

F-Secure Client Security 7



Nye trusler, der spredes hurtigt, er i vækst i takt med, at virusforfattere søger økonomisk vinding. Moderne professionelle cyber-kriminelle ønsker at arbejde ubemærket, og de bruger avancerede teknologier til at skjule deres "værk" for datasikkerhedsløsninger. Deres angreb er også mere målrettede, og en enkelt virksomhed eller computer kan derfor blive udsat for et bestemt malwareangreb. Og hvis antivirusprogrammet ikke kan finde det, kan ingen. Skjult spyware kan f.eks. medføre alvorlige skader for virksomheder ved at sende fortrolige oplysninger ud og sænke computerydelse og -produktivitet. Moderne internettrusler kræver proaktiv beskyttelse og overvågning af mistænkelig softwareadfærd på systemerne sammen med traditionel signaturbaseret beskyttelse. F-Secure® Client Security™ leverer centralt styret, avanceret proaktiv beskyttelse mod traditionelle og nye zero-day-trusler til virksomheders stationære og bærbare computere.

Automatisk beskyttelse mod virus i realtid

F-Secure Client Security standser automatisk angreb fra virus og ondsindet kode i realtid, uanset om det sker via e-mail, internettet, disketter eller cd-rom'er. Ved at scanne POP3-, IMAP4-, SMTP- og HTTP-trafik forhindres virus i at blive sendt ud eller modtaget via e-mail eller internettet. Med flere scanningsprogrammer sikres optimal beskyttelse mod virus. Af hensyn til nemmere installation leder F-Secure Client Security efter antivirusprogrammer, der kan være i konflikt med hinanden, og fjerner dem automatisk under installationen. Virusdefinitionsdata-baser opdateres transparent og automatisk en til to gange dagligt med minimal brug af båndbredde. Med den fejlsikrede funktion sørger F-Secure Client Security for opdateret beskyttelse mod nye virus, selvom der ikke kan oprettes forbindelse til den primære server.

F-Secure DeepGuard

F-Secure DeepGuard™ er en unik HIPS-teknologi (Host-based Intrusion Prevention System) forstået på den måde, at den kombinerer avanceret heuristik, sandboxing og blokering på kørselstidspunktet, som arbejder gnidningsløst sammen med traditionelle definitionsbaserede scanningsystemer. Denne enestående flerlagede løsning gør programmet mere anvendeligt ved at reducere antallet af falske alarmer. Tæt integration med programstyring reducerer også antallet af pop op-meddelelser. Alle F-Secure DeepGuard-installationer udgør et verdensomspændende netværk, som undersøger et stort antal ukendte programmer. Det gør det muligt at finde og undersøge mulige ondsindede programmer meget hurtigere end før og levere nye virusdefinitioner.

F-Secure BlackLight

Rootkit bruges ofte til at skjule ondsindet software som f.eks. virus, spyware, adware, bagdøre, trojanske heste og orme. F-Secure BlackLight™ er en on-demand rootkit-scanner, som undersøger systemet på et dybt niveau og registrerer objekter, som er skjulte for brugeren og sikkerhedssoftware. Det er en adfærdsbaseret registreringsteknologi, som sammenligner to visninger og identificerer forskellen ("cross-view-diff"). Den tager to visninger af systemet: en visning på lavt niveau på systemet og en visning, som brugeren kan se, f.eks. via Windows Stifinder eller Jobliste. Enhver forskel mellem disse to visninger anses for at være et rootkit. Takket være den enestående fjernadministrationsmulighed kan administratorerne scanne hele virksomhedens netværk i perioder uden spidsbelastning og uden at påvirke netværksbrug.

Hovedfunktioner

- > Automatisk realtidsbeskyttelse
- > Beskyttelse mod ukendte trusler via F-Secure DeepGuard
- > Rootkit-scanning med F-Secure BlackLight
- > Scanning af e-mail og internet
- > Beskyttelse mod spyware
- > Cisco NAC-understøttelse til nye sikkerhedsindstillinger og virusdefinitioner for computere, der opretter forbindelse til virksomhedens netværk
- > Netværkskarantæne kontrollerer sikkerhedsniveauet for bærbare computere, der opretter forbindelse til internettet uden for kontorlokalerne
- > Automatiske opdateringer af antivirus, antispyware, DeepGuard og BlackLight med fejlsikret system
- > Firewall med forebyggelse af indtrængning
- > Programstyring
- > Automatiske sikkerhedsniveauer
- > Virusnyheder til skrivebord eller administrator
- > Central administration

Integreret desktop-firewall

Den integrerede desktop-firewall med stateful inspection leverer robust overvågning og filtrering af internettrafik og forhindrer uautoriseret adgang til arbejdsstationer via netværket. Den skjuler også arbejdsstationerne for internethackere og netværksorme. Funktionen til forebyggelse af indtrængning analyserer internettrafik og registrerer samt blokerer automatisk for mistænkelig netværkstrafik, f.eks. portscanninger, og netværksorme.

Programstyring

Med F-Secure Client Security kan netværksadministratorer centralt styre de programmer på arbejdsstationer, som kan få adgang til internettet. Det forhindrer slutbrugere i at køre forbudte programmer, som kan gøre det muligt for hackere og orme at snige sig ind.

Antispyware

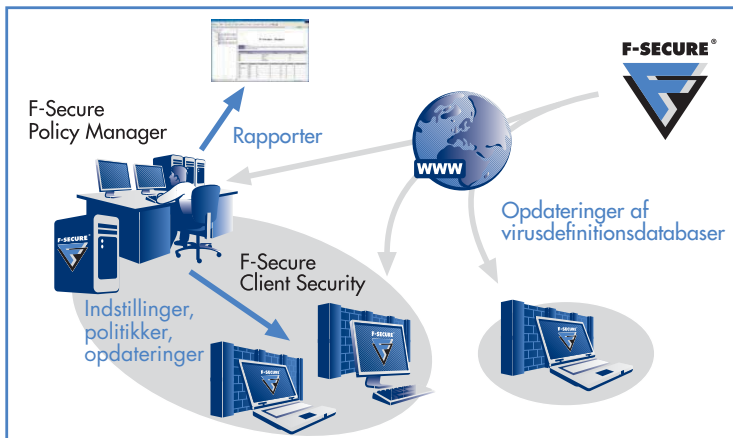
Spyware er software, som typisk bliver installeret på computere uden brugerens viden, f.eks. via søgning på internettet. Kommerciel spyware stjæler ofte brugeroplysninger, f.eks. om vaner på internettet, og rapporterer dem til reklamefirmaer. I værste fald kan spyware sende personlige oplysninger som f.eks. adgangskoder og e-mails til hackere. F-Secure Client Security finder og fjerner disse hemmeligt installerede datasporingskomponenter.

Automatisk ændring af sikkerhedsniveau

F-Secure Client Security tilpasser automatisk sikkerhedsniveauet efter forholdene. Når en computer opretter forbindelse til virksomhedens netværk, bruges kontorindstillingerne. Når en computer opretter forbindelse til internettet uden for virksomhedens netværk, f.eks. hjemmefra eller på et hotel, anvendes der automatisk strengere indstillinger.

Omfattende central administration og rapportering

Med F-Secure Policy Manager™ – et program omfattet af licensen – kan netværksadministratorer fjerninstallere, -konfigurere og -overvåge F-Secure Client Security fra én central placering. Administratorer kan låse slutbrugernes grænseflade- og sikkerhedsindstillinger for at forhindre brugere uden administratorrettigheder i at omgå sikkerhedsindstillinger. F-Secure Client Security genererer også omfattende rapporter, f.eks. om sikkerhedsadvarsler, virusinfektionshastigheder og opdateringer af virusdefinitionsdatabaser. Rapporterne og indstillingerne kan justeres på netværket, sikkerhedsdomænet eller individuelt værtniveau.



VB 100%-prisen for F-Secure Anti-Virus Client Security "Virus Bulletin, februar & juni 2006, februar 2005"



Checkmark Levels 1 og 2 "West Coast Labs, maj 2006"

Understøttede platforme

Produkt

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

Administrationsværktøjer

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

* Kan fås i 2007 til 32-bit miljøer

Understøttede sprog

F-Secure Client Security
Tjekkisk, dansk, hollandsk, engelsk
finsk, fransk, tysk, græsk
ungarsk, italiensk, japansk
norsk, polsk, portugisisk
portugisisk (Brasilien), slovensk
spansk, svensk, tyrkisk
F-Secure Policy Manager
Engelsk, fransk, tysk, japansk

"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.

fscs061114dan