KASPERSKY SECURITY ДЛЯ СЕРВЕРОВ СОВМЕСТНОЙ РАБОТЫ

Защита данных и контроль платформ совместной работы, в т. ч. ферм серверов Microsoft® SharePoint®.

Платформы, используемые для обмена файлами и данными, могут способствовать быстрому распространению вредоносного ПО и других информационных угроз в корпоративной сети. Чтобы обеспечить безопасную и бесперебойную совместную работу с документами, «Лаборатория Касперского» разработала решение, в котором эффективные технологии защиты от вредоносных атак и утечки конфиденциальных данных сочетаются с простотой управления и удобством использования.

ПРЕИМУЩЕСТВА РЕШЕНИЯ

- Удостоенное наград антивирусное ядро
- Контроль над распространением конфиденциальной информации
- Контроль доступа к данным
- Облачная защита в режиме реального времени (Kaspersky Security Network)
- Файловая и контентная фильтрация
- Защита от фишинга
- Резервное копирование данных
- Централизованное гибкое управление
- Удобная консоль администрирования

Основные возможности

ВСЕСТОРОННЯЯ ЗАЩИТА SHAREPOINT-ПЛАТФОРМЫ

Традиционные решения для защиты рабочих мест не подходят для обеспечения безопасности Microsoft SharePoint Server, поскольку в этом случае весь контент хранится в SQL-базе. Удостоенные многочисленных наград передовые технологии защиты от вредоносного ПО в составе Kaspersky Security для серверов совместной работы обеспечивают максимальный уровень безопасности всей фермы серверов SharePoint, а также их пользователей. Мощная защита от всех типов угроз, в том числе новых и сложных, осуществляется при поддержке облачной сети безопасности Kaspersky Security Network, а технология блокирования фишинговых ссылок обеспечивает защиту совместно используемых данных от любых интернет-угроз.

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ

Для надежного контроля и защиты документооборота компании необходимо эффективно выявлять конфиденциальную информацию в потоке данных. Kaspersky Security для серверов совместной работы проверяет каждый документ, загружаемый на серверы SharePoint, на наличие конфиденциальной информации, используя для этого предустановленные или ваши собственные словари, а также категории данных. Особое внимание уделяется контролю и защите персональных данных и данных банковских карт, а возможность поиска структурированной информации позволяет контролировать распространение, например, клиентских баз.

ПРИМЕНЕНИЕ ПОЛИТИК ДОКУМЕНТООБОРОТА

Функции контентной и файловой фильтрации обеспечивают четкое применение стандартов и политик документооборота, выявляя и блокируя нежелательный контент, а также исключая хранение файлов (в том числе файлов заданного формата), не соответствующих политике безопасности, принятой в организации.

ПРОСТОТА УПРАВЛЕНИЯ

Управление защитой всей фермы серверов может осуществляться централизованно с помощью единой интуитивно понятной консоли. Простое и удобное администрирование не требует специального обучения IT-персонала.

Ключевые функции

ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО

- **Проверка при доступе**. Файлы проверяются в режиме реального времени при их загрузке на сервер или скачивании.
- **Проверка в фоновом режиме**. Файлы, хранящиеся на сервере, регулярно проверяются с использованием новейших антивирусных сигнатур.
- **Интеграция с Kaspersky Security Network**. Облачная сеть безопасности позволяет обеспечить защиту в режиме реального времени, в том числе от угроз «нулевого дня».

ПОДДЕРЖКА ПОЛИТИК ДОКУМЕНТООБОРОТА КОМПАНИИ

- Файловая фильтрация помогает обеспечить соблюдение политик хранения документов и позволяет снизить нагрузку на файловые хранилища. Решение анализирует действительные форматы файлов независимо от присвоенных им расширений, что позволяет исключить использование файла с запрещенным расширением вопреки политике безопасности, принятой в компании.
- Защита всех видов репозиториев SharePoint, в том числе вики-сайтов и блогов.
- Контентная фильтрация предотвращает хранение файлов с нежелательным контентом независимо от типа файла. Анализ содержимого каждого файла производится по ключевым словам. Предусмотрена возможность создания и использования собственных словарей для контентной фильтрации.

ГИБКОЕ УПРАВЛЕНИЕ

- Управление всей фермой серверов может осуществляться централизованно с помощью единой консоли с интуитивно понятным интерфейсом, включающим все наиболее распространенные сценарии администрирования.
- Удобная в использовании единая информационная панель обеспечивает мгновенный доступ к информации о текущем статусе защиты, версии антивирусных баз и статусе лицензии для всех защищаемых серверов.
- Резервное копирование измененных файлов позволяет восстановить исходные файлы в случае инцидента, а подробная информация об измененных файлах может затем использоваться в ходе его расследования.
- Интеграция с Active Directory® позволяет использовать авторизацию пользователей Active Directory.

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ

- Kaspersky Security для серверов совместной работы проверяет документы, загружаемые на серверы SharePoint, на наличие конфиденциальной информации. В решении реализованы модули, позволяющие выявлять конкретные типы данных, отвечающие определенным стандартам – например, персональные данные (в соответствии с законом ФЗ-152 «О защите персональных данных») или данные стандарта PCI DSS (стандарт безопасности данных в индустрии платежных карт). Кроме того, документы проверяются по предустановленным, регулярно обновляемым тематическим словарям, включающим такие категории, как «Финансы», «Административные документы» и «Оскорбительная и ненормативная лексика», а также по словарям, созданным IT-специалистами организации.
- Структурированная информация, обнаруженная в каком-либо документе, автоматически расценивается как потенциально конфиденциальная. Это дает возможность контролировать распространение сложных массивов информации, например клиентских баз.

КАК ПРИОБРЕСТИ

Kaspersky Security для серверов совместной работы можно приобрести в составе Kaspersky Total Security для бизнеса или как отдельное решение.

Внимание: при покупке данного продукта функционал контроля над распространением конфиденциальной информации приобретается дополнительно.

ПОДРОБНЕЕ:

http://www.kaspersky.ru/collaboration-security

KASPERSKY lab