

# F-Secure Client Security 7



Nieuwe, zich snel verspreidende, bedreigingen duiken op nu virusmakers hun zakken proberen te vullen. De moderne en professionele cybercriminelen willen onopgemerkt blijven. Ze gebruiken geavanceerde technieken om hun creaties verborgen te houden voor de programma's die uw gegevens beveiligen. Hun aanvallen zijn ook meer gericht, waardoor één specifiek bedrijf of computer het slachtoffer kan worden van een aanval met malware. En als het antivirusprogramma het niet kan ontdekken, kan niemand het. Verborgene spyware kan bijvoorbeeld enorme schade aanrichten aan bedrijven door vertrouwelijke informatie te verzenden of door de prestaties en productiviteit van de computers te verslechteren. Moderne bedreigingen van internet vereisen niet alleen de traditionele, op 'patroon' gebaseerde beveiliging, maar ook een proactieve beveiliging en het controleren van verdacht gedrag in software. F-Secure® Client Security™ biedt centraal beheerde, geavanceerde en proactieve beveiliging tegen traditionele en nieuwe zero-daybedreigingen voor desktop- en laptopcomputers.

## Automatische realtime antivirusbeveiliging

F-Secure Client Security stopt (realtime) automatisch virussen en aanvallen met schadelijke codes, of die aanvallen nu via e-mail, het web, diskettes of cd-roms zijn. Doordat POP3-, IMAP4-, SMTP- en HTTP-verkeer wordt gescand, kunnen virussen niet worden verzonden of ontvangen via e-mail of het web. Meerdere scanengines zorgen voor een uitstekende beveiliging tegen virussen. Om de installatie te vergemakkelijken, zoekt F-Secure Client Security naar antivirusprogramma's die een conflict kunnen opleveren en verwijdert deze tijdens de installatie. De databases met virusdefinities zijn overzichtelijk en worden een of twee keer per dag automatisch bijgewerkt, waarbij slechts weinig bandbreedte wordt gebruikt. De fail-over functie zorgt ervoor dat zelfs als de hoofdservers onbereikbaar is, F-Secure Client Security de nieuwste beveiliging tegen nieuwe virussen kan blijven bieden.

## F-Secure DeepGuard

F-Secure DeepGuard™ is een unieke, op hosts gebaseerde technologie voor beveiliging tegen onrechtmatige toegang (Host-based Intrusion Prevention System, HIPS). Geavanceerde methodiek, sandboxing en het in realtime blokkeren op basis van gedrag worden probleemloos gecombineerd met conventionele op definitie gebaseerde scansystemen. Deze unieke, veelzijdige aanpak verhoogt het gebruikersgemak door minder vaak een loos alarm te geven. Door goede integratie met het beheer van toepassingen, wordt ook het aantal pop-ups kleiner. Alle computers waarop F-Secure DeepGuard is geïnstalleerd vormen samen een wereldwijd netwerk dat een groot aantal onbekende toepassingen onderzoekt. Dit maakt het mogelijk dat potentieel schadelijke programma's een stuk sneller worden ontdekt en onderzocht en dat snel nieuwe virusdefinities worden aangeboden.

## F-Secure BlackLight

Vaak worden rootkits gebruikt om schadelijke software zoals virussen, spyware, adware, backdoors, trojaanse paarden en wormen te verbergen. F-Secure BlackLight™ is een rootkitscanner op aanvraag die het systeem op een diep niveau onderzoekt op objecten die verborgen zijn voor de gebruiker en beveiligingssoftware. Het is een op gedrag gebaseerde detectietechniek die twee overzichten vergelijkt en het verschil identificeert ("cross-view-diff"). Er worden twee overzichten van het systeem gemaakt: een overzicht op diep niveau van het systeem en een overzicht op een niveau dat de gebruiker te zien krijgt, bijvoorbeeld met Windows Verkenner of Taakbeheer. Elk verschil tussen deze overzichten wordt gezien als een rootkit. Dankzij de unieke mogelijkheid voor beheer op afstand, kunnen beheerders, zonder dat het netwerkgebruik wordt beïnvloed, een geheel bedrijfsnetwerk scannen tijdens perioden met weinig activiteit.

## Belangrijkste kenmerken

- > Realtime automatische antivirusbeveiliging
- > Beveiliging tegen onbekende bedreigingen met F-Secure DeepGuard
- > Scannen naar rootkits met F-Secure BlackLight
- > Scannen van e-mail en het web
- > Beveiliging tegen spyware
- > Ondersteuning van Cisco NAC voor nieuwe beveiligingsinstellingen en virusdefinities op computers die verbinding maken met het bedrijfsnetwerk
- > Netwerkquarantaine verzekert ook buiten het kantoor een goed beveiligingsniveau als een laptop verbinding maakt met internet
- > Automatische updates voor antivirus, anti-spyware, DeepGuard en BlackLight, en een fail-over systeem
- > Firewall met beveiliging tegen onrechtmatige toegang
- > Toepassingsbeheer
- > Automatische beveiligingsniveau's
- > Virusnieuws voor de gebruiker en de beheerder
- > Centraal beheer

## Geïntegreerde firewall

Met de geïntegreerde firewall die beschikt over dynamische pakketfilters wordt internetverkeer gecontroleerd en gefilterd, waardoor onbevoegde toegang tot werkstations over een netwerk wordt voorkomen. Bovendien verbergt het de werkstations voor hackers op internet en voor andere netwerkwormen. De functie voor het voorkomen van onrechtmatige toegang analyseert internetverkeer en detecteert automatisch verdacht netwerkverkeer, zoals poortscans en netwerkwormen, en houdt dit tegen.

## Toepassingsbeheer

Met F-Secure Client Security kunnen netwerkbeheerders de werkstationtoepassingen die toegang hebben tot internet, vanaf één locatie beheren. Hiermee wordt voorkomen dat eindgebruikers verborgen toepassingen uitvoeren die hackers en wormen in staat stelt in de computer te komen.

## Anti-Spyware

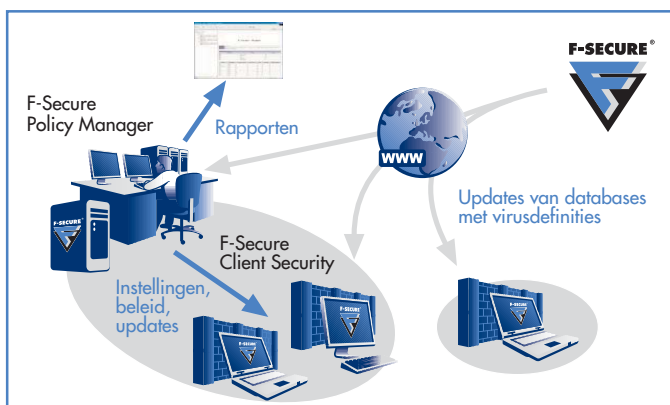
Spyware is software die op computers wordt geïnstalleerd zonder dat de gebruiker daar weet van heeft. Dit kan bijvoorbeeld gebeuren tijdens het surfen op het web. Commerciële spyware steelt over het algemeen gebruikersinformatie, zoals surfgedrag, en geeft die door aan adverteerders. In het ergste geval kan spyware persoonlijke gegevens zoals wachtwoorden en e-mails naar hackers doorsturen. F-Secure Client Security detecteert en verwijdert zulke heimelijk geïnstalleerde onderdelen voor gegevenstracering.

## Automatische aanpassing van beveiligingsniveau's

F-Secure Client Security past automatisch het beveiligingsniveau aan de omstandigheden aan. Wanneer een computer verbinding maakt met het bedrijfsnetwerk, worden kantoorinstellingen gebruikt. Wanneer de computer buiten het bedrijfsnetwerk verbinding maakt met internet, zoals thuis of in een hotel, worden automatisch striktere instellingen toegepast.

## Uitgebreid centraal beheer en rapportage

Met F-Secure Policy Manager™, een softwareprogramma dat deel uitmaakt van de licentie, kunnen netwerkbeheerders op afstand F-Secure Client Security installeren, configureren, controleren en beheren vanaf één centrale locatie. Beheerders kunnen de interface- en beveiligingsinstellingen van de eindgebruiker vergrendelen om te voorkomen dat gebruikers zonder beheerdersrechten de beveiligingsinstellingen kunnen omzeilen. F-Secure Client Security maakt ook uitgebreide rapporten, zoals van beveiligingswaarschuwingen, virusinfectiewaarden en updates van de databases van virusdefinities. De rapporten en instellingen kunnen worden aangepast voor het niveau van een netwerk, een beveiligingsdomein of een individuele host.



VB100%-prijs voor F-Secure Anti-Virus Client Security "Virus Bulletin, februari & juni 2006, februari 2005"



Checkmark-niveau's 1 en 2 "West Coast Labs, mei 2006"

## Ondersteunde 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

### Beheerprogramma's

F-Secure Policy Manager Console  
Windows 2000/XP/Server 2003  
F-Secure Policy Manager Server en  
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

\* Beschikbaar in 2007 in 32-bit-omgevingen

## Ondersteunde talen

F-Secure Client Security  
Deens, Duits, Engels, Fins  
Frans, Grieks, Hongaars, Italiaans  
Japans, Nederlands, Noors  
Pools, Portugees, Portugees (Braziliaans)  
Sloveens, Spaans  
Tsjechisch, Turks, Zweeds  
F-Secure Policy Manager  
Engels, Duits, Frans, Japans

F-Secure® en het driehoekige symbool zijn gedeponeerde handelsmerken van F-Secure Corporation en productnamen en symbolen/logo's van F-Secure zijn handelsmerken of gedeponeerde handelsmerken van F-Secure Corporation. Andere hier genoemde product- en bedrijfsnamen kunnen handelsmerken zijn van de respectieve eigenaren. Copyright © 2006 F-Secure Corporation. Alle rechten voorbehouden.

fscs061114nld