Reliable protection for Linux-based servers and workstations

Often the OS of choice for high-performance servers and cost-efficient workstations, Linux is gaining a major foothold in business. Its increased adoption is driving the need for appropriate protection, and its presence in a growing range of business-critical systems makes securing Linux-based servers and endpoints against rapidly evolving threats a matter of vital importance.

Kaspersky Endpoint Security for Linux provides Next Generation protection against all types of cyberthreat, on a full range of Linux platforms. The application delivers multi-layered protection with minimal impact on other applications or on overall system performance, and is available within our comprehensive product portfolio, including in Kaspersky Endpoint Security for Business.

Highlights

Next Generation protection

Our proactive security technologies help minimize opportunities for threats to reach your endpoints – and help identify and block threats that do make it into your Linux environment. As well as detecting and blocking threats that target Linux computers, the application also watches out for Windows and Mac-based threats that could be sitting on one of your Linux nodes or inside your Linux-based file storage.

High level of usability and performance

The application is specifically designed to have minimal impact on other programs and on overall system performance. The graphical user interface (GUI) is designed for major desktop environments and this, together with improved command line management capabilities, simplifies task execution and daily reporting.

Single management console

All security functions are easily controlled via a single management console – Kaspersky Security Center – that also acts as a central point for managing many other Kaspersky Lab security applications.

Help meet regulatory requirements

The safety of sensitive data is at the top of every business’s security agenda. Kaspersky Security for Linux supports this with essential functionality to strengthen security and aid compliance with key principles such as PCI DDS and SWIFT usage requirements.

Kaspersky Security Network

Kaspersky Security Network is a sophisticated distributed infrastructure which delivers a faster-than-ever response to new threats, improving the performance of protection components and minimizing the risk of false positives.

Part of a single product – no hidden costs

Protection for Linux-based devices is just one of the applications built into Kaspersky Endpoint Security for Business and other products. There are no hidden costs - one product means one license, with everything you need to protect your IT estate.
Features

Multi-layered protection

**Protection from zero-day attacks**

Cloud-assisted threat intelligence from the Kaspersky Security Network enables a near real-time, rapid detection and response to Linux and other OS threats, with minimum false positives or workflow disruption.

**Behavior Detection**

Behavior Detection provides proactive defenses, identifying and extracting suspicious behavior patterns and effectively protecting your system against advanced threats.

**Network Threat Protection**

Our Network Threat Protection helps to prevent network threats – including port scanning, denial-of-service attacks and buffer-overruns. It constantly monitors network activities and, if it detects suspicious behavior, runs predefined responses.

**Web Threat Protection and anti-phishing**

Our Web Threat Protection delivers a near-100% threat detection rate of threats in web traffic, and blocks harmful scripts. Web Threat Protection monitors web traffic for attempts to visit phishing websites – and blocks access to them. To check links on web pages for phishing threats and malicious web addresses, Kaspersky Endpoint Security uses the application databases, heuristic analysis and data from Kaspersky Security Network.

**Reduce exposure to attacks with device control**

Device control reduces your attack surface and helps keep users safe and compliant with security policies.

**Anti-ransomware**

Contains a unique anti-cryptor mechanism capable of blocking the encryption of files on shared resources by a malicious process running on another machine on the same network.

**File Integrity Monitor**

File Integrity Monitor can guarantee the integrity of system files, logs and critical applications by tracking unauthorized changes in important files and directories.

Optimized performance

**Load balancing**

Built-in resource load balancing and optimized scanning technology – with the option to exclude trusted processes – enhances overall performance while reducing resource consumption.

**Fanotify support**

Supports fanotify and allows on-access scanning to run on kernels, without needing to compile additional modules.

Beyond security management

**Firewall management**

Allows you to configure and manage built-in Linux OS firewall settings; the application enables the creation of firewall rules policies, network activity logs and security incident reviews, all from one place.

**Graphical user interface**

The GUI is optimized for Linux and this, together with improved command line management capabilities, simplifies task execution and daily reporting.

**Uninterrupted operation**

Following an OS update on a workstation or server, there’s no need to re-install or undertake a fresh install – protection is up and running without the need for administrator involvement.

System requirements

For the most complete, up-to-date requirements, please refer to the [Knowledge Base](https://www.kaspersky.com).