

F-Secure Client Security 8



Le moderne minacce provenienti da Internet rendono necessaria una protezione proattiva e il monitoraggio del comportamento di software sospetti nel sistema, combinati con la tradizionale protezione basata sulle firme. F-Secure® Client Security™ fornisce una protezione proattiva con gestione centralizzata di desktop e laptop contro i malware tradizionali e le nuove minacce zero-day.

Protezione automatica in tempo reale

F-Secure Client Security blocca automaticamente i virus, gli spyware e i codici pericolosi in tempo reale, diffusi mediante posta elettronica, web o supporti rimovibili, come chiavette USB. Mediante la scansione del traffico POP3, IMAP4, SMTP e HTTP, la soluzione evita l'invio e la ricezione dei virus via posta elettronica o Web. Per rendere più semplice l'installazione, F-Secure Client Security riconosce i programmi antivirus che potrebbero entrare in conflitto e li rimuove automaticamente durante l'installazione.

Aggiornamenti automatici e trasparenti

I motori di scansione aggiornabili consentono una manutenzione veloce e senza problemi e offrono risposte rapide e semplici alle minacce in continua evoluzione. I database di definizione virus vengono aggiornati automaticamente e con la massima trasparenza almeno una volta al giorno. La funzionalità per il recupero degli aggiornamenti dalle postazioni vicine, consente il download del database da altri client interni alla LAN, minimizzando l'utilizzo della banda. La funzionalità fail-over garantisce una protezione aggiornata contro i nuovi virus anche nel caso in cui il server principale non sia raggiungibile.

F-Secure DeepGuard 2.0

F-Secure DeepGuard™ è una tecnologia esclusiva di prevenzione delle intrusioni basata sull'host HIPS (Host-based Intrusion Prevention System) di rete e combina un motore euristico avanzato, il sandboxing e il blocco comportamentale in runtime. Si integra perfettamente con i sistemi di scansione basati sulle definizioni dei virus. Questo particolare approccio multilivello aumenta la fruibilità e riduce il numero di falsi allarmi. Le query di rete aumentano la velocità di risposta, diminuendo al minimo la necessità di intervento da parte dell'utente. La forte integrazione con il controllo delle applicazioni riduce significativamente la quantità di popup.

F-Secure BlackLight

I rootkit vengono utilizzati per celare software pericolosi come virus, spyware, adware, backdoor, trojan e worm. F-Secure BlackLight™ gestibile in remoto è uno scanner per rootkit su richiesta che esamina i comportamenti del sistema in profondità rilevando oggetti che sono nascosti all'utente e al software di protezione.

Protezione automatica in tempo reale

Protezione contro le minacce sconosciute, grazie a F-Secure DeepGuard

Scansione contro i rootkit con F-Secure BlackLight

Scansione di posta elettronica e navigazione Web

Protezione antispyware

Firewall per la prevenzione dalle intrusioni

Controllo applicazioni

Aggiornamenti automatici per Antivirus, antispyware, DeepGuard e BlackLight con sistema fail-over

Recupero di aggiornamenti relativi alle definizioni dei virus all'interno della rete LAN

Protezione IPv6 completa

Quarantena per la rete che garantisce il livello di protezione dei portatili che si collegano a Internet dall'esterno delle strutture aziendali

Selezione automatica dei profili firewall (ufficio o cellulare) in base alla posizione di rete

Gestione centralizzata

Firewall desktop integrato

Il firewall desktop integrato con analisi di tipo stateful difende le workstation da accessi non autorizzati grazie al monitoraggio e al filtraggio costante del traffico Internet. Protegge inoltre le workstation da hacker e worm. Il controllo applicazioni consente agli amministratori di rete di gestire in modo centralizzato le applicazioni che accedono a Internet.

Gestione e generazione report centralizzati completi

Grazie a F-Secure Policy Manager™, un software incluso nella licenza, gli amministratori di rete possono installare, configurare e monitorare F-Secure Client Security da una posizione centralizzata remota. Possono, inoltre, bloccare le interfacce utenti finali e le impostazioni per la protezione per evitare che gli utenti senza il diritto di amministrazione eludano le impostazioni di protezione. F-Secure Client Security genera inoltre report completi che includono avvisi di protezione, percentuali di infezioni e aggiornamenti alle definizioni dei virus. Le impostazioni possono essere regolate a livello di dominio o a livello host individuale.



Premio VB100% per F-Secure Client Security "Virus Bulletin, aprile 2008"



Riconoscimento per F-Secure DeepGuard e BlackLight "SC Magazine, giugno 2007"

Piattaforme supportate

F-Secure Client Security
Windows 2000 (SP 4 o versione successiva)
Windows XP (SP 2 o versione successiva)
Windows Vista a 32 bit e a 64 bit

Strumenti di gestione

F-Secure Policy Manager Server e
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
Anche per Server
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

Lingue supportate

F-Secure Client Security
ceco, danese, olandese, inglese
finlandese, francese, tedesco, greco
ungherese, italiano, giapponese
norvegese, polacco, portoghese
portoghese (brasiliano) sloveno
spagnolo, svedese, turco

F-Secure Policy Manager
inglese, francese, tedesco e giapponese

"F-Secure" e il simbolo triangolo F-Secure, i nomi prodotto e relative combinazioni sono marchi di fabbrica o marchi registrati di F-Secure Corporation. Altre denominazioni citate a scopo puramente informativo possono essere marchi di proprietà delle rispettive aziende. Copyright © 2009 F-Secure Corporation. Tutti i diritti riservati.

fscs800_ita_2009-06-04