F-Secure

DATA SHEET

F-Secure Anti-Virus Client Security

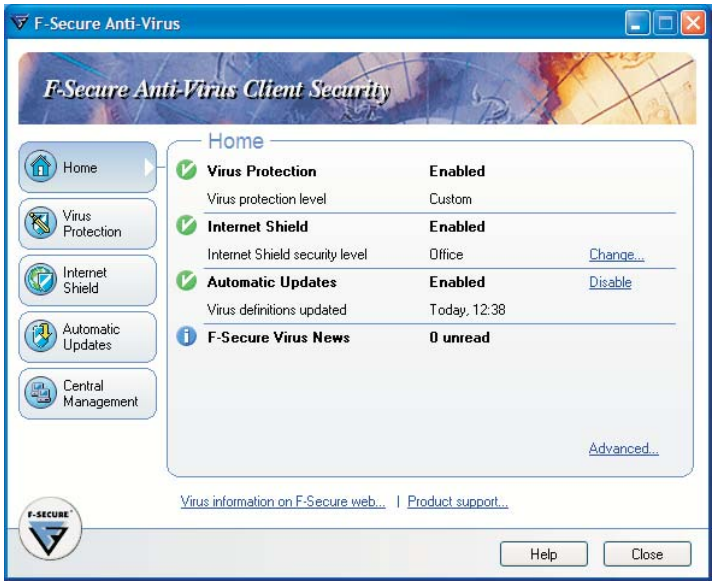
Worms and viruses such as Nimda and Slammer are becoming more complex and faster spreading. The worms take advantage of multiple hacker techniques to spread, using vulnerabilities in the software and operating systems. They exploit fast Internet connections and bypass virus shields using non-protected channels, such as peer-to-peer networks, to sneak in to the corporate workstations. F-Secure® Anti-Virus Client Security™ offers protection against new breeds of threats. The centrally managed solution consists of tightly integrated virus protection, proactive personal firewall, intrusion prevention and application control software for desktop and laptop computers.

Automatic Real-Time Antivirus Protection

Viruses and malicious code attacking via e-mail, the web, floppy disks and CD-ROMs are automatically stopped in real-time. The scanning of POP3 and SMTP mail traffic ensures that no viruses are sent out or received through e-mail. Multiple scanning engines ensure flawless protection against viruses in the wild. To ease installation, the software seeks for other, potentially conflicting antivirus programs and automatically removes them during installation.

Automatic Virus Definition Updates and Fail-over

Virus definition databases are transparently and automatically updated typically 1-2 times per day with minimal bandwidth use. The fail-over feature ensures that antivirus software will get the latest cure against new viruses even if the primary delivery server is unreachable. For example, if the HTTP download from the company server fails, the program can fetch downloads directly from F-Secure. The digitally signed virus definition delivery makes sure that the virus definition updates are genuine. Furthermore, virus removal tools can be distributed with virus definition updates.



KEY FEATURES

Real-Time Automatic Protection
Viruses, worms, spyware and Trojans attacing via e-mail, web or floppy disks are stopped in real-time.

E-mail Scanning
POP3 and SMTP traffic are scanned for viruses.

Automatic Virus Definition Updates with Fail-over
Virus definition updates are transparently and automatically updated 1-2 times per day, using a fail-safe method.

Firewall with Intrusion Prevention
Hackers and the new breed of worms are detected and blocked.

Application Control
Applications connecting to the Internet can be centrally controlled and blocked.

Automatic Security Levels
Security levels are automatically adapted on the basis of location.

Virus News
News of latest virus threats are delivered instantly around the globe.

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

F-Secure Corporation, Tammasaarenkatu 7, PL 24, FIN-00181 Helsinki, Finland
*Tel. +358 9 2520 0700, Fax +358 9 2520 5001, E-Mail: Helsinki@F-Secure.com, **www.F-Secure.com***

F-Secure

Integrated Desktop Firewall
The integrated desktop firewall with stateful inspection provides robust monitoring and filtering of Internet traffic preventing unauthorized access to the workstations over the network and hides the workstation from Internet hackers and network worms.

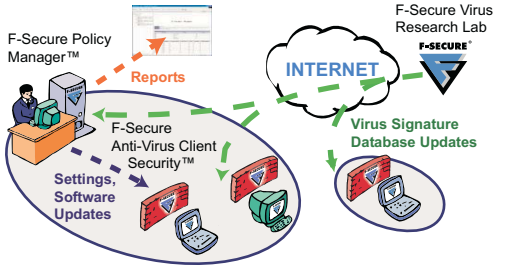
Intrusion Prevention
Intrusion prevention adds a new layer of protection to the integrated firewall. The software analyzes Internet traffic and automatically detects and blocks suspicious network traffic such as port scans and network worms, like the Slammer.

Application Control
The network administrator is able to centrally control, from one location, the applications on the workstations that are allowed to access the Internet. Thus the end-users cannot run forbidden applications (such as peer-to-peer networking) that may allow hackers and worms to sneak in.

Automatic Seurity Level Change
Depending on the location, the program can automatically adapt the security level accordingly. When connected to the corporate network, office settings are in use and are automatically changed to more strict security settings when plugged into the Internet e.g. from home or hotel.

Virus News to the Desktop
Virus notifications of serious security events can be delivered to the administrator or to the end-users, instantly around the globe. This ensures that the administrator is immediately aware of new security threats and able to respond accordingly.

Comprehensive Central Management and Reporting
With F-Secure Policy Manager – a software included in the license – the network administrator can, from one central location, remotely install, configure and monitor the software. The administrator can lock the end-user interface and settings, and thereby prevent by-passing of the protection. The software can also generate extensive reports including security alerts, virus infection rates, virus definition database dates etc. The reports and settings can be adjusted at the network, security domain or individual host level.



SUPPORTED PLATFORMS

PRODUCT
F-Secure Anti-Virus Client Security
Windows 98/NT/2000/XP

MANAGEMENT TOOLS
F-Secure Policy Manager Console
Windows NT/2000/ME/XP

F-Secure Policy Manager Server
Windows NT/2000/2003
Red Hat 8.0, SuSE 8.0

F-Secure Policy Manager Reporting Option
Windows NT/2000/XP
Red Hat 8.0, SuSE 8.0

F-Secure Anti-Virus Proxy
Windows NT/2000

SUPPORTED LANGUAGES

F-Secure Anti-Virus Client Security
English, Finnish, French, German, Italian, Swedish

F-Secure Policy Manager
English

www.F-Secure.com

avcs030624