



Trend Micro™ ServerProtect™ for Linux™

Stops Viruses from Spreading through Linux Servers

Linux Acceptance on the Rise

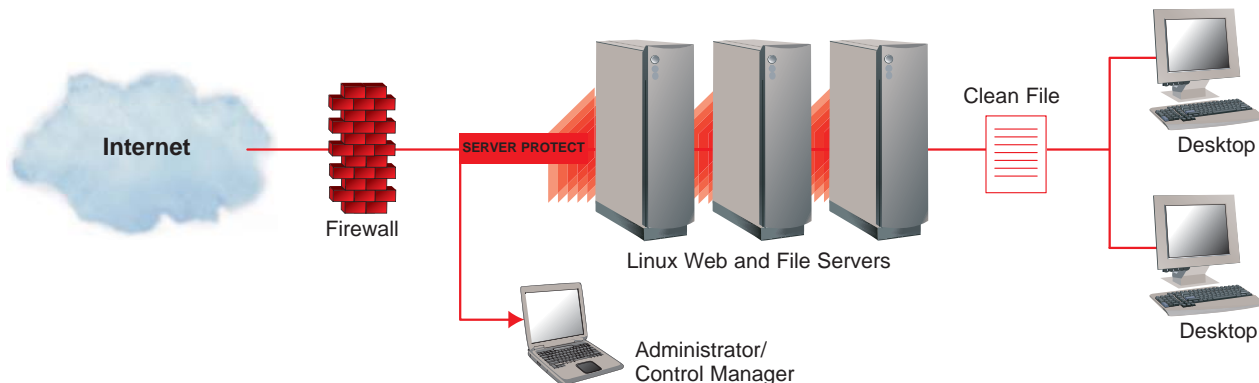
According to Gartner Dataquest, Linux-server market share will rise to 26.2% by 2010. With this increased corporate and government adoption of the Linux platform, it has become increasingly difficult for businesses to provide comprehensive virus protection for the entire network. Administrators are struggling to maintain corporate antivirus policies that extend critical protection to Linux servers.

Supporting Corporate Antivirus Policies for Linux

Trend Micro ServerProtect for Linux 2.5 offers comprehensive real-time protection for enterprise web-servers and file-servers, preventing them from spreading malware to internal or external endpoints. Designed to protect Linux servers from inadvertently hosting viruses, Trojan horses, bots, and other malware, ServerProtect for Linux is a key component in the comprehensive threat prevention offered by Trend Micro™ Enterprise Protection Strategy. The solution's stability and reliability is evidenced by certifications from all major Linux vendors, including Redhat™, Novell™, IBM™, and Virus Bulletin.

- **Central Management.** Seamless integration with Trend Micro Control Manager™ framework enables central management of attack information, policy deployment, pattern file and scan engine deployment, and reports on policy implementation.
- **Easy to Install.** A web-based interface supports multiple simultaneous remote installations as well as central update and configuration that accelerate the rollout process on the broadest range of Linux distributions.
- **High Performance.** Real-time, on-demand, and scheduled scanning uses the latest multi-threaded scanning engine for highest performance and kernel-level scanning to help minimize performance degradation.

ServerProtect prevents suspect files from reaching end users by notifying the administrator. What's more, ServerProtect blocks infected files from re-entering the system, defending the network from possible re-infection.



KEY BENEFITS

- Ensures Linux servers comply with corporate antivirus policies
- Central management and reporting ease administration
- Installs easily on the widest range of Linux platforms
- Part of Trend Micro Enterprise Protection Strategy to protect against everyday threats
- Enhanced performance with kernel-level, multi-thread scanning

“ We were most concerned with our rapidly growing Linux servers and the ServerProtect for Linux console enables us to handle maintenance tasks, including pattern file and scan engine updates, virus log compilations, and real-time scanning parameter configuration.”

—Luis Azevedo,
Consultant, Serpro



Trend Micro™ ServerProtect™ for Linux™

Reliable, High-Performance Scanning

- Helps ensure reliable scanning via use of an International Computer Security Association (ICSA) and Virus Bulletin (VB) certified scan engine
- Decreases performance impact through lower resource utilization on the server
- Designed to minimize performance degradation by performing kernel-level scanning for viruses and malicious code—one of the few solutions to provide this capability
- Adjustable CPU utilization during scan process minimizes performance impact and reduces scanning time
- Supports multiple scheduled updates per server or for all servers

Comprehensive Central Management and Reporting

- Supports central threat management on Linux servers to provide protection against everyday threats even before a pattern is available
- Integration with Control Manger enables administrators to set a policy applicable to all Linux systems, and deploy simultaneous updates
- Supports secure socket layer (SSL) protocol to maximize protection of data transfer during remote management administration
- Helps dramatically reduce maintenance efforts through automatic component updates

Policy Enforcement and Event Alerts

- Enables antivirus policy enforcement and accelerates update deployment through automatic updates of virus patterns and scan engines
- Allows administrators to stay apprised of virus or program events through email notifications and SNMP traps

TrendLabsSM

Trend Micro ServerProtect for Linux is powered by TrendLabs, a global network of research centers committed to constant threat surveillance and attack prevention. By continuously monitoring the Internet and customer networks, TrendLabs' security specialists develop both Internet and customer-specific threat intelligence. With accurate, real-time data, TrendLabs delivers more effective, timely security measures designed to detect, pre-empt, and eliminate attacks.

Trend Micro Enterprise Protection Strategy

Trend Micro Enterprise Protection Strategy (EPS) is a security framework that integrates multiple layers of products and services—for intelligent, comprehensive protection against known and unknown threats. This framework includes innovative new content security solutions that monitor customer-specific networks while accurately detecting unknown threats in real time. Seamless intra-product collaboration and centrally-managed security provide better protection against viruses, Trojans, worms, spam, botnets, spyware, and phishing. As a complete framework, EPS delivers ongoing security designed to monitor the Internet and customer networks, enforce corporate security policies, prevent threats from damaging assets, and recover quickly to ensure business continuity.

Trend Micro Inc.

10101 N. De Anza Blvd.
Cupertino, CA, 95014, USA
Toll free: 1+800-228-5651
Phone: 1+408-257-1500
Fax: 1+408-257-2003
www.trendmicro.com

System Requirements

System requirements change periodically. For the latest updates please visit the Server Protect for Linux product page at www.trendmicro.com.

Linux Server/Client

- Intel™ Pentium™ II 266 MHz or higher processor
- AMD™ Athlon™ processor
- 256MB RAM or more (512MB recommended for application/file servers)
- 50MB disk space for /opt directory and 50MB disk space for /tmp directory
- Red Hat™ Enterprise Linux (AS, ES, WS) 4.0
- SuSE™ Linux Enterprise Server 9
- Novell™ Linux Desktop 9
- Debian 3.1

Web-based Management Console

- Microsoft™ Internet Explorer 5.5 with Service Pack 2 or higher
- Mozilla 1.6 or higher
- Mozilla Firefox 1.0 or higher