DeviceLock®

ПРОГРАММНЫЙ КОМПЛЕКС ЗАЩИТЫ ОТ УТЕЧЕК ДАННЫХ С КОРПОРАТИВНЫХ КОМПЬЮТЕРОВ

Зачем нужны DLP-средства защиты от утечек данных?

Ценные корпоративные данные, которые ваша организация пытается защитить с помощью межсетевых экранов и паролей, буквально утекают сквозь пальцы инсайдеров. Это происходит как случайно, так и в результате умышленных действий – неправомерного копирования информации с рабочих компьютеров на флеш-накопители, MP3-плееры, смартфоны, карманные и планшетные компьютеры, CD/DVD-диски и другие носители данных. Кроме того, данные могут бесконтрольно передаваться инсайдерами через электронную почту, службы мгновенного обмена сообщениями, веб-формы, форумы и социальные сети. Беспроводные интерфейсы – Wi-Fi, Bluetooth и Infrared – наравне с каналами локальной синхронизации данных с мобильными устройствами открывают дополнительные пути для утечек информации с пользовательских компьютеров организации. Помимо инсайдерских угроз другой опасный сценарий утечек реализуется при заражении компьютеров вредоносными программами, которые могут записывать вводимый с клавиатуры текст или отдельные виды хранимых в оперативной памяти компьютера данных и впоследствии передавать их в Интернет по протоколам электронной почты (SMTP) или файлового обмена (FTP). В то время, как ни одна из этих уязвимостей не устраняется ни традиционными механизмами сетевой безопасности, ни встроенными средствами контроля ОС Windows, программный комплекс DeviceLock® Endpoint DLP Suite эффективно предотвращает утечки данных с корпоративных компьютеров, используя полный набор механизмов контекстного контроля операций с данными а также технологии их контентной фильтрации.

Контекстный контроль и контентная фильтрация

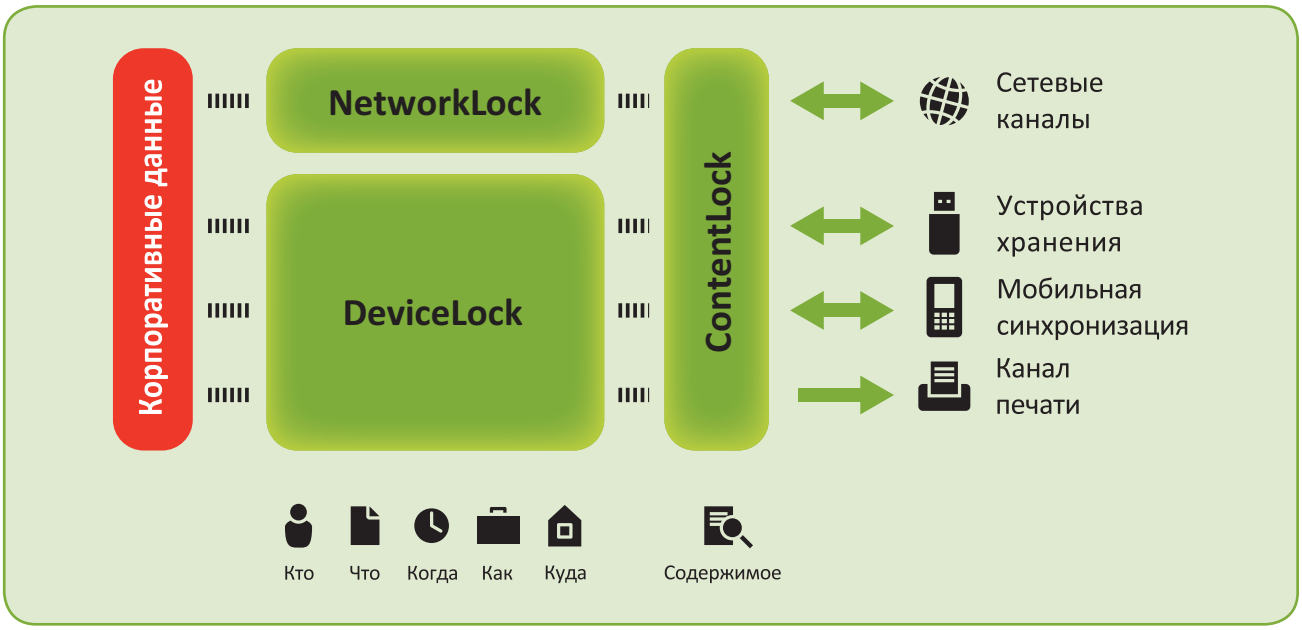
Наиболее эффективный подход к защите от утечек информации с компьютеров начинается с использования, прежде всего, механизмов контекстного контроля – запрета или разрешения передачи данных для конкретных пользователей в зависимости от форматов данных, типов интерфейсов и устройств, сетевых протоколов, направления передачи, дня недели и времени суток и т.д.

Однако, во многих случаях требуется более глубокий уровень контроля – например, проверка содержимого передаваемых данных на наличие персональной или конфиденциальной информации в условиях, когда порты ввода-вывода не должны блокироваться, чтобы не нарушать производственные процессы, но отдельные пользователи входят в «группу риска», поскольку подозреваются в причастности к нарушениям корпоративной политики информационной безопасности. В подобных ситуациях дополнительно к контекстному контролю необходимо применение технологий контентного анализа и фильтрации, позволяющих выявить и предотвратить передачу неавторизованных данных, не препятствуя при этом информационному обмену в рамках служебных обязанностей сотрудников.

Программный комплекс DeviceLock Endpoint DLP Suite использует как контекстные, так и основанный на анализе контента методы контроля данных, обеспечивая надежную защиту от информационных утечек с пользовательских компьютеров и серверов корпоративных ИС при минимальных затратах на приобретение и обслуживание комплекса. Контекстные механизмы DeviceLock реализуют гранулированный контроль доступа пользователей к широкому спектру периферийных устройств и каналов ввода-вывода, включая сетевые коммуникации. Дальнейшее повышение уровня защиты достигается за счет применения методов контентного анализа и фильтрации данных, что позволяет предотвратить их несанкционированное копирование на внешние накопители и Plug-and-Play устройства а также передачу по сетевым протоколам за пределы корпоративной сети.

Наряду с методами активного контроля эффективность применения DeviceLock обеспечивается за счет детального протоколирования действий пользователей и административного персонала, а также селективного теневого копирования передаваемых данных для их последующего анализа, в том числе с использованием методов полнотекстового поиска.

Для администраторов информационной безопасности DeviceLock предлагает наиболее рациональный и удобный подход к управлению DLP-системой – с использованием объектов групповых политик домена Microsoft Active Directory и интегрированной в редактор групповых политик (GPO Editor) консоли DeviceLock. При этом политики DeviceLock автоматически распространяются средствами директории как интегральная часть ее групповых политик на все компьютеры домена. Такое решение позволяет службе информационной безопасности централизованно и оперативно управлять DLP-политиками в масштабах всей организации, а их исполнение распределенными агентами DeviceLock обеспечивает точное соответствие между бизнес-функциями пользователей и их правами на передачу и хранение информации на рабочих компьютерах. Не менее важно, что агенты DeviceLock не оказывают сколь-либо заметного влияния на их производительность, работают в самозащищенном режиме и остаются полностью прозрачными для пользователей, не нарушающих дисциплину работы с данными.



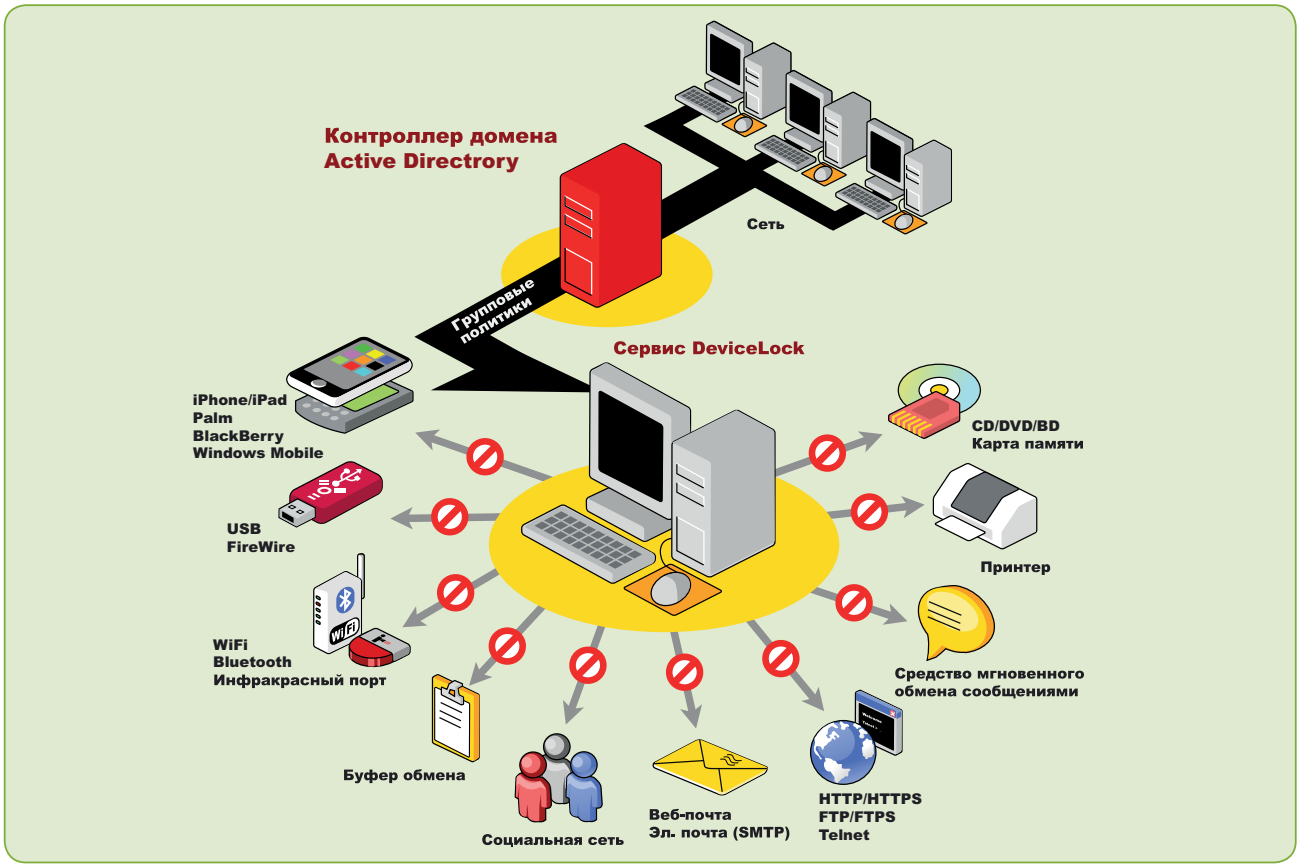
Базисный функциональный компонент комплекса – DeviceLock – позволяет контролировать доступ пользователей к различным интерфейсам (портам) компьютера и его периферийным устройствам в зависимости от их типа, класса, модели и уникального идентификатора, дня недели и времени суток, форматов файлов, а также типов операций с данными, включая чтение, запись, форматирование носителей. Компонент NetworkLock расширяет функции контекстного контроля на сетевые коммуникации пользователей, а компонент ContentLock обеспечивает контентный анализ и фильтрацию данных в каналах передачи, контролируемых DeviceLock и NetworkLock.

Модульная структура и лицензирование

Комплекс DeviceLock Endpoint DLP Suite состоит из взаимодополняющих функциональных модулей – DeviceLock, NetworkLock, ContentLock и DeviceLock Search Server, лицензируемых в любых комбинациях на основе базисного модуля DeviceLock. Выборочное лицензирование модулей позволяет оптимальным образом удовлетворить требования организаций по защите от утечек данных с компьютеров корпоративных ИС при минимизации расходов на приобретение и эксплуатацию DLP-решений.

- Базисный компонент DeviceLock поддерживает полный набор механизмов контекстного контроля доступа пользователей, а также обеспечивает событийное протоколирование и теневое копирование данных для всех локальных каналов ввода-вывода на защищаемых компьютерах, включая периферийные устройства и интерфейсы, системный буфер обмена, локально подсоединенные смартфоны и КПК, а также канал печати документов на локальные и сетевые принтеры. Кроме того, компонент DeviceLock служит в качестве инфраструктурной платформы для других компонентов комплекса и реализует все функции его централизованного управления и администрирования.
- Опциональный компонент NetworkLock™ обеспечивает контекстный контроль каналов сетевых коммуникаций компьютеров, включая распознавание сетевых протоколов независимо от используемых портов, детектирование коммуникационных приложений и их селективную блокировку, реконструкцию сообщений и сессий с восстановлением файлов, данных и параметров, а также событийное протоколирование и теневое копирование передаваемых данных.
- Опциональный компонент ContentLock™ реализует механизмы мониторинга и контентной фильтрации файлов, копируемых на съемные носители и иные Plug-n-Play устройства, а также объектов данных, перехваченных NetworkLock при их передаче по сетевым каналам связи – включая содержимое электронной почты, мгновенных сообщений, web-форм, публикаций социальных сетей, файловых обменов и telnet-сессий.
- Опциональный компонент DeviceLock Search Server (DLSS) обеспечивает полнотекстовый поиск по централизованным базам данных теневого копирования и событийного протоколирования DeviceLock. Использование DLSS позволяет значительно снизить трудозатратность и повысить эффективность процессов аудита и расследования инцидентов информационной безопасности, связанных с утечками информации, их криминалистического анализа и сбора доказательной базы.

Компоненты комплекса DeviceLock Endpoint DLP Suite лицензируются по функционально-модульному принципу. Базисный модуль контроля DeviceLock обязателен для любой инсталляции комплекса и может использоваться независимо. Опционально лицензируемые компоненты ContentLock, NetworkLock и DLSS могут приобретаться дополнительно к DeviceLock и независимо друг от друга, что обеспечивает пользователям поэтапное и экономное расширение функционала их DLP-решений в соответствии с ростом потребностей. Поскольку инсталляционный пакет DeviceLock включает все компоненты комплекса, активация опциональных лицензий не требует переустановки каких-либо его частей.



- **Полная интеграция консоли управления политиками и агентами DeviceLock Group Policy Manager в средства управления платформы Active Directory а также Microsoft Group Policy Management Console обеспечивает высокую масштабируемость DLP-решений на базе DeviceLock Endpoint DLP Suite.**

Характеристики и преимущества DeviceLock

Централизованное управление с интеграцией в групповые политики Active Directory. Полная интеграция централизованного управления DeviceLock в групповые политики Windows позволяет автоматически устанавливать DeviceLock на новые компьютеры, подключаемые к корпоративной сети, а также оперативно управлять политиками контроля доступа, контентной фильтрации, аудита и теневого копирования агентов DeviceLock на защищаемых компьютерах. Наиболее популярная среди пользователей консоль управления DeviceLock Group Policy Manager представляет собой оснастку для Microsoft Management Console (MMC), встраиваемую в стандартную оснастку Group Policy, которая входит в состав Windows 2000 и более поздних операционных систем. Благодаря привычному и интуитивно понятному для сетевых администраторов интерфейсу управление DeviceLock является простым и не требует написания дополнительных скриптов, изменения схемы домена или шаблонов ADO. Для организаций, не использующих Active Directory, в комплексе DeviceLock предусмотрена дополнительная консоль с MMC-подобным графическим интерфейсом – DeviceLock Enterprise Manager, которая позволяет централизованно управлять агентами DeviceLock на любых компьютерах, выбирая их напрямую из служб каталогов LDAP (таких как Novell eDirectory, Open LDAP и т.п.). Агенты могут быть установлены на удаленные компьютеры с уже заданными политиками безопасности и конфигурационными настройками путем развертывания специально созданного установочного пакета Microsoft Installer (MSI). Такой MSI-пакет создается администратором при помощи консоли управления DeviceLock. XML-шаблоны DLP-политик могут создаваться, экспортироваться и использоваться на всех типах консолей управления DeviceLock.

Поддержка RSoP. Стандартная оснастка Resultant Set of Policy (RSoP) позволяет администраторам DeviceLock просматривать исполняемые агентами DLP-политики а также проверять консистентность их набора, подготавливаемого для доставки на агенты DeviceLock.

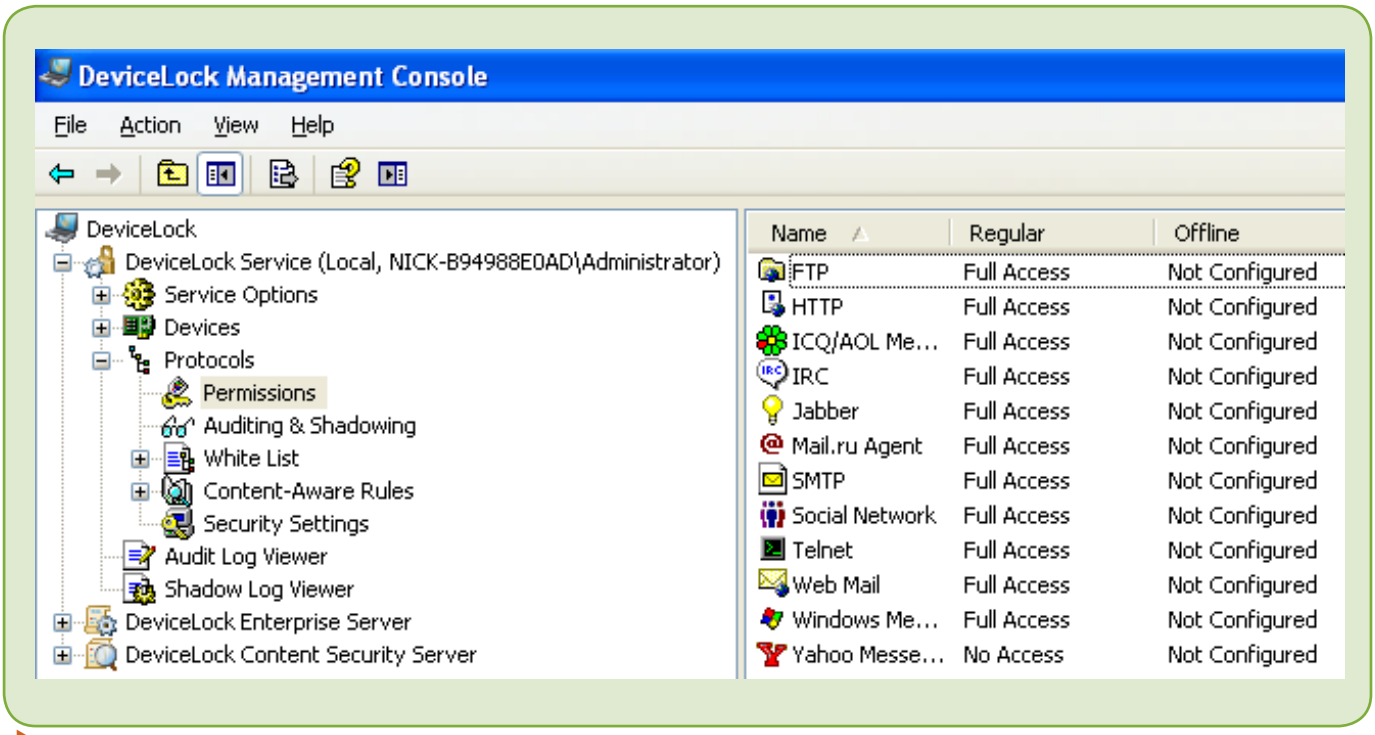
Белый список USB-устройств. Для каждого пользователя или группы можно задать свой "белый" список устройств, доступ к которым будет всегда разрешен. Устройства можно идентифицировать по модели и по уникальному серийному номеру.

Белый список носителей. DeviceLock позволяет идентифицировать определенный CD/DVD-диск на основе записанных на него данных и разрешить его использование, даже если сам CD/DVD-привод заблокирован. Для каждого пользователя или группы можно задать свой "белый" список носителей.

Временный белый список. Позволяет предоставлять временный доступ к устройствам при отсутствии сетевого подключения к агенту. Администратор сообщает пользователю специальный короткий буквенно-цифровой код (например, по телефону), который временно разблокирует доступ только к требуемому устройству.

Белый список сетевых протоколов. Модуль NetworkLock позволяет задавать политики безопасности, основанные на принципе "белого" списка сетевых протоколов, который дополнительно может детализироваться по IP-адресам, их диапазонам и маскам подсетей, сетевым портам и их диапазонам, а также критериям «больше чем/меньше чем» для этих параметров.

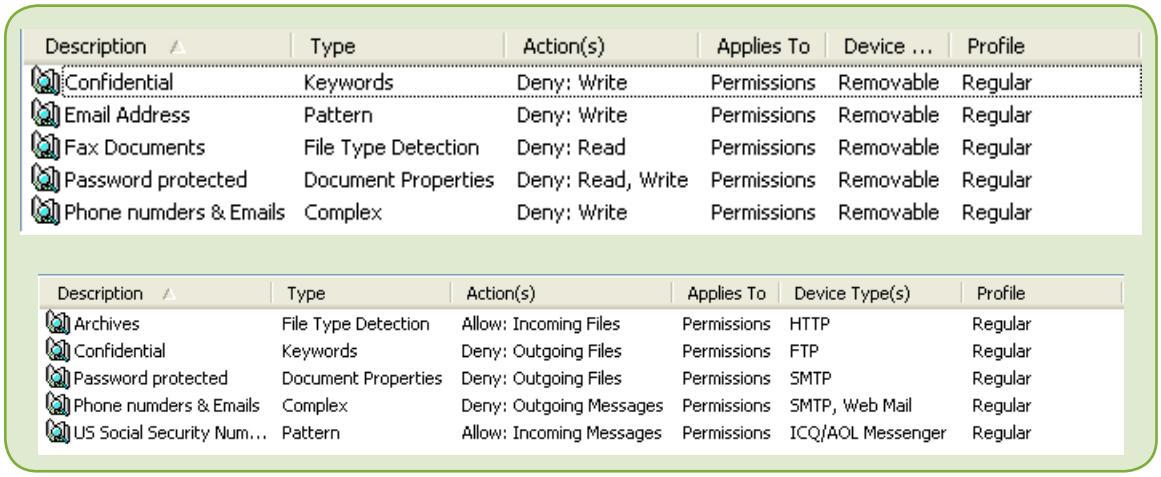
Контроль сетевых коммуникаций. Использующий методы глубокого пакетного анализа модуль NetworkLock обеспечивает детектирование и селективную блокировку сетевых протоколов и коммуникационных приложений независимо от используемых ими портов, реконструкцию сессий и сообщений с восстановлением передаваемых файлов и иных данных для их оперативного анализа, теневое копирование а также событийное протоколирование действий пользователей. NetworkLock позволяет контролировать коммуникации пользователей через популярные сетевые приложения, включая передачу почтовых сообщений по открытым и SSL-защищенным SMTP-сессиям (с раздельным контролем



С помощью NetworkLock организации могут гибко контролировать и аудировать доступ пользователей их корпоративных ИС к популярным сетевым приложениям, включая web-доступ в Интернет, SMTP- и web-почту, социальные сети, блоги, службы мгновенных сообщений (мессенджеры), передачу файлов, telnet-сессии и т.д.

сообщений и вложений), web-доступ и другие HTTP/HTTPS-приложения, web-почту Gmail, Yahoo! Mail, Windows Live Mail, мессенджеры ICQ, MSN Messenger, Jabber, IRC, Yahoo! Messenger, Mail.ru Agent, социальные сети Twitter, Facebook, LiveJournal, LinkedIn, MySpace, Одноклассники, ВКонтакте, передачу файлов по протоколам FTP и FTP-SSL, а также Telnet-сессии.

Контентная фильтрация. Технологии парсинга и контентного анализа ContentLock позволяют выделять и фильтровать текстовое содержимое более чем 80 файловых форматов и иных типов данных, копируемых на съемные носители а также передаваемых по сетевым каналам связи, контролируемым модулем NetworkLock, включая сообщения электронной почты, мгновенные сообщения, веб-формы, обмены социальных сетей и т.д. Политика фильтрации базируется на сочетании поиска по ключевым словам и шаблонам регулярных выражений (RegExp) с численными порогами срабатывания. При создании правил фильтрации шаблоны можно объединять в сколь угодно сложные комбинации с использованием логических функций «И» и «ИЛИ», таким образом задавая комплексные образцы для поиска и фильтрации контента. Набор более чем 50 параметров, используемых для задания шаблонов, включает идентификаторы пользователей и их групп, идентификаторы компьютеров и типы их интерфейсов, устройства, типы каналов и направление передачи данных, диапазоны дат и времени и многие другие. В продукт встроены наборы готовых



Description	Type	Action(s)	Applies To	Device ...	Profile
Confidential	Keywords	Deny: Write	Permissions	Removable	Regular
Email Address	Pattern	Deny: Write	Permissions	Removable	Regular
Fax Documents	File Type Detection	Deny: Read	Permissions	Removable	Regular
Password protected	Document Properties	Deny: Read, Write	Permissions	Removable	Regular
Phone numders & Emails	Complex	Deny: Write	Permissions	Removable	Regular

Description	Type	Action(s)	Applies To	Device Type(s)	Profile
Archives	File Type Detection	Allow: Incoming Files	Permissions	HTTP	Regular
Confidential	Keywords	Deny: Outgoing Files	Permissions	FTP	Regular
Password protected	Document Properties	Deny: Outgoing Files	Permissions	SMTP	Regular
Phone numders & Emails	Complex	Deny: Outgoing Messages	Permissions	SMTP, Web Mail	Regular
US Social Security Num...	Pattern	Allow: Incoming Messages	Permissions	ICQ/AOL Messenger	Regular

Конфигурационные экраны с правилами контентной фильтрации для типа устройства (верний экран) и коммуникационных протоколов (нижнее окно). Использование словарей ключевых слов и шаблонов упрощает конфигурирование сложных политик.

шаблонов для наиболее распространенных видов защищаемой информации, включая номера кредитных карт, банковских счетов, водительских удостоверений, идентификаторы социального страхования, телефонные номера, адреса и т.д. Помимо этого в качестве параметров правил фильтрации можно использовать встроенные отраслевые терминологические словари а также словари, которые пользователи могут создавать самостоятельно с учетом специфики их организации.

Контроль по типу файлов. DeviceLock позволяет контролировать доступ пользователей к операциям с файлами в зависимости от их типов (форматов). Основанный на сигнатурной обработке бинарного содержимого файлов метод детектирования позволяет безошибочно идентифицировать более 4000 файловых форматов и нечувствителен к фальсификации их расширений. Контроль по типу файлов осуществляется дополнительно к правам пользователей, заданным на уровне типа устройства или сетевого протокола.

Контроль буфера обмена. DeviceLock позволяет превентивно предотвращать потенциальные утечки данных еще до того, как они передаются с компьютеров – когда пользователи намеренно или случайно копируют данные между различными приложениями и документами через встроенный в ОС Windows буфер обмена. Политики контроля DeviceLock могут быть настроены для выборочной блокировки и аудита операций передачи данных через системный буфер между различными приложениями (например, из Microsoft Word в Excel или в OpenOffice). Контекстный контроль доступа пользователей к операциям буфера обмена обеспечивается на уровне объектов и типов данных – включая файлы, текстовые данные, графические изображения, аудиофрагменты (например, записи, сделанные Windows Sound Recorder). Кроме того, DeviceLock поддерживает селективное блокирование «снимков экрана», выполняемых как стандартной функцией Windows PrintScreen, так и аналогичными функциями различных приложений.

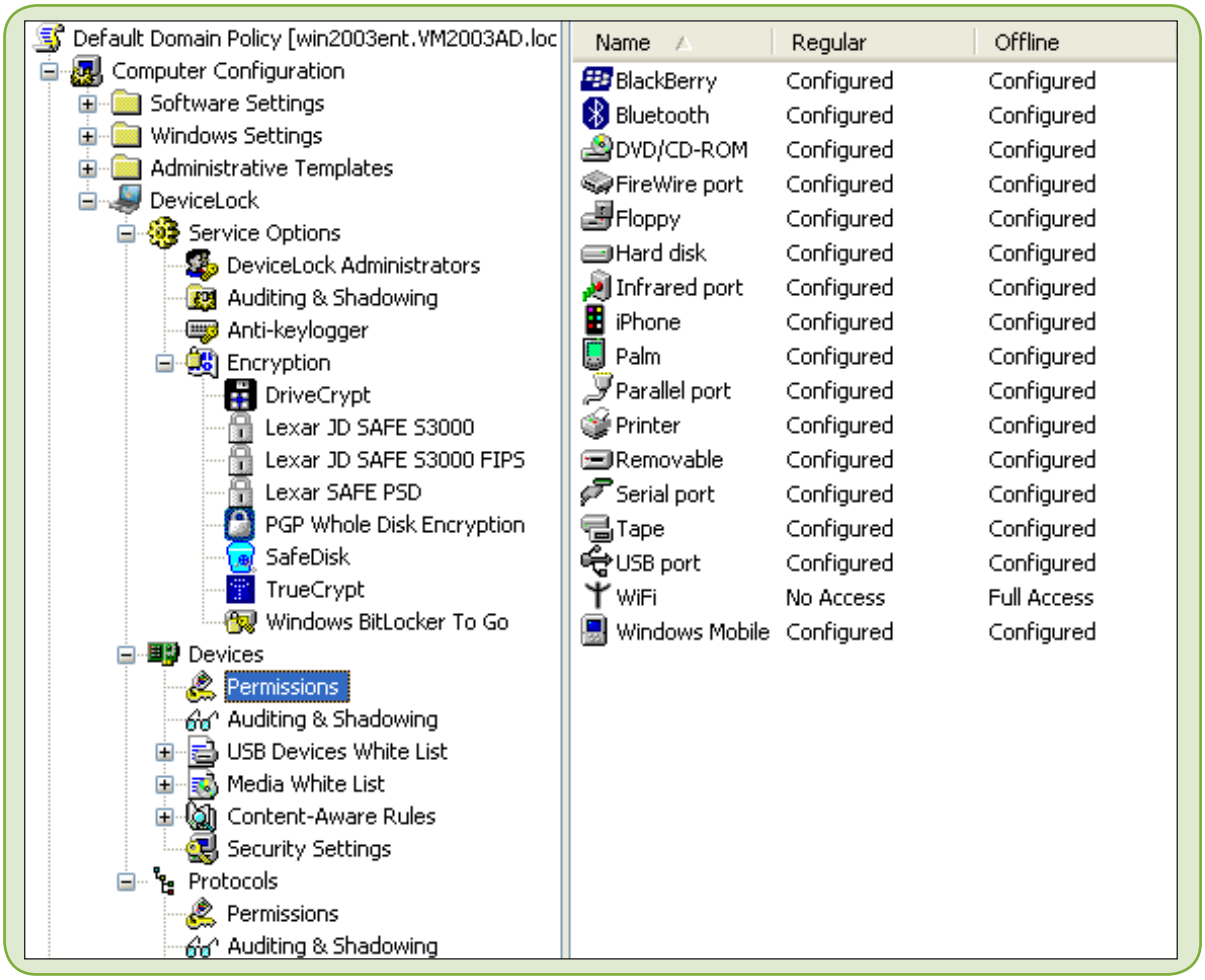
Контроль синхронизации с мобильными устройствами. Уникальная патентованная технология собственной разработки позволяет DeviceLock оперативно контролировать процесс обмена данными между компьютером и мобильными устройствами на платформах Windows Mobile, Palm, iPhone, iPod touch, и iPad, локально подключенными по интерфейсам USB, COM, IrDA, Bluetooth, и Wi-Fi. DeviceLock перехватывает, анализирует и фильтрует синхронизируемые данные с точностью до их типа, включая файлы, почтовые сообщения, контанкты, заметки, эккаунты и т.д., дополнительно обеспечивая событийное протоколирование операций обмена а также теневое копирование данных согласно централизованно задаваемым политикам. Контроль локальной синхронизации обеспечивает значительное повышение уровня защиты от утечек данных с корпоративных компьютеров в повседневных ситуациях, когда сотрудники подключают к ним свои личные смартфоны или КПК и по халатности, из-за ошибок или намеренно копируют на них служебную и деловую информацию.

Контроль печати документов. Используя технологию перехвата операций системного спулера печати, DeviceLock обеспечивает организациям возможность централизованно контролировать доступ сотрудников с их рабочих компьютеров к любым типам принтеров, включая сетевые, подключенные локально, а также виртуальные принтеры печати в файл. В случае подключения принтеров к USB порту доступ к ним может контролироваться с точностью вплоть до модели а также уникального идентификатора отдельного принтера. DeviceLock протоколирует связанные с процессами печати события и автоматически передает

их в центральную базу данных, где они сохраняются для целей аудита. Правила протоколирования задаются с тем же уровнем гранулированности, что и политика доступа к принтерам. Столь же гибко конфигурируется политика теневого копирования посланных на печать документов, копии которых сохраняются и передаются в центральную базу данных сервера DeviceLock Enterprise Server для их анализа.

Интеграция с внешними средствами шифрования. DeviceLock позволяет задавать специальные политики доступа к съемным дискам, зашифрованным при помощи внешних программных средств шифрования. Используя такие политики, можно, например, разрешить запись только зашифрованных данных на съемные устройства и запретить запись незашифрованных данных. DeviceLock обнаруживает и контролирует доступ пользователей к зашифрованным дискам, созданным продуктами BitLocker To Go (встроенное в ОС Windows средство шифрования данных на съемных носителях), ViPNet SafeDisk (продукт российской компании Инфотекс, сертифицирован ФСБ России как СКЗИ), PGP Whole Disk Encryption, SecurStar DriveCrypt и TrueCrypt (USB-флеш и другие съемные устройства), а также к флеш-дискам Lexar JumpDrive SAFE S3000 и Lexar SAFE PSD, поддерживающим аппаратное шифрование данных.

Политики автономного и оперативного режима. Для более гибкой защиты компьютера от утечек данных агенты DeviceLock могут применять разные политики в зависимости от того, подключен ли компьютер к корпоративной сети или работает автономно. В оперативном режиме компьютер работает, если он либо подключен к сети, либо с него доступен контроллер домена или DeviceLock Enterprise Server. В противном



С помощью MMC-оснастки DeviceLock Group Policy Manager администраторы DeviceLock могут централизованно управлять политиками защиты от утечек данных через все типы потенциально опасных каналов коммуникаций, интерфейсов и устройств на компьютерах в масштабе всего леса доменов Active Directory организации.

случае компьютер работает автономно. Детектирование режима работы и переключение между заданными для них политиками DeviceLock осуществляется агентом автоматически. Применение различных политик связано с разницей профилей угроз для разных режимов работы компьютера – например, для запрета использования адаптеров Wi-Fi, когда компьютер подключен к офисной сети компании, и снятия этого ограничения, когда командированный сотрудник включает компьютер в гостинице.

Обнаружение и блокирование аппаратных кейлоггеров. DeviceLock обнаруживает USB-кейлоггеры и блокирует подсоединенные к ним клавиатуры. Кроме того, добавляя к вводимым с клавиатуры данным «цифровой белый шум», DeviceLock делает бесполезным использование PS/2 кейлоггеров, поскольку выделение подлинных «клавиатурных» сигналов из записанного в память кейлоггера «шума» практически невозможно.

Защита от локального администратора. Функция DeviceLock Administrators обеспечивает защиту от удаления агента DeviceLock, изменения конфигурации или нарушения его работоспособности со стороны пользователей даже в тех случаях, когда они имеют полные административные привилегии на локальных компьютерах. При активированной функции DeviceLock Administrators никто, кроме авторизованных администраторов DeviceLock, не может подключиться к агенту, остановить или удалить его.

Режим наблюдения

Внедрение решений на базе продуктов DeviceLock часто начинается с режима наблюдения, когда права пользователей по передаче и хранению данных никак не ограничиваются, однако, служба информационной безопасности организации использует установленные на рабочих компьютерах агенты DeviceLock для всеобъемлющего протоколирования, сбора и анализа информации о характере поведения и уровне соответствия пользователей требованиям административно установленной политики безопасности корпоративных данных. Результаты наблюдения используются при создании профилей потоков данных для различных категорий работников и – на их основе – разработки базовых ограничительных DLP-политик, которые активируются на этапе полнофункционального внедрения DeviceLock. Кроме того, нередко уже на этапе наблюдения DeviceLock позволяет выявить и устранить серьезные нарушения или преступную деятельность со стороны инсайдеров.

Протоколирование и поддержка централизованного аудита. DeviceLock позволяет протоколировать все действия пользователей с устройствами и файлами (копирование, чтение, удаление и т.п.) а также изменения в настройках агента Devicelock, время его старта и остановки. DeviceLock использует стандартную подсистему событийного протоколирования Windows, а также автоматически собирает данные аудита с удаленных компьютеров в локальной сети и хранит их в центральной базе данных SQL сервера DeviceLock Enterprise Server (DLES). Доступ к базе данных DLES имеют только авторизованные администраторы DeviceLock, что обеспечивает ее защиту от удаления и искажения со стороны пользователей, даже если они обладают локальными административными правами. Для равномерного распределения нагрузки в локальной сети можно установить несколько экземпляров DLES, которые, в свою очередь, используют любое количество SQL-серверов для хранения данных.

Теневое копирование. Функция теневого копирования DeviceLock позволяет сохранять точную копию данных, копируемых пользователями на внешние устройства, печатаемых на локальные и сетевые принтеры, передаваемых по сети а также через последовательные или параллельные порты. Теневые копии файлов и данных, включая файлы, извлеченные из ISO-образов CD/DVD/BD дисков, сохраняются в SQL-базе данных сервера DLES. Характеристики событийного протоколирования и теневого копирования в DeviceLock гибко настраиваются для эффективного использования сетевых ресурсов и ресурсов БД SQL-сервера с помощью таких механизмов, как потоковое сжатие данных аудита и теневого копирования, контроль пропускной способности сети, автоматический выбор оптимального сервера DLES и локальной квоты кэша данных аудита и теневого копирования. Реализованная в ContentLock технология контентной фильтрации данных теневого копирования позволяет сохранять в центральной базе копии только тех документов и объектов, которые значимы для задач аудита информационной безопасности, расследований нештатных ситуаций и криминалистического анализа. В результате на порядки снижаются требования к емкости хранилищ теневых копий и пропускной способности каналов связи при их передаче в центральную базу DLES. Контентный анализ данных теневого копирования поддержан для всех основных каналов передачи данных, включая съемные носители и plug-n-play устройства памяти, сетевые коммуникации, синхронизацию данных с локально подключенными смартфонами, а также канал печати документов.

Централизованный мониторинг. С помощью DeviceLock Enterprise Server (DLES) администраторы DeviceLock могут оперативно контролировать текущее состояние агентов на удаленных компьютерах посредством их периодического опроса и сохранения в журнале мониторинга информации о текущем состоянии, версии и настройках агентов. Кроме того, для указанных администратором компьютеров DLES может сравнивать текущие DLP-политики агентов с эталонными политиками, регистрировать информацию о выявленных отклонениях в журнал мониторинга, а также автоматически заменять текущие политики на эталонные.

Отчеты. DeviceLock поддерживает формирование графические отчетов на основе данных журналов аудита и теневого копирования, хранимых на сервере DeviceLock Enterprise Server. Отчеты могут автоматически отсылаться на заданный адрес электронной почты. Кроме того, DeviceLock позволяет формировать отчеты по установленным настройкам, применяемым на агентах DeviceLock, а также по Plug-n-Play устройствам (USB, FireWire и PCMCIA), которые используются на защищаемых DeviceLock компьютерах.

Сервер полнотекстового поиска. Опционально лицензируемый компонент DeviceLock Search Server (DLSS) позволяет осуществлять полнотекстовый поиск по содержимому файлов теневого копирования и журналам аудита, хранящимся в центральной базе данных сервера DeviceLock Enterprise Server. Использование DLSS значительно снижает трудоемкость и повышает эффективность процессов аудита и расследования инцидентов информационной безопасности, включая задачи криминалистического анализа и сбора доказательной базы. К основным характеристикам DLSS относятся поддержка более 80 наиболее распространенных форматов, морфологический поиск и фильтрация «стоп-слов» в текстах на семи языках, включая русский, комбинирование слов и фраз и использование регулярных выражений в строке поиска, поддержка шаблонов и специальных символов, поиск по полям документов и численным диапазонам, сортировка представления результатов поиска по релевантности, весовым коэффициентам терминов и полей документов. Кроме того, DLSS поддерживает создание индексов по содержимому полей событийных записей DeviceLock, что позволяет эффективно дополнять поиск по документам в теневой базе – например, поисковые запросы могут уточняться значениями таких параметров лог-записей, как имена пользователей, идентификаторы компьютеров, диапазон дат событий, типы операций, размеры и имена файлов, идентификаторы периферийных устройств и т.д. Поддержка в DLSS индексирования и полнотекстного поиска по текстовому содержимому заданий печати в форматах PCL и PostScript позволила полностью автоматизировать анализ текстовых данных в теневых копиях PCL и PostScript документов и сократить его время до диапазона секунд вне зависимости от размера базы поиска. Особенно важное для российских организаций преимущество текстового парсинга PostScript документов в DLSS состоит в корректном распознавании образов кириллических знаков, что делает индексацию и поиск уникально точными.

Техническая спецификация

Инфраструктурные (инсталлируемые) компоненты
- Агент DeviceLock
- DeviceLock Enterprise Server (DLES)
- Consoles: DeviceLock Group Policy Manager (DLGPM)
  DeviceLock Management Console (DLM)
  DeviceLock Enterprise Manager (DLEM)

Лицензируемые модули
- DeviceLock (базисный)
- NetworkLock
- ContentLock
- DeviceLock Search Server (DLSS)

Контролируемые интерфейсы
- USB, FireWire, инфракрасный, последовательный и параллельный порты

Контролируемые типы устройств
- Floppy-приводы, приводы CD-ROM/DVD/BD, любые съемные носители данных (флэш, карты памяти и др.), жесткие диски, ленточные накопители, адаптеры Wi-Fi, адаптеры Bluetooth, устройства Apple iPhone/iPod touch/iPad, BlackBerry, мобильные устройства под управлением Windows Mobile и Palm OS, принтеры (локальные, сетевые и виртуальные), модемы, цифровые камеры, сканнеры

Контроль буфера обмена
- Контроль операций обмена данными между приложениями
- Раздельный контроль типов данных: файлы, текстовые данные, графические данные, аудио данные, данные неидентифицированного типа
- Контроль снимков экрана (для приложений и функции PrintScreen)

Контролируемые типы данных
- Более 4000 типов файлов
- Объекты протоколов синхронизации с мобильными устройствами: Microsoft ActiveSync, Palm HotSync, iTunes
- Контроль текста в графических изображениях (встроенных в документы Microsoft Office и Adobe PDF или отдельных графических файлах)

Контролируемые сетевые коммуникации
- Web-почта: Gmail, Yahoo!Mail, Windows Live Mail
- Социальные сети: Facebook,Twitter, LiveJournal, LinkedIn, MySpace, Odnoklassniki, Vkontakte
- Службы мгновенных сообщений: ICQ/AOL, MSN Messenger, Jabber, IRC, Yahoo! Messenger, Mail.ru Agent
- Сетевые протоколы: HTTP/HTTP over SSL, SMTP/SMTP over SSL, FTP/FTP over SSL, Telnet

Технологии контентной фильтрации
- Поиск по ключевым словам
- Поиск по шаблонам на базе регулярных выражений с числовыми и булевыми порогами срабатывания
- Поиск по встроенным комплексным шаблонам регулярных выражений (номера кредитных карт, адреса, паспортные данные и т.д.)
- Встроенные отраслевые терминологические словари

Каналы контентной фильтрации
- Съемные носители данных и Plug-n-Play устройства памяти
- Сетевые коммуникации

Форматы файлов – контентная фильтрация
- Более 80 форматов файлов, включая Microsoft Office, Adobe PDF, OpenOffice, Lotus 1-2-3, WordPerfect, WordStar, Quattro Pro, архивы и репозитории электронной почты, CSV, DBF, XML, Unicode, GZIP, RAR, ZIP, др.

Контентная фильтрация при теневом копировании
- Все форматы файлов контентной фильтрации
- Каналы: съемные носители данных и Plug-n-Play устройства памяти, сетевые коммуникации, локальная синхронизация с мобильными устройствами, операции буфера обмена, канал печати документов

Полнотекстовый поиск
- Все форматы файлов контентной фильтрации
- Задания на печать в форматах PCL и Postscript
- Индексирование и поиск: комбинация слов, фраз, регулярных выражений, специальных символов, численных диапазонов, полей документов, записей журналов аудита
- Морфологический поиск и фильтрация «стоп-слов»: русский, английский, французский, немецкий, итальянский, японский, испанский
- Сортировка результатов поиска: комбинация слов и фраз по логике «И», релевантность, весовые коэффициенты терминов и полей документов

Интеграция с криптографическими продуктами
- Windows 7 BitLocker To Go
- PGP Whole Disk Encryption
- TrueCrypt
- SecurStar DriveCrypt (DCPPE)
- SafeDisk (Инфотекс)
- Lexar Media SAFE S1100 & S3000 Series

Взаимозависимости функциональных компонентов
- ContentLock, NetworkLock и DLSS требуют использования базисного модуля DeviceLock
- ContentLock требует использования NetworkLock для фильтрации контента сетевых коммуникаций

System Requirements
- Системные требования: Windows NT 4.0/2000/XP/Vista/7 или Server 2003/2008 (32-bit/64-bit versions); CPU Pentium 4, 64MB RAM, HDD 25MB
- Консоли управления DeviceLock: Windows NT 4.0/2000/XP/Vista/7 или Server 2003/2008 (32-bit/64-bit); CPU Pentium 4, 2GB RAM, HDD 800GB
- Сервер DeviceLock Enterprise Server: Windows Server 2003 R2; 2xCPU Intel Xeon Quad-Core 2.33GHz, RAM 8GB, HDD 800GB; MSEE/MSDE или MS SQL Server

ЗАО «Смарт Лайн Инк»

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

Тел. (495) 967-99-60

[www.devicelock.com/ru]