

F-Secure Client Security 7



Es gibt immer mehr sich schnell verbreitende Bedrohungen, da Virenautoren nach finanziellem Gewinn streben. Moderne, professionell arbeitende Internetkriminelle wollen unbemerkt bleiben und nutzen fortschrittliche Technologien, um ihre Werke vor Datensicherheitslösungen zu verbergen. Ihre Angriffe sind außerdem gezielter, sodass ein einziges Unternehmen oder ein einziger Computer zum Opfer einer bestimmten Malware werden kann. Und wenn das Antivirenprogramm dies nicht merkt, merkt es niemand. Verborgene Spyware kann beispielsweise erhebliche Schäden in Unternehmen verursachen, indem vertrauliche Informationen versendet sowie die Leistung und Produktivität der Computer herabgesetzt werden. Moderne Bedrohungen aus dem Internet erfordern sowohl einen aktiven Schutz als auch die Überwachung von verdächtigem Verhalten der Software in den Systemen, kombiniert mit traditionellem signaturbasiertem Schutz. F-Secure® Client Security™ bietet zentral verwalteten, fortschrittlichen und aktiven Schutz gegen herkömmliche und neue Zero-Day-Bedrohungen für Desktop- und Laptop-Computer von Unternehmen.

Automatischer Echtzeitschutz vor Viren

F-Secure Client Security stoppt automatisch und in Echtzeit Viren und anderen bösartigen Code, die Ihren Computer per E-Mail, über das Internet, Disketten oder CD-ROMs angreifen. Indem das Programm POP3, IMAP4, SMTP und HTTP-Verkehr scannt, wird verhindert, dass Viren über E-Mails oder das Internet versendet oder empfangen werden. Mehrere Scan-Module sorgen für einen reibungslosen Schutz vor allen verbreiteten Viren. Um die Installation zu vereinfachen, sucht F-Secure Client Security nach anderen Virenschutzprogrammen, die möglicherweise Konflikte verursachen, und entfernt diese automatisch während der Installation. Virendefinitionsdatenbanken werden mehrmals täglich automatisch unter Verwendung minimaler Bandbreite aktualisiert. Durch die Failover-Funktion wird gewährleistet, dass F-Secure Client Security einen aktuellen Schutz gegen neue Viren bietet, selbst wenn der Updateserver nicht zur Verfügung steht.

F-Secure DeepGuard

F-Secure DeepGuard™ ist ein einzigartiges hostbasiertes Intrusion Prevention-System (HIPS), da es fortschrittliche Heuristik, Sandboxing-Funktionen und verhaltensbasierte Laufzeitblockierung vereint, die nahtlos mit konventionellen definitionsbasierten Scanning-Systemen zusammenarbeiten. Dieser einzigartige, vielschichtige Ansatz bietet zusätzliche Benutzerfreundlichkeit, da die Anzahl der falschen Alarme reduziert wird. Die enge Integration in die Anwendungssteuerung reduziert außerdem die Anzahl der Popups. Alle F-Secure DeepGuard-Installationen bilden ein globales Netzwerk, das eine Vielzahl unbekannter Anwendungen überprüft. So ist es möglich, eventuell bösartige Programme viel schneller zu entdecken und zu untersuchen als zuvor und neue Virendefinitionen zu bieten.

F-Secure BlackLight

Rootkits verbergen häufig Malware wie Viren, Spyware, Adware, Backdoors, Trojaner und Würmer vor Antivirenprogrammen. F-Secure BlackLight™ ist ein On-Demand-Rootkit-Scanner, der das System auf einer tiefen Ebene untersucht und Objekte findet, die dem Benutzer und der Sicherheitssoftware verborgen bleiben. Er bietet eine verhaltensbasierte Erkennungstechnologie, die zwei Ansichten vergleicht und die Unterschiede feststellt („Cross-View-Diff“). Dazu werden zwei Ansichten des Systems verwendet: eine niedrige Ebene des Systems und eine Ansicht, die dem Benutzer zugänglich wäre, z. B. mithilfe des Windows Explorer oder Task Manager. Jeder Unterschied zwischen diesen beiden Ansichten wird als Rootkit identifiziert. Dank der einzigartigen Remote-Verwaltungsfunktion können Administratoren während ruhigerer Geschäftszeiten ganze Firmennetzwerke überprüfen, ohne dass sich dies auf die Nutzbarkeit des Netzwerks auswirkt.

Hauptfunktionen

- > Automatischer Echtzeitschutz
- > Schutz vor unbekanntem Bedrohungen durch F-Secure DeepGuard
- > Rootkit-Scanning mit F-Secure BlackLight
- > E-Mail- und Web Scanning
- > Schutz vor Spyware
- > Cisco NAC-Unterstützung für aktuelle Sicherheitseinstellungen und Virendefinitionen von Computern, die eine Verbindung mit dem Firmennetzwerk herstellen
- > Netzwerk-Quarantäne überwacht die Sicherheitsstufe von Laptops, die außerhalb des Büros eine Verbindung zum Internet herstellen
- > Automatische Updates für Anti-Virus, Anti-Spyware, DeepGuard und BlackLight mit Failover-Funktion
- > Firewall mit Intrusion Prevention
- > Anwendungssteuerung
- > Automatische Sicherheitsstufen
- > Neue Informationen zu Computerviren an das Desktop oder den Administrator
- > Zentralverwaltung

Integrierte Desktop-Firewall

Die integrierte Desktop-Firewall bietet eine solide Überwachung und Filterung des Internet-Datenverkehrs, wodurch der unbefugte Zugriff über das Netzwerk auf Arbeitsstationen unmöglich wird. Sie schützt die Arbeitsstationen auch vor Internet-Hackern und Netzwerkwürmern und hält eine eventuelle Infektion auf eine einzelne Maschine begrenzt. Die Eindringenschutzfunktion analysiert den Internetdatenverkehr und erkennt und blockiert dabei automatisch verdächtigen Netzwerkdatenverkehr wie Port-Scans und Netzwerkwürmer.

Anwendungssteuerung

F-Secure Client Security ermöglicht es Netzwerkadministratoren, zentral von einem Standort aus die Anwendungen auf Arbeitsstationen zu kontrollieren, die auf das Internet zugreifen können. Dadurch können Endbenutzer keine verbotenen Anwendungen ausführen, die es Hackern und Wurmern möglich machen, in das Netzwerk einzudringen.

Anti-Spyware

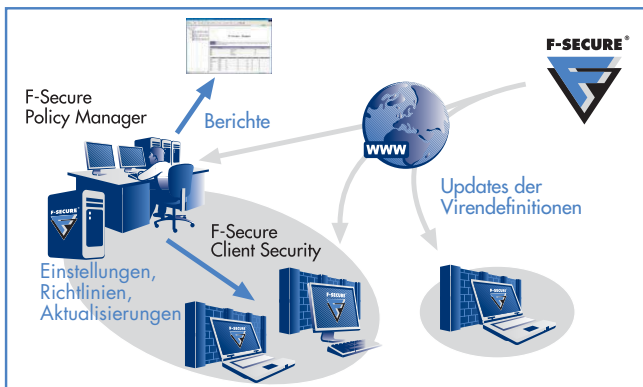
Spyware ist eine Software, die normalerweise ohne Wissen des Benutzers, z. B. beim Surfen im Internet, auf dem Computer installiert wird. Kommerzielle Spyware stiehlt häufig Informationen von Benutzern, wie beispielsweise Daten zu besuchten Internetseiten, und gibt diese Informationen an Werbeunternehmen weiter. Im schlimmsten Fall kann Spyware persönliche Daten wie Passwörter oder E-Mails an Hacker senden. F-Secure Client Security erkennt und entfernt diese heimlich installierten Komponenten zur Aufzeichnung von Daten.

Automatisches Ändern der Sicherheitsstufen

F-Secure Client Security passt die Sicherheitsstufe automatisch an. Wenn ein Computer eine Verbindung zum Netzwerk eines Unternehmens herstellt, werden die dort gültigen Einstellungen verwendet. Wenn ein Computer außerhalb des Unternehmensnetzwerks eine Verbindung zum Internet herstellt, beispielsweise von Zuhause oder von einem Hotel aus, werden automatisch strengere Einstellungen angewendet.

Umfassende zentrale Verwaltung und Berichte

Mit F-Secure Policy Manager™ – einer in der Lizenz enthaltenen Software – kann der Netzwerkadministrator F-Secure Client Security von einem zentralen Standort aus per Fernzugriff installieren, konfigurieren und überwachen. Administratoren können die Benutzeroberfläche sowie die Sicherheitseinstellungen der Endbenutzer blockieren, damit Benutzer ohne Administratorrechte die Sicherheitseinstellungen nicht umgehen können. F-Secure Client Security erstellt auch ausführliche Berichte, beispielsweise Sicherheitsalarme, Virendefinitionsraten sowie Aktualisierungen für die Virendefinitionsdatenbanken. Die Berichte und Einstellungen können an das Netzwerk, die Sicherheitsdomäne oder einen individuellen Host-Level angepasst werden.



VB100%-Auszeichnung für F-Secure Anti-Virus Client Security
"Virus Bulletin, Februar & Juni 2006, Februar 2005"



Checkmark-Zertifizierung
Level 1 und 2
„West Coast Labs,
November 2003“

Unterstützte Plattformen

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

Verwaltungstools

- F-Secure Policy Manager-Konsole
 - Windows 2000/XP/Server 2003
- F-Secure Policy Manager Server und 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

* Verfügbar im Jahr 2007 in 32-Bit-Umgebungen.

Unterstützte Sprachen

- F-Secure Client Security
 - Tschechisch, Dänisch, Niederländisch, Englisch, Finnisch, Französisch, Deutsch, Griechisch, Ungarisch, Italienisch, Japanisch, Norwegisch, Polnisch, Portugiesisch (brasilianisch), Portugiesisch, Slowenisch, Spanisch, Schwedisch, Türkisch
- F-Secure Policy Manager
 - Englisch, Französisch, Deutsch, Japanisch

"F-Secure" und das Dreiecksymbol sind eingetragene Marken der F-Secure Corporation, und F-Secure-Produktnamen und -Symbole/Logos sind Marken oder eingetragene Marken der F-Secure Corporation. Andere in diesem Dokument erwähnte Produkt- und Firmennamen können Marken ihrer jeweiligen Eigentümer sein.
Copyright © 2006 F-Secure Corporation. Alle Rechte vorbehalten.

fscs061114ger