



Key Features and Benefits

Key Features

Protection for unknown threats

- > **F-Secure DeepGuard™** is a Host-based Intrusion Prevention System (HIPS). By combining behavior monitoring, sandboxing, and heuristics, it accurately analyzes the unknown malware it encounters. It prevents unknown malware from accessing or harming the corporate system and the malicious code from executing. F-Secure DeepGuard reduces false alarms. The integration of F-Secure DeepGuard to antivirus and firewall enable sending samples of a new malware directly from the program to F-Secure. This way new virus definition updates can be distributed quickly to other users. F-Secure DeepGuard works with application control, which reduces the number of pop-ups displayed on the screen.
- > **F-Secure BlackLight™** examines the system at a deep level and detects rootkits and objects hidden from users. Using remote management, the administrator can control the whole business network and scan it, for example, during off peak periods, without affecting network use. The integration of BlackLight to antivirus enables automatic scanning of all hidden items. Rootkit scanning is included in the full system scan.

Virus and Spyware Protection

- > **Robust protection.** F-Secure Antivirus products have continuously received the Virus Bulletin 100% (VB100) award and scored highest in tests by the Virus TestCenter of the University of Hamburg.
- > **Multiple scanning engines.** Multiple scanning engines each specialize for different tasks, thus providing high protection against different kind of threats.
- > **Automatic fail-over mechanism.** The automatic fail-over mechanism ensures that the antivirus software gets the latest fixes against the new viruses and spyware even if the primary delivery server is unavailable. For example, if the virus definition download from the Policy Manager or Policy Manager Proxy fails, F-Secure Client Security can fetch the definitions from a secondary update location, for example, directly from F-Secure, using incremental download technology.
- > **Enhanced clean up for complex viruses.** Thanks to digitally signed virus definition updates, the virus cleanup routines include powerful mechanisms that can handle even the most complex viruses.
- > **Frequent virus definition updates.** Since around 10 new viruses are found each day, protection against the latest threats needs to be updated daily. F-Secure updates virus definitions up to two times a day to ensure that our customers have the best possible protection.
- > **Incremental virus definition delivery.** As the virus definition updates are published at short intervals, the communication method for delivering the updates to the customer workstations and servers must be solid and bandwidth-efficient. The F-Secure technology of delivering virus definitions incrementally, which works transparently in the background, prevents wasting network bandwidth. For larger

organization with remote offices, F-Secure Policy Manager Proxy offers a solution for delivering the updates to the remote office with limited Internet bandwidth capacity.

- > **Rapid response.** In virus protection, speed of response is an essential factor in the quality of protection. Minutes can count, making the difference whether your system survives an attack or not. F-Secure has a proven track record of reacting fast to new threats and staying one step ahead of the industry in developing protection against new malware.
- > **E-mail and WEB traffic scanning.** F-Secure Client Security scans the content of incoming POP3, IMAP4, HTTP, and outgoing SMTP mail traffic. This ensures that no viruses are sent out from the workstation and no viruses are received through e-mail. E-mail and WEB traffic scanning works with any client that uses SMTP/POP3/IMAP4/HTTP.
- > **Predefined antivirus profiles.** F-Secure Client Security provides three different profiles for antivirus protection (high, normal and off), as well as an option to customize the profile.

Integrated desktop firewall

- > **Stateful inspection.** Stateful inspection means that F-Secure Client Security can automatically and securely open and close communication ports for the requesting software, leaving no ports open to hackers. A filtering engine monitors all communications to and from the computer. Stateful inspection prevents unauthorized access to workstations over the network and hides the workstations from Internet hackers and network worms.
- > **Packet logging.** Packet logging provides detailed information for further investigation in standard tcpdump and syslog format.
- > **Centrally managed application control.** F-Secure Policy Manager allows the IT administrator to control which applications on the workstations or laptops are allowed to connect to the Internet. By controlling the list of allowed applications, F-Secure Policy Manager prevents end users from running forbidden applications, such as peer-to-peer networking applications, on corporate workstations or laptops.
- > **Automatic location-based security level change.** The network administrator can define office profiles and mobile network protection profiles for corporate laptops. When the laptop is connected to a network outside corporate premises, F-Secure Client Security automatically chooses which profile to use.
- > **Built-in and custom security levels.** In addition to the built-in security levels, F-Secure Client Security provides a set of custom security levels that can be easily switched by the user. The network administrator can switch the security level of all workstation and laptop computers.
- > **Centralized alerting of hacking attempts.** Through F-Secure Policy Manager Console the network administrator can see the status of blocked hacking activities in all corporate workstations and laptops.

Integrated Intrusion Protection

- > **Protection against fingerprinting attempts.** F-Secure Client Security protects against the most common operating system fingerprinting attempts, such as nmap, and CyberCop.
- > **Protection against port scans.** F-Secure Client Security protects the workstations and the laptop computers against port scans that hackers use for seeking vulnerable computers in the Internet.
- > **Protection against network worms.** F-Secure Client Security protects against network worms, such as Slammer, Kletz, and MyDoom.

Quarantined Security

- > **Support for Cisco Network Admission Control.** By supporting Cisco Network Admission Control (NAC), F-Secure Client Security makes sure that the workstations and laptops connecting to the corporate network have fresh security settings and virus definitions.
- > **Network Quarantine.** In addition to assuring the security level of laptops connecting inside the corporate network, F-Secure Client Security provides network quarantine that assures the security level of laptops connecting to the Internet outside office premises.

Integrated Virus News

- > **Virus news** delivers instant notifications of serious security events. This feature can be turned off for normal end users, but for network administrators it provides valuable information. Based on the information, the administrator can take necessary action to protect the network against new viruses or denial of service attacks.

Easy installation

- > Installation of F-Secure Policy Manager requires less than 15 steps

Wide language support

- > F-Secure Client Security supports 18 different languages.

Benefits

F-Secure Client Security protects against new types of worms and viruses. It minimizes the risk of confidential information leaking through forbidden networking software. F-Secure Client Security includes:

- > A proactive firewall with intrusion protection system to protect against fast-spreading threats
- > Active and up-to-date protection by powerful antivirus software
- > Real-time protection against spyware and adware
- > Protection for zero day attacks through system monitoring
- > Fast virus definition updates and response
- > Control of networking applications

F-Secure Client Security offers the following benefits:

- > **Professional protection.** F-Secure Client Security protects against traditional and new malware outbreaks and intrusions by combining a definition-based protection with an advanced behavior monitoring. Tightly-integrated antivirus, firewall, antispyware, rootkit scanning, and Host-based Intrusion System (HIPS) coupled with the industry's fastest virus definition update service ensure effective protection against complex viruses and worms.
- > **Easy to install and use.** F-Secure Client Security is easy to install and use. The IT administrator can remotely install the workstation software. The software installation automatically removes existing antivirus products, which keeps the implementation cost low. The same console is used to configure and view the antivirus status in the network. F-Secure Client Security works automatically, updating the virus definitions from the F-Secure Virus Research Lab and uses the virus definitions to check the latest threats.
- > **Business enhancer.** With F-Secure Client Security, the protection is always on regardless of the time and place where the laptop is connected to the network. The software allows the user to do business in more flexible ways without having to worry about viruses and hackers.
- > **Future-proof investment.** F-Secure Client Security scales up with your business. The IT administrator can add workstations, servers, or even entire remote offices from a central location. F-Secure Anti-Virus solutions are also available for mobile devices. Whether the company is large or small, F-Secure Client Security scales to the needs.

