Kaspersky® Endpoint Security for Linux

Zuverlässiger Schutz für Linux-basierte Server und Workstations

Linux ist oft die erste Wahl für leistungsstarke Server und kosteneffiziente Workstations und nimmt somit an Beliebtheit immer mehr zu. Seine zunehmende Anwendung erfordert einen angemessenen Schutz und angesichts seiner Präsenz in einem wachsenden Spektrum geschäftskritischer Systeme gewinnt das Sichern der Linux-basierten Server und Endpoints vor sich rasch entwickelnden Bedrohungen entscheidend an Bedeutung.

Kaspersky Endpoint Security for Linux bietet Next Generation-Schutz vor Cyberbedrohungen aller Art für eine umfassende Palette von Linux-Plattformen. Das Programm bietet mehrschichtigen Schutz bei minimaler Beeinträchtigung der anderen Programme oder der Systemleistung insgesamt. Es ist ein Bestandteil unseres umfassenden Produktportfolios - auch von Kaspersky Endpoint Security for Business.

Führend und anerkannt

Allein 2017 haben die Sicherheitsprodukte von Kaspersky Lab an 86 unabhängigen Tests und Bewertungen teilgenommen – mit 72 Siegen und 78 Top-3-Platzierungen. Die weltweit vielfach getesteten und preisgekrönten Sicherheitstechnologien erreichen höhere Erkennungsraten als die von anderen führenden Anbietern.

Kaspersky HuMachine™-Konzept

Funktionen für maschinelles Lernen, globale Big Data Threat Intelligence und zwei Jahrzehnte menschlicher Expertise sorgen gemeinsam für optimalen Schutz bei optimaler Effizienz.

Kaspersky Security Network

Das Kaspersky Security Network (KSN) ist eine komplexe verteilte Infrastruktur, die schneller als jemals zuvor auf neue Bedrohungen reagiert, die Leistung von Schutzkomponenten verbessert und das Risiko von Fehlalarmen (False-Positives) minimiert.

Integriert in ein einziges Produkt- keine versteckten Kosten

Der Schutz für Linux-basierte Geräte ist nur eines der Programme, die in Kaspersky Endpoint Security for Business und andere Produkte integriert sind. Es gibt keine versteckten Kosten: Ein Produkt heißt eine Lizenz – alles, was Sie brauchen, um Ihren IT-Bestand zu schützen.

Wichtigste Vorteile

Next Generation-Schutz

Unsere vorausschauenden Sicherheitstechnologien helfen Ihnen, die möglichen Bedrohungen, die Ihre Endpoints erreichen, zu minimieren. Zudem tragen sie dazu bei, Bedrohungen, die bis in Ihre Linux-Umgebung vordringen, zu identifizieren und zu blockieren. Neben dem Erkennen und Blockieren von gezielten Bedrohungen für Linux-Computer untersucht das Programm ebenfalls auf nach Bedrohungen für Windows und Mac, die sich auf einem Ihrer Linux-Knoten oder in der Linux-basierten Dateispeicherung befinden könnten.

Hohes Niveau an Bedienbarkeit und Leistung

Bei der Entwicklung des Programms stand vor allem die minimale Auswirkung auf andere Programme und die Gesamtleistung des Systems im Fokus. Die grafische Benutzeroberfläche (GUI) ist für größere Desktop-Umgebungen konzipiert. Dies, zusammen mit verbessertem Befehlszeilenmanagement, vereinfacht die Ausführung von Aufgaben und die tägliche Berichterstattung.

Zentrale Verwaltungskonsole

Alle Sicherheitsfunktionen lassen sich leicht über eine einzige Verwaltungskonsole, das Kaspersky Security Center, steuern. Dieses agiert auch als zentraler Punkt für die Verwaltung vieler anderer Sicherheitsprogramme von Kaspersky Lab.

Funktionen

Mehrstufiger Schutz

Schutz vor Zero-Day-Angriffen

Die Cloud-basierte Threat Intelligence des Kaspersky Security Network ermöglicht die schnelle Erkennung und Reaktion auf Linux- und andere BS-Bedrohungen nahezu in Echtzeit mit minimalen Fehlalarmen oder Workflow-Störungen.

Schutz vor Ransomware

Enthält einen einzigartigen Antiverschlüsselungsmechanismus, der die Verschlüsselung von Dateien in gemeinsam genutzten Ressourcen blockiert, um die Ausführung schädlicher Prozesse auf einer anderen Maschine desselben Netzwerks zu verhindern.

Erkennung von „bodiless“ Malware

Durch das Scannen von Bootsektoren auf Festplatten sowie des Arbeitsspeichers gestarteter Prozesse können Bedrohungen wie z. B. „bodiless“ oder reine Arbeitsspeicher-Malware entdeckt werden.

Dateiintegritätsüberwachung

Kann die Integrität von Systemdateien, Protokollen und kritischen Programmen garantieren, indem unbefugte Änderungen an wichtigen Dateien und Verzeichnissen verfolgt werden.

Echtzeit- und On-Demand-Scanning

Beobachtet alle Dateien, die gestartet oder geöffnet werden und desinfiziert infizierte Dateien. Scannt bestimmte Bereiche des Systems nach einem Zeitplan oder bedarfsabhängig und unterstützt das Scannen von Dateien nach Benutzern ohne entsprechende Berechtigungen.

Optimierte Systemleistung

Load Balancing

Das integrierte Ressourcen-Load Balancing und die optimierte Scanner-Technologie – mit der Option zum Ausschluss vertrauenswürdiger Hersteller – erhöht die Gesamtleistung bei gleichzeitiger Reduzierung des Ressourcenverbrauchs.

Fanotify

Unterstützt Fanotify und ermöglicht die On-Access-Prüfung für Kernels, ohne dass zusätzliche Module kompiliert werden müssen.

Ressourceneinsparungen

Automatische Anpassung der Nutzung von Systemressourcen und Durchführung von Selbstkontrollen zur Reduktion der Serverauslastung bei gleichzeitiger Wahrung der optimalen Sicherheitsniveaus.

Mehr als nur Sicherheitsverwaltung

Firewall-Management

Ermöglicht Ihnen die Konfiguration und Verwaltung von integrierten Firewall-Einstellungen des Linux-Betriebssystems: Das Programm ermöglicht die Erstellung von Richtlinien für Firewall-Regeln, Protokollen für Netzwerkaktivitäten und Prüfungen von Sicherheitsvorfällen, alles von einem Ort aus.

Grafische Benutzeroberfläche

Die grafische Benutzeroberfläche (GUI) ist für Linux optimiert. Zusammen mit verbessertem Befehlszeilenmanagement, vereinfacht dies die Ausführung von Aufgaben und die tägliche Berichterstattung.

Unterbrechungsfreier Betrieb

Nach Betriebssystem-Updates auf einer Workstation oder einem Server ist keine Wieder- oder Neuinstallation notwendig. Der Schutz ist aktiv, ohne dass ein Administrator eingreifen muss.

Systemanforderungen

Die vollständigen aktuellen Anforderungen finden Sie in der Wissensdatenbank.

Allgemeine Anforderungen

- Intel Core-2-Duo-Prozessor mit 1,86 GHz oder höher
- RAM: 1 GB bei einem 32-Bit-Betriebssystem (2 GB bei einem 64-Bit-Betriebssystem)
- 1 GB freier Festplattenspeicher

Betriebssysteme

- CentOS 6.9 x86/x64
- Debian GNU/Linux 8.9 x86/x64 oder höher
- Red Hat® Enterprise Linux® 7.4 x64 oder höher
- Ubuntu Server 16.04 LTS x64 oder höher
- openSUSE® 42.3 oder höher

Systemanforderungen für ein Abonnement

Wenden Sie sich an Ihren Kaspersky-Partner vor Ort, um die Verfügbarkeit von Monatsabonnements für Ihr Land zu prüfen. Die entsprechenden Systemanforderungen finden Sie hier.

Hinweise zum Kauf

Kaspersky Endpoint Security for Linux ist in folgenden Produkten enthalten:

- Kaspersky Total Security for Business
- Kaspersky Endpoint Security for Business Advanced
- Kaspersky Endpoint Security for Business Select

Die oben genannten Produkte können auch im Abonnement bezogen werden – mit flexibler, monatlicher Lizenzierung.

Sie können sie auch als eigenständige Lösungen, Kaspersky Security for File Server und Kaspersky Hybrid Cloud Security, erwerben.

Informationen zu Partnern in Ihrer Nähe finden Sie hier:
https://www.kaspersky.de/partners

#truecybersecurity
#HuMachine

www.kaspersky.de