KASPERSKY SECURITY ДЛЯ СИСТЕМ ХРАНЕНИЯ ДАННЫХ

Высокоэффективная защита хранилищ EMC, NetApp и Hitachi

Общие сведения

В современных IT-инфраструктурах вредоносное ПО может распространяться с огромной скоростью. В условиях постоянно растущего числа угроз один-единственный зараженный файл, попавший в хранилище, подвергает риску каждый узел корпоративной сети.

Решение Kaspersky Security для систем хранения данных предлагает надежную, высокоэффективную и масштабируемую защиту ценной и конфиденциальной корпоративной информации, хранящейся в системах EMC Isilon™, Celerra и VNX™, NetApp, Hitachi и IBM.

ПРЕИМУЩЕСТВА РЕШЕНИЯ

- Защита систем хранения EMC, NetApp, Hitachi и IBM от вредоносного ПО в режиме реального времени
- Поддержка антивирусного агента Celerra (CAVA), а также протоколов RPC и ICAP
- Задачи проверки критических областей
- Гибкая настройка параметров проверки
- Масштабируемость и отказоустойчивость
- Оптимизация использования системных ресурсов
- Защита терминальных серверов
- Поддержка кластеров
- Сертификат совместимости с VMware
- Технологии iSwift и iChecker для оптимизации антивирусной проверки
- Управление с помощью Kaspersky Security Center
- Отчеты о работе решения
- Поддержка протоколов SNMP/MOM

Основные возможности

ВСЕСТОРОННЯЯ ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

Постоянная проактивная защита сетевых устройств хранения данных (NAS). Мощное антивирусное ядро, разработанное «Лабораторией Касперского», проверяет каждый файл при его запуске или изменении на наличие всех видов вредоносного ПО, в том числе вирусов, червей и троянцев. Расширенный эвристический анализ позволяет успешно выявлять даже новые и неизвестные угрозы.

ОПТИМИЗАЦИЯ ПРОИЗВОДИТЕЛЬНОСТИ

Высокоэффективная проверка с использованием оптимизированной технологии сканирования и возможностью гибкой настройки исключений из проверки обеспечивает максимальный уровень безопасности при минимальном влиянии на работу системы.

БЕСПЕРЕБОЙНАЯ РАБОТА

Исключительная отказоустойчивость достигается благодаря тесной интеграции и слаженной работе всех компонентов решения. В результате мы имеем стабильно работающее, отказоустойчивое решение, которое в случае принудительного завершения работы автоматически перезапускается, обеспечивая надежную и непрерывную защиту.

ПРОСТОЕ УПРАВЛЕНИЕ

Установка и настройка защиты серверов производятся удаленно, без необходимости перезагружать систему. Управление приложением Kaspersky Security для систем хранения данных, а также другими решениями «Лаборатории Касперского» осуществляется с помощью единой консоли Kaspersky Security Center с простым, интуитивно понятным интерфейсом.

Ключевые функции

НЕПРЕРЫВНАЯ ПРОАКТИВНАЯ ЗАЩИТА
Передовое антивирусное ядро «Лаборатории Касперского», созданное ведущими мировыми экспертами в области IT-безопасности, обеспечивает эффективную проактивную защиту от новых и потенциальных угроз с помощью мощных интеллектуальных технологий обнаружения.

АВТОМАТИЧЕСКИЕ ОБНОВЛЕНИЯ
Антивирусные базы обновляются автоматически без необходимости прерывать проверку, что позволяет обеспечить непрерывную защиту и снизить нагрузку на администратора.

ИСКЛЮЧЕНИЕ ПРОЦЕССОВ ИЗ ПРОВЕРКИ И ДОВЕРЕННЫЕ ЗОНЫ
Гибкая настройка сканирования позволяет создавать так называемые «доверенные зоны», которые могут быть исключены из проверки, наряду с определенными форматами файлов и процессами, такими как резервное копирование.

ПРОВЕРКА ОБЪЕКТОВ АВТОЗАПУСКА
Чтобы обеспечить усиленную защиту серверов, можно проводить проверку файлов автозапуска и операционной системы. Это позволяет предотвратить запуск вредоносного ПО во время загрузки системы.

Администрирование

ЦЕНТРАЛИЗОВАННАЯ УСТАНОВКА И УПРАВЛЕНИЕ
Удаленная установка, настройка и администрирование, в том числе отправка уведомлений, установка обновлений и формирование детальных отчетов, осуществляются через единую консоль управления Kaspersky Security Center с интуитивно понятным интерфейсом. Кроме того, возможно управление с помощью командной строки.

РАЗДЕЛЕНИЕ ПРАВ АДМИНИСТРАТОРОВ
Администраторам можно присваивать различные права на основе ролей в соответствии с требованиями корпоративной политики IT-безопасности.

ГИБКАЯ ПРОВЕРКА И ОПТИМИЗАЦИЯ ПРОИЗВОДИТЕЛЬНОСТИ
Широкие возможности сканирования позволяют сократить время проверки и настройки, что способствует сбалансированному распределению нагрузки и оптимизации работы серверов. Администратор может настраивать глубину, объем и время сканирования, задавая типы файлов и области, которые нуждаются в проверке. Проверку по требованию также можно запланировать заранее, назначив ее на период низкой активности сервера.

ЗАЩИТА СИСТЕМ HSM И DAS
Решение поддерживает автономные режимы проверки, что позволяет обеспечить эффективную защиту иерархических систем хранения данных (HSM). Защита систем хранения с прямым подключением (DAS) способствует внедрению экономичных решений для хранения данных.

ПОДДЕРЖКА ВСЕХ ОСНОВНЫХ ПРОТОКОЛОВ
Kaspersky Security для систем хранения данных поддерживает основные протоколы, используемые различными системами хранения данных — RPC и ICAP, а также антивирусный агент Celerra (CAVA-агент).

ЗАЩИТА ВИРТУАЛЬНЫХ СИСТЕМ И ТЕРМИНАЛЬНЫХ СЕРВЕРОВ
Благодаря своей гибкости решение обеспечивает безопасность виртуальных (гостевых) операционных систем в средах Hyper-V® и VMware, а также инфраструктур терминальных серверов Microsoft® и Citrix®.

ГИБКАЯ СИСТЕМА ОТЧЕТОВ
Работу приложения можно контролировать, используя наглядные отчеты, а также просматривая журнал событий Microsoft Windows® или Kaspersky Security Center. Инструменты поиска и система фильтров позволяют быстро получать доступ к нужным данным в журналах большого объема.

КАК ПРИОБРЕСТИ
Kaspersky Security для систем хранения данных можно приобрести у компании-партнера «Лаборатории Касперского». Контактная информация и адреса партнеров представлены на нашем сайте в разделе http://www.kaspersky.ru/find_partner_office

ПОДРОБНЕЕ:
http://www.kaspersky.ru/storage-security

KASPERSKY lab