

F-Secure Client Security 8



Tietokoneiden suojaaminen moderneilta Internet-uhilta edellyttää ennakoivaa tietoturva- ja ohjelmien toiminnan seuranta epäilyttävien piirteiden havaitsemiseksi. Lisäksi tarvitaan perinteinen virustunnisteisiin perustuva suoja. F-Secure® Client Security™ on keskitetysti hallittava ja ennakoiva tietoturvaratkaisu. Se suojaa yrityksen työasemat ja kannettavat tietokoneet sekä perinteisiltä haittaohjelmilta ja viruksilta että uusilta nollapäiväuhilta.

Automaattinen käytönaikainen suojaus

F-Secure Client Security estää automaattisesti ja käytönaikaisesti virusten, vakoiluohjelmien ja muiden haittaohjelmien hyökkäykset, tulevatpa ne sitten sähköpostista, Internetistä tai tallennusvälineistä, kuten USB-tikuilta. Ratkaisu valvoo sähköposti- ja selainliikennettä estäen viruksien lähettämisen tai vastaanottamisen. F-Secure Client Security helpottaa asennusta tunnistamalla asennuksen yhteydessä automaattisesti useimmat ristiriitoja aiheuttavat virustentorjuntaohjelmistot ja poistamalla ne käytöstä.

Huomaamattomat automaattiset päivitykset

Koska tarkistusohjelma on päivitettävissä, ylläpito käy nopeasti ja huolettomasti. Samasta syystä tarkistusohjelma suojaa tehokkaasti jatkuvasti kehittyviltä uhilta. Virustunnisteet päivittyvät huomaamatta ja automaattisesti ainakin kerran päivässä. Lähivertaisverkkotoiminto (neighbourcasting) mahdollistaa tunnisteiden lataamisen muista lähiverkon asiakassovelluksista. Näin tietoliikenneaistaa käytetään mahdollisimman vähän. Päivityksen varmistustoiminto pitää F-Secure Client Securityn suojauksen ajan tasalla silloinkin, kun ensisijaiseen päivityspalvelimeen ei saada yhteyttä.

F-Secure DeepGuard 2.0

F-Secure DeepGuard™ on ainulaatuinen työaseman tietomurrot estävä verkkoteknologia (NHIPS) . Sen ominaisuuksissa heuristinen analyysi, käyttöjärjestelmästä eristetty koekäyttö ja käytönaikainen haittakäyttötymisen esto yhdistyvät verkkokyselyihin. Lisäksi teknologia toimii saumattomasti yhdessä perinteisten tunnisteisiin perustuvien tarkistusjärjestelmien kanssa. Monitasoinen järjestelmä parantaa käytettävyyttä pienentämällä värien hälytyksien määrää. Verkkokyselyt nopeuttavat vasteaikaa ja vähentävät käyttäjän toimien tarvetta. Tiivis toiminta yhdessä sovellusten hallinnan kanssa vähentää ponnahdusikkunoiden määrää.

F-Secure BlackLight

Rootkit-ohjelmia käytetään usein piilottamaan haittaohjelmia, kuten viruksia, vakoiluohjelmia, mainosohjelmia, takaovia, troijalaisia ja matoja. Keskitetysti hallittava F-Secure BlackLight™ on käytönaikainen rootkit-tarkistusohjelma. Se tutkii järjestelmän toiminnallisuutta syvätasolla ja tunnistaa kohteet, jotka ovat piiloutuneet käyttäjältä ja perinteisiltä tietoturvaohjelmistoilta.

Automaattinen käytönaikainen suojaus

Tuntemattomilta uhilta suojaava F-Secure DeepGuard

Rootkit-tarkistusohjelma, F-Secure BlackLight

Sähköpostin ja selainliikenteen tarkistus

Vakoiluohjelmien torjunta

Tietomurtojen estotoiminnon sisältävä palomuri

Sovellusten hallinta

Automaattiset ja varmistetut päivitykset: virustentorjunta, vakoiluohjelmien torjunta, DeepGuard ja BlackLight

Lähivertaisverkkotoiminto virustunnisteiden lähiverkkojakeluun

Kattava IPv6-suojaus

Cisco NAC -tuki

Verkosta eristäminen, joka takaa kannettavien tietokoneiden tietoturvatason käytettäessä Internetiä toimiston ulkopuolelta

Automaattinen palomuuriprofiilin valinta - esimerkiksi toimisto tai mobiili - verkkosijainnin mukaan.

Virusuutiset työpöydälle tai verkonvalvojalle

Sisäänrakennettu palomuuuri

Sisäänrakennettu palomuuuri suodattaa saapuvan ja lähtevän liikenteen tehokkaasti ehkäisten näin työasemien luvattoman käytön verkon välityksellä. Palomuuuri piilottaa työasemat hakkereilta ja verkkomadoilta. Sovellusten hallinnalla verkonvalvojat voivat keskitetysti hallita työasemasovelluksia, jotka käyttävät Internetiä.

Kattava keskitetty hallinta ja raportointi

Lisänsiin sisältyvän F-Secure Policy Manager™ -hallintaohjelman avulla ylläpitäjät voivat keskitetysti asentaa F-Secure Client Security -ohjelmiston sekä ylläpitää ja valvoa sitä. Peruskäyttäjän käyttöliittymä ja tietoturva-asetukset ovat lukittavissa. Tämä estää peruskäyttäjiä kiertämästä tietoturva-asetuksia. F-Secure Client Securityn asetukset, tilatiedot ja tietoturvahälytykset ovat reaaliaikaisesti seurattavissa selainpohjaisen Web Reporting -raportointiliittymän kautta. Asetukset ovat mukautettavissa verkon, tietoturvatoinialueen tai yksittäisen työaseman tasolla.



VB 100%-palkinto F-Secure Client Security -tuotteelle: Virus Bulletin, huhtikuu 2008



Tunnustus F-Secure DeepGuard- ja BlackLight-tekniologioille: SC Magazine, kesäkuu 2007

Tuetut käyttöympäristöt

F-Secure Client Security
Windows 2000 (SP 4 tai uudempi)
Windows XP (SP 2 tai uudempi)
Windows Vista (32- ja 64-bittinen versio)

Hallintatyökalut

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 kuin palvelinversio sekä
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

Tuetut kielet

F-Secure Client Security
tšekki, tanska, hollanti, englanti
suomi, ranska, saksa, kreikka
unkari, italia, japani
norja, puola, portugali
(Portugali ja Brasilia), sloveeni
espanja, ruotsi, turkki

F-Secure Policy Manager
englanti, japani, ranska, saksa

"F-Secure" ja kolmiosymboli ovat F-Secure Corporationin rekisteröityjä tavaramerkkejä, ja F-Securen tuotenimet sekä symbolit ja logot ovat F-Secure Corporationin tavaramerkkejä tai rekisteröityjä tavaramerkkejä. Muut mainitut tuote- ja yritysnimet saattavat olla omistajiensa tavaramerkkejä. Copyright © 2008 F-Secure Corporation. Kaikki oikeudet pidätetään.

fscs800_fin_2008-09-25