

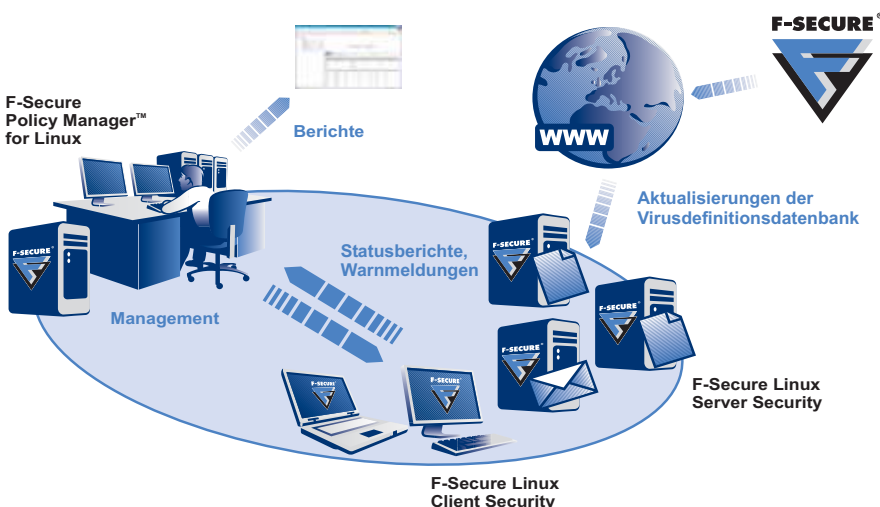
F-Secure Linux Client Security



Viren, Würmer, Trojaner, Riskware und Spyware stellen heute das größte Risiko für die IT-Sicherheit in Unternehmen weltweit dar. Hacker suchen aktiv nach ungeschützten Systemen, die wichtige Daten enthalten, sowie nach Computern, die auch für andere Zwecke genutzt werden könnten, wie die Verbreitung von illegalem Material oder die Vorbereitung von Angriffen auf andere Systeme.

Unternehmen jeder Größe suchen nach Sicherheitslösungen mit niedrigen Gesamtbetriebskosten. F-Secure® Linux Client Security™ schützt Linux-Workstations effizient vor Malware und Netzwerkangriffen.

F-Secure Linux Client Security ist eine integrierte, sofort einsatzfähige Sicherheitslösung mit einem starken Echtzeit-Virenschutz und einer Funktion zur Host Intrusion Prevention (HIPS), die Schutz vor unbefugten Verbindungsversuchen aus Netzwerken und unbefugten Systemänderungen sowie Schutz vor Userspace- und Kernel-Rootkits bietet. Diese Lösung kann problemlos in gemischten Umgebungen bereitgestellt und verwaltet werden, in denen eine nicht geschützte Linux-Workstation potenziell zum Ziel von Angriffen durch böswilligen Code werden und daher ein ganzes Unternehmen destabilisieren kann.



Hauptfunktionen

Umfassender Schutz vor Malware

F-Secure Linux Client Security stoppt sämtliche Malware-Arten, einschließlich Linux- und Windows-Viren, DOS-Dateiviren und Makroviren, die Microsoft Office-Dateien infizieren. Die Integration mehrerer Programme zum Scannen nach Viren in ein Produkt gewährleistet den bestmöglichen Schutz vor aktuellen und zukünftigen Sicherheitsrisiken.

Firewall

Die integrierte Firewall stellt sicher, dass keine Viren, Hacker und andere Eindringlinge die Workstation via Netzwerkwürmern entern.

Erkennung und Verhinderung von Host-Eindringlingen

Die Funktion zur Host Intrusion Prevention (HIPS) schließt Hackern und Crackern sämtliche Hintertüren und verhindert so die unbefugte Manipulation wichtiger Dateien, unbefugte Systemänderungen oder das Speichern unerwünschter Dateien auf Firmen-Workstations.

Zentrale Verwaltung

Die Software kann per Fernzugriff installiert, konfiguriert und von einem zentralen Standort aus überwacht werden. Die Client-Konfiguration kann für permanenten Schutz gesperrt werden.

Verbesserte Leistung

F-Secure Linux Client Security unterstützt sowohl 32- als auch 64-Bit-Plattformen. Die aktuelle Version 5.50 bietet verschiedene Leistungs- und Stabilitätsverbesserungen.

Umfassende Unterstützung für Linux-Distributionen

Die Liste der getesteten und unterstützten Linux-Distributionen umfasst etwa 30 unterschiedliche Systeme.

Antiviren-Scans in Echtzeit und ohne großen Aufwand

Scans in Echtzeit stellen sicher, dass die Benutzer keine infizierten Inhalte auf ihren Workstations und Desktops verarbeiten, ohne dass dies von der Software bemerkt wird. Administratoren können bedarfsmäßige Scans durchführen, diese planen oder Parameter für Scans in Echtzeit über das zentrale Verwaltungssystem festlegen.

Firewall-Verwaltung

Dieses Produkt stellt stabile Überwachungs- und Filterfunktionen für den Internet-Datenverkehr bereit, verhindert unerlaubte Zugriffe auf die Server über das Netzwerk und macht Server im Internet unsichtbar, um sie vor Hackern und Netzwerkwürmern zu schützen.

Erkennung und Verhinderung von Host-Eindringlingen

Kernel-Speicherschutz und Kernel-Modulüberprüfung in Verbindung mit Systemintegritätsprüfungen verschließen Hackern und Crackern sämtliche Hintertüren und verhindern so die Installation von Rootkits, die Manipulation kritischer Dateien oder das Speichern unerwünschter Dateien auf Firmen-Desktops.

Zentrale Verwaltung, Berichterstellung und Warnung

Durch die Integration in das zentrale Verwaltungssystem von F-Secure, F-Secure Policy Manager™, erhalten Administratoren im Falle von Sicherheitsrisiken oder Virenaktivität automatisch eine Nachricht. Über F-Secure Policy Manager können Administratoren ihre Sicherheitsrichtlinien problemlos bearbeiten und umsetzen.

Automatische Aktualisierung der Virensignaturen

Die Aktualisierung von Virensignaturdatenbanken geschieht automatisch und sicher. Die Dateien werden automatisch im Hintergrund heruntergeladen. So können sich Systemadministratoren jederzeit sicher sein, dass sie die neuesten Updates erhalten, ohne dass sie selbst im Web danach suchen müssen.

Sicherheitsverwaltungssystem für alle Betriebssysteme

Mithilfe des F-Secure Policy Manager können Sie sowohl die Sicherheit von Linux- als auch von Windows-Desktops, -Servern und -Gateways verwalten. Das Verwaltungssystem unterstützt sowohl Linux als auch Windows.

Plattformen

32-bit

Novell Linux Desktop 9
SUSE Linux 9.0
SUSE Linux 9.1
SUSE Linux 9.2
SUSE Linux 9.3
SUSE Linux 10
SUSE Linux 10.1
SUSE Linux 10.2
Ubuntu 5.10 (Breezy)
Ubuntu 6.06 (Dapper Drake)
SUSE Linux Enterprise Server 8
SUSE Linux Enterprise Server 9
SUSE Linux Enterprise Server 10
SUSE Linux Enterprise Desktop 10
Red Hat Enterprise Linux 4
Red Hat Enterprise Linux 3
Red Hat Enterprise Linux 2.1 AS
Fedora Core 5
Miracle Linux 2.1
Asianux 2.0
Turbolinux 10
Debian 3.1

64-bit

(AMD64/EM64T mit 32-Bit-Kompatibilitätspaket)

SUSE Linux Enterprise Server 9
SUSE Linux Enterprise Server 10
SUSE Linux Enterprise Desktop 10
Red Hat Enterprise Linux 4
Asianux 2.0
Turbolinux 10

Sprachen

Englisch
Japanisch
Deutsch

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 © 2007 F-Secure Corporation. Alle Rechte vorbehalten.

fscl070515ger