DeviceLock®

DISCOVERY

DeviceLock Discovery, самостоятельный функциональный компонент программного комплекса DeviceLock DLP Suite, позволяет организациям контролировать местоположение и уровень защищенности конфиденциальных корпоративных данных, хранимых в ИТ-инфраструктуре организации ("data-at-rest"), в целях проактивного предотвращения их утечек и обеспечения соответствия корпоративным стандартам безопасности и требованиям отраслевых и государственных регуляторов.

Посредством автоматического сканирования данных, размещенных на рабочих станциях и серверах Windows внутри корпоративной сети, внутренних сетевых ресурсах и системах хранения данных, DeviceLock Discovery обнаруживает документы и файлы, содержимое которых нарушает политику безопасного хранения корпоративных данных, осуществляет с ними различные опциональные превентивно-защитные действия, заданные в DLP-политике, а также может инициировать внешние процедуры управления инцидентами, направляя оперативные тревожные оповещения в SIEM-системы, используемые в организации.

Структура

При развертывании в качестве автономного решения DeviceLock Discovery включает в себя следующие компоненты:

Сервер DeviceLock Discovery – серверный компонент, осуществляющий удаленное сканирование файлов на общедоступных сетевых ресурсах по протоколу SMB/CIFS, а также обеспечивающий развертывание и управление легковесными агентами DeviceLock Discovery на контролируемых компьютерах. Структурно DeviceLock Discovery Server является частью сервера DeviceLock Content Security Server.

Агент DeviceLock Discovery – клиентское программное обеспечение, используемое для сканирования локальной файловой системы на рабочих станциях и серверах Windows, а также доступных с контролируемого компьютера общих сетевых ресурсов и подключенных сменных накопителей.

Консоль управления – графический интерфейс пользователя (GUI), предназначенный для централизованного управления компонентами DeviceLock Discovery. В зависимости от специфики развертывания и особенностей инфраструктуры администраторы DeviceLock могут использовать разные консоли управления, включая DeviceLock Management Console и DeviceLock WebConsole.

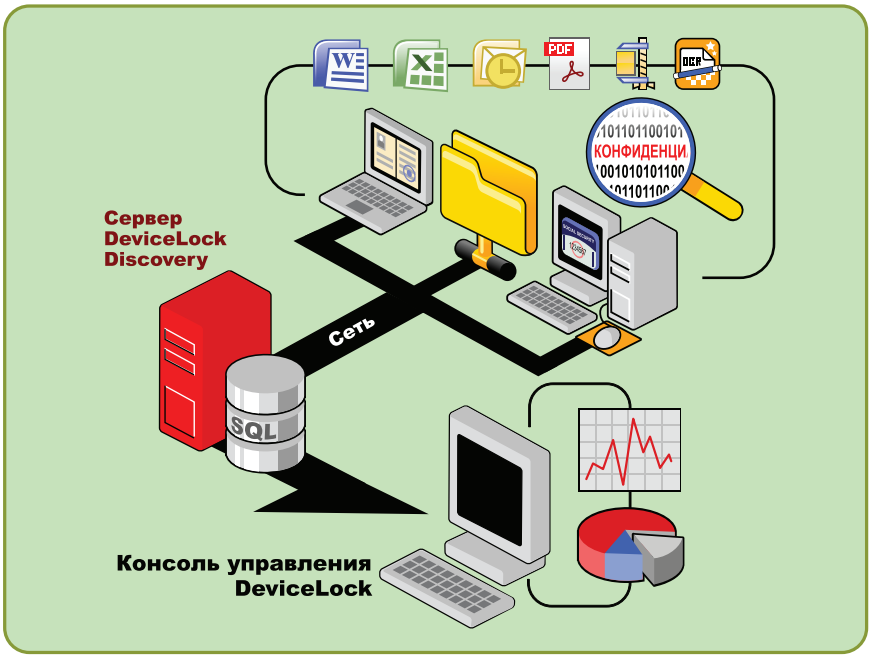
DeviceLock Discovery при эксплуатации совместно с другими компонентами комплекса DeviceLock DLP Suite может использовать для сканирования и обнаружения мощности полнофункциональных агентов DeviceLock DLP.

Выполняемые операции

В зависимости от топологии локальной сети и других специфических особенностей защищаемой ИТ-среды DeviceLock Discovery может выполнять сканирование в нескольких режимах: удаленное (без агента), агентское и гибридное.

Режим удаленного сканирования (без использования агента) применяется сервером DeviceLock Discovery для сканирования систем хранения данных и общих сетевых ресурсов, доступных по протоколу SMB. В этом режиме файлы загружаются на сервер DeviceLock Discovery, где производится инспектирование и анализ содержимого с последующими действиями по устранению нарушений, выполняемыми также по протоколу SMB. Удаленное сканирование является единственным способом контроля хранимых данных на компьютерах под управлением операционных систем, не поддерживаемых DeviceLock (таких, как Linux и др.), а также NAS-устройствах.

Режим агентского сканирования (с использованием локального агента) применяется для сканирования локальных файловых систем на компьютерах, где функционируют агенты Discovery или DeviceLock DLP, а также на сетевых ресурсах, доступных с этих компьютеров. В этом режиме содержимое файлов на рабочих станциях проверяется агентами локально с применением заданных действий по устранению нарушений в зависимости от обнаруженного контента. Файлы, хранимые на общедоступных сетевых ресурсах, загружаются на компьютер по протоколу SMB, где агент проверяет их содержимое, выявляет нарушения и применяет заданные действия. Помимо ключевой возможности сканирования локальных файловых систем на корпоративных компьютерах, режим агентского сканирования обеспечивает существенное преимущество в производительности. Во-первых, сканирование локальной файловой системы не требует передачи файлов на центральный сервер по



DeviceLock Discovery: Сканирование и обнаружение хранимых данных в сети и на рабочих станциях

сети, а значит, не снижает ее пропускную способность. Во-вторых, распределение процессорной нагрузки при инспектировании содержимого локальных файлов на множество агентов существенно снижает нагрузку на сервер Discovery.

Режим гибридного сканирования сочетает два вышеописанных режима, осуществляемых одновременно соответствующими компонентами DeviceLock Discovery. Сочетание режимов удаленного и агентского сканирования не только повышает степень безопасности хранения данных, но и позволяет администраторам DeviceLock создавать эффективные политики обнаружения контента в ИТ-инфраструктуре организации для достижения оптимального сочетания производительности и сетевой нагрузки.

Сканирование DeviceLock Discovery может быть инициировано вручную администратором или автоматически сервером в соответствии с заданным расписанием. В качестве целевых узлов для сканирования задаются определенные компьютеры или группы компьютеров, общие сетевые ресурсы и хранилища в корпоративной сети. Агенты DeviceLock Discovery устанавливаются и удаляются с целевых компьютеров сервером DeviceLock Discovery автоматически и незаметно для пользователей.

Обнаружение информационного содержимого

DeviceLock Discovery позволяет инспектировать текстовые и бинарные данные, а также метаданные документов и другие типы данных.

Для обнаружения структурированного текстового содержимого DeviceLock Discovery применяет такие технологии контентного анализа, как поиск по ключевым словам и словарям, по целым словам или частичному совпадению; поиск по встроенным комплексным шаблонам регулярных выражений; анализ по цифровым отпечаткам (с частичным или полным соответствием с заданным образцом) с поддержкой классификации образцов. Продукт поставляется со встроенными промышленными и геоспецифичными терминологическими словарями, предопределенными шаблонами регулярных выражений для наиболее распространенных видов конфиденциальной информации, таких как номера паспортов, кредитных карт, транспортных средств и банковских счетов, адреса, и др. Кроме того, реализована возможность разработки собственных словарей и шаблонов, а также модификации встроенных. Точность детектирования контента повышается за счет использования морфологического анализа словоформ заданных ключевых слов на русском, английском и других языках, а также поддержке транслитерации для русского языка.

Для детектирования неструктурированных текстовых и бинарных данных в DeviceLock Discovery применяется технология цифровых отпечатков, позволяющая надежно идентифицировать классифицированные файлы по их содержимому с учетом заданных уровней классификации («Секретно», «Конфиденциально», «ДСП» и т.п.). 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 целиком, так и выявить их частичное соответствие, например, после изменения оригинального документа, или обнаружить наличие в документе заданного содержимого как части документа. Таким образом, цифровые отпечатки дают возможность надежно идентифицировать классифицированные файлы по их содержимому, несмотря на возможные искажения и изменения, вызванные добавлением несущественной информации или «шумов», таких как отдельные символы, незначащие слова и т.д. База данных цифровых отпечатков формируется вручную либо наполняется автоматически при обработке образцов конфиденциальных документов, помещенных в папки соответствующих уровней классификации. Существует пять предопределенных уровней классификации, также возможно добавлять или определять свои собственные категории.

Определение реального типа файла – еще один способ инспекции данных, используемый DeviceLock Discovery как отдельно, так и в сочетании с проверкой их текстового содержимого и сравнением с образцами цифровых отпечатков. Определение типов файлов основано на бинарно-сигнатурном методе и не зависит от расширения файла. Кроме того, DeviceLock Discovery позволяет инспектировать и использовать в качестве критериев для обнаружения метаданные и расширенные свойства файлов и документов, а также распознавать и использовать метки классификации, назначенные документам и файлам классификатором Boldon James.

Встроенный модуль оптического распознавания символов (OCR) позволяет DeviceLock Discovery проверять текстовое содержимое графических файлов более чем 30 форматов, а также изображений, встроенных в документы и другие объекты данных. Благодаря распознаванию более 30 языков в сочетании с поддержкой встроенных промышленных словарей и регулярных выражений, высокоэффективный OCR-модуль обеспечивает DeviceLock Discovery возможность обнаруживать и контролировать конфиденциальные данные, представленные в графической форме, предотвращая их утечку.

Высокая гибкость детектирования контента хранимых данных в DeviceLock Discovery достигается благодаря возможности задания комплексных правил, в которых множественные методы обнаружения текста, бинарных данных и типов данных с различными критериями соответствия могут комбинироваться с использованием логических операторов (И/ИЛИ/НЕ) для создания контентно-зависимых правил любой сложности и глубины.

Действия по устранению нарушений

В случае обнаружения в сканируемых объектах данных содержимого конфиденциального характера DeviceLock Discovery может в соответствии с заданной DLP-политикой автоматически выполнить следующие превентивные действия по устранению выявленных нарушений: удаление, гарантированное удаление, удаление контейнера/архива (если нарушение выявлено в файле внутри контейнера или архива), изменение прав доступа (только для файловой системы NTFS), протоколирование, тревожное оповещение администратора, оповещение локального пользователя, шифрование (только с использованием EFS в файловой системе NTFS).

Лицензирование

В соответствии с принципами гибкого функционально-инкрементального лицензирования комплекса DeviceLock DLP Suite, компонент DeviceLock Discovery может приобретаться и использоваться как самостоятельный продукт независимо от прочих компонентов комплекса. Лицензии на DeviceLock Discovery могут быть приобретены как на один из компонентов комплекса DeviceLock DLP Suite, дополняя уже имеющиеся компоненты DLP-системы. Возможен и обратный порядок, когда пользователи, изначально использующие только лицензии DeviceLock Discovery, могут расширить уровень DLP-защиты корпоративных данных за счет приобретения лицензий на другие функциональные компоненты DeviceLock DLP Suite. При первичном приобретении лицензий на все компоненты комплекса DeviceLock DLP Suite в целом, включая DeviceLock Discovery, предусмотрена существенная скидка.

Техническая спецификация

Инфраструктурные (инсталлируемые) компоненты

- DeviceLock Discovery Server (компонент DeviceLock Content Security Server)
- DeviceLock Discovery Agent
- DeviceLock Agent (при использовании совместно с DeviceLock Endpoint DLP)
- Консоли управления: DeviceLock Management Console (MMC-оснастка) или DeviceLock WebConsole с поддержкой Apache

Цели сканирования

- Рабочие станции и серверы Windows (файловая система, репозитории электронной почты, подключенные периферийные устройства), общие сетевые ресурсы, сетевые хранилища

Обнаруживаемые данные

- **Контролируемые виды данных:** 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
- **Оптическое распознавание символов (OCR):** резидентный OCR модуль с распознаванием 30+ языков, включая русский, с поддержкой перевернутых/ зеркалированных/ инвертированных изображений

Режимы сканирования

- Агентское, удаленное (без агента), гибридное, ручной и автоматический (в соответствии с расписанием)

Действия по устранению нарушений

- Удаление, гарантированное удаление, удаление контейнера (если нарушение выявлено внутри контейнера), задание прав доступа (для файловой системы NTFS), протоколирование, оповещение администратора, оповещение локального пользователя, шифрование (для EFS в файловой системе NTFS)

Прочее

- Статическое и динамическое формирование списка сканируемых целей, графические отчеты, автоматическая установка и удаление агента

Системные требования

- **DeviceLock Discovery Server:** Windows Server 2003-2019 (32/64-бита), Microsoft RDS, Citrix XenServer, VMware vSphere Desktop; 2xCPU Intel Xeon Quad-Core 2.33 Гц, память 8 Гб, диск 800 Гб; SQL Express или MS SQL Server 2005-2017
- **Агенты:** Windows 2000/XP/Vista/7/8/8.1/10/Server 2003-2019 (32/64-бита); Microsoft RDS, Citrix XenDesktop/XenApp, Citrix XenServer, VMware Horizon View; VMware Workstation, VMware Player, Oracle VM VirtualBox, Windows Virtual PC; 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

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

[www.devicelock.com/ru]