

Kaspersky Anti-Virus 8.0 für Linux File Server

Kaspersky Anti-Virus 8.0 für Linux File Server schützt Datei-Server unter Linux und FreeBSD optimal vor Schadprogrammen.

Große Unternehmensnetze beherbergen häufig Datei-Server, die auf verschiedenen Plattformen laufen. Die Ansprüche an den Datenschutz sind bei Datei-Servern generell hoch. Daher benötigen sie eine zuverlässige Sicherheitslösung wie Kaspersky Open Space Security.

HIGHLIGHTS

NEU! Kaspersky Web Management Console. Ein Dashboard in der neuen Web-Konsole zeigt den Status der Anwendung in Echtzeit an. Zudem lässt sich die Software darüber konfigurieren und verwalten.

Hohe Leistung. Eine effiziente Antiviren-Engine mit optimierten Scan-Technologien, Server Load Balancing sowie dem Ausschluss vertrauenswürdiger Prozesse von der Überprüfung erhöht die Leistung und reduziert den Ressourcenbedarf.

Zuverlässigkeit. Die Anwendung startet automatisch erneut, wenn es zu Störungen am Server kommt oder er gezwungen ist herunterzufahren. Somit wird ein stabiler Schutz gewährleistet.

NEU! Support für FreeBSD. Das Programm unterstützt die aktuellen Versionen von FreeBSD, d.h. es kann auch in Netzwerken mit diesem weniger verbreiteten Betriebssystem verwendet werden.

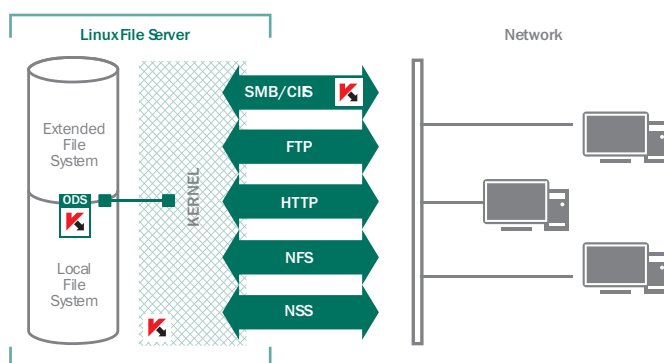
NEU! VMware Ready. Die Anwendung schützt alle Dateien, welche auf Linux-/FreeBSD-basierten Datei-Servern gespeichert werden, unabhängig davon, ob der Server auf einem physischen Computer oder einer virtuellen Maschine läuft.

NEU! Integration des Samba Servers

FUNKTIONEN

Optimierter Schutz für Datei-Server

Die Architektur von Kaspersky Anti-Virus 8.0 für Linux File Server bietet einen vielschichtigen Schutz für Linux-Server und heterogene Netzwerke, wobei die Funktionen gleichzeitig auf der gesamten Dateisystem-Ebene und der Ebene des SMB-/CIFS-Datentransfer-Protokolls (Samba-Server) arbeiten. Das Hauptmodul des Virenschutzes – ein Interceptor auf Kernel-Level – schützt das Dateisystem des Servers in Echtzeit. Der Schutz erstreckt sich auch auf lokale Ressourcen und Remote-Ressourcen im Server-Dateisystem, welche über eine Vielzahl von Datenübertragungsprotokollen erreicht werden können.



Effektiver Schutz gegen Malware

NEU! Verbesserte Antiviren-Engine. Neue heuristische Technologien kombiniert mit traditionellen Signatur-basierten Malware-Erkennungs-Methoden helfen, die Erkennung von Malware zu verbessern und gewährleisten proaktiven Schutz vor neuen Schadprogrammen.

Echtzeitschutz und On-Demand-Schutz. Die Anwendung scannt alle Dateien, die gestartet, geöffnet oder modifiziert werden und desinfiziert oder löscht alle infizierten Dateien. Darüber hinaus werden verdächtige Dateien oder Inhalte in einem Quarantäne-Bereich isoliert, bevor sie einer weiteren Analyse unterzogen werden. Die Anwendung durchsucht die angegebenen Bereiche des Systems zeitgesteuert oder auf Anfrage durch den System-Administrator.

NEU! Quarantäne- und Backup-Speicher. Wenn ein verdächtiges Objekt gefunden wird, wird dies in Quarantäne verschoben. Vor dem Löschen oder Ändern einer Datei wird eine Kopie des Originals zusammen mit all seinen Attributen im Backup-Ordner angelegt. Dies bedeutet, dass unabhängig von den Maßnahmen des Antiviren-Programms der Dokumenten-Workflow nicht unterbrochen wird.

Hohe Leistung

Server Load Balancing. Das Programm hilft, den Ressourcenverbrauch des Servers zwischen Antiviren-Software und anderen Anwendungen nach Prioritäten aufzuteilen. So kann z. B. der Viren-Scan im Hintergrund ausgeführt werden, während die Server-Software aktualisiert wird. Hierdurch werden die Server-Ausfallzeiten verringert.

Kontinuierlicher Server-Betrieb. Der Server muss nicht neu gestartet werden, wenn das Antiviren-Programm installiert oder aktualisiert wird – ein wichtiges Merkmal für die meisten Firmennetzwerke, wo Neustarts des Servers unerwünscht oder gar unmöglich sind. Der Dauerbetrieb der Server-Software sorgt so für einen unterbrechungsfreien Betrieb der Geschäftsprozesse eines Unternehmens.

Updates der Datenbanken. Die Aktualisierung der Antiviren-Datenbanken kann manuell nach Bedarf oder automatisch von Kaspersky-Servern beziehungsweise von lokalen Unternehmens-Servern durchgeführt werden. Das Programm wählt automatisch den am wenigsten ausgelasteten Update-Server.

Alternativ können Updates vom Server des Kaspersky Administration Kit heruntergeladen werden. Dies trägt dazu bei, dass die Updates schneller installiert werden und der Traffic im Netzwerk reduziert wird, wenn mehrere Produkte von Kaspersky Lab im Netzwerk installiert sind.

Flexible Administration

NEU! Zentrale Installation und Verwaltung. Über das Kaspersky Administration Kit, ein zentrales Management-Tool, kann die Anwendung auf mehreren Servern gleichzeitig remote konfiguriert und verwaltet werden.

Große Auswahl an Management-Tools. Der Administrator kann zwischen drei Management-Tools wählen: der Kaspersky Web Management Console, dem Kaspersky Administration Kit oder dem Kommandozeilen-Management.

Einfache Installation. Die Installation des Produkts dauert nur wenige Minuten und erfordert die Installation von nur einem Paket.

Flexible Scan-Einstellungen. Die Anwendung bietet eine breite Palette von Einstellungen. Der Administrator kann:

- den Grad des Virenschutzes anpassen
- unterschiedliche Einstellungen für unterschiedliche Nutzer zuweisen, welche auf geschützte Objekte auf dem Dateiserver zugreifen
- Scan-Ausnahmen spezifizieren
- Aktionen für verdächtige oder infizierte Objekte nach Art der Bedrohung festlegen
- Start des Scanners nach einem selbstgewählten Zeitplan durchführen

Die breite Palette von Einstellungen ermöglicht eine Optimierung der Server-Auslastung und gewährleistet eine flexible Verwaltung der unternehmensweiten Netzwerksicherheit.

Reporting-System. Der System-Administrator kann die Anwendung über grafische Berichte, über eine Web-Oberfläche im PDF- oder XLS-Format oder über die Konsole des Kaspersky Administration Kit überwachen.

Reports können für bestimmte Komponenten im HTML- oder CSV-Format über die Kommandozeile angezeigt werden.

Benachrichtigung über sicherheitsrelevante Ereignisse. In die Anwendung ist eine umfangreiche Liste von Ereignissen implementiert, die dem Administrator per SMS, Instant Message, SMTP oder über das Kaspersky Administration Kit mitgeteilt werden können. Die Anwendung unterstützt das Simple Network Management Protocol (SNMP).

Kaspersky Labs GmbH
Despag-Straße 3
85055 Ingolstadt
Deutschland
www.kaspersky.de
E-Mail: DEBusiness@kaspersky.de
Telefon +49 (0) 841 98 189 590
Telefax +49 (0) 841 98 189 100

Kaspersky Labs GmbH
Wienerbergstraße 11/12a
1100 Wien
Österreich
www.kaspersky.at
E-Mail: teamaustria@kaspersky.ch
Telefon +43 (0) 1 99 460 6400
Telefax +43 (0) 1 99 460 5000

Kaspersky Labs GmbH
Allmendstraße 1
6312 Steinhausen/Zug
Schweiz
www.kaspersky.ch
E-Mail: teamswiss@kaspersky.ch

SYSTEMANFORDERUNGEN

Minimum-Hardware-Anforderungen:

- Intel Pentium® II Prozessor 400 MHz oder höher
- 512 MB RAM
- Swap-Partition: mindestens 1 GB
- 2 GB freier Festplattenspeicher

Unterstützte Betriebssysteme:

- Red Hat Enterprise Linux 5.5 Server
- Fedora 13
- CentOS 5.5
- SUSE Linux Enterprise Server 10 SP3, 11 SP1
- Novell OES 2 SP2
- OpenSUSE Linux 11.3
- Mandriva Enterprise Server 5.1 (nur 32 Bit)
- Ubuntu 10.04 LTS Server Edition
- Debian GNU/Linux 5.0.5
- FreeBSD 7.3, 8.1

Besuchen Sie www.kaspersky.de, um mehr über die Anwendung zu erfahren.

Kaspersky Anti-Virus 8.0 für Linux File Server kann als Bestandteil von Kaspersky Open Space Security und Kaspersky Anti-Virus für File Server erworben werden.

Eine Liste der Partner von Kaspersky Lab ist hier verfügbar: www.kaspersky.de/partner_finden

Oktober 2010