DeviceLock®

ПРЕДОТВРАЩЕНИЕ УТЕЧЕК ИНФОРМАЦИИ

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, смартфоны и планшеты, другие носители данных, а также печати на принтерах. Информация может бесконтрольно передаваться инсайдерами через электронную почту, службы мгновенного обмена сообщениями, веб-формы, форумы и социальные сети. Беспроводные интерфейсы – Wi-Fi, Bluetooth и LTE – наравне с каналами локальной синхронизации данных с мобильными устройствами открывают дополнительные пути для утечек информации с пользовательских компьютеров организации. В то время как ни одна из этих уязвимостей не устраняется ни традиционными механизмами сетевой безопасности, ни встроенными средствами контроля ОС, программный комплекс DeviceLock® DLP эффективно предотвращает утечки данных с корпоративных компьютеров, используя полный набор механизмов контекстного контроля операций с данными, а также технологии их контентной фильтрации. Поддержка виртуальных и терминальных сред в DeviceLock® DLP существенно расширяет возможности служб информационной безопасности в решении задачи предотвращения утечек данных при использовании различных решений виртуализации рабочих сред, созданных как в форме локальных виртуальных машин, так и терминальных сессий рабочих столов или опубликованных приложений на гипервизорах. Наконец, предлагаемые DeviceLock® DLP возможности обнаружения конфиденциальной информации позволяют предотвратить утечки данных, хранимых на рабочих станциях и корпоративных сетевых хранилищах.

ПРОГРАММНЫЙ КОМПЛЕКС ЗАЩИТЫ ОТ УТЕЧЕК ДАННЫХ С КОРПОРАТИВНЫХ КОМПЬЮТЕРОВ

Контекстный контроль и контентная фильтрация

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

Однако, во многих случаях требуется более глубокий уровень контроля, нежели только ограничения на уровне контекста. Например, передача файлов и документов, содержащих персональные данные или конфиденциальную информацию, допускается только для доверенных лиц, при этом коммуникационные каналы в целом не должны блокироваться, чтобы не нарушать производственные процессы. В таком сценарии дополнительно к контекстному контролю необходимо применение технологий контентного анализа и фильтрации, позволяющих выявить и предотвратить несанкционированную передачу данных ограниченного доступа, а следовательно, их утечку, не препятствуя при этом информационному обмену в рамках служебных обязанностей сотрудников.

Программный комплекс DeviceLock DLP использует как контекстные, так и основанные на анализе содержимого методы контроля данных, обеспечивая надежную защиту от утечек информации с корпоративных компьютеров при минимальных затратах на приобретение и обслуживание комплекса. Многоуровневая инспекция потоков данных, реализованная в DeviceLock DLP, обеспечивает избирательный контроль использования широкого спектра периферийных устройств и сетевых коммуникаций. Применение методов контентного анализа и фильтрации данных позволяет контролировать и предотвращать несанкционированную печать конфиденциальной информации на принтерах, сохранение на внешних накопителях и Plug-and-Play устройствах, передачу по электронной почте, через Skype и другие коммуникационные сетевые каналы.

Технологии контентного анализа также являются фундаментом для превентивной борьбы с утечками - они используются в компоненте DeviceLock Discovery, выполняющем автоматическое обнаружение данных, хранимых на сетевых хранилищах и корпоративных компьютерах.

С помощью DeviceLock DLP службы ИБ могут реализовать классический сценарий минимальных привилегий, когда доступ к устройствам и каналам сетевых коммуникаций ограничен бизнес-задачами сотрудников. В таком сценарии беспрепятственная передача и хранение возможны только для связанных с бизнес-функцией данных, а попытки несанкционированной намеренной или случайной передачи, печати или сохранения данных на внешние устройства будут детектированы и при необходимости заблокированы.

DeviceLock DLP независимо от установленных прав доступа обеспечивает детальное протоколирование действий пользователей и администраторов, а также селективное теневое копирование передаваемых данных для их последующего анализа, в том числе с использованием методов полнотекстового поиска.

Расширяя возможности предотвращения утечек данных, DeviceLock Discovery позволяет автоматически сканировать рабочие станции, серверы и сетевые хранилища, инспектируя содержимое файлов на них в целях выявления и устранения нарушений корпоративной политики безопасного хранения данных.

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.

Предоставляемая DeviceLock DLP возможность обеспечить избирательный контроль различных каналов утечки корпоративных данных в сочетании с контролем хранимых на рабочих станциях конфиденциальных документов открывает организациям безопасный путь для разрешения своим сотрудникам контролируемо использовать сетевые сервисы и различные устройства в целях повышения эффективности работы без угрозы утечки данных, причем вне зависимости от места работы сотрудников – в офисе, в пути или дома, с корпоративного компьютера, ноутбука или планшета.

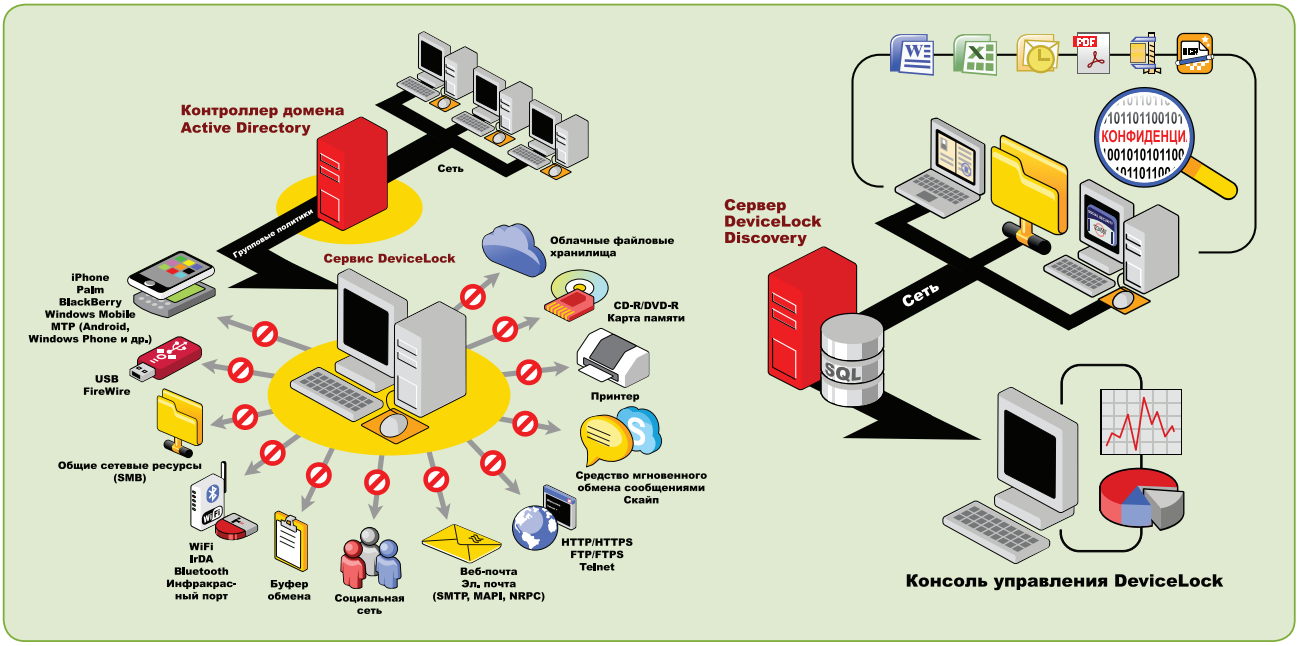
Базисный компонент DeviceLock контролирует доступ к интерфейсам (портам) компьютера и его периферийным устройствам. Компонент NetworkLock расширяет функции контекстного контроля на сетевые коммуникации, а компонент ContentLock обеспечивает контентный анализ и фильтрацию данных в каналах передачи. Search Server обеспечивает полнотекстовый поиск по базам данных теневого копирования и событийного протоколирования. DeviceLock Discovery обнаруживает документы с критическим содержимым и осуществляет различные действия с обнаруженными документами.

Модульная структура и лицензирование

Программный комплекс DeviceLock DLP состоит из взаимодополняющих функциональных модулей – DeviceLock, NetworkLock, ContentLock, DeviceLock Discovery и DeviceLock Search Server (DLSS), лицензируемых опционально в любых комбинациях для решения задач служб информационной безопасности.

- Базисный компонент **DeviceLock** предоставляет 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, MTP-устройства (такие как телефоны на базе Android, Windows Phone и т.п.), канал печати документов на локальные и сетевые принтеры, а также перенаправленные в терминальные и виртуальные среды устройства, буфер обмена и принтеры. Кроме того, компонент DeviceLock служит в качестве инфраструктурной платформы для других компонентов комплекса и реализует все функции его централизованного управления и администрирования.
- 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.
- Компонент **ContentLock** реализует механизмы мониторинга и контентной фильтрации файлов, копируемых на съемные носители и иные Plug-and-Play устройства, а также объектов данных, перехваченных NetworkLock при их передаче по сетевым каналам связи – включая содержимое электронной почты, мгновенных сообщений, веб-форм, публикаций социальных сетей, файловых обменов и т.д.
- Компонент **DeviceLock Discovery** выполняет автоматическое сканирование рабочих станций и корпоративных сетевых ресурсов, и на основании заданных политик обнаруживает документы и файлы с критическим содержимым, осуществляет различные опциональные действия с обнаруженными файлами, а также может инициировать процедуры управления инцидентами, направляя тревожные оповещения в режиме реального времени. Компонент DeviceLock Discovery лицензируется самостоятельно, независимо от прочих компонентов.
- 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 DLP лицензируются по функционально-модульному принципу. Лицензионная политика предусматривает как приобретение лицензий на комплекс в целом, так и выборочное лицензирование по отдельным модулям. Базисный модуль 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 функционального арсенала DLP-решения в соответствии с ростом потребностей. Поскольку инсталляционный пакет DeviceLock DLP включает все компоненты комплекса, активация опциональных лицензий не потребует переустановки каких-либо его частей, равно как и дополнительной установки компонентов.



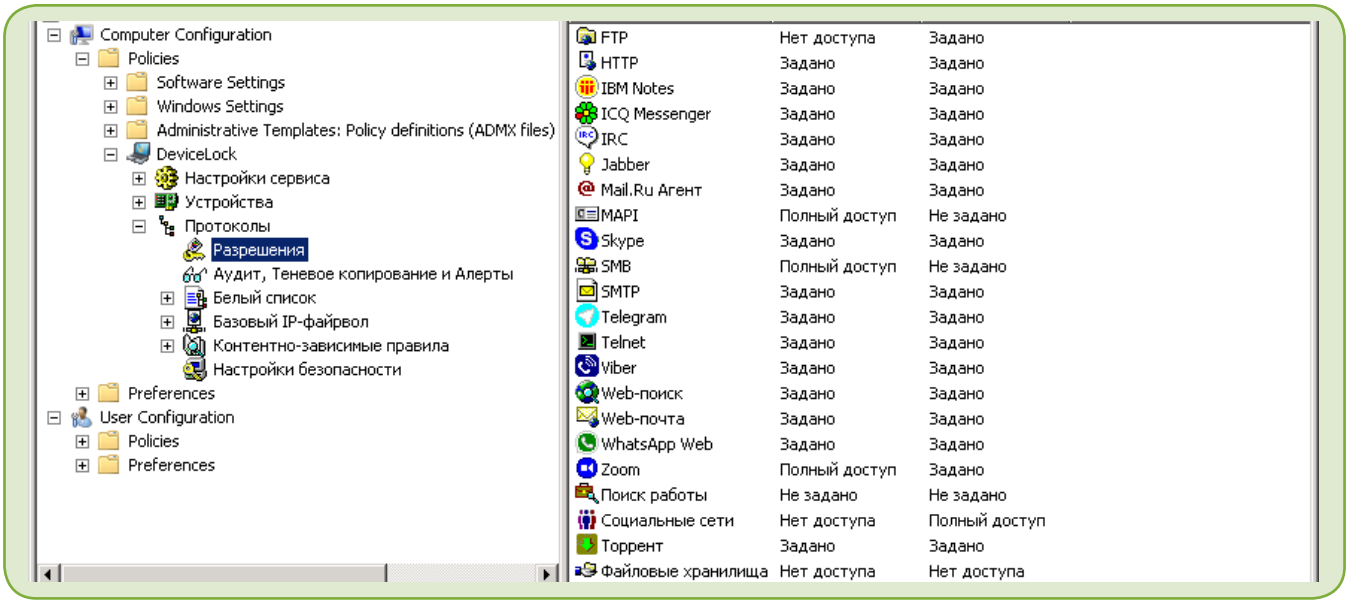
- **Полная интеграция консоли управления политиками и агентами в Microsoft Active Directory, а также Microsoft Group Policy Management Console обеспечивает высокую масштабируемость DLP-решений на базе DeviceLock DLP. DeviceLock Discovery автоматически сканирует данные, размещенные на внутренних сетевых ресурсах, системах хранения данных и рабочих станциях как внутри, так и вне корпоративной сети.**

Характеристики и преимущества DeviceLock DLP

Контроль сетевых коммуникаций. Использующий методы глубокого пакетного анализа (DPI) модуль NetworkLock обеспечивает детектирование и селективную блокировку сетевых протоколов и приложений независимо от используемых ими портов и типа подключения, реконструкцию сессий и сообщений с восстановлением передаваемых файлов и иных данных для их оперативного анализа, теневое копирование и событийное протоколирование действий пользователей. NetworkLock позволяет контролировать коммуникации пользователей через популярные сетевые приложения, включая передачу почтовых сообщений по открытым и SSL-защищенным SMTP-сессиям и протоколам MAPI/NRPC с раздельным контролем сообщений и вложений, веб-доступ и HTTP/HTTPS-приложения, веб-почту, мессенджеры, социальные сети, поисковые системы, передачу файлов в облачные сетевые хранилища и по протоколам SMB, FTP/FTP-SSL, а также Telnet-сессии, Torrent и Tor.

Контентная фильтрация. Технологии контентного анализа и фильтрации, реализованные в модуле ContentLock, позволяют в режиме реального времени анализировать и фильтровать текстовое и бинарное содержимое данных, копируемых на съемные носители, в буфер обмена, печатаемых документов, а также данных, передаваемых по сетевым каналам связи, включая сообщения и вложения в электронной почте, мессенджерах, веб-формах, социальных сетях, файлообменных сервисах, поисковых системах, SMB-ресурсах и т.д. Данные извлекаются из 150+ файловых форматов и иных типов данных, включая снимки экрана, графические файлы и внедренные в документы изображения. Контентная фильтрация структурированных данных основывается на использовании шаблонов регулярных выражений (RegExp), анализе по ключевым словам, с поддержкой встроенных отраслевых терминологических словарей и готовых наборов шаблонов регулярных выражений. Для детектирования неструктурированных текстовых и бинарных данных используется технология цифровых отпечатков, позволяющая надежно идентифицировать классифицированные файлы по их содержимому с учетом заданных уровней важности или секретности («Секретно», «Конфиденциально», «ДСП» и т.п.). При создании правил контентной фильтрации условия детектирования можно объединять в сколь угодно сложные комбинации с использованием логических функций «И» и «ИЛИ». Кроме того, правилами анализа содержимого могут проверяться также метаданные документов, а набор более чем 50 параметров, используемых для задания правил анализа контента, включает также идентификаторы пользователей и их групп, имена компьютеров и типы их интерфейсов, устройства, типы каналов и направление передачи данных, диапазоны дат и времени и многое другое. Кроме того, ContentLock распознает метки, присвоенные документам классификатором Boldon James.

Контроль хранимых данных. DeviceLock Discovery позволяет службам ИБ реализовать превентивную защиту от утечек данных посредством автоматического сканирования рабочих станций и систем хранения данных в целях обнаружения файлов и данных, хранимых с нарушениями корпоративной политики безопасного хранения данных. При обнаружении таких данных DeviceLock Discovery выполняет различные опциональные действия для устранения нарушений, а также может инициировать процедуры управления инцидентами, направляя тревожные оповещения в реальном режиме времени. Благодаря использованию возможностей контентного анализа, включая поддержку OCR, DeviceLock Discovery может обнаруживать текстовые данные в файлах более чем 100 форматов и более 40 типов архивов, в том числе вложенных, а также в графических файлах и внедренных в документы изображениях. В зависимости от топологии и особенностей локальной сети DeviceLock Discovery может выполнять сканирование в различных режимах – с применением собственного агента Discovery, удаленно с сервера Discovery или в смешанном варианте. Сканирование может быть запущено вручную или автоматически в соответствии с заданным расписанием для предопределенных групп компьютеров и сетевых хранилищ. Агенты Discovery полностью автоматически и прозрачно устанавливаются и удаляются сервером DeviceLock Discovery. При использовании совместно с другими компонентами комплекса DeviceLock DLP компонент Discovery может использовать функциональные возможности агентов DeviceLock для сканирования данных, хранимых на рабочих станциях и доступных с них сетевых ресурсах.



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

Преимущества архитектуры DeviceLock DLP. Исполнительные агенты DeviceLock DLP, устанавливаемые на каждом защищаемом компьютере, реализуют все функции контроля доступа к локальным устройствам и сетевым протоколам и сервисам, равно как и проверку содержимого передаваемых файлов и данных, в том числе с использованием резидентного модуля оптического распознавания символов (OCR), без передачи каких-либо данных на сервер для их проверки и анализа. Такая архитектура (применение полнофункциональных Endpoint-агентов) позволяет создавать сложно распределенную DLP-систему, работоспособность которой не зависит от местонахождения сотрудника в пределах корпоративного периметра или вне его, от способа передачи данных по каналам сетевых коммуникаций (через корпоративный шлюз, Wi-Fi или 4G/LTE). Таким образом полностью решается задача контроля сотрудников в любых сценариях, как внутри офиса, так и мобильных пользователей. Агенты DeviceLock не зависят от наличия подключения к серверам и получают DLP-политики вместе с объектами Group Policy (если используется интеграция DeviceLock с доменом Active Directory), либо политики DeviceLock передаются на агенты напрямую из консолей управления DLP-системой или сервером DeviceLock Enterprise Server. Такая реализация устраняет зависимость процедуры управления DLP-системой от доступности DLP-сервера.

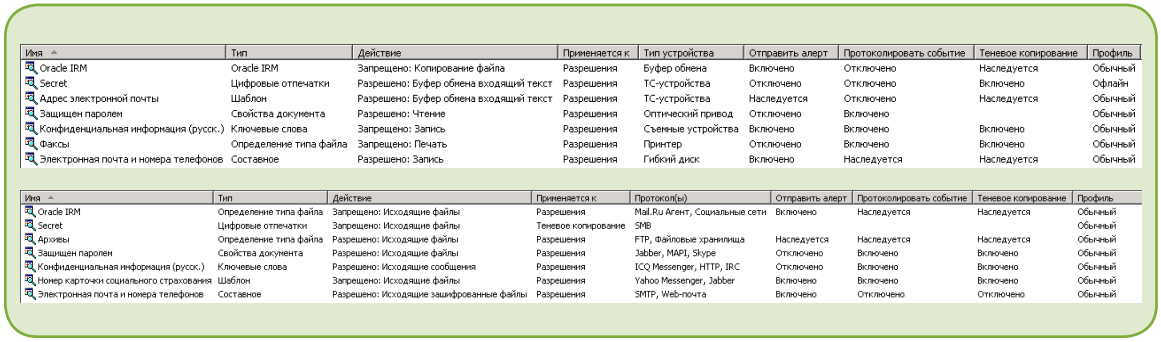
Централизованное управление через интеграцию в групповые политики Active Directory. Полная интеграция централизованного управления DeviceLock в групповые политики Windows позволяет автоматически устанавливать DeviceLock на новые компьютеры, подключаемые к корпоративной сети, а также оперативно управлять политиками контроля доступа, контентной фильтрации, аудита и теневого копирования агентов DeviceLock на защищаемых компьютерах и в виртуальных средах. Консоль управления DeviceLock прозрачно встраивается в стандартную оснастку Group Policy Editor. Благодаря привычному и интуитивно понятному для сетевых администраторов интерфейсу управление DeviceLock является простым и не требует написания дополнительных скриптов, изменения схемы домена или ADM-шаблонов.

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. Детектирование режима работы и переключение между заданными для них политиками осуществляется агентом DeviceLock автоматически. Применение двух наборов политик может быть использовано для реализации различных сценариев противодействия угрозам утечки в разных режимах доступности корпоративных данных – 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.

Тревожные оповещения. DeviceLock обеспечивает тревожные оповещения администратора в реальном режиме времени (алертинг). Оповещения могут отправляться по протоколам SMTP, SYSLOG и/или SNMP. Предусмотрено два типа оповещений: административные (изменение настроек сервиса, остановка агента DeviceLock, изменения в списке администраторов DeviceLock Administrators, неуспешные попытки пользователя внести изменения в политики и т.п.) и специфичные для устройств и протоколов. Тревожные оповещения настраиваются администратором аналогично правилам протоколирования, но при этом не заменяют его.

Резидентный модуль оптического распознавания символов (OCR). В дополнение к контентной фильтрации текстовых данных, встроенный резидентный модуль оптического распознавания символов (OCR) позволяет DeviceLock быстро, эффективно и точно извлекать и инспектировать текстовые данные из рисунков в документах и графических файлах множества форматов. Модуль OCR в DeviceLock распознает более 30 языков, что позволяет эффективно применять технологии контентного анализа к тексту, представленному в графической форме. Уникальная особенность DeviceLock в том, что OCR-модуль является встроенным во все активные компоненты DeviceLock (агент DeviceLock, сервер и агент DeviceLock Discovery) и не требует отдельной установки и настройки. Такая распределенная инфраструктура OCR значительно снижает общую нагрузку решения, поскольку графические объекты, размещенные на рабочих станциях, обрабатываются локальным модулем OCR непосредственно на рабочей станции без передачи файлов по сети, не создавая дополнительную нагрузку на серверные компоненты комплекса и существенно снижая сетевой трафик в корпоративной сети.

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. DeviceLock протоколирует связанные с процессами печати события и автоматически передает их в центральную базу данных, где они сохраняются для целей аудита. Для документов, отправленных на печать, могут быть созданы и так же сохранены в базе данных теневые копии для их последующего анализа.



Имя	Тип	Действие	Применяется к	Тип устройства	Отправить алерт	Протоколировать событие	Теневое копирование	Профиль
Oracle IRM	Oracle IRM	Запрещено: Копирование файла	Разрешения	Буфер обмена	Включено	Отключено	Наследуется	Обычный
Secret	Цифровые отпечатки	Разрешено: Буфер обмена входящий текст	Разрешения	ТС-устройства	Отключено	Отключено	Включено	Офлайн
Адрес электронной почты	Шаблон	Разрешено: Буфер обмена входящий текст	Разрешения	ТС-устройства	Наследуется	Отключено	Наследуется	Обычный
Защищен паролем	Свойства документа	Разрешено: Чтение	Разрешения	Оптический привод	Отключено	Включено		Обычный
Конфиденциальная информация (русск.)	Ключевые слова	Запрещено: Запись	Разрешения	Съемные устройства	Включено	Включено	Включено	Обычный
Факсы	Определение типа файла	Запрещено: Печать	Разрешения	Принтер	Отключено	Включено	Включено	Обычный
Электронная почта и номера телефонов	Составное	Разрешено: Запись	Разрешения	Гибкий диск	Включено	Наследуется	Наследуется	Обычный

Имя	Тип	Действие	Применяется к	Протокол(ы)	Отправить алерт	Протоколировать событие	Теневое копирование	Профиль
Oracle IRM	Определение типа файла	Запрещено: Исходящие файлы	Разрешения	Mail.Ru Агент, Социальные сети	Включено	Наследуется	Наследуется	Обычный
Secret	Цифровые отпечатки	Запрещено: Исходящие файлы	Теневое копирование	SMB				Обычный
Архивы	Определение типа файла	Разрешено: Исходящие файлы	Разрешения	FTP, Файловые хранилища	Наследуется	Наследуется	Наследуется	Обычный
Защищен паролем	Свойства документа	Разрешено: Исходящие файлы	Разрешения	Jabber, MAPI, Skype	Отключено	Включено	Включено	Обычный
Конфиденциальная информация (русск.)	Ключевые слова	Разрешено: Исходящие сообщения	Разрешения	ICQ Messenger, HTTP, IRC	Отключено	Включено	Включено	Обычный
Номер карточки социального страхования	Шаблон	Запрещено: Исходящие файлы	Разрешения	Yahoo Messenger, Jabber	Включено	Включено	Включено	Обычный
Электронная почта и номера телефонов	Составное	Разрешено: Исходящие зашифрованные файлы	Разрешения	SMTP, Web-почта	Включено	Отключено	Отключено	Обычный

Задание DLP-политик с применением методов контентной фильтрации для устройств (верхнее окно) и сетевых протоколов (нижнее окно). Использование словарей ключевых слов и шаблонов упрощает конфигурирование сложных DLP-политик.

Контроль буфера обмена. DeviceLock позволяет превентивно предотвращать потенциальные утечки еще до момента передачи данных – 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. Функция контроля буфера обмена играет значительную роль в защите терминальных и виртуальных сред в стратегии BYOD. Блокирование снимков экрана, контроль передачи объектов и данных из терминальной среды в память личного устройства пользователя, настраиваемое для выбранных пользователей и групп, предотвращает использование одного из классических методов утечки данных в терминальных и виртуальных средах.

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 5000 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.

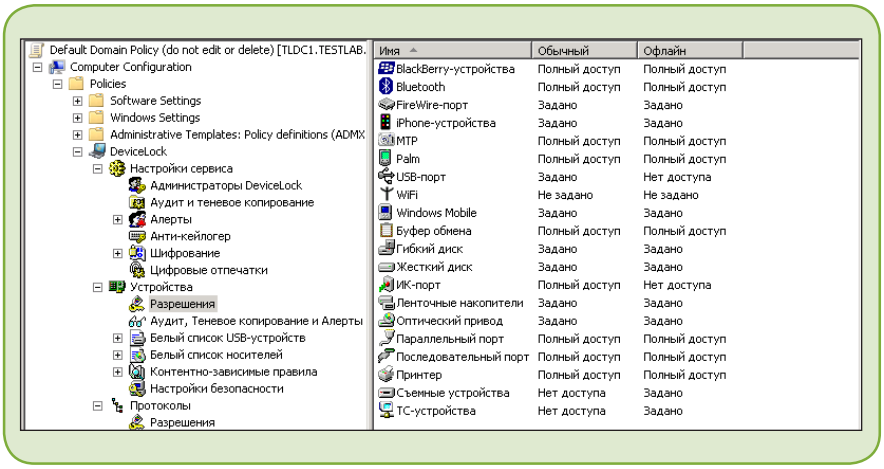
Белые списки и исключения. Для каждого пользователя или группы можно задать свой Белый список устройств, доступ к которым будет всегда разрешен. Устройства можно идентифицировать по производителю, модели и по уникальному серийному номеру. При отсутствии сетевого подключения к агенту администратор может предоставить временный доступ к устройствам, обменявшись с пользователем короткими буквенно-цифровыми кодами, уникальными для каждого устройства. Кроме того, DeviceLock позволяет идентифицировать определенный CD/DVD/BD-диск на основе записанных на него данных и разрешить его использование, даже если сам привод заблокирован. По аналогии с Белым списком USB-устройств, в модуле NetworkLock реализован Белый список сетевых протоколов, позволяющий гибко предоставлять доступ отдельным пользователям только к тем сервисам и узлам, которые необходимы им для работы. Этот Белый список задается по IP-адресам, их диапазонам и маскам подсетей, по сетевым портам, а также по идентификаторам отправителей и получателей почты и мгновенных сообщений.

Контроль синхронизации с мобильными устройствами. Уникальная патентованная технология собственной разработки позволяет анализировать и фильтровать данные, синхронизируемые между компьютером и мобильными устройствами, работающими под управлением ОС Windows Mobile, iOS и Palm OS независимо от способа их подключения. Для различных объектов (файлы, контакты, почта и т.д.), передаваемых с компьютера на КПК и наоборот, можно задать разрешения и включить аудит и теневое копирование.

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 данных только на зашифрованные съемные устройства и запретить запись на незашифрованные.

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.



С помощью оснастки DeviceLock Group Policy Manager администраторы могут централизованно управлять политиками защиты от утечек данных на компьютерах в масштабе всего леса Active Directory организации.

Режим наблюдения

Внедрение DLP-системы на базе DeviceLock DLP нередко начинается с режима наблюдения, когда права пользователей по передаче и хранению данных никак не ограничиваются, но при этом служба ИБ использует возможности всеобъемлющего протоколирования и теневого копирования в DeviceLock DLP для сбора и анализа информации о характере поведения и уровне соответствия пользователей требованиям корпоративной политики безопасности. По итогам анализа результатов наблюдения и определения потоков данных от различных категорий сотрудников создаются DLP-политики с контекстными ограничениями и контентной фильтрацией для запуска DLP-системы в полнофункциональном режиме с включенными функциями предотвращения утечки данных. Как правило, уже на этапе наблюдения DeviceLock позволяет выявить и устранить серьезные нарушения или преступную деятельность со стороны злоумышленников.

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 событийного протоколирования с удаленных компьютеров в локальной сети и хранит их в базе данных сервера DeviceLock Enterprise Server (DLES) для целей централизованного аудита. 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 каналам сетевых коммуникаций, а также через COM и LPT порты. Теневые копии файлов и данных, включая файлы, извлеченные из ISO-образов CD/DVD/BD-дисков, сохраняются в базе данных сервера DLES. Параметры 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. Технологии контентной фильтрации в DeviceLock DLP позволяют выборочно сохранять копии только тех документов и объектов, которые значимы для задач аудита информационной безопасности, расследований нештатных ситуаций и инцидентов, а также исключить из теневого копирования данные, которые недопустимо централизованно хранить и обрабатывать, например, приватные данные сотрудников. 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 при теневом копировании поддерживается для всех основных каналов передачи данных, включая съемные носители, каналы сетевых коммуникаций, канал печати документов и др.

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 DLP формирует сводные статистические и графические отчеты, в том числе динамический граф связей, 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-and-Play устройствам, используемым 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. К основным характеристикам DLSS относятся поддержка более 160 наиболее распространенных файловых 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 содержимому заданий печати в форматах PCL и PostScript позволила полностью автоматизировать анализ 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. Также предусмотрена возможность запуска поисковых запросов по расписанию с поддержкой инкрементального поиска и автоматической отправкой результатов поиска по электронной почте.

Техническая спецификация

Устанавливаемые модули и компоненты

- Исполнительные агенты и серверные компоненты: DeviceLock Agent (Windows и Apple OS X), DeviceLock Discovery Agent (Windows), DeviceLock Enterprise Server, DeviceLock Content Security Server (Discovery Server, Search Server)
- Консоли управления: DeviceLock Group Policy Manager (оснастка для Microsoft GPMC), DeviceLock Management Console (оснастка MMC), DeviceLock Enterprise Manager, DeviceLock WebConsole

Контролируемые порты

- **Windows:** USB, FireWire, инфракрасный, последовательный и параллельный
- **Mac:** USB, FireWire, последовательный
- **Терминальные сессии/BYOD:** USB, последовательный

Контролируемые типы устройств

- **Windows:** съемные носители данных (флэш, карты памяти, eSATA и др.), приводы CD-ROM/DVD/BD, дискеты, жесткие диски, ленточные накопители, адаптеры Wi-Fi и Bluetooth, устройства Apple iPhone/iPod touch/iPad, BlackBerry, Windows Mobile и Palm, MTP-устройства (телефоны на базе Android, Windows Phone и др.), принтеры (локальные, сетевые и виртуальные), модемы, цифровые камеры, сканнеры
- **Mac:** съемные носители данных, жесткие диски, приводы CD-ROM/DVD/BD, адаптеры Wi-Fi и Bluetooth
- **Терминальные сессии/BYOD:** перенаправленные диски (съемные, оптические, жесткие), USB-устройства

Контроль буфера обмена (Windows)

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

Контролируемые сетевые коммуникации

- **Эл. почта**: SMTP/SMTPS, Microsoft Outlook (MAPI), IBM Notes
- **Веб-почта**: Почта Mail.Ru, Рамблер-Почта, Яндекс.Почта, Gmail, AOL Mail, Hotmail/Outlook.com, Yahoo! Mail, GMX.de, Web.de, T-online.de, freenet.de, Outlook Web App/Access (OWA), NAVER, ABV Mail
- **Социальные сети (включая мобильные версии):** ВКонтакте, Одноклассники, LiveJournal, LiveInternet.ru, Facebook, Twitter, Google+, LinkedIn, Tumblr, MySpace, XING.com, MeinVZ.de, StudiVZ.de, Disqus
- **Сетевые сервисы файлового обмена и синхронизации:** Яндекс.Диск, Облако Mail.Ru, Google Drive, Dropbox, OneDrive, Box, iCloud, Amazon S3, GMX.de, Web.de, MagentaCLOUD, freenet.de, Sendspace, MediaFire, WeTransfer, 4shared, GitHub, MEGA, AnonFile, dmca.gripe, DropMeFiles, Easyupload.io, Files.fm, Gofile.io, transfer.sh, TransFiles.ru и Uploadfiles.io
- **Службы мгновенных сообщений:** Skype/Skype for Web/Skype for Business/Microsoft Lync 2013, Telegram, Агент Mail.Ru, Zoom, Viber, Jabber, ICQ, Windows Messenger, IRC, WhatsApp
- **Веб-поиск:** Google, Яндекс, Bing, Baidu, Yahoo, Поиск Mail.Ru, Ask.com, AOL Search, Рамблер, Wolfram Alpha, DuckDuckGo, WebCrawler, Search.com, Wayback Machine, Dogpile, StartPage, Excite, NAVER, Web.de
- **Поиск работы:** hh.ru, Яндекс.Работа, Rabota.ru, SuperJob.ru, Авито, CareerBuilder, College Recruiter, craigslist, Dice, Glassdoor, GovernmentJobs, HeadHunter.com, Hired, Indeed, JobisJob, Mediabistro, Monster, Simply Hired, Ladders, us.jobs, USAJOBS, ZipRecruiter
- **Сетевые протоколы:** HTTP/HTTP-SSL, FTP/FTP-SSL, Telnet
- **Прочее:** файловые ресурсы (SMB), частные беседы (Private Conversations) Skype, звонки Skype, Torrent, трафик Tor Browser

Контентная фильтрация

- **Контролируемые каналы:** сменные накопители (USB, дискеты, оптические и жесткие диски), принтеры (локальные, сетевые, виртуальные), буфер обмена, каналы сетевых коммуникаций (электронная и веб-почта, мессенджеры, социальные сети, файлообменные сервисы, веб-поиск и поиск работы, HTTP/HTTPS, FTP/FTPS, SMB)
- **Контролируемые типы содержимого:** текст, бинарные данные, типы данных
- **Методы детектирования текстового контента:** поиск по ключевым словам и словарям (160+ встроенных отраслевых терминологических словарей, возможность создания собственных словарей) с применением морфологического анализа (для английского, русского и других языков) по целым словам или частичному совпадению, с поддержкой транслитерации для русского языка; поиск по встроенным комплексным шаблонам регулярных выражений (90+ встроенных шаблонов, возможность создания собственных шаблонов); анализ по цифровым отпечаткам (с частичным или полным соответствием с заданным образцом) с поддержкой классификации образцов
- **Методы детектирования бинарного контента:** анализ по цифровым отпечаткам
- **Контролируемые текстовые данные:** более 100 распознаваемых форматов файлов и 40+ типов архивов, текстовые данные в электронных сообщениях, веб-формах, текст в изображениях, запечатанные документы Oracle IRM, данные с метками классификатора Boldon James
- **Контролируемые типы данных:** более 5300 типов файлов, свойства файлов и документов, объекты буфера обмена (файлы, текст, изображения, аудио, прочее), объекты протоколов синхронизации с мобильными устройствами, контроль текста в графических изображениях (встроенных в документы Microsoft Office, AutoCAD и Adobe PDF или отдельных графических файлах), запечатанные документы Oracle IRM, объекты данных с метками классификатора Boldon James
- **Контентная фильтрация при теневом копировании:** для всех контролируемых каналов и типов данных
- **Оптическое распознавание символов (OCR):** резидентный OCR модуль с распознаванием 30+ языков, включая русский, с поддержкой перевернутых/зеркалированных/инвертированных изображений

Интеграция с криптографическими продуктами

- **Windows:** Windows BitLocker To Go™, Sophos® SafeGuard Easy®, SecurStar® DriveCrypt®, TrueCrypt®, PGP® Whole Disk Encryption, Инфотекс SafeDisk®, Lexar® S1100/S3000, SafeToGo, Рутокен Диск
- **Mac:** Apple® OS X FileVault

Выявление несанкционированного содержимого

- **Сканируются:** рабочие станции и серверы Windows (файловая система, репозитории электронной почты, подключенные периферийные устройства), общие сетевые ресурсы, сетевые хранилища, папки облачных сервисов файлового обмена
- **Режимы сканирования:** с использованием агента, удаленное (без агента), смешанное
- **Запуск задач сканирования:** ручной и автоматический (в соответствии с расписанием)
- **Выполняемые действия:** удаление, гарантированное удаление, удаление контейнера (если нарушение выявлено внутри контейнера или архива), задание прав доступа (для файловой системы NTFS), протоколирование, оповещение администратора, оповещение локального пользователя, шифрование (EFS в файловой системе NTFS)
- **Прочее:** статическое и динамическое формирование списка сканируемых компьютеров, графические отчеты, автоматическая установка и удаление агента

Программно-аппаратные требования

- **Агенты**: Windows NT/2000/XP/Vista/7/8/8.1/10/Server 2003-2019 (32/64-бита); Apple OS X 10.6.8-10.15 (32/64-бита); Microsoft RDS, Citrix XenDesktop/XenApp, Citrix XenServer, VMware Horizon View; VMware Workstation, VMware Player, Oracle VM VirtualBox, Virtual PC, Hyper-V; CPU Pentium 4, память 512 Мб, диск 400 Мб
- **Консоли**: Windows 2000/XP/Vista/7/8/8.1/10/Server 2003-2019 (32/64-бита); CPU Pentium 4, память 512 Мб, диск 1 Гб
- **DeviceLock Enterprise Server, DeviceLock Discovery Server, DeviceLock Search Server:** Windows Server 2003-2019 (32/64-бита), Microsoft RDS, Citrix XenServer, VMware vSphere Desktop; 2xCPU Intel Xeon Quad-Core 2.33 Ггц, память 8 Гб, диск 800 Гб; SQL Express/MS SQL Server 2005-2017 или PostgreSQL 9.5 (и более новые)

АО «Смарт Лайн Инк»
107023, г. Москва, Семеновская
Малая ул, д.9, стр. 14Б
Тел. (495) 647-99-37

[www.devicelock.com/ru]