DeviceLock DLP
Proactive Endpoint Security

DeviceLock DLP Suite 8.3

Новые возможности

СЕРГЕЙ ВАХОНИН

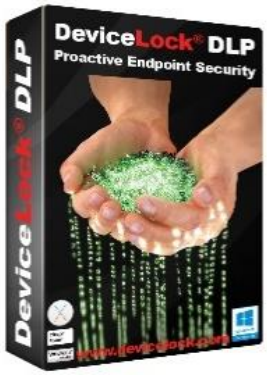
Директор по решениям

Смарт Лайн Инк / DeviceLock, Inc.

EMAIL SV@DEVICELOCK.COM

АО Смарт Лайн Инк
Москва, 06/2018

АО «Смарт Лайн Инк» - 20 лет на рынке информационной безопасности



ПЕРВАЯ ВЕРСИЯ
DEVICELOCK -
1996

Продукт

Программный комплекс **DeviceLock DLP**

Система защиты информации для организаций, которым необходимо простое и доступное решение по предотвращению утечек данных с корпоративных компьютеров под управлением Windows и MacOS, а также виртуализованных рабочих сред и приложений Windows.

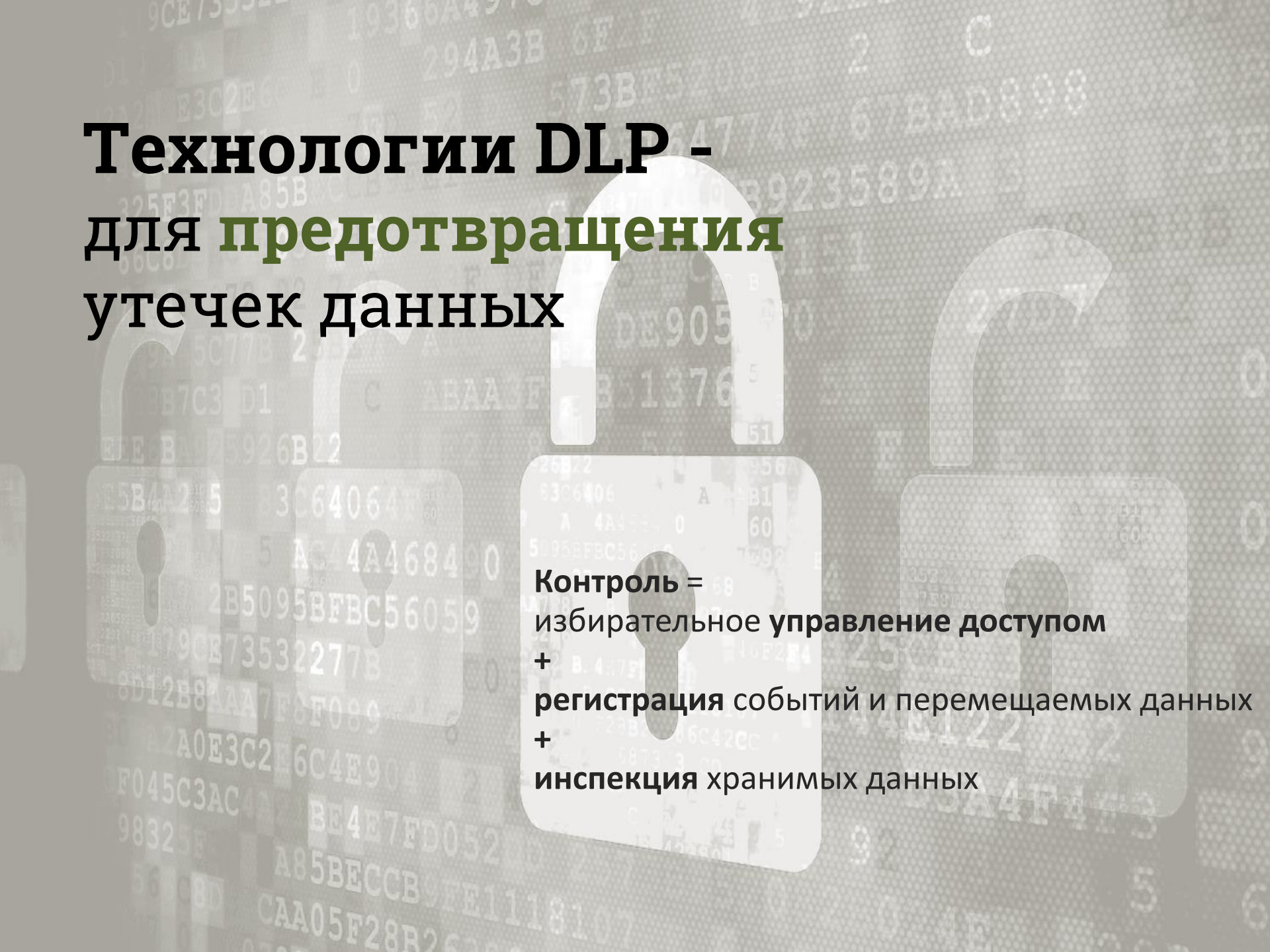
Смарт Лайн Инк / DeviceLock, Inc.

Отечественная компания с штаб-квартирой и офисом разработки **в Москве** (АО «Смарт Лайн Инк),
офисами продаж в США (DeviceLock NA, San Ramon, California), Канаде (DeviceLock Canada, North Vancouver), Великобритании (DeviceLock UK, London), Германии (DeviceLock Europe GmbH, Ratingen), Италии (DeviceLock Italy, Milan),
а также партнерской сетью по всему миру.

Более 70 000 пользователей при более чем 7 000 000 инсталляций по всему миру

DeviceLock - 20 лет на рынке информационной безопасности всего мира

Технологии DLP - для **предотвращения** утечек данных



Контроль =
избирательное **управление доступом**
+
регистрация событий и перемещаемых данных
+
инспекция хранимых данных

Решение? DLP-системы!

Информация – это «кровь» корпоративных ИТ, и ровно так же, как потеря крови смертельно опасна для жизни человека, утечки данных из корпоративной среды и от ее пользователей опасны для бизнеса.

Защита стратегически важной информации от утечек (утери, хищения)

Непрерывный контроль всех возможных каналов информационного обмена и хранимых данных:

- Тотальный или выборочный контроль технических каналов утечки информации на рабочих ПК
- **Предотвращение** утечек == **блокировка** недопустимых попыток передачи данных

Минимизация рисков репутационного ущерба и коммерческих потерь. Соответствие требованиям регуляторов (Complience)

Обеспечение соответствия требованиям стандартов и законов 152ФЗ, СТО БР, PCI DSS, SOX, HIPAA, Basel II и т.д. за счет **полноценного контроля** каналов передачи данных и устройств хранения информации, журналирования событий и инструментария расследования инцидентов.

Архивирование и анализ передаваемой информации. Выявление инцидентов постфактум и в реальном времени.

- Повышение эффективности службы информационной безопасности – реагирование в реальном масштабе времени на события, связанные с вопросами защиты данных
- Аудит журналов DLP-системы и архива перехваченного трафика и передаваемых/печатаемых/сохраняемых файлов и документов, попыток и/или фактов передачи данных, включая проверку содержимого переданных и/или заблокированных файлов и документов.
- Выявление инсайдеров-злоумышленников. Выявление нелояльных сотрудников.

Контроль исполнения корпоративной политики безопасного хранения

Превентивная защита данных, размещенных в корпоративных сетевых хранилищах и общих сетевых ресурсах, файловых системах на пользовательских компьютерах.

Принципы полноценного контроля каналов передачи данных

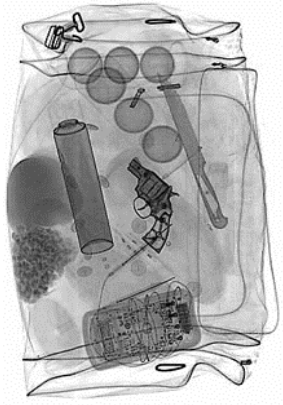
Автоматическое принятие решений о возможности передачи/печати/сохранения на основе двух взаимодополняющих методов

Контекстный контроль

- Пользователь, его права, группы, в которых он состоит и т.п.
- Дата и время
- Местонахождение
- Источник / адресат
- Тип файла
- Направление передачи данных

Контентный анализ и фильтрация (проверка содержимого)

- Ключевые слова и сочетания слов, морфологический анализ, транслитерация, промышленные словари
- Встроенные шаблоны данных (номера карт страхования, кредитных карт, др.)
- Цифровые отпечатки (fingerprinting)
- Проверка архивов и вложенных архивов, встроенных в файлы-контейнеры
- Возможность проверки как сообщений, так и вложений почты и мессенджеров
- Прочие критерии проверки



«Точки применения» технологий контентного анализа

Когда может выполняться анализ содержимого файлов и данных?

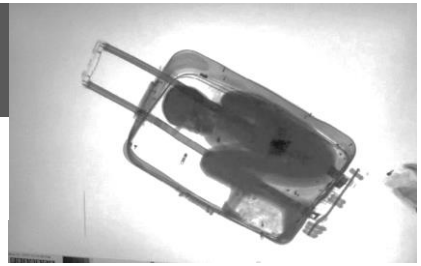
Анализ **хранимых** данных (discovery)

Анализ **передаваемых** данных **в реальном времени** (передача, сохранение, печать)

Анализ **перехваченных** данных (полнотекстовый поиск, фильтрация результатов по контенту)

Проверять содержимое документов и переписки можно не только после того, как состоится утечка!

#если нашли утечку – значит не было утечки!
#проведение расследования



Следствия отсутствия механизма контентной фильтрации в реальном времени в DLP-системе:
- в архиве DLP-системы хранятся ВСЕ перехваченные данные, без разделения на корпоративные и личные.
- Блокировка каналов передачи данных целиком там, где можно делать исключения, блокируя только передачу данных ограниченного доступа

Предотвратить утечки в любых сценариях!

Равносильная DLP-защита для пользователей внутри и вне корпоративной сети

- Офисные пользователи
- Мобильные сотрудники (в командировке, дома, …)

Защита от вмешательства пользователя,

- в особенности с правами локального системного администратора

Сочетание контекстных и контентных механизмов для эффективной реализации принципа наименьших привилегий

- Сценарий минимальных привилегий: ограничить до минимума разрешенные каналы передачи данных – без нарушения бизнес-процессов…
- …а также использовать инспекцию содержимого (контента) для блокировки потоков данных, нерелевантных для бизнес-процессов.

Защита информации приобретает решающее значение в сегодняшней гиперсетевой реальности, когда повсеместные мобильные коммуникации, высокоскоростной Интернет, социальные медиа, электронная почта и масса других потребительских приложений, низкая стоимость и практически неограниченная емкость съемных накопителей, а также коммерциализация киберпреступности создают синергический эффект резкого увеличения количества и уровня угроз безопасности ИТ.
Основной причиной утечек является человеческая натура - люди совершают случайные ошибки, могут небрежно относиться к обработке и обеспечению безопасности данных, а некоторые и вовсе действуют злоумышленно.

DeviceLock DLP – настоящее DLP для защиты информации

DeviceLock DLP

ПРЕДОТВРАЩЕНИЕ УТЕЧЕК ДАННЫХ и МОНИТОРИНГ СОБЫТИЙ

в режиме реального времени, в любых сценариях!

…устройства и интерфейсы

…каналы сетевых коммуникаций

…с применением технологий контентной фильтрации

+ собственный поисковый сервер

+ сканирование хранимых данных

Типовые задачи, решаемые DeviceLock DLP

Предотвращение утечек через устройства и сетевые каналы, доступ к которым не требуется по работе.
Выборочный **контроль и ограничение** доступа пользователей **ко всем типам локальных устройств и портов** компьютеров.
Гибкий **контроль** пользовательских коммуникаций, осуществляемых через распространенные **сетевые приложения и протоколы**.

Журналирование действий пользователей.
Детальное событийное **протоколирование** заданных действий пользователей, включая **теневое копирование** (сохранение точных копий) данных, с хранением журналов в **централизованном или распределенном архиве**.
Создание теневых копий при срабатывании правил анализа содержимого.

Предоставление доступа только к **авторизованным устройствам USB (Белые Списки)** – постоянное или временное (для однократного использования или на срок до одного месяца) к определенным устройствам, в т.ч. в условиях отсутствия соединения удаленного компьютера с корпоративной сетью.

Анализ данных в режиме реального времени для предотвращения утечек данных ограниченного доступа (контентная фильтрация), **оперативного оповещения** служб ИБ, **избирательного теневого копирования**.
Выборочное предоставление или запрет пользователям возможности передачи/печати/сохранения данных по результатам проверки разрешенных типов файлов, анализа текстового и бинарного содержимого данных (контентного анализа) в файлах или сеансах обмена сообщениями, с использованием методов контентной фильтрации: анализ по ключевым словам, расширенным свойствам документов, шаблонам регулярных выражений, цифровым отпечаткам, с использованием морфологического анализа ключевых слов на 8 распространенных языках. Детектирование и защита конфиденциальных данных, представленных в графической форме, с помощью встроенного модуля оптического распознавания символов (OCR).

Защита данных, хранимых в корпоративной ИС, для обеспечения политики безопасного хранения данных – сканирование и обнаружение конфиденциальной информации на корпоративных хранилищах, сетевых ресурсах и пользовательских компьютеров с применением заданных действий по устранению выявленных нарушений.

Типовые задачи, решаемые DeviceLock DLP

Обеспечение оперативной реакции службы ИБ на инциденты - оповещения системы безопасности о событиях в реальном времени через инструменты SMTP/SNMP/SIEM.

Анализ действий пользователей на основании данных централизованного архива – полнотекстовый поиск по базе данных для выявления и расследования инцидентов, создание статистических и графических отчетов, включая интерактивный граф связей пользователей.

DLP-контроль для виртуальных и терминальных сред

DeviceLock Virtual DLP: контроль буфера обмена и перенаправленных устройств в терминальных сессиях, без установки дополнительных агентов на удаленные/мобильные устройства и тонкие клиенты.

Работа в любых виртуальных средах.

Защита данных на компьютерах, не подключенных к корпоративной сети.
Автономная полноценная работа агента DeviceLock на любых Windows- и Mac-компьютерах.
Реализация гибкого подхода к защите для пользователей в **онлайн- и оффлайн-режимах**.

Принудительное шифрование (или запрет шифрования) **съемных накопителей**
Интеграция с внешними программными и аппаратными **средствами шифрования** съёмных носителей (определение прав доступа к шифрованным носителям).

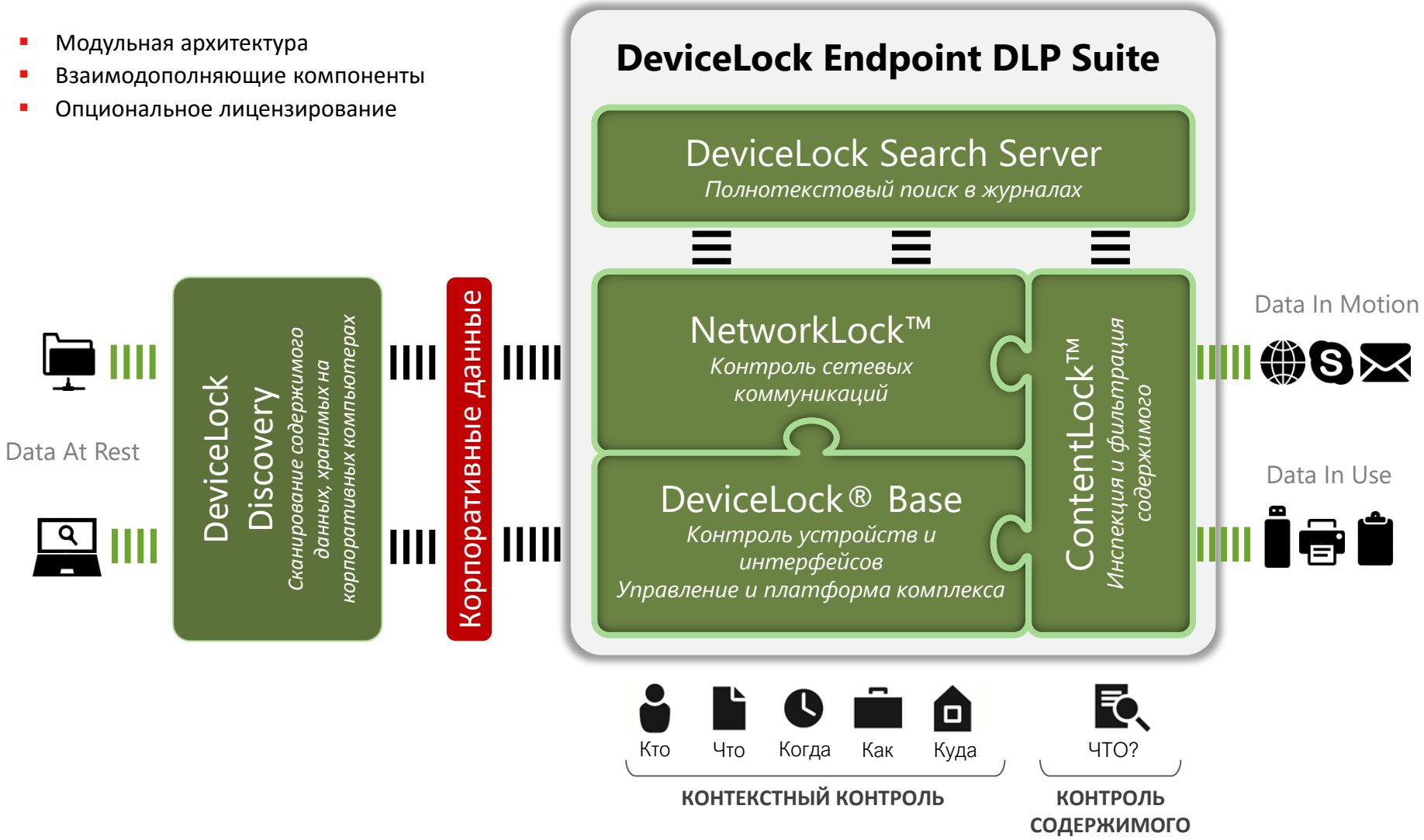
Защита от пользователей, обладающих локальными административными правами.
Предотвращение остановки или удаления агента, защита политик и журналов в локальном хранилище.

Детектирование и блокировка клавиатурных шпионов (USB и PS/2).

Контроль доступа пользователей к локальным портам и периферийным устройствам **на компьютерах Mac** под управлением Apple OS X.

Комплекс DeviceLock DLP Suite

- Модульная архитектура
- Взаимодополняющие компоненты
- Опциональное лицензирование

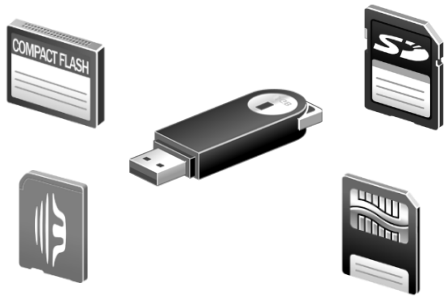


Компонент DeviceLock: контроль устройств и интерфейсов

DeviceLock Base обеспечивает **контроль доступа** к устройствам и интерфейсам, событийное **протоколирование** (аудит), тревожные оповещения и теневое копирование, а также реализует такие функции, как **Белые списки USB-устройств** и CD/DVD носителей, **защиту** агента DeviceLock от локального администратора, поддержку сторонних криптопродуктов, обнаружение и блокирование аппаратных кейлоггеров и др.

Устройства хранения данных, буфер обмена

Флеш-накопители, карты памяти

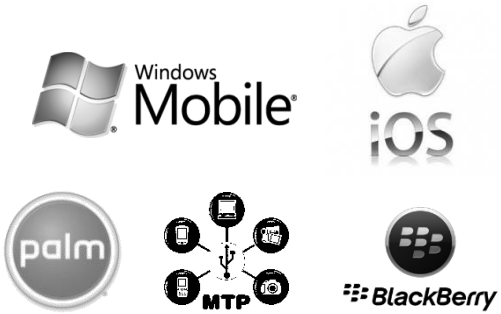


Интерфейсы подключения

Терминальные сессии и виртуальные среды

Канал печати

Мобильные устройства



Компонент NetworkLock: защита от угроз сетевого происхождения

NetworkLock обеспечивает избирательный контекстный контроль каналов сетевых коммуникаций, событийное протоколирование (аудит), тревожные оповещения и теневое копирование для них.

Почтовые протоколы и веб-почта

- MAPI
- SMTP
- SMTP-SSL
- Lotus

Социальные сети

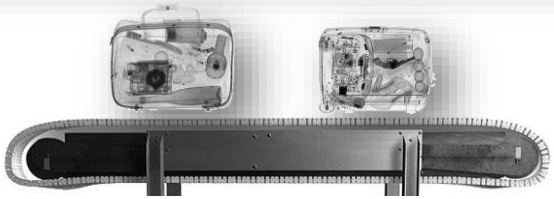
Службы мгновенных сообщений

Интернет протоколы

- HTTP/HTTPS
- FTP
- FTP-SSL
- Telnet
- Torrent

Сетевые сервисы файлового обмена и синхронизации, внутрисетевые файловые ресурсы

Компонент ContentLock: контентный анализ и фильтрация



Контентная фильтрация данных и файлов в реальном времени или в асинхронном режиме

Используемые методы

Поиск **по ключевым словам** и сочетания слов,
Использование шаблонов **регулярных выражений**.

Морфологический анализ заданных слов на русском, английском и других языках. Поддержка **транслитерации.**

Встроенные промышленные и геоспецифичные терминологические **словари**.

Бинарно-сигнатурное определение более 5 300 типов файлов. Анализ архивов и контейнеров.

Встроенный высокоэффективный модуль **оптического распознавания символов** (**OCR**).

Цифровые отпечатки (fingerprinting).

Все используемые методы контентной фильтрации могут быть объединены в правила любого уровня сложности на базе различных численных и логических условий.

Варианты применения

1 КОНТРОЛЬ ДОСТУПА

К данным или каналам их передачи – для разрешения (при запрете доступа к каналу) или блокировки передачи недопустимого содержимого.
Синхронная обработка

2 ТЕНЕВОЕ КОПИРОВАНИЕ

Запись полных копий данных
Синхронная обработка

3 ОБНАРУЖЕНИЕ

Протоколирование попыток доступа или передачи данных, тревожные оповещения
Асинхронная обработка

Контентный анализ и фильтрация

Локальные каналы

Съемные накопители

Диски Floppy, CD/DVD/BD

Канал печати документов (локальная и сетевая печать)

Системный буфер обмена Windows Clipboard

Снимки экранов по клавише PrintScreen и сторонними приложениями

Перенаправленные в терминальную сессию диски и буфер обмена терминальной сессии

Каналы сетевых коммуникаций

Электронная почта

Сервисы Web-почты

Социальные сети

Мессенджеры

Web-доступ к облачным хранилищам

Передача файлов по протоколу FTP

Web-приложения HTTP/HTTPS

Передача файлов по локальной сети в общие папки по протоколу 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, объекты данных 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

DeviceLock Discovery

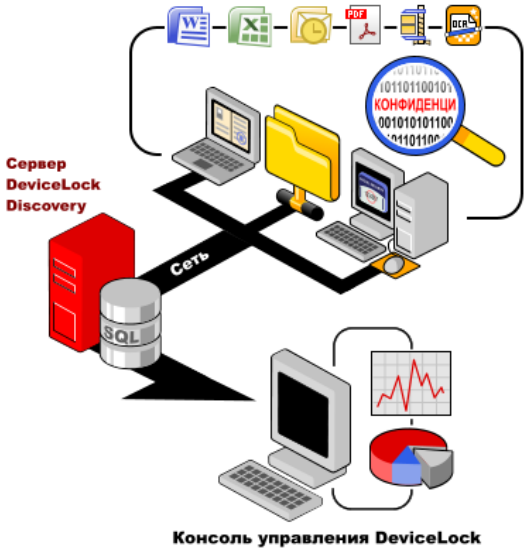
- Самостоятельный продукт или функциональный компонент программного комплекса DeviceLock DLP
- Позволяет организациям получить контроль над хранимыми данными
- Способствует достижению соответствия корпоративным стандартам безопасности и требованиям регуляторов

Установка и удаление сканирующих агентов выполняется в автоматическом режиме, незаметно для пользователей.

Сканирование инициируется вручную или автоматически сервером в соответствии с заданным расписанием.

- **Сетевые ресурсы** общего доступа и системы хранения данных (SAN/NAS), доступные по протоколу SMB
- **Рабочие станции** пользователей под управлением ОС Windows: локальные файловые системы и подключенные устройства хранения

- Автоматически **сканирует и проверяет** содержимое файлов
- **Обнаруживает** контент, хранимый с нарушением корпоративной политики безопасного хранения данныъ
- **Устраняет** нарушения политик безопасности data-at-rest - выполняет различные опциональные действия, записывает события нарушений в журнал, оповещает службу ИБ и пользователя, создает отчеты о результатах выполнения задач сканирования и обнаружения



DeviceLock Search Server

DeviceLock Search Server – опциональный компонент DeviceLock DLP, позволяет проводить быстрый и удобный аудит журналов событий и теневых копий, упрощает и ускоряет выявление и расследование инцидентов.

Производит **полнотекстовый поиск** по базам данных теневого копирования (в том числе **внутри** сохраненных файлов) и журналам событийного протоколирования, хранящимся на сервере DeviceLock Enterprise Server (в связанной SQL-базе данных).

- Индексирование и поиск: комбинация слов, фраз, регулярных выражений, специальных символов, численных диапазонов, полей документов, записей журналов событийного протоколирования;
- Морфологический поиск и фильтрация «стоп-слов».

Автоматически распознаёт, индексирует, находит и отображает документы в архиве

- 80+ файловых форматов:
- Adobe Acrobat (PDF), Ami Pro, архивы (GZIP, RAR, ZIP), Lotus 1-2-3, Microsoft Access, Microsoft Excel, Microsoft PowerPoint, Microsoft Word, Microsoft Works, OpenOffice (документы, таблицы и презентации), Quattro Pro, WordPerfect, Wordstar и многих других;
- По определённым параметрам записи.

Поддерживает автоматизированный запуск поисковых запросов по расписанию, с инкрементальным анализом результатов поиска (AutoSearch)

Демонстрация новых возможностей DeviceLock DLP

Некоторые сценарии предотвращения утечки данных в реальном времени

ИЛЬШАТ ЛАТЫПОВ

Инженер-аналитик

Смарт Лайн Инк

DeviceLock DLP 8.3 – новые функции и возможности

Новый метод детектирования содержимого – **Цифровые отпечатки** ("Document Fingerprints"). Данная технология основана на сравнении коротких буквенно-цифровых хэшей инспектируемых документов и файлов, также называемых цифровыми отпечатками или фингерпринтами, с хэшами, хранимыми в коллекции (базе данных) цифровых отпечатков. Это позволяет однозначно идентифицировать содержимое документов или файлов для решения различных задач обеспечения безопасности данных.

Существенное улучшение функции контроля сетевого протокола **SMB**. Наиболее значимые изменения включают контроль входящих файлов на уровне разрешений для протокола, возможность контроля исходящих файлов по содержимому на уровне контентно-зависимых правил для разрешений.

boldonjames
A QinetiQ Company

Поддержка меток классификатора **Boldon James** в составных документах, а также документах MS Office современных форматов и PDF-файлах как расширение контентных групп Document Properties для контентно-зависимых правил.

Возможность задавать **пользовательские свойства** документов в контентных группах Document Properties и их значений для поиска заданных параметров в соответствующих пользовательских свойствах составных документов, а также документов MS Office современных форматов и PDF-файлах.

Оптимизированный контроль мессенджера Skype для новых версий **Skype 8.x** и **Skype 12.x**.

Цифровые отпечатки в DeviceLock DLP 8.3

Технология детектирования содержимого по цифровым отпечаткам ("Document Fingerprints") основана на сравнении коротких буквенно-цифровых хэшей инспектируемых документов и файлов, также называемых цифровыми отпечатками или фингерпринтами, с хэшами, хранимыми в коллекции (базе данных) цифровых отпечатков. Это позволяет однозначно идентифицировать содержимое документов или файлов для решения различных задач обеспечения безопасности данных.

Цифровой отпечаток (fingerprint) - набор буквенно-цифровых строк (хэшей), однозначно идентифицирующих документ или файл и его содержимое.

При использовании цифровых отпечатков DeviceLock снимает цифровые отпечатки с образцов конфиденциальных документов, а затем сравнивает их с цифровыми отпечатками проверяемых документов. Если процент “соответствия отпечатков” превышает требуемый порог в соответствии с настройкой, проверяемые документы считаются конфиденциальными, и к ним применяются все необходимые действия по обеспечению безопасности.

Конфиденциальные документы и другие информационные активы, требующие защиты, могут быть распределены по классификациям с определенными уровнями важности или секретности (например, “Для служебного пользования”, “Конфиденциально”, “Секретно” и “Совершенно секретно”). Документы и файлы могут быть классифицированы путем сравнения их отпечатков с отпечатками документов и файлов известных классификаций.

Сервер DeviceLock Enterprise Server хранит цифровые отпечатки предоставленных ему образцов информации в собственной базе данных отпечатков. При проверке источника информации (например, документа или файла) DeviceLock может сравнивать цифровые отпечатки источника с отпечатками определенной классификации из базы данных и вычислять их процент соответствия. Если процент соответствия превышает установленный порог, DeviceLock соответствующим образом классифицирует проверенную информацию. Образцы информационных ресурсов (документы, файлы и т.п.), отпечатки которых собраны и сохранены в базе данных, называются источниками отпечатков. Эти образцы могут быть изменены, добавлены или удалены, или уровень их секретности может со временем меняться. Для того, чтобы база данных учитывала все такие изменения, сервер регулярно выполняет задачи классификации, что приводит к обновлению хранилища отпечатков.

Сценарий: запись документа на съемный накопитель

USB-накопители разрешены только определенной группе.
Допускается использование только авторизованных накопителей.
Задача: предотвратить запись документа MS Word с конфиденциальным содержимым на USB-накопитель.
Все факты записи должны журналироваться, с созданием теневой копии.
При попытке записи документа с конфиденциальным содержимым следует отправлять тревожное оповещение.

- Доступ предоставляется отдельным пользователям и группам
- Используется Белый список USB-устройств
- Инспекция текстового содержимого (контентная фильтрация)
- Создание записи в логе, теневой копии
- Тревожное оповещение

Сценарий: отправка финансовой информации по электронной почте

Допускается передача по электронной почте сообщений, содержащих документы с секретной, только на адреса руководства компании.

Задача: не допускать передачу документов, отпечатки которых классифицируются как секретные, по протоколу SMTP неавторизованным получателям.
Создавать теневую копию при любых попытках передачи (разрешенных и запрещенных).

- Анализ по цифровым отпечаткам
- Контроль адресов получателей сообщения
- Создание теневой копии
- Контроль на уровне протокола SMTP (любой клиент)

Сценарий: расширенный контроль Skype

Использование Skype разрешено для всех пользователей только для передачи сообщений (чат), голосового и видео- общения.

Задача: не допускается передача документов внутреннего пользования через Skype, разрешены чат, аудио- и видео-конференции.
Уведомлять пользователя о недопустимости передачи файлов.
Вести журналирование попыток передачи файлов и содержимого чата.

- Доступ предоставляется всем пользователям и группам
- Передача документов внутреннего пользования запрещена
- Журналирование попыток передачи файлов
- Теневое копирование чата Skype
- Вывод сообщения в трее о запрете передачи файла

Сценарий: ограниченное использование сервисов веб-почты

Использование сетевых ресурсов(SMB) разрешено, но не допускается передача документов MS Office и архивов.

Задача: блокировать передачу файлов MS Office и архивов по SMB. Журналировать использование SMB.

Доступ предоставляется всем пользователям и группам

Передача документов MS Office и архивов запрещена

Журналирование использования SMB ресурсов

СПАСИБО
ЗА ВНИМАНИЕ!

www.DeviceLock.com