

What's new in the F-Secure Client Security 7



F-Secure Client Security 7

- > Remotely managed **F-Secure DeepGuard™** prevents previously unknown malware accessing or harming your system by observing the heart of your computer and preventing the malicious code from executing. It is a Host-based Intrusion Prevention System (HIPS) that uniquely combines heuristics, sandboxing, and behavior blocking. You save money when you can avoid the mess that malware could cause.
- > Remotely-managed **F-Secure Blacklight™** detects rootkits at the deepest level of your computer and finds the hidden intruders. It is an on-demand rootkit scanner that uses behavior-based detection technology. You can save your reputation by catching rootkits before they have time to carry out any criminal actions using your computer.
- > **Extended spyware** detection and removal – better detection rate and more frequent updates
- > **Full quarantine** of viruses, spyware and riskware - if the malware is inside a valuable document, the document can be rescued
- > **Improved Automatic Update System** - completely redesigned automatic update system provides greater control and service over database update delivery (lighter, better reliability and performance).
- > **Performance improvements** – changes in the product architecture decrease the number of running process and improve the performance
- > **Remote management**, in addition to previous features, also for rootkit and other previously unknown malware detection – a unique and easy-to-use tool for administrators to fight against hidden intruders as well as traditional viruses and hackers.



F-Secure Anti-Virus Client Security 6

- > **Short response time to virus outbreaks, faster than major competitors** – reliable protection
- > **Frequent and digitally signed virus definition updates** – always up-to-date protection
- > **Real-time automatic protection** against malicious code attacking via e-mail, web, floppy disks and CD-ROMs.
- > **E-mail scan (POP3, IMAP4, SMTP)** prevents viruses from being sent out or received through e-mail.
- > **Web scan (HTTP)** prevents viruses from being received through web browsing.
- > **Personal firewall with stateful inspection** prevent unauthorized access to workstations over the network and hides the workstations from Internet hackers and network worms.
- > **Intrusion prevention of firewall** analyzes Internet traffic and automatically detects and blocks suspicious network traffic (port scans, network worms).
- > **Automatic security levels** for different premises (office, home etc.)
- > **Spyware and adware detection and removal.** These get installed through web browsing or as an additional component of a freeware or shareware application. Spyware often steals information (passwords, e-mails and web-browsing habits) and reports them to advertising companies.
- > **Cisco NAC v.1** support makes sure that the laptops and workstations connecting to the company network have fresh security settings and virus definitions.
- > **Network quarantine** assures the security level of laptops connecting to the Internet outside office premises.
- > **Application control for administrators** offer a central control of the workstation applications that are allowed to access the Internet.
- > **Virus and spyware updates with fail-over mechanism** i.e. it ensures an up-to-date protection against new viruses even if the primary delivery server is unreachable.
- > **Virus news** of serious security events are instantly delivered to administrators or end-users around the globe
- > **Comprehensive central management and reporting** with F-Secure Policy Manager. Remote installation, configuration and monitoring from one central location.