

Trend Micro™ ServerProtect™ for Linux™

Stops Malware from Spreading through Linux Servers

Linux-based servers frequently interact with clients running other operating systems, such as Microsoft™ Windows™. They store and serve files created on and for those platforms. At the same time, the increasing popularity of the Linux platform has resulted in the growth of viruses and other malware specifically targeting Linux servers. With Linux now representing 15-20% of the worldwide server market and growing, these attacks are becoming more frequent and more severe. Thus, securing Linux-based servers from hosting infected files is imperative for any enterprise.

Trend Micro ServerProtect for Linux 3.0 offers comprehensive real-time protection for enterprise web-servers and file-servers, preventing them from spreading viruses, spyware, and other Web threats to internal or external endpoints. Managed through an intuitive portable Web-based console, ServerProtect provides centralized virus/malware scanning, pattern updates, event reporting, and configuration. The solution's stability and reliability is evidenced by certifications from all major Linux vendors. ServerProtect for Linux is a key component in the comprehensive threat prevention offered by Trend Micro™ Enterprise Protection Strategy.

KEY FEATURES

Powerful Antivirus and Spyware Protection

- Scans, detects and removes viruses in real time
- Now with enhanced spyware detection and removal capability
- Scan engine certified by International Computer Security Association (ICSA) for reliable scanning

Higher Performance and Flexibility

- Real-time, on-demand, and scheduled scanning uses latest multi-threaded scanning engine for highest performance while kernel-level scanning minimizes performance degradation
- Adjustable CPU utilization during scan process allows users to balance performance impact and scanning time
- Kernel Hook Module (KHM) is now open to General Public License to allow customers to recompile to fit to their own customized kernel variants

Antivirus Policy Compliance

- 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

Centralized Management and Reporting

- Seamless integration with Trend Micro Control Manager™, centralized threat management console
- Enables central management of attack information, policy deployment, pattern file and scan engine deployment, and reports on policy implementation
- Reduces maintenance efforts through automatic component updates

SOFTWARE

Protection Points

- Linux file servers
- Linux Web and application servers

Threat Protection

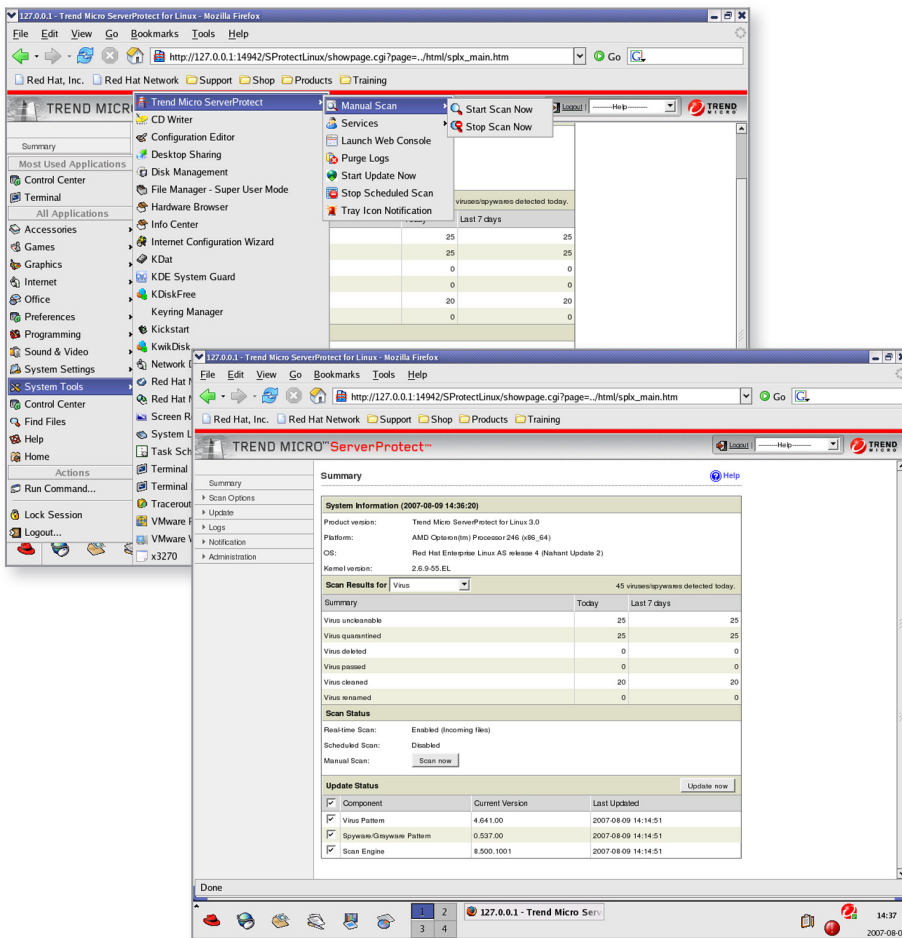
- Viruses
- Spyware

KEY BENEFITS

- Key component of comprehensive threat protection across heterogeneous networks
- Delivers high performance with kernel level, multi-threaded scanning
- Ensures compliance with corporate antivirus policies
- Simplifies administration through central management and reporting
- Installs easily on the widest range of Linux platforms

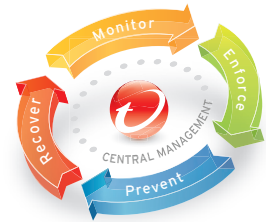
“We were most concerned with our rapidly growing Linux servers and the ServerProtect for Linux console enables us to handle maintenance tasks including pattern file and scan engine updates, virus log combinations, and real-time scanning parameter configuration.”

—Luis Azevedo
Consultant, Serpro



Enterprise Protection Strategy

Trend Micro Enterprise Protection Strategy provides a comprehensive, multi-layered security framework—for superior protection against known and unknown threats. ServerProtect tightly integrates with other Trend Micro products to protect critical points on the network. The combined security solution can be centrally managed through Trend Micro Control Manager.



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, prevent, and eliminate attacks.

CERTIFICATION



MINIMUM SYSTEM REQUIREMENTS

System requirements change periodically. For the latest updates please visit the ServerProtect for Linux product page at <http://uk.trendmicro.com>.

Linux[™] Server/Client

- Intel[™] Pentium[™] II 266 MHz or higher processor
- AMD[™] Athlon[™] processor or higher
- 256MB RAM or more (512MB recommended for application/file servers)
- 75MB disk space for /opt directory and 50MB disk space for /tmp directory
- Red Hat[™] Enterprise Linux 4 (AS, ES, WS, Desktop)
- Red Hat[™] Enterprise Linux 5 (Server or Desktop)
- Novell SUSE[™] Linux Enterprise 10 (Server or Desktop)

Web-based Management Console

- Microsoft[™] Internet Explorer 5.5 with Service Pack 2 or higher
- Mozilla[™] 1.7 or higher
- Mozilla Firefox[™] 1.0 or higher

X Window for Quick Access Console

- KDE 3.3 or higher

Trend Micro Control Manager[™]

- Trend Micro Control Manager version 3.5 with Patch 3 or higher

