▶KASPERSKY SECURITY ДЛЯ СИСТЕМ ХРАНЕНИЯ ДАННЫХ

Высокоэффективная защита хранилищ EMC и NetApp

ОБЩИЕ СВЕДЕНИЯ

Вредоносное ПО может распространиться по сети организации с огромной скоростью. В условиях постоянно растущего числа угроз один-единственный зараженный файл, случайно помещенный в хранилище, немедленно подвергает риску каждый узел корпоративной сети.

Решение Kaspersky Security для систем хранения данных предлагает надежную, высокоэффективную и масштабируемую защиту ценных корпоративных данных, хранящихся в системах EMC® VNX™ и NetApp.

- Защита от вредоносного ПО в режиме реального времени
- Защита систем хранения EMC VNX и NetApp
- Специальные задачи для проверки критических областей системы
- Гибкая настройка параметров проверки
- Масштабируемость и отказоустойчивость
- Адаптивное использование ресурсов системы
- Защита терминальных серверов
- Поддержка кластеров
- Сертификат совместимости с VMware
- Технологии iSwift и iChecker для оптимизации проверки
- Управление с помощью Kaspersky Security Center
- Отчеты о работе приложения
- Поддержка протоколов SNMP/MOM

ОСОБЕННОСТИ ПРИЛОЖЕНИЯ

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

Оптимизированная технология сканирования с возможностью гибкой настройки исключений из проверки обеспечивает максимальный уровень безопасности при минимальном влиянии на работу системы.

НАДЕЖНОСТЬ

Исключительная отказоустойчивость достигается благодаря тесной интеграции и слаженной работе всех компонентов решения. В случае принудительного завершения работы решение автоматически перезапускается, обеспечивая непрерывную защиту.

ПРОСТОТА УПРАВЛЕНИЯ

Установка и настройка защиты серверов производится 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.

ВОЗМОЖНОСТИ ПРИЛОЖЕНИЯ

НЕПРЕРЫВНАЯ ПРОАКТИВНАЯ ЗАЩИТА
Передовое антивирусное ядро «Лаборатории Касперского» обеспечивает эффективную проактивную защиту от уже существующих 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
Глубину сканирования можно тонко настраивать, создавая так называемые «доверенные зоны», которые могут быть исключены из проверки, наряду с определенными форматами файлов и процессами (например, резервным копированием).

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.

ГИБКАЯ ПРОВЕРКА И ОПТИМИЗАЦИЯ ПРОИЗВОДИТЕЛЬНОСТИ
Широкие возможности сканирования позволяют сократить время проверки, 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 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.

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®.

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 через собственную консоль продукта или с помощью командной строки.

РАЗДЕЛЕНИЕ ПРАВ АДМИНИСТРАТОРОВ
Администраторам каждого сервера можно присвоить различные права, что помогает соблюсти специфические требования корпоративной политики IT-безопасности.

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.

СИСТЕМНЫЕ ТРЕБОВАНИЯ

ОБОРУДОВАНИЕ
- x86-совместимые системы в однопроцессорной и многопроцессорной конфигурации
- x86-64-совместимые системы в однопроцессорной и многопроцессорной конфигурации

ДИСКОВОЕ ПРОСТРАНСТВО
- Для установки всех программных компонентов: 70 МБ
- Для хранения объектов в карантине и в резервном хранилище: 400 МБ (рекомендуется)
- Для хранения журналов: 1 ГБ (рекомендуется)
- Для хранения баз данных: 2 ГБ (рекомендуется)

МИНИМАЛЬНАЯ КОНФИГУРАЦИЯ
- Процессор (1 Core) 1,4 ГГц
- Объем оперативной памяти: 1 ГБ
- 4 ГБ свободного места на жестком диске

РЕКОМЕНДУЕМАЯ КОНФИГУРАЦИЯ
- Процессор (4 Core) 2,4 ГГц
- Объем оперативной памяти: 2 ГБ
- 4 ГБ свободного места на жестком диске

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
- Microsoft Windows Server® 2003/2003 R2 x86/x64 Standard/ Enterprise Edition
- Microsoft Windows Server 2008/2008 R2 x86/x64 Standard/ Enterprise/Datacenter Edition
- Microsoft Windows Server 2012/20012 R2 Essentials / Standard / Foundation / Datacenter
- Microsoft Windows Hyper-V Server 2008 R2
- Microsoft Windows Hyper-V Server 2012/2012 R2
- Microsoft Windows Storage Server 2008 R2 / 2012 / 2012 R2

СЕРВЕРЫ
- Microsoft Terminal на базе Windows Server 2003
- Microsoft Terminal на базе Windows Server 2008
- Microsoft Terminal на базе Windows Server 2012/ 2012 R2
- Citrix Presentation Server™ 4.0, 4.5
- Citrix XenApp™ 4.5, 5.0, 6.0, 6.5
- Citrix XenDesktop® 7.0, 7.1, 7.5

ПЛАТФОРМЫ ХРАНЕНИЯ ДАННЫХ
Файловые хранилища EMC Celerra® / VNX
- EMC DART 6.0.36 или более поздняя версия
- Celerra Antivirus Agent (CAVA) 4.5.2.3 или более поздняя версия

Требования для хранилища NetApp
- Data ONTAP 7.x и Data ONTAP 8.x, режим 7-mode
- Data ONTAP 8.2.1 или более поздняя версия, режим Cluster mode

vmware READY

Windows Server 2012 R2 Certified

KS-Storage/Version 0.2/May14/Global

KASPERSKY lab