Kaspersky® Endpoint Security для Linux

Надежная защита для серверов и рабочих станций под управлением Linux

В корпоративном секторе все чаще встречается ОС Linux, которая используется для высокопроизводительных серверов и экономичных рабочих станций. Вместе с популярностью Linux растет и спрос на соответствующие средства защиты. Для критически важных для бизнеса систем особенно актуальной проблемой становится защита серверов и рабочих мест Linux от быстро развивающихся угроз.

Kaspersky Endpoint Security для Linux предоставляет защиту нового поколения от всех современных киберугроз для широкого диапазона платформ Linux. Это приложение обеспечивает многоуровневую защиту с минимальным воздействием на другие приложения и общую производительность системы и входит в том числе в состав Kaspersky Security для бизнеса.

Признанный лидер

В 2017 г. «Лаборатория Касперского» приняла участие в 86 независимых обзорах. В 72 случаях наши продукты были признаны лучшими и 78 раз они оказались в первой тройке.

Концепция Kaspersky HuMachine™

Сочетание возможностей машинного обучения, глобальной аналитики больших данных и опыта экспертов, накопленного за два десятилетия, обеспечивает оптимальную защиту и эффективность работы.

Сеть Kaspersky Security Network

Облачная сеть безопасности Kaspersky Security Network – это сложная распределенная инфраструктура, которая обеспечивает максимально быстрое реагирование на новые угрозы, повышая эффективность защитных компонентов и минимизируя риск ложных срабатываний.

Часть единого продукта – никаких скрытых расходов

Защита для устройств Linux – это лишь одно из приложений, входящих в состав Kaspersky Security для бизнеса и других продуктов. Никаких скрытых расходов: один продукт – это одна лицензия, и все, что требуется для защиты IT-инфраструктуры.

Основные преимущества

Защита нового поколения

Наш проактивный подход к безопасности позволяет предотвратить возможности проникновения вредоносного ПО на рабочие станции и сервера, а также выявить и заблокировать те угрозы, которым все-таки удалось попасть на устройства Linux. Помимо обнаружения и блокирования атак, направленных на компьютеры Linux, Kaspersky Security для бизнеса также отслеживает угрозы для систем Windows и Mac, которые могут скрываться на одном из узлов Linux или в файловом хранилище на платформе этой ОС.

Удобство использования и высокая производительность

Приложение разработано с учетом минимального воздействия на работу других программ и общую производительность системы. Оптимизированный для большинства рабочих столов графический пользовательский интерфейс (GUI) и улучшенные возможности управления с помощью командной строки упрощают выполнение задач и создание ежедневных отчетов.

Единая консоль управления

Все функции безопасности легко контролировать из единой консоли управления – Kaspersky Security Center, которая также используется в качестве центра управления множеством других защитных решений «Лаборатории Касперского».

Возможности

Многоуровневая защита

Защита от атак «нулевого дня»

Облачный анализ угроз с помощью сети Kaspersky Security Network позволяет быстро обнаруживать угрозы для Linux и других ОС и устранять их практически в режиме реального времени с минимальным количеством ложных срабатываний или прерываний рабочих процессов.

Защита от программ-вымогателей

Содержит уникальный механизм защиты, который блокирует шифрование общих файловых ресурсов вредоносным процессом, запущенным на другом компьютере в той же сети.

Обнаружение бесфайловых вредоносных программ

Сканирование загрузочных секторов дисков и памяти запущенных процессов выявляет хорошо замаскированные угрозы, например так называемые бесфайловые вирусы в оперативной памяти.

Мониторинг целостности файлов

Обеспечивает целостность системных файлов, журналов и критически важных приложений, отслеживая несанкционированные изменения важных файлов и каталогов.

Проверка в режиме реального времени и по запросу

Наблюдает за всеми запускаемыми или открываемыми файлами и обезвреживает зараженные файлы. Проверяет заданные области системы по расписанию или по требованию с поддержкой проверки файлов непривилегированных пользователей.

Оптимизация производительности

Распределение нагрузки

Встроенная технология распределения нагрузки на ресурсы и оптимизированной проверки с возможностью исключения надежных процессов повышает производительность и снижает потребление ресурсов.

Поддержка fanotify

Позволяет выполнять проверку в процессе допуска в ядре без компилирования дополнительных модулей.

Экономия ресурсов

Автоматически регулирует использование системных ресурсов и применяет самоуправление для снижения нагрузки на сервер с сохранением оптимальных уровней защиты.

Не только управление защитой

Управление сетевым экраном

Позволяет настраивать параметры встроенного сетевого экрана ОС Linux и управлять ими. Приложение поддерживает создание политик правил сетевого экрана, журналов активности и обзоров инцидентов безопасности из единого центра.

Графический пользовательский интерфейс

Оптимизированный для ОС Linux графический пользовательский интерфейс (GUI) и улучшенные возможности управления с помощью командной строки упрощают выполнение задач и создание ежедневных отчетов.

Бесперебойная работа

После обновления операционной системы на рабочей станции или сервере нет необходимости переустанавливать решение – защита начнет работу немедленно и без участия администраторов.

Системные требования

Самую полную и актуальную версию требований см. в Базе знаний.

Общие требования:

- Процессор Intel Core 2 Duo с частотой 1,86 ГГц или выше
- Объем оперативной памяти: 1 ГБ для 32-разрядной ОС (2 ГБ для 64-разрядной ОС)
- 1 ГБ свободного пространства на диске

Операционные системы

- CentOS-6.9 x86/x64
- Debian GNU/Linux 8.9 x86/x64 или более поздней версии
- Red Hat® Enterprise Linux® 7.4 x64 или более поздней версии
- Ubuntu Server 16.04 LTS x64 или более поздней версии
- openSUSE® 42.3 или более поздней версии

www.kaspersky.ru

#ИстиннаяБезопасность