

# KASPERSKY SECURITY ДЛЯ ФАЙЛОВЫХ СЕРВЕРОВ

*Надежная защита ваших данных*

Всего один зараженный файл на корпоративном сервере может распространиться на все компьютеры локальной сети. Поэтому решение для защиты файловых серверов должно не только обеспечивать защиту важной информации, но и не позволять вредоносному ПО проникать в резервные копии файлов, что приводит к повторным заражениям.

Kaspersky Security для файловых серверов – это экономически эффективное, надежное и масштабируемое решение для защиты файловых хранилищ с общим доступом, не оказывающее заметного влияния на производительность системы.

## ПРЕИМУЩЕСТВА РЕШЕНИЯ

- Защита от вредоносного ПО в режиме реального времени
- Интеллектуальные технологии сканирования
- Гибкие настройки проверки
- Доверенные зоны
- Карантин и резервное хранилище
- Централизованное управление через Kaspersky Security Center
- Подробные отчеты

## ПОДДЕРЖИВАЕМЫЕ ПЛАТФОРМЫ

- Windows®, Linux® и FreeBSD™
- Терминальные серверы Citrix и Microsoft®
- Серверные кластеры
- Hyper-V®
- VMware®

## Основные возможности

### ВСЕСТОРОННЯЯ ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО

Удостоенное многочисленных наград антивирусное ядро «Лаборатории Касперского» обеспечивает всестороннюю защиту сервера от вредоносных и опасных программ, блокируя даже новейшие известные и потенциальные угрозы. Это позволяет свести к минимуму перебои в рабочих процессах предприятия, вызванные вредоносным ПО, а также уменьшить связанные с ними затраты.

### ВЫСОКАЯ ПРОИЗВОДИТЕЛЬНОСТЬ И НАДЕЖНОСТЬ

Kaspersky Security для файловых серверов не замедляет работу системы и не мешает рабочим процессам даже в условиях высокой нагрузки на сеть. Какой бы сложной ни была ваша IT-инфраструктура, вы можете рассчитывать на стабильность ее работы и высокую производительность.

### ПОДДЕРЖКА РАЗЛИЧНЫХ ПЛАТФОРМ

Единое эффективное защитное решение поддерживает новейшие платформы и серверы, включая терминальные, кластерные и виртуальные, и не вызывает проблем совместимости в гетерогенных сетях.

### МОЩНАЯ СИСТЕМА УПРАВЛЕНИЯ И ОТЧЕТНОСТИ

Удобные, интуитивно понятные инструменты управления, сведения о статусе защиты серверов, гибкие настройки времени сканирования и система подробных отчетов обеспечивают эффективный контроль безопасности файловых серверов, что помогает сократить расходы на их содержание.

### ПРОАКТИВНАЯ ЗАЩИТА

Решение содержит эвристический сканер, способный обнаруживать с высокой точностью даже то вредоносное ПО, сигнатуры которого еще не были добавлены в базу данных.

### ОБЛАЧНАЯ ЗАЩИТА

Облачная репутационная база угроз Kaspersky Security Network (KSN) обеспечивает скорейшее реагирование на новые угрозы, увеличивает эффективность защиты и уменьшает риск ложных срабатываний.

### КОНТРОЛЬ ЗАПУСКА ПРИЛОЖЕНИЙ НА СЕРВЕРАХ

Контроль запуска приложений обеспечивает исключительную защиту. С помощью правил можно разрешить или запретить запуск исполняемых файлов, скриптов или пакетов MSI, а также загрузку на сервер модулей DLL.

### ЗАЩИТА ОБЩИХ ПАПОК ОТ ПРОГРАММ-ШИФРОВАЛЬЩИКОВ

Если на какой-либо машине замечены попытки шифрования, приложение блокирует ее доступ к любым сетевым файловым ресурсам.

## Ключевые функции

- Защита от вредоносного ПО в режиме реального времени для файловых серверов на базе последних версий Windows (включая Windows Server® 2012/R2), Linux и FreeBSD (включая версию Samba для обеих ОС)
- Защита терминальных серверов Citrix и Microsoft
- Полная поддержка серверных кластеров
- Масштабируемость – возможность расширения системы защиты по мере роста компании, поддержка и защита даже самых сложных гетерогенных IT-инфраструктур
- Надежность, стабильность и высокая отказоустойчивость
- Оптимизированная интеллектуальная технология сканирования с гибкими настройками, включающая проверку по требованию и проверку критических областей системы
- Доверенные зоны – позволяют исключить из проверки доверенные процессы и хранилища, что повышает производительность системы защиты, снижая потребление ресурсов при сканировании
- Карантин и резервное копирование файлов перед их лечением или удалением позволяют в случае инцидента восстановить данные, необходимые для его анализа
- Изолирование зараженных рабочих мест
- Централизованная установка, управление и обновление
- Гибкие сценарии реагирования на инциденты
- Подробные отчеты о статусе защиты сети
- Система уведомлений о работе приложений
- Поддержка иерархических систем хранения данных (HSM)
- Поддержка Hyper-V и XenDesktop
- Сертификат VMware Ready
- Поддержка ReFS

### КАК ПРИОБРЕСТИ

Решение Kaspersky Security для файловых серверов доступно в составе следующих продуктов линейки Kaspersky Security для бизнеса:

- Kaspersky Endpoint Security для бизнеса СТАНДАРТНЫЙ (без Контроля запуска приложений)
- Kaspersky Endpoint Security для бизнеса РАСШИРЕННЫЙ
- Kaspersky Total Security для бизнеса

Кроме того, Kaspersky Security для файловых серверов можно приобрести отдельно. Чтобы выбрать нужный вам продукт, проконсультируйтесь с партнером «Лаборатории Касперского». Контактная информация и адреса партнеров представлены на нашем сайте в разделе [kaspersky.ru/find\\_partner\\_office](https://kaspersky.ru/find_partner_office)

### ПОДРОБНЕЕ:

[kaspersky.ru/business](https://kaspersky.ru/business)