibility and detection problems with its more powerful and scalable technology, regardless of the system the virus is stored in or made for.

- The application scans for and removes all types of viruses, Trojans, spyware, malicious and potentially hostile programs from incoming and outgoing mail messages and attachments in most formats.
- Powerful command line scanner runs a scan with strictly required programs like any directory or files in your computer especially those that are newly downloaded or installed files.
- Provides automatic and incremental updates.
- DNAScan technology helps to shield businesses from zero-day and targeted attacks.
- Scans files inside archive attachments (ZIP, ARJ, GZIP, RAR, TAR, CAB etc.) using information about file type, name and message size.

Robust anti-spam engine

Powerful spam filters ensure that fewer spam emails get through the email system. This helps prevent businesses from zero-day spam attacks and outbursts.

Black and White lists for email communication

Personal and global black lists and white lists can be maintained to restrict or allow email communication from senders that are known to be either malicious or genuine. These lists can be incorporated on a server wide basis or to machines on an individual basis.

Effective attachment filters

Outgoing and incoming attachments are persistently scanned to detect any prevalent threats or files that could violate copyright policies or lead to data theft or company liability. Details significant to the attachment size, nature and content are scanned actively.

Automatic Updates

Quick Heal Mail Protection can be configured to upgrade the scan engine automatically.

- With an active Internet connection antivirus updates are released on daily basis.
- The updates are incremental and smaller in size that guarantee that your protection is always up-to-date without utilizing too much of your Internet bandwidth.

Simple Deployment and maintenance

Web-based user interface makes configuration and monitoring of the protection from any platform workstation. Allows users to set up personal black lists and white lists and manage their own quarantined items.

Easy Integration

Simple to install and easy to use. Quick Heal Mail Protection for Linux can be easily integrated with popular Linux-based Mail Transfer Agents (MTAs) like Sendmail, Qmail, Postfix, Exim, PostMaster etc.

Flexible reporting and log distribution

The dashboard provides a unified platform for threat reports and notifications. These reports can be customized extensively based on past incidents to inform system administrators as well as document owners about active threats. The reports can also be viewed in multiple formats to facilitate easy distribution. A detailed log is also maintained that allows easy scrutiny to study threat patterns.

Product Highlights

Powerful and advanced scan engine based on platform-independent technology prevents internal threats from utilizing your resources to spread viruses or spam.

- Potential threats are monitored and analyzed in real-time to block dangerous actions, before any harm is caused.
- Helps businesses to enforce their email usage policy and can help to address corporate liability issues that can arise when users try to distribute illegal music or video files via the corporate email system.
- Easy integration with most popular Linux Mail Transfer Agents.

System Requirements

To use Quick Heal Mail Protection for Linux,must meet following system requirements:

Platforms

- Redhat Linux 8.0 and above
- SuSe Linux 7.2
- Mandrake 8.0 and above

Minimum system requirement

- 300 MHz Pentium Processor
- 128 MB of RAM or higher
- 40 MB of hard disk space
- DVD or CD-ROM drive

Mail Servers

- Sendmail
- Qmail
- Postfix
- Exim
- PostMaster etc.