

F-Secure Client Security 7



New fast-spreading threats are on the rise as virus writers seek for financial gain. Modern professional cyber-criminals want to stay unnoticed, and they are using advanced technologies to hide their creations from data security solutions. Their attacks are also more targeted, thus a single company or computer might be the recipient of a specific malware assault. And if the antivirus cannot detect it, nobody does. For example, a hiding spyware can cause severe damage to companies by sending out confidential information and lowering computer performance and productivity. Modern Internet threats require proactive protection and the monitoring of suspicious software behaviour in the systems combined with traditional signature-based protection. F-Secure® Client Security™ provides centrally managed, advanced proactive protection against traditional and new zero-day threats. for corporate desktop and laptop computers.

Automatic Real-Time Antivirus Protection

F-Secure Client Security automatically stops viruses and malicious code attacks in real-time whether via e-mail, the web, floppy disks or CD-ROMs. By scanning POP3, IMAP4, SMTP and HTTP traffic, it prevents viruses from being sent out or received through e-mail or web. Multiple scanning engines ensure flawless protection against viruses in the wild. To ease installation, F-Secure Client Security seeks for potentially conflicting antivirus programs and automatically removes them during installation. Virus definition databases are transparently and automatically updated once to twice a day with minimal use of bandwidth. The fail-over feature ensures that F-Secure Client Security offers up-to-date protection against new viruses even if the primary delivery server is unreachable.

F-Secure DeepGuard

F-Secure DeepGuard™ is a unique Host-based Intrusion Prevention System (HIPS) technology in the sense that it combines advanced heuristics, sandboxing and run-time behavioural blocking that work seamlessly with conventional definition-based scanning systems. This unique multi-tier approach adds usability by decreasing the amount of false alarms. Tight integration to application control also reduces the amount of pop-ups. All F-Secure DeepGuard installations form a world-wide network examining a large number of unknown applications. This makes it possible to detect and investigate possible malicious programs a lot faster than before and to deliver new virus definitions.

F-Secure BlackLight

Rootkit is often used to hide malicious software like viruses, spyware, adware, backdoors, trojans and worms. F-Secure BlackLight™ is an on-demand rootkit scanner that examines the system at a deep level detecting objects that are hidden from the user and security software. It is a behavior-based detection technology that compares two views and identifies the difference ("cross-view-diff"). It takes two views of the system: a low level of the system and a view that the user would see e.g. through Windows Explorer or Task Manager. Any difference between these views is considered a rootkit. Thanks to its unique remote management possibility, the administrators can scan the entire company network during off peak periods, without affecting network usage.

Key Features

- > Real-Time Automatic Protection
- > Protection for Unknown Threats through F-Secure DeepGuard™
- > Rootkit scanning with F-Secure BlackLight™
- > E-mail and Web Scanning
- > Spyware Protection
- > Cisco NAC Support for fresh security settings and virus definitions of computers connecting to the company network
- > Network Quarantine assures the security level of laptops connecting to the Internet outside office premises
- > Automatic Anti-Virus, Anti-Spyware, DeepGuard and BlackLight updates with Fail-Over system
- > Firewall with Intrusion Prevention
- > Application Control
- > Automatic Security Levels
- > Virus News to desktop or administrator
- > Central Management

Integrated Desktop Firewall

The integrated desktop firewall with stateful inspection provides robust monitoring and filtering of Internet traffic preventing unauthorized access to workstations over the network. It also hides the workstations from Internet hackers and network worms. The intrusion prevention feature analyzes Internet traffic and automatically detects and blocks suspicious network traffic, such as port scans, and network worms.

Application Control

F-Secure Client Security allows network administrators to centrally control from one location the workstation applications that are allowed to access the Internet. This prevents end-users from running forbidden applications that may allow hackers and worms to sneak in.

Anti-Spyware

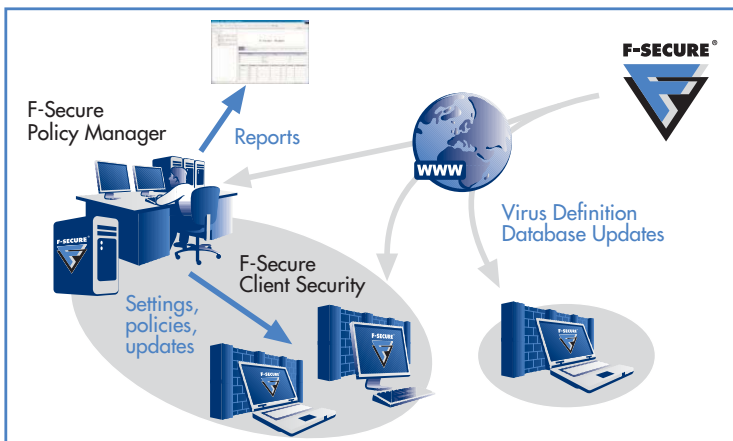
Spyware is a software that gets installed on computers typically without the users' knowledge e.g. through web browsing. Commercial spyware often steals user information, such as web-browsing habits and reports them to advertising companies. In the worst instance spyware can transmit personal details like passwords and e-mails to hackers. F-Secure Client Security detects and removes these secretly installed data tracking components.

Automatic Security Level Change

F-Secure Client Security automatically adapts the security level to the conditions. When a computer connects to the corporate network, office settings are in use. When a computer connects to the Internet outside the corporate network, for example, from home or in a hotel, stricter settings are automatically applied.

Comprehensive Central Management and Reporting

With F-Secure Policy Manager™ – a software program included in the license – network administrators can remotely install, configure and monitor F-Secure Client Security from one central location. Administrators can lock the end-user interface and security settings to prevent the users without administrator rights from bypassing security settings. F-Secure Client Security also generates extensive reports, such as security alerts, virus infection rates, and virus definition database updates. The reports and settings can be adjusted at the network, security domain or at an individual host level.



VB100% award for F-Secure Anti-Virus Client Security "Virus Bulletin, February & June 2006, February 2005"



Checkmark Levels 1 and 2 "West Coast Labs, May 2006"

Supported Platforms

Product

- F-Secure Client Security 7.x
 - Windows 2000 Professional SP4, rollup 1,
 - Windows XP Professional/Home SP2
 - Windows Vista *
- F-Secure Anti-Virus Client Security 5.x
 - Windows 98/NT/2000/XP/ME

Management Tools

- F-Secure Policy Manager Console
 - Windows 2000/XP/Server 2003
- F-Secure Policy Manager Server and F-Secure Policy Manager Web Reporting
 - Windows 2000/2003 Server
 - Red Hat Enterprise Linux ES 3.0-4.0
 - SUSE Linux 9.0-10.0
 - Debian 3.1
- F-Secure Policy Manager Proxy
 - Windows 2000/XP/2003

* Available in 2007 in 32-bit environments

Supported Languages

- F-Secure Client Security
 - Czech, Danish, Dutch, English
 - Finnish, French, German, Greek
 - Hungarian, Italy, Japanese
 - Norwegian, Polish, Portuguese
 - Portuguese (Brazilian), Slovenian
 - Spanish, Swedish, Turkish

- F-Secure Policy Manager
 - English, French, German, Japanese

"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.

fscs061114