

F-Secure Client Security 7



Los nuevos ataques de rápida propagación van en aumento ya que los creadores de virus buscan un beneficio económico. Los cibercriminales profesionales actuales desean pasar desapercibidos y utilizan las tecnologías más avanzadas para ocultar sus acciones a las soluciones de seguridad de datos. Además, los objetivos de sus ataques están más definidos, por lo que el destinatario del ataque de un malware específico puede ser una única empresa o equipo. Si el antivirus no puede detectar el ataque, no es posible detectarlo de ninguna otra manera. Por ejemplo, un spyware oculto puede provocar graves daños a las empresas enviando información confidencial y reduciendo la productividad y el rendimiento de los equipos. Las amenazas de Internet actuales requieren una protección proactiva y la supervisión del comportamiento de los programas de software sospechosos en los sistemas combinadas con la protección basada en firmas tradicional. F-Secure® Client Security™ proporciona una administración centralizada, una protección proactiva avanzada frente a los ataques tradicionales y a los nuevos ataques de "día cero" (ataques que aprovechan vulnerabilidades de software desconocidas) contra los equipos de sobremesa y portátiles de una empresa.

Protección antivirus en tiempo real automática

F-Secure Client Security detiene automáticamente ataques de códigos dañinos y virus en tiempo real a través de correo electrónico, Internet, disquetes o CD-ROM. Mediante el análisis del tráfico POP3, IMAP4, SMTP y HTTP, evita el envío o la recepción de virus a través del correo electrónico o de Internet. Varios motores de análisis garantizan una protección perfecta frente a los virus activos. Para una instalación sencilla, F-Secure Client Security busca posibles programas conflictivos y los elimina automáticamente durante la instalación. Las bases de datos de definición de virus se actualizan automáticamente y de forma clara para el usuario dos veces al día con un uso de banda mínimo. La función de respaldo garantiza que F-Secure Client Security pueda ofrecer protección actualizada frente a virus nuevos, aunque no sea posible establecer conexión con el servidor de distribución principal.

F-Secure DeepGuard

F-Secure DeepGuard™ es una tecnología HIPS (Host-based Intrusion Prevention System, sistema de prevención de intrusiones basado en host) extraordinaria, en el sentido en que combina bloqueo por análisis de comportamiento en tiempo de ejecución, un entorno aislado y heurística avanzada, que funciona a la perfección con los sistemas de análisis basados en definiciones convencionales. Este extraordinario enfoque de varios niveles incorpora capacidad de uso gracias a la reducción de la cantidad de falsas alarmas. La firme integración con el control de aplicaciones también reduce la cantidad de ventanas emergentes. Todas las instalaciones de F-Secure DeepGuard forman una red mundial que analiza un gran número de aplicaciones desconocidas. Esto hace posible detectar e investigar posibles programas dañinos de una forma mucho más rápida que antes y proporcionar nuevas definiciones de virus.

F-Secure BlackLight

A menudo, los rootkits se utilizan para ocultar programas de software dañinos como, por ejemplo, virus, spyware, adware, backdoor, gusanos y troyanos. F-Secure BlackLight™ es un analizador de rootkits a petición que analiza el sistema de forma exhaustiva detectando los objetos ocultos para el usuario y los software de seguridad. Se trata de una tecnología de detección basada en comportamiento que compara dos vistas e identifica las diferencias ("cross-view-diff"). Toma dos vistas del sistema: un nivel inferior del sistema y una vista de lo que el usuario vería, por ejemplo, a través de Windows Explorer o el Administrador de tareas. Cualquier diferencia entre estas vistas se considera un rootkit. Gracias a su extraordinario potencial de administración remota, los administradores pueden analizar la red corporativa completa durante los períodos de menor uso, sin que esto afecte al rendimiento de la red.

Funciones clave

- > Protección automática en tiempo real
- > Protección frente a ataques desconocidos a través de F-Secure DeepGuard
- > Análisis de rootkits con F-Secure BlackLight
- > Análisis de correo electrónico e Internet
- > Protección contra spyware
- > Compatibilidad con Cisco NAC para una configuración novedosa de la seguridad y definiciones de virus en los equipos conectados a la red corporativa
- > Cuarentena de la red que garantiza el nivel de seguridad de los equipos portátiles conectados a Internet fuera de las instalaciones de la oficina
- > Actualizaciones automáticas de antivirus, antispayware, DeepGuard y BlackLight con sistema de respaldo
- > Cortafuegos con protección contra intrusos
- > Control de aplicaciones
- > Niveles de seguridad automáticos
- > Noticias sobre virus para los equipos de sobremesa o el administrador
- > Administración central

Cortafuegos de escritorio integrado

El cortafuegos de escritorio integrado con inspección completa del estado proporciona una supervisión exhaustiva y un filtrado del tráfico de Internet, lo que evita el acceso no autorizado a las estaciones de trabajo a través de la red. También oculta las estaciones de trabajo a los gusanos de red y a los piratas informáticos que actúan a través de Internet. La función de protección contra intrusos analiza el tráfico de Internet, y detecta automáticamente y bloquea el tráfico de red sospechoso como, por ejemplo, las exploraciones de puertos y los gusanos de red.

Control de aplicaciones

F-Secure Client Security permite a los administradores de red controlar de forma centralizada desde una única ubicación las aplicaciones de las estaciones de trabajo con autorización para acceder a Internet. Así se evita que los usuarios finales ejecuten aplicaciones prohibidas que puedan permitir a los piratas informáticos y a los gusanos acceder a los equipos sin el conocimiento del usuario.

Antispyware

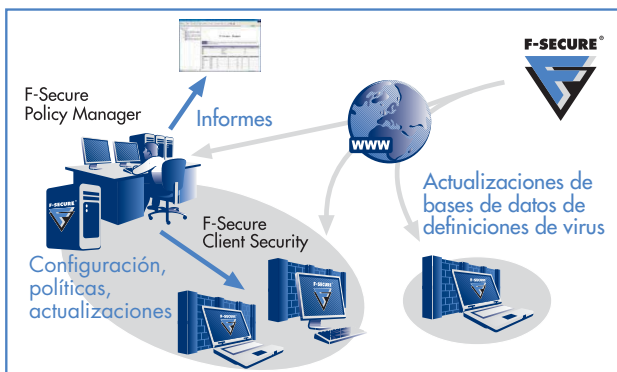
Spyware es un software que se instala en los equipos generalmente sin el conocimiento del usuario, por ejemplo, a través de la navegación en Internet. El spyware comercial suele robar información como, por ejemplo, los hábitos de navegación en Internet y se los facilita a empresas de publicidad. En el peor de los casos, los spyware pueden transmitir detalles personales como, por ejemplo, contraseñas y mensajes de correo electrónico a los piratas informáticos. F-Secure Client Security detecta y elimina estos componentes de seguimiento de datos instalados sin conocimiento del usuario.

Cambio del nivel de seguridad automático

F-Secure Client Security adapta automáticamente el nivel de seguridad a las condiciones. Cuando un equipo se conecta a la red corporativa, se utiliza la configuración de la oficina. Cuando un equipo se conecta a Internet fuera de la red corporativa, por ejemplo, desde casa o en un hotel, se aplica automáticamente una configuración más estricta.

Administración central integral y creación de informes

Con F-Secure Policy Manager™ – un programa de software incluido en la licencia – los administradores de red pueden instalar de forma remota, configurar y supervisar F-Secure Client Security desde una ubicación central. Los administradores pueden bloquear la interfaz de usuario final y la configuración de seguridad para evitar que los usuarios sin derechos de administrador se salten la configuración de seguridad. F-Secure Client Security también genera informes exhaustivos como, por ejemplo, alertas de seguridad, índices de infección por virus y actualizaciones de bases de datos de definiciones de virus. La configuración y los informes se pueden ajustar a la red, a un dominio de seguridad o un equipo individual.



Premio VB 100% para F-Secure Anti-Virus Client Security
"Virus Bulletin, febrero y junio de 2006, febrero de 2005"



Certificación Checkmark, niveles 1 y 2
"West Coast Labs, mayo de 2006"

Plataformas compatibles

Producto

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

Herramientas de administración

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

* Disponible en 2007 en los entornos de 32 bits

Idiomas compatibles

F-Secure Client Security
Checo, danés, neerlandés, inglés
finés, francés, alemán, griego
húngaro, italiano, japonés
noruego, polaco, portugués
portugués (Brasil), eslovaco
español, sueco, turco
F-Secure Policy Manager
Inglés, francés, alemán, japonés

"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.

fscs061114spa