

“Белая Книга” DeviceLock



Оглавление:

- [Почему DeviceLock?](#)
- [Каковы специфические характеристики DeviceLock?](#)
- [Кому необходим DeviceLock?](#)
- [Как работает DeviceLock?](#)
- [Кто разработал DeviceLock?](#)
- [Где получить DeviceLock?](#)
- [Техническая поддержка DeviceLock](#)
- [Цены](#)
- [Как купить DeviceLock?](#)
- [Контактная информация](#)

Почему DeviceLock?

Контроль за тем, что было выгружено или закачено в локальную сеть компании, является одной из основных задач службы информационной безопасности. И эта работа становится сложнее с каждым днём. Быстро возрастающее количество переносных USB-накопителей является грозным предзнаменованием. Рынок этих устройств растет по экспоненте, с каждым днем устройства становятся быстрее, увеличивается их производительность и уменьшается размер. Необходимо принимать во внимание устройства Bluetooth и WiFi, которые, обеспечивая простоту использования, по умолчанию устанавливают связь с любым клиентом в пределах своих границ, а эти границы могут быть удивительно широкими.

Инвестиции в сетевые экраны, шифрование данных, иные технологии и средства контроля, разработанные для защиты данных от хищения через Интернет, постоянно увеличиваются. Однако эти меры обеспечивают слабую защиту от доступа к информации через локальные незащищенные устройства и порты. Они не остановят сотрудника компании, который приносит на работу двухгигабайтный жесткий диск, подключает его к USB-порту и начинает скачивать конфиденциальную информацию. Не смогут они воспрепятствовать и обиженному служащему, который использует подобные устройства для загрузки троянов или других вредоносных программ в сеть.

Встроенные механизмы распределения прав доступа и задания политик безопасности в операционных системах Windows не позволяют контролировать доступ к USB-портам и устройствам. Тем не менее, использование неавторизованных USB-устройств представляет угрозу корпоративным сетям и данным. Причем не только конфиденциальная информация может «уйти» из корпоративной сети через USB-порт, но и вирусы или троянские программы могут быть занесены внутрь корпоративной сети, минуя серверные файрволы и антивирусы. Точно так же дело обстоит с записывающими CD/DVD-приводами и с FireWire-устройствами. Современные MP3-плееры имеют объемные встроенные жесткие диски и быстрые интерфейсы для подключения к компьютеру. Все это делает невозможным контроль использования несанкционированных устройств хранения информации административными мерами.

Тут как раз и приходит на помощь программное решение DeviceLock, которое с 1996 года разрабатывает компания Смарт Лайн Инк (SmartLine Inc). Механизм аутентификации USB-устройств, встроенный в DeviceLock, является незаменимым и подчас безальтернативным решением проблем внутренней корпоративной безопасности.

DeviceLock полностью интегрируется в подсистему безопасности Windows, функционируя на уровне ядра системы, и обеспечивает прозрачную для пользователя защиту.

Каковы специфические характеристики DeviceLock?

Обеспечивая контроль над пользователями, имеющими доступ к портам и устройствам локального компьютера, DeviceLock закрывает потенциальную гигантскую брешь в защите простым и экономичным способом. В сравнении с решениями, требующими наличия физических хранилищ и управления аппаратными замками и ключами, предлагаемое решение значительно дешевле и проще для внедрения на предприятии. В сравнении с другими программными средствами (такими, как изменение BIOS), DeviceLock является более элегантным, простым и масштабируемым решением.

DeviceLock позволяет контролировать весь спектр потенциально опасных устройств: USB-порты, дисководы, CD/DVD-приводы, а также FireWire, инфракрасные, принтерные (LPT) и модемные (COM) порты, WiFi и Bluetooth-адаптеры, а также позволяет осуществлять детальный аудит действий пользователя с устройствами и файлами.

DeviceLock поддерживает функцию теневого копирования данных. Все файлы, копируемые пользователем на внешние носители (CD/DVD, дискеты, флеш-диски, и т.п.), будут зеркалироваться и сохраняться для последующего просмотра администратором. Сохраняются полные копии файлов. Теневое копирование – это расширение функции аудита, и оно также может быть включено для отдельных пользователей или групп пользователей.

DeviceLock позволяет назначать права доступа для пользователей и групп пользователей, имеет систему удаленного управления, позволяющую обеспечивать доступ ко всем возможным функциям программы. Уникальность программы состоит в том, что кроме управления через собственную централизованную консоль, DeviceLock может управляться через групповые политики Windows в домене Active Directory, благодаря чему легко интегрируется в любую инфраструктуру организаций любого масштаба. Так, один из клиентов Smart Лайн Инк контролирует свою сеть, включающую около 68 000 компьютеров, с помощью DeviceLock.

«Белый список» USB-устройств позволяет авторизовать определенные модели устройств, которые не будут заблокированы несмотря на установленные разрешения, и поддерживает устройства с уникальными серийными номерами. Таким образом, возможно разрешить доступ к определенному устройству и при этом заблокировать доступ к другим подобным устройствам этой же модели этого же производителя.

DeviceLock также имеет функцию авторизации носителей, аналогичную «белому списку» USB-устройств и позволяющую идентифицировать определенный CD/DVD-диск на основе записанных на него данных и разрешить его использование, даже если сам привод CD/DVD-ROM заблокирован.

Нередко сотрудники обладают привилегиями локальных администраторов на своих компьютерах, что позволяет рядовым пользователям удалять любые установленные на их компьютерах программы, в том числе программы защиты информации, антивирусы и т.п. DeviceLock позволяет задавать список учетных записей (пользователи и/или группы), которым будет разрешено администрировать (устанавливать, удалять, менять разрешения и другие установки, и т.д.) DeviceLock. В этом случае даже пользователи, которые имеют привилегии локального администратора, не смогут изменить настройки или удалить программу со своих компьютеров, если они не входят в список администраторов DeviceLock.

DeviceLock применяется для защиты информации в любых организациях, использующих компьютеры, работающие под управлением MS Windows NT/2000/XP/2003 – как стационарные компьютеры, так и переносные. Будучи однажды установленным, DeviceLock успешно функционирует вне зависимости от наличия подключения компьютера к локальной сети, что обеспечивает защиту информации для мобильных пользователей.

Кому необходим DeviceLock?

Быстро растущее число пользователей DeviceLock включает государственные органы, работающие с конфиденциальной информацией, и другие средние и крупные компании, нуждающиеся в контроле доступа к устройствам для приема, передачи или обработки данных.

Программный продукт стремительно развивается и разрабатывается в соответствии с потребностями мирового рынка информационной безопасности.

Качество и надежность программы подтверждают более 50 тысяч клиентов Смарт Лайн Инк во всем мире – банки, страховые компании, военные и государственные организации, крупные корпорации (нефтегазовая отрасль, машиностроение, энергетика) и другие коммерческие организации, медицинские, учебные и научно-исследовательские учреждения.

За время выхода на российский рынок программа завоевала авторитет крупнейших российских компаний, а также компаний малого и среднего бизнеса. Вот что говорят о программе российские клиенты:

- *"DeviceLock – это наиболее простое и эффективное программное решение. У нас не возникло никаких проблем с его установкой. Системный администратор и пользователи остались довольны результатами внедрения программы DeviceLock."* (Еськин В.В., начальник отдела информационной безопасности Ханты-Мансийского банка).
- *"ПО DeviceLock позволило не только ограничить время и виды используемых сотрудниками Банка внешних носителей информации, но и вести контроль их использования с протоколированием времени и названия модифицируемого файла. Тем самым с внедрением программы был закрыт потенциальный канал утечки информации в информационной системе Банка. Нас также устроило соотношение цены и качества программного продукта DeviceLock."* (Андрей Широков, начальник отдела информационной безопасности Банка «КОЛЬЦО УРАЛА»).
- *"Мы пришли к выводу, что DeviceLock – это простое в использовании и относительно недорогое программное решение. Руководство института и системный администратор остались довольны результатами внедрения программы DeviceLock."* (Галина Шипкова, главный специалист отдела информационных технологий ФГУП «Атомэнергопроект»).
- *"Использовать программное решение DeviceLock нам рекомендовали в московском представительстве Microsoft. Установить DeviceLock было очень легко. Администрация библиотеки осталась довольна внедрением DeviceLock, так как была устранена основная проблема, связанная с несанкционированным копированием материалов."* (Корытин А.А., заведующий центром информационных технологий, «Российская государственная библиотека»).

Как работает DeviceLock?

DeviceLock состоит из трех частей: агента, сервера и консоли управления:

1. DeviceLock Service – это ядро системы DeviceLock. Агент устанавливается на каждый компьютер, автоматически запускается и обеспечивает защиту устройств на машине-клиенте, в то же время оставаясь невидимым для локального пользователя.

2. DeviceLock Enterprise Server – это дополнительный необязательный компонент, используемый для централизованного сбора и хранения данных теневого копирования и журналов. DeviceLock Enterprise Server использует MS SQL Server для хранения данных.
3. Консоль управления – это интерфейс контроля, который системный администратор использует для удаленного управления любой системой, на которой установлен агент. DeviceLock поставляется с тремя различными консолями управления: DeviceLock Management Console, DeviceLock Enterprise Manager и DeviceLock Group Policy Manager.

Кто разработал DeviceLock?

Разработчик DeviceLock – ЗАО “Смарт Лайн Инк”. Основанная в 1996 году, российская компания Смарт Лайн Инк (SmartLine Inc) занимается разработкой программного обеспечения для администрирования компьютерных сетей. Качество и надежность продуктов Смарт Лайн Инк подтверждают более 55 тысяч клиентов в 80-ти странах мира – государственные, военные, медицинские, образовательные, крупнейшие финансовые и коммерческие учреждения, а также компании малого и среднего бизнеса. Программное обеспечение Смарт Лайн Инк установлено на более чем 3 000 000 компьютерах. В число клиентов компании входят Центральный Банк РФ, Сбербанк России, ОАО "Силловые машины", ВТБ 24, Российская государственная библиотека, BAE SYSTEMS, AEROTEC Engineering GmbH, HSBC Bank, Barclays Bank, Chase Manhattan Bank. Смарт Лайн Инк – международная компания с офисами в Лондоне, Милане, Москве, Ратингене (Германия) и Сан Рамоне (штат Калифорния, США). Основной офис разработки программных продуктов Смарт Лайн Инк находится в Москве.

Где получить DeviceLock?

Бесплатная, полностью функциональная демо-версия доступна для скачивания на нашем сайте: www.deviceclock.com/ru/dl/download.html

Техническая поддержка DeviceLock

Техническая поддержка доступна для пользователей DeviceLock круглосуточно, без праздников и выходных, на русском, английском и немецком языках:
www.deviceclock.com/support/ticket_list.php

Также на нашем сайте вы можете найти разнообразную информацию по поддержке, включая описания известных проблем и часто задаваемые вопросы (FAQ):
www.deviceclock.com/ru/support.html

Цены

Стоимость DeviceLock – 1300 рублей (включая НДС) за лицензию на одно рабочее место. Скидки доступны для многопользовательских лицензий. Расценки на многопользовательские лицензии приведены на сайте:
www.deviceclock.com/ru/dl/register.html

Как купить DeviceLock?

Для получения информации о том, как оформить заказ, смотрите:
www.deviceclock.com/ru/dl/register.html

Контактная информация

ЗАО "Смарт Лайн Инк"

Москва, Б. Семеновская ул., д. 40, офис 301

Телефон: +7 (495) 967-99-60, +7 (495) 366-21-93 (контактное лицо – Анастасия Дементьева)

Отдел продаж: sales@devicelock.com

Тех. поддержка: support@devicelock.com