

# F-Secure Client Security 8



Arvutite kaitsmine tänapäevaste internetiohtude eest nõuab koos traditsioonilise signatuuripõhise turbega ka ennetava kaitse rakendamist ja süsteemis kahtlase tarkvarakäitumuse jälgimist. F-Secure® Client Security™ pakub korporatiivtöölaudadele ja sülearvutitele keskse haldusega ennetavat kaitset nii tavapärase pahavara kui uute zero-day ohtude vastu.

## Automaatne kaitse reaajas

F-Secure Client Security peatab reaajas automaatselt viirused, nuhkvara ja pahatahtliku sisuga koodid, mis levivad nii e-posti, veebi kui eemaldatavate meediumite, näiteks USB-mäluseadmete kaudu. POP3-, IMAP4-, SMTP- ja HTTP-liikluse skannimisega takistab lahendus viiruste saatmist ja vastuvõtmist e-posti või veebi kaudu. Installimise hõlbustamiseks tuvastab F-Secure Client Security konfliktid viirusetõrjeprogrammid ja eemaldab need automaatselt installimise käigus.

## Automaatsed ja taustalttöötavad värskendused

Värskendatav skannimismootor võimaldab kiiret ja muretu hooldust ning reageerib nobedalt ja sujuvalt pidevalt muutuvaile ohtudele. Viirusedefinitsioonide andmebaase värskendatakse automaatselt taustal vähemalt kord päevas. Naaberhõive funktsioon võimaldab andmebaaside allalaadimisi ka teistelt LAN-sisestelt klientidelt, minimeerides seeläbi ribalaiuse kasutamist. Tõrkesiirde funktsioon kindlustab selle, et F-Secure Client Security pakub ajakohast kaitset uute viiruste vastu isegi siis, kui esmane edastusserver on parasjagu kättesaamatu.

## F-Secure DeepGuard 2.0

F-Secure DeepGuard™ kujutab endast ainulaadset võrgu hosti-põhise sissetungi takistamise süsteemi (NHIPS) tehnoloogiat. See ühendab täiustatud heuristilist, sandboxing ja käitusfaasi käitumusblokeerimist ning võrgupäringuid. Samuti töötab see tõrgeteta koos harilike definitsioonipõhiste skannimissüsteemidega. Selline ainulaadne mitmeastmeline lähenemine tõstab tänu valehäirete arvu vähendamisele kasutusväärtust. Võrgupäringud suurendavad reaktsiooni kiirust ja kahandavad kasutaja seotust protsessiga. Rakendushaldusega integreeritus vähendab ka hüpikteadete arvu.

## F-Secure BlackLight

Viiruste, nuhkvara, reklaamvara, tagauste, Trooja hobuste, ussviiruste ja muu pahavara peitmiseks kasutatakse sageli juurkomplekte. F-Secure BlackLight™ on tellitav juurkomplekt-skanner, mis uurib süsteemi käitumust süvatasandil, tuvastades kasutaja ja turvatarkvara eest peidetud objekte.

Automaatne kaitse reaajas

Kaitse tundmatute ohtude eest  
F-Secure DeepGuard'i abil

Juurkomplekti skannimine F-Secure  
BlackLight'iga

E-posti ja veebi skannimine

Kaitse nuhkvara eest

Tulemüür koos sissetungitõkkega

Rakendushaldus

Automaatne viirusetõrje,  
nuhkvaratõrje, DeepGuard'i ja  
BlackLight'i värskendamine  
tõrkesiirde süsteemiga

LAN-sisene naaberhõive  
viirusedefinitsioonide  
värskendustele

Täielik IPv6-kaitse

Cisco NAC tugi

Võrgukarantiin, mis tagab  
väljaspool kontoriruumi  
internetiga ühendatud sülearvutite  
turvalisustaseme.

Tulemüüri profiilide – näiteks  
kontor või mobiilne – automaatne  
valimine võrgu asukoha baasil.

Viiruseid puudutavad uudised  
töölauale või süsteemiülemale

Keskhaldu

## Integreeritud töölaua tulemüür

Olekukontrolliga integreeritud töölaua tulemüür võimaldab internetiliikluse esmast jälgimist ja filtreerimist ning takistab võrgu kaudu volitamata juurdepääsu tööjaamadele. Samuti peidab see tööjaamad häkkerite ja võrgu-ussviiruste eest. Rakendushaldus võimaldab võrguülematel tsentraliseeritult hallata tööjaamade internetijuurdepääsuga rakendusi.

## Terviklik tsentraliseeritud haldamine ja aruandlus

F-Secure Policy Manager™ – litsentsile lisatud tarkvaraprogrammi – abil saavad võrguülemad ühest kesksest asukohast distantsilt installida, konfigurereida ja jälgida F-Secure Client Security rakendust. Ülemad saavad lukustada lõppkasutaja liidese ja turvasätteid, et vältida turvasätetest möödahiilimist ülemaõigusteta kasutajate poolt. F-Secure Client Security genereerib lisaks ka mahukat aruandlust, näiteks turvahäirete, viirustesse nakatumise määrade ja viirusedefinitsioonide andmebaaside värskenduste aruanded. Sätteid saab reguleerida võrgutasandile, turvadomeeni tasandile või individuaalse hosti tasandile.



VB100% Award F-Secure Client Security'le: "Virus Bulletin, aprill 2008"



Tunnustus F-Secure DeepGuard'ile ja BlackLight'ile: "SC Magazine, juuni 2007"

## Toetatavad platvormid

F-Secure Client Security  
Windows 2000 (SP 4 või kõrgem)  
Windows XP (SP 2 või kõrgem)  
Windows Vista 32- ja 64-bitine

## Haldustööriistad

F-Secure Policy Manager Server ja  
F-Secure Policy Manager Web Reporting  
Windows 2000/2003/2008 Server  
Red Hat Enterprise Linux 3, 4, 5  
SUSE Linux Enterprise Server 9, 10  
OpenSUSE 10.3  
Debian 4.0  
Ubuntu 8.04

F-Secure Policy Manager Console  
Sama, mis Server + puhul  
Windows 2000/XP/Vista

F-Secure Policy Manager Proxy  
Windows 2000/2003  
Red Hat Enterprise Linux 3, 4  
SUSE Linux 9, 10  
SUSE Linux Enterprise Server 9  
Debian 3.1

## Toetatavad keeled

F-Secure Client Security  
tšehhi, taani, hollandi, inglise  
soome, prantsuse, saksa, kreeka  
ungari, itaalia, jaapani  
norra, poola, portugali  
portugali (brasiilia), sloveenia  
hispaania, rootsi, türgi

F-Secure Policy Manager  
inglise, prantsuse, saksa, jaapani

"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 © 2008 F-Secure Corporation. All rights reserved.

fscs800\_ee\_2008-09-19