KASPERSKY SECURITY ДЛЯ WINDOWS SERVER®

Специализированное решение для высокопроизводительных корпоративных серверов

По мере того как корпоративные IT-сети становятся все сложнее, возрастают и требования к защите серверов. Один зараженный файл, оказавшийся на корпоративном сервере, может распространиться на все компьютеры сети, причинив огромный ущерб.

Kaspersky Security для Windows Server – это экономичное, надежное и легко масштабируемое защитное решение для хранилищ файлов с совместным доступом, которое не оказывает заметного влияния на производительность системы. Оно не только защитит критически важную информацию от новейших угроз, но и не позволит вредоносному ПО проникнуть в резервные копии файлов и вызвать повторные инциденты.

Преимущества решения

ЗАЩИТА ОТ ИЗВЕСТНЫХ, НЕИЗВЕСТНЫХ И КОМПЛЕКСНЫХ УГРОЗ

Надежное антивирусное ядро обеспечивает ускоренную проверку и меньшее воздействие на системные ресурсы, позволяя достичь высочайшего уровня обнаружения угроз при помощи облачной сети безопасности (Kaspersky Security Network).

ПЕРЕДОВАЯ ЗАЩИТА ДЛЯ КРИТИЧЕСКИ ВАЖНЫХ СЕРВЕРОВ

Надежный контроль запуска программ в сочетании с глобальной сетью сбора данных об угрозах и средством защиты от программ-шифровальщиков (Anti-Cryptor) создает дополнительные уровни безопасности для корпоративных систем хранения и серверов.

СЕРТИФИКАЦИЯ СОВМЕСТИМОСТИ

Совместимость приложения с платформами виртуализации и операционными системами подтверждена сертификатами.

Возможности решения

ЭФФЕКТИВНАЯ ЗАЩИТА ОТ ВРЕДОНОСНЫХ ПРОГРАММ

Постоянная антивирусная защита и проверка по требованию. Приложение проверяет каждый запущенный или измененный файл, выполняет лечение или удаление зараженных объектов, а также помещает подозрительные объекты в карантин. При установке нового ПО или обнаружении подозрительного файла администратор может проверить соответствующие области на наличие вредоносного ПО.

Облачная защита серверов. Облачная репутационная база Kaspersky Security Network (KSN) обеспечивает максимально быстрое реагирование на новые угрозы, повышая эффективность защитных компонентов и минимизируя риск ложных срабатываний.

Надежный контроль запуска программ на серверах. Высочайший уровень безопасности за счет настройки правил, разрешающих или блокирующих запуск исполняемых файлов, сценариев и пакетов MSI, а также загрузку файлов DLL на серверы.

Защита папок с совместным доступом от программ-шифровальщиков (Anti-Cryptor). При выявлении действий по шифрованию файлов приложение блокирует доступ машины-источника ко всем сетевым файловым ресурсам.

Блокирование доступа к сети хостам, выполняющим подозрительные действия. Возможность блокировать доступ компьютера к общим сетевым папкам на защищаемом сервере, если при выполнении задач защиты в режиме реального времени или предотвращении вредоносного шифрования обнаружилось, что этот компьютер осуществляет вредоносные действия.

Проактивная защита от вредоносного ПО. Передовые технологии защиты от вредоносного ПО, в том числе эвристический анализатор, который выявляет вредоносные программы, даже если их сигнатуры еще не добавлены в антивирусные базы.

Проверка критических областей операционной системы. Можно запустить специальную задачу для проверки тех областей операционной системы, которые наиболее подвержены заражению. Например, проверка файлов автозапуска помогает предотвратить запуск вредоносного ПО при загрузке операционной системы и позволяет выявить любые скрытые процессы.

Гибкие настройки проверки. Настраиваемая проверка файлов позволяет администратору выполнять следующие действия:

- исключать определенные процессы из проверки;
- настраивать глубину проверки;
- указывать, какие типы файлов требуют обязательной проверки, а какие должны быть исключены из проверки;
- задавать действия при обнаружении подозрительных и зараженных объектов в зависимости от типов угроз.

Такой подход оптимизирует нагрузку на сервер и обеспечивает гибкое управление безопасностью корпоративной сети.

Защита терминальных и виртуальных серверов. Приложение защищает терминальные серверы Microsoft® Terminal Services (серверы со службами терминалов Microsoft®) и Citrix XenApp®, обеспечивая безопасность конечных пользователей, которые работают в режиме публикации рабочего стола или приложений, а также оповещая их о событиях. Поддерживаются виртуальные среды на основе Hyper-V®, XenDesktop® и VMware®.

Поддержка кластеров. Приложение полностью подходит для серверных кластеров сложной архитектуры: оно защищает и локальные диски серверов, и общие диски кластера, которыми в данный момент владеет защищаемый узел.

Высокая производительность

Масштабируемость. При использовании многопроцессорных серверов администратор может задавать количество рабочих процессов защитного приложения для ускорения обработки запросов к серверу.

Распределение нагрузки. Доступно распределение ресурсов между решением Kaspersky Security для Windows Server и другими приложениями (в соответствии с заранее заданными приоритетами). Проверка на вредоносное ПО может выполняться в фоновом режиме.

Выбор доверенных процессов. Чтобы оптимизировать производительность, администратор может исключить из проверки безопасные процессы, такие как резервное копирование данных или дефрагментация жесткого диска.

Непрерывная работа серверов. Решение Kaspersky Security для Windows Server не требует перезагрузки сервера при установке и обновлении защиты от вредоносного ПО.

Гибкое администрирование

Разнообразие средств управления. Приложением можно управлять напрямую или удаленно через Microsoft Management Console, Kaspersky Security Center или используя командную строку. Новая версия продукта снабжена интуитивно понятным графическим интерфейсом для Microsoft Management Console.

Простые средства установки и администрирования. Kaspersky Security Center – это консоль управления, позволяющая удаленно устанавливать и настраивать приложение на нескольких серверах одновременно, а также управлять работой приложения и получать обновления и уведомления.

Разделение прав администраторов. Каждому серверному администратору можно предоставить собственный уровень полномочий, обеспечив соблюдение требований IT-отдела и правил внутренней безопасности.

Гибкая настройка времени проверки. Приложение позволяет задать время начала и окончания антивирусной проверки, чтобы снизить вероятность сбоев и оптимизировать использование серверных ресурсов.

Система уведомлений. Приложение позволяет оповещать администратора о широком спектре событий. Уведомления направляются посредством службы сообщений или по электронной почте. Поддерживается протокол Simple Network Management Protocol (SNMP) и работа с Microsoft Operations Manager (MOM). Кроме того, администратор может отслеживать работу приложения по журналам событий Microsoft Windows или Kaspersky Security Center.

КАК ПРИОБРЕСТИ

Приложение Kaspersky Security для Windows Server можно приобрести в составе следующих продуктов:

- Kaspersky Endpoint Security для бизнеса СТАНДАРТНЫЙ (без Контроля запуска программ)
- Kaspersky Endpoint Security для бизнеса РАСШИРЕННЫЙ
- Kaspersky Total Security для бизнеса
- Kaspersky Security для файловых серверов
- Kaspersky Security для систем хранения данных

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

ПОДРОБНЕЕ:
kaspersky.ru/business

© АО «Лаборатория Касперского», 2016. Все права защищены. Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей. Citrix, XenApp и XenDesktop являются товарными знаками компании Citrix Systems, Inc. и/или одной или более из ее дочерних компаний и могут быть зарегистрированы в США (в Бюро по регистрации патентов и товарных знаков) и в других странах. Microsoft, Windows, Windows Server и Hyper-V — товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах. VMware – товарный знак VMware, Inc. или зарегистрированный в США или других юрисдикциях товарный знак VMware, Inc.