

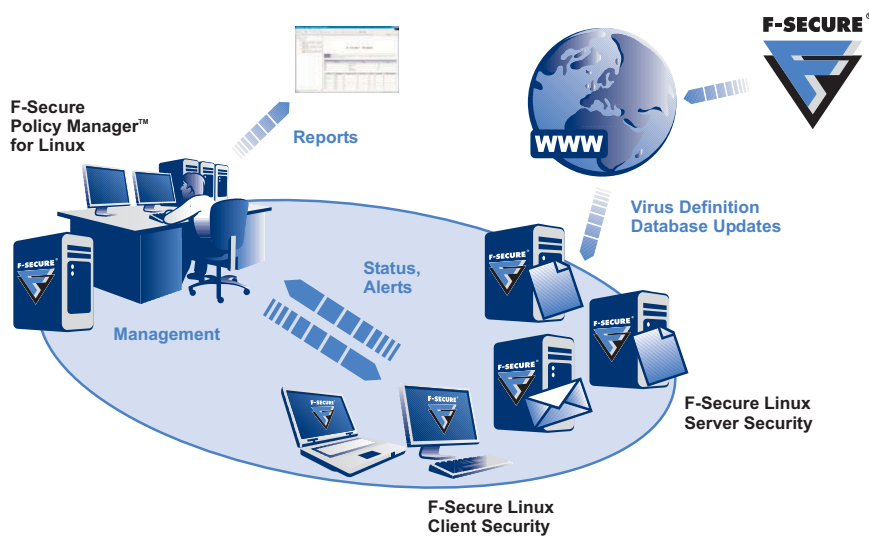
# F-Secure Linux Server Security



Viruses, worms, trojans, riskware and spyware are seen today as the biggest IT security threat to organizations around the world. Hackers are also actively looking for unprotected systems that contain important data or machines that could be used for other purposes such as distributing illegal material or creating attacks against other systems.

Businesses of all size are looking for a low TCO security solution. F-Secure® Linux Server Security™ protects Linux servers and network storages against malware, spyware, riskware and attacks from the network effectively.

F-Secure Linux Server Security is an integrated, out-of-the-box ready security solution with strong realtime antivirus protection, host intrusion prevention (HIPS) functionality protecting against unauthorized connection attempts from network, unauthorized system modifications, user space and kernel rootkits, now including protection against spyware and riskware too. Solution can be easily deployed and managed in mixed environments where an unprotected Linux server is a potential vector for an attack or malicious content thus making a corporation vulnerable. The solution supports scanning messaging content in established system using third party solutions like Mailscanner, AmaViS or similar.



## Key Features

### Comprehensive protection against malware

F-Secure Linux Server Security stops all types of malware, including; Linux and Windows viruses, DOS file viruses and macro viruses that infect Microsoft Office files as well as riskware and spyware. Multiple virus scanning engines integrated into one product ensure the best possible protection against current and future malware.

### Firewall

The integrated firewall makes sure that viruses, hackers and other intruders are not entering the servers by using network worms.

### Host Intrusion Prevention and Detection

The intrusion prevention functionality keeps hackers and crackers from entering and opening backdoors, changing important files, unauthorized system modifications or saving unwanted files on corporate servers.

### Centralized Management

The software can be remotely installed, configured and monitored from one central location. The client configuration can be locked for always-on protection.

### Enhanced Performance

F-Secure Linux Server Security supports now both 32 and 64-bit platforms. The latest 5.50 version includes several performance and stability improvements.,

### Extensive Linux distribution support

The list of tested and supported Linux distributions includes around 30 different systems.

### Ease of use and compatibility with other F-Secure solutions

With F-Secure Linux Server Security administrators will be able to control and monitor the security of Linux servers as easily as they have been able to do on the Windows side.

### Real-time, on the fly anti-virus scanning

Real-time scanning makes sure that users who connect with infected machines to the corporate file servers are not able to save any infected material to the servers. Administrators can specify on demand scans, schedule them or set parameters for real-time scanning from the centralized management system.

### Firewall management

The product provides robust monitoring and filtering of Internet traffic preventing unauthorized access to the servers over the network and hides the servers from hackers and network worms.

### Host Intrusion Detection and Prevention

The kernel memory protection and kernel module verification together with system integrity checking functionality keeps hackers and crackers from opening backdoors, installing rootkits, changing critical files or saving unwanted files on corporate servers and desktops.

### Centralized management, reporting and alerting

By integrating to F-Secure's centralized management system, the F-Secure Policy Manager™, the products will automatically notify the administrators of any security incidents or virus activity. Administrators can also easily change and enforce the security policies via the F-Secure Policy Manager.

### Automatic Virus Definition Updates

Updating of virus definition databases is automatic and secure. The files are automatically downloaded in the background. The system administrator can always be sure that he has the latest updates without having to search on the Web.

### Security management system for all operating systems

With F-Secure Policy Manager you can manage the security of both Linux and Windows desktops, servers and gateways. The management system also supports both Linux and Windows.

## Platforms

### 32-bit

Novell Linux Desktop 9  
SUSE Linux 9.0  
SUSE Linux 9.1  
SUSE Linux 9.2  
SUSE Linux 9.3  
SUSE Linux 10  
SUSE Linux 10.1  
SUSE Linux 10.2  
Ubuntu 5.10 (Breezy)  
Ubuntu 6.06 (Dapper Drake)  
SUSE Linux Enterprise Server 8  
SUSE Linux Enterprise Server 9  
SUSE Linux Enterprise Server 10  
SUSE Linux Enterprise Desktop 10  
Red Hat Enterprise Linux 4  
Red Hat Enterprise Linux 3  
Red Hat Enterprise Linux 2.1 AS  
Fedora Core 5  
Miracle Linux 2.1  
Asianux 2.0  
Turbolinux 10  
Debian 3.1

### 64-bit

#### (AMD64/EM64T, with 32-bit compatibility packages)

SUSE Linux Enterprise Server 9  
SUSE Linux Enterprise Server 10  
SUSE Linux Enterprise Desktop 10  
Red Hat Enterprise Linux 4  
Asianux 2.0  
Turbolinux 10

## Languages

English  
Japanese  
German

"F-Secure" and the triangle symbol are registered trademarks of F-Secure Corporation and F-Secure product names and symbols/logos are either trademarks or registered trademarks of F-Secure Corporation. Other product and company names mentioned herein may be trademarks of their respective owners.  
Copyright © 2006 F-Secure Corporation. All rights reserved.

fssl070410