DeviceLock DLP
Proactive Endpoint Security

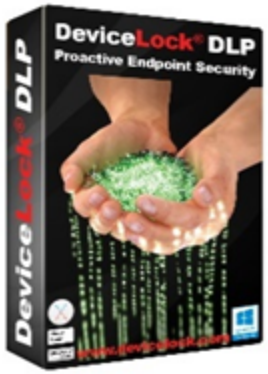
Контроль сетевых коммуникаций в гибридной DLP-системе

Сценарии использования DeviceLock EtherSensor

СЕРГЕЙ ВАХОНИН
Директор по решениям
Смарт Лайн Инк / DeviceLock, Inc.
EMAIL SV@DEVICELOCK.COM

АО Смарт Лайн Инк
Москва, 12/2018

DeviceLock – больше 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

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 DLP

Клиент	Количество сотрудников	Объем внедрения (количество агентов)
Vodafone, Индия	>50000	28500
Банк России (ЦБ), РФ	>60000	>10000
Metro C&C Group, Германия	>10000	10500
HONG KONG POLICE FORCE, Гонконг	>30000	16000
Best Buy, США/Канада	>30000	15000
Промсвязьбанк, РФ	>10000	5000

Крупнейшие клиенты DeviceLock DLP – крупные предприятия, проходящие аудит на предмет соблюдения безопасности обработки конфиденциальных корпоративных и персональных данных, правительственные учреждения, обрабатывающие секретную информацию, нуждающиеся в защите корпоративных данных, предотвращении утечек данных и контроле их использования и перемещения.

##	Государство / регион
1	Российская Федерация и СНГ
2	Япония
3	Германия
4	США и Канада
5	Великобритания
6	Китай и Гонконг
7	Ближневосточный регион (ОАЭ, Оман, Кувейт)

География использования DeviceLock

Технологии DLP - для **предотвращения** утечек данных

Какие глобальные задачи призваны решать 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
- Блокирование утечек == остановка (intercept) недопустимых попыток передачи данных

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

Обеспечение соответствия требованиям стандартов 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 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

DeviceLock DLP – настоящее DLP

DeviceLock DLP

ПРЕДОТВРАЩЕНИЕ УТЕЧЕК ДАННЫХ и МОНИТОРИНГ СОБЫТИЙ

в режиме реального времени, в любых сценариях!

...устройства и интерфейсы

...каналы сетевых коммуникаций

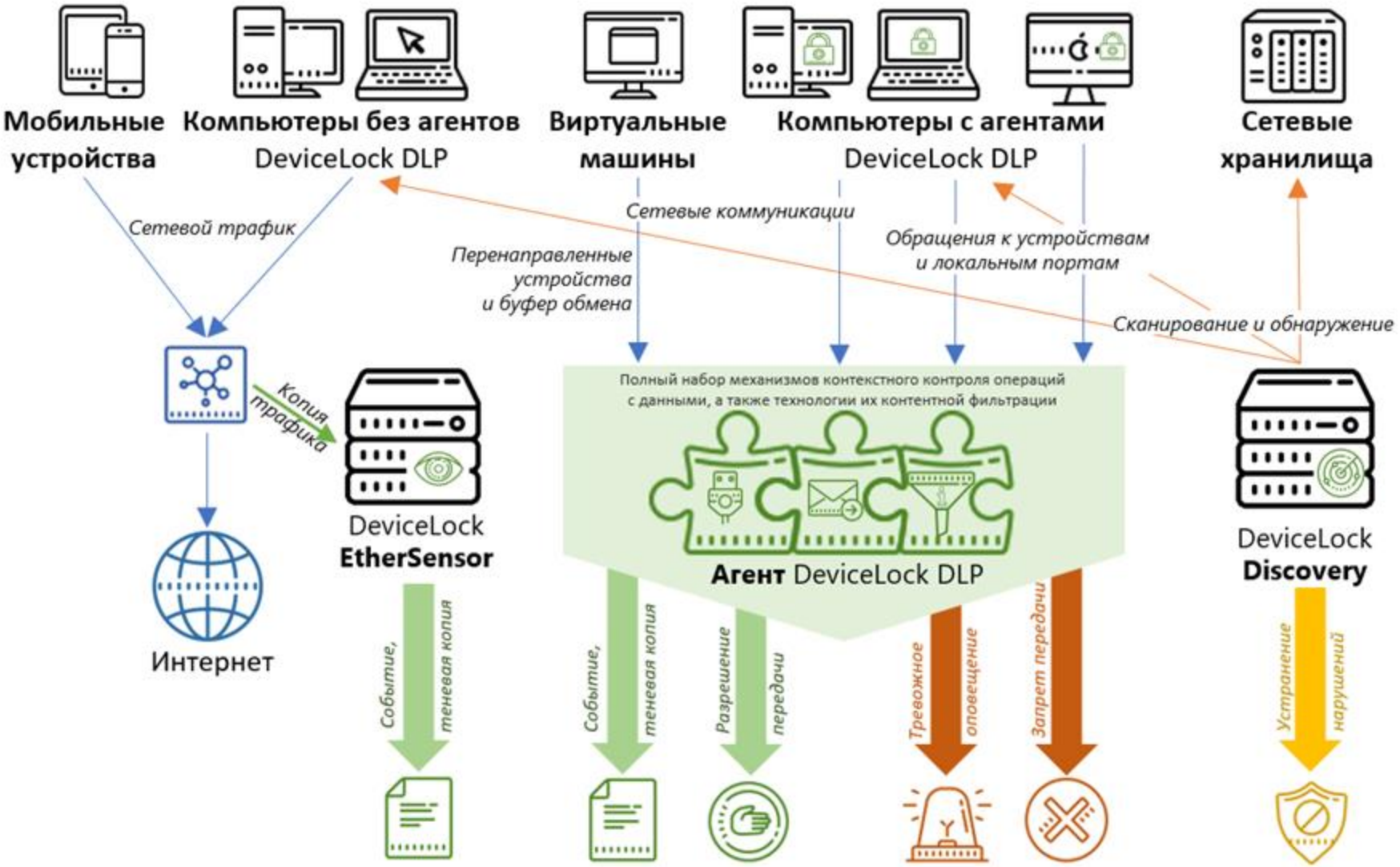
...с применением технологий контентной фильтрации

в режиме реального времени

+ сканирование хранимых данных

+ собственный поисковый сервер

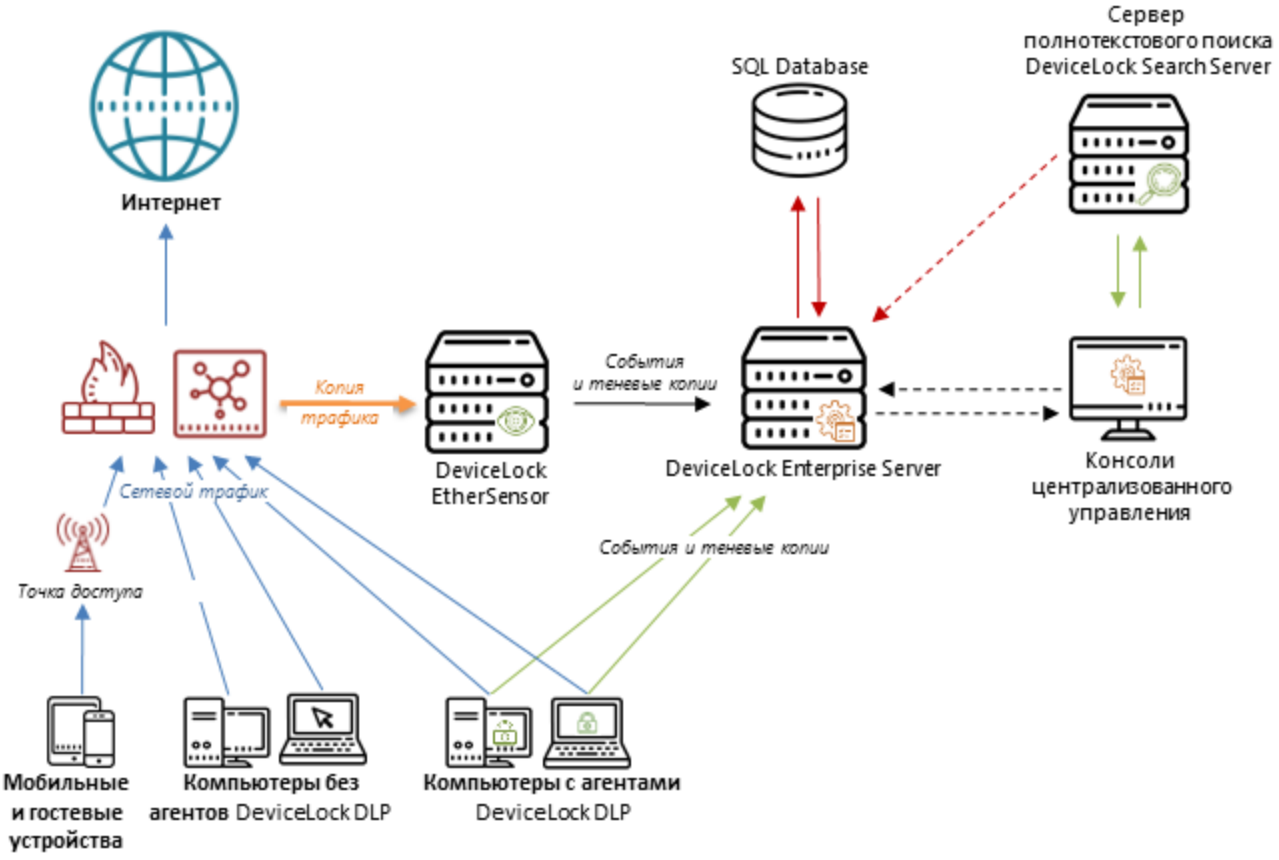
DeviceLock DLP в одной картинке



Архитектура гибридной DLP-системы DeviceLock DLP

Гибридная DLP-система эффективно решает сразу несколько проблем и задач, стоящих перед службами информационной безопасности – мониторинга сетевого трафика с компьютеров и мобильных устройств, на которых по техническим причинам невозможно установить или эксплуатировать DLP-агент, либо снижения нагрузки на рабочие станции пользователей за счет раздельного контроля различных сетевых сервисов и протоколов на разных уровнях.

Автоматическое переключение различных комбинаций DLP-политик для контроля сетевого трафика в агенте DeviceLock DLP в зависимости от наличия подключения к корпоративной сети и/или корпоративным серверам позволяет обеспечить чрезвычайно гибкий контроль пользователей, когда, например, на уровне агента при нахождении лэптопа в офисе сохраняется контроль устройств, принтеров и особо критичных сетевых приложений и сервисов, в том числе с применением контентной фильтрации в режиме реального времени, а контроль и инспекция других сетевых протоколов и сервисов возлагается на сервер EtherSensor.



Журналирование, теневое копирование, отчеты и полнотекстовый поиск

DeviceLock Enterprise Server

- *Нелицензируемый компонент*
- Централизованное **управление** агентами и политиками
- Централизованный **сбор журналов** и данных теневого копирования
  - Мульти-серверная архитектура
  - Контроль пропускной способности и переключение между серверами агентом
  - Профилирование трафика и сжатие данных для их оптимальной доставки
  - Централизованное хранение данных в базе данных SQL
- **Мониторинг** статуса агентов и целостности политик
- Настраиваемые встроенные **статистические отчеты**

DeviceLock Search Server

- *Опциональный компонент*
- Облегчает аудит журналов и теневых копий, поиск и выявление инцидентов безопасности
- Обеспечивает полнотекстовый поиск в центральной базе данных аудита и теневого копирования
  - Более 160 поддерживаемых форматов файлов и архивов, фильтрация основных и неучитываемых слов, булева логика поиска и многое другое
- Автоматический запуск поисковых запросов с по расписанию с поддержкой инкрементального поиска и автоматической отправкой результатов поиска по электронной почте
- Встроенный OCR модуль

Endpoint-агент – ключевой компонент комплекса DeviceLock DLP

DEVICELOCK DLP

- DEVICELOCK **ENDPOINT DLP SUITE**
  - DEVICELOCK
  - NETWORKLOCK
  - CONTENTLOCK
  - SEARCH SERVER
- DEVICELOCK **DISCOVERY**

Агент
DeviceLock DLP

DeviceLock Base
Контекстный контроль периферийных устройств, локальных портов и интерфейсов

NetworkLock
Контекстный контроль каналов сетевых коммуникаций

ContentLock
Контентный анализ и фильтрация в реальном времени

Endpoint-Агент
DeviceLock DLP

Анализ попытки передачи данных с принятием решения о разрешении или запрете и других видах реакции

Данные

Контекстный контроль устройств, портов и интерфейсов

Контроль по контекстным параметрам

Кто? Что? Когда? Куда? Как?

Контентная фильтрация

в реальном времени

Инспекция контента

Содержимое?

Принятие решения на основании анализа содержимого

Контекстный контроль каналов сетевых коммуникаций

Разрешение передачи

Событие, теневая копия

Тревожное оповещение

Запрет передачи

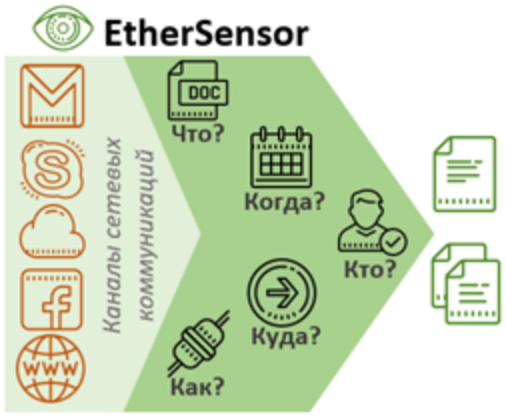
Мониторинг сетевого трафика: сервер DeviceLock EtherSensor

DeviceLock EtherSensor

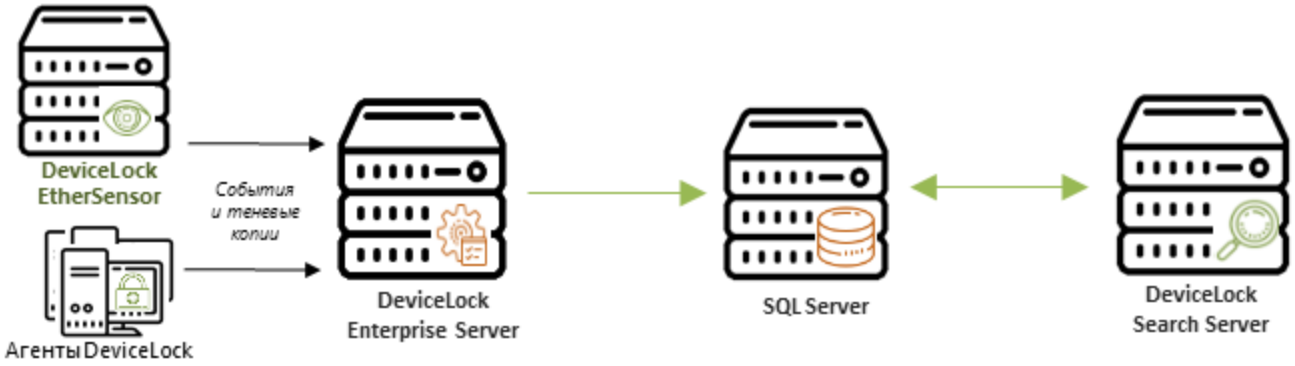
- *Самостоятельный компонент комплекса*
- перехват зеркалированного сетевого трафика канального уровня;
- анализ перехваченного (зеркалированного) трафика для извлечения из него полезных объектов уровня приложения (объекты, их контент, события и т.д.);
- сохранение результатов анализа в базе данных сервера DeviceLock Enterprise Server.

Сервер EtherSensor позволяет протоколировать сетевые события и передаваемые по сети сообщения и файлы, не задействуя при этом агенты DeviceLock, в целях контроля использования внутрикорпоративной и внешней электронной почты (включая входящую почту), веб-почты, социальных сетей, широкого ряда мессенджеров, сервисов поиска работы, форумов и блогов. Также перехватываются и протоколируются передача файлов по протоколам HTTP, FTP и в облачные хранилища. Перехваченные данные сохраняются в базе данных в DeviceLock DLP для последующего хранения и анализа, включая возможности полнотекстового поиска с помощью DeviceLock Search Server.

EtherSensor функционирует без использования агентов DeviceLock, устанавливаемых на рабочих станциях для реализации других функций DLP-контроля. Высокая производительность EtherSensor позволяет использовать серийное серверное оборудование или среду виртуализации для анализа больших потоков данных (гигабиты в секунду без потери пакетов) при достаточно низких системных требованиях. EtherSensor работает в пассивном режиме получения сетевого трафика, следовательно, никак не воздействует на сетевую инфраструктуру и не требует ее изменения, кроме необходимости отведения копии сетевого трафика с помощью зеркалирования трафика или сетевого ответвителя на EtherSensor.



***Единая база событий и теневых копий**, наполняемая как данными с EtherSensor, так и данными с агентов DeviceLock, позволяет выявлять инциденты информационной безопасности для широчайшего спектра потенциальных каналов утечки данных.*



EtherSensor: контролируемые сетевые коммуникации

Входящая и исходящая веб-почта: выделение из трафика методом пассивного перехвата входящих и исходящих сообщений служб веб-почты: Mail.RU, Yandex.RU, Pochta.RU, GMail и т.п.(40+ доменов), а также сервисов на популярных webmail-движках.

Электронная почта: выделение из трафика методом пассивного перехвата сообщений электронной почты, передаваемых по протоколам SMTP, POP3 и IMAP4.

Социальные сети: выделение из трафика методом пассивного перехвата сообщений разных типов (авторизация, сообщения, комментарии и т.п.) в социальных сетях и на форумах: Facebook, LinkedIn, Vk.com, Odnoklassniki, Mamba.ru, phpbb, ipb, vbulletin, mybb, а также SMS/MMS-сообщения пользователей, отправляемые через специализированные веб-сервисы (500+ доменов).

Протоколы и службы передачи файлов: выделение из трафика методом пассивного перехвата файлов, передаваемых по протоколам HTTP, FTP, SMB/CIFS и WebDAV.

Сервисы мгновенных сообщений: выделение из трафика методом пассивного перехвата сообщений, отправляемых и получаемых через службы мгновенных сообщений, работающие по протоколам IRC, MSN, XMPP/Jabber, MRA, YAHOO и OSCAR (ICQ, Skype, Google Hangout, Mail.ru Агент и т.п.).

Сервисы поиска работы: выделение из трафика методом пассивного перехвата сообщений, вакансий, откликов и других событий сервисов вакансий и поиска работы, таких как HH.ru, SuperJob.ru, Job.ru и т.п. (150+ доменов).

Почтовая служба IBM (Lotus) Notes: выделение из трафика методом пассивного перехвата сообщений, вакансий, откликов и других событий сервисов вакансий и поиска работы, таких как HH.ru, SuperJob.ru, Job.ru и т.п. (150+ доменов).

Источники данных для EtherSensor

Сетевые интерфейсы физического или виртуального сервера EtherSensor подключаются к Mirror-порту (SPAN, rx и tx пакеты) для прослушивания трафика с критичных устройств или целых сегментов сети. Аналогично настраивается интеграция с решениями класса NGFW, способными расшифровывать SSL/TLS (PaloAlto Networks, FortiGate, и т.д.), когда копия расшифрованного SSL-трафика направляется на сетевой интерфейс EtherSensor для анализа.

Прокси-серверы при условии ICAP-интеграции, имеющие возможность расшифровки HTTPS-трафика и передачи результатов по ICAP в EtherSensor (Blue Coat SG, Cisco WSA, SQUID и т.д).

PCAP-файлы на файловой системе. EtherSensor периодически опрашивает каталог на предмет появления новых PCAP-файлов с записанным трафиком. При обнаружении такие файлы немедленно обрабатываются и анализируются EtherSensor.

Lotus Notes Transaction Log для получения всех сообщений, проходящих через почтовую систему IBM (Lotus) Notes. Также производится обнаружение почтовых сообщений Lotus Notes в обрабатываемом трафике.

Плагин для сервера Microsoft Skype for Business (Lync) с ролью Edge, отправляющий копию переписки на сервер EtherSensor.

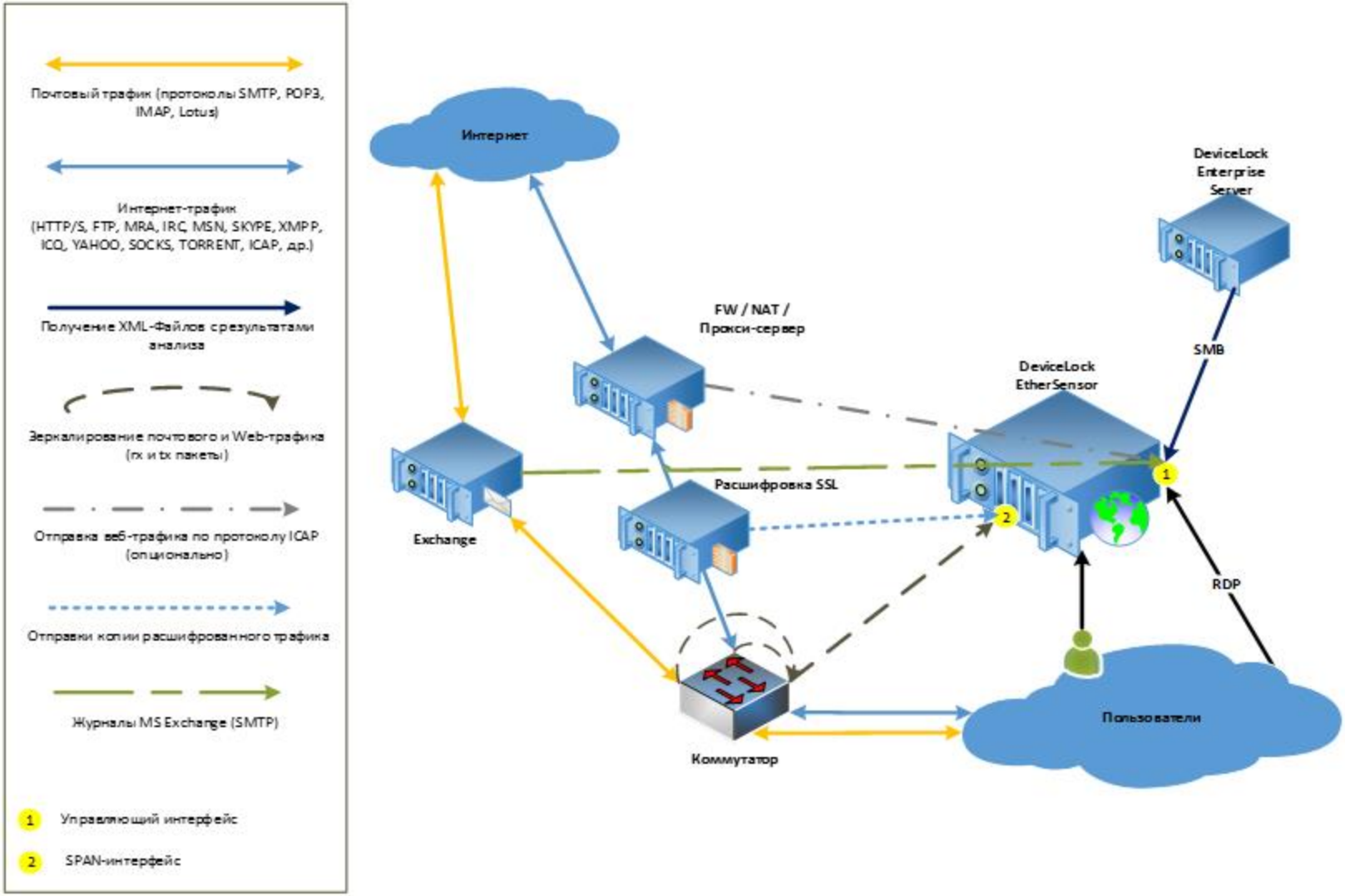
Сервер EtherSensor реконструирует и анализирует объекты трафика, начиная с уровня 2 модели OSI и до уровня 7 – объекты, специфические для определённого приложения, пользователя и Интернет-сервиса. Количество поддерживаемых сервисов превышает несколько тысяч.

Полученные в результате перехвата данные проходят предварительную фильтрацию с целью исключения заведомо неинтересного или мусорного трафика с использованием технологии Berkeley Packet Filter (BPF), которая позволяет предоставлять для дальнейшего анализа данные именно из тех сегментов сети, которые востребованы службой ИБ.

Для решения задачи анализа SSL/TLS трафика EtherSensor может использовать программный компонент SSLSplitter или стороннее решение, имеющее функцию расшифровки SSL, например, методом MITM. Кроме того, встроенный ICAP-сервер позволяет серверу EtherSensor взаимодействовать с ICAP-клиентами, обрабатывающими HTTPS-трафик.

SSLSplitter устанавливается “в разрыв” сети на периметре организации, функционируя на физическом или виртуальном сервере. SSLSplitter работает по принципу подмены сертификатов (Man-In-The-Middle). SSL-соединения определяются не по порту назначения соединения, а с использованием сигнатур.

Как работает EtherSensor



Сценарии использования EtherSensor в гибридной DLP-системе DeviceLock DLP

1 Мониторинг сетевого трафика при невозможности использовать endpoint-агенты.

Решение задачи контроля сетевого трафика обеспечивается перехватом и анализом трафика на уровне сети – прослушиванием трафика с зеркальных портов сервера, интеграцией с NGFW-устройствами и прокси-серверами, другими методами, не требующими установки агента на рабочих станциях, что с успехом обеспечивается сервером EtherSensor. При этом задача DLP-контроля периферийных устройств и портов рабочих станций выполняется агентом DeviceLock (на операционных системах Windows и MacOS), а в базе данных сервера DeviceLock Enterprise Server для централизованного анализа собираются события и данные как от EtherSensor в части объектов сетевого трафика, так и от агентов DeviceLock в части контроля устройств.

2 Мониторинг сетевых коммуникаций при недопустимости блокировки передачи данных по сети.

Традиционная сетецентричная DLP-система Enterprise-уровня, способная отслеживать и анализировать трафик на очень больших потоках (вплоть до анализа трафика от сотен тысяч сотрудников) с низкими затратами на развертывание и текущую эксплуатацию, а также незначительными требованиями по техническому оснащению. Контроль доступа к локальным портам и интерфейсам, периферийным устройствам выполняется агентами.

3 Раздельный контроль сетевых коммуникаций в зависимости от подключения к корпоративной сети.

Автоматическое переключение различных комбинаций DLP-политик для контроля сетевого трафика (различных комбинаций правил и параметров контроля) в агенте DeviceLock DLP в зависимости от наличия подключения к корпоративной сети и/или корпоративным серверам позволяет обеспечить чрезвычайно гибкий, раздельный контроль сетевых коммуникаций пользователей, когда, например, на уровне агента при нахождении лэптопа в офисе сохраняется контроль особо критичных сетевых приложений и сервисов, в том числе с применением контентной фильтрации в режиме реального времени в целях предотвращения утечки конфиденциальной информации, а инспекция других сетевых протоколов и сервисов возлагается на модуль EtherSensor.

Сценарии использования EtherSensor в гибридной DLP-системе DeviceLock DLP

4 Селективный контроль по типам сетевых коммуникаций.

Критическая часть сетевых приложений, рассматриваемых как потенциальные каналы утечки конфиденциальных данных (например, мессенджеры с возможностью передачи файлов), равно как и локальные порты и устройства, контролируются агентом DeviceLock. Процессы передачи данных ограниченного доступа (также на уровне агента, «в разрыв») подвергаются в режиме реального времени анализу содержимого с принятием решений о допустимости передачи, либо о создании теневой копии для значимых для целей расследования инцидентов, либо о направлении тревожного оповещения по факту срабатывания DLP-правила.

Контроль прочих сетевых коммуникаций, рассматриваемых как имеющие меньшую степень риска с точки зрения противодействия утечки данным (когда для решения задач информационной безопасности достаточно мониторинга и анализа переданных данных, например, для серфинга веб-сайтов и сервисов поиска работы) выполняется сервером EtherSensor посредством перехвата и анализа сетевого трафика на уровне периметра.

«Мониторинг всего трафика (EtherSensor) + Селективная блокировка недопустимых попыток (агент DeviceLock DLP)» - качественный баланс возможностей и рисков: риски, связанные с блокировкой, делегируются агентам на защищаемых компьютерах, а задачи мониторинга сетевого трафика и детектирования событий безопасности по всей сети в целом поручаются серверу EtherSensor.

5 Избирательный контроль пользователей и компьютеров.

Полнофункциональные агенты DeviceLock выполняют непосредственно и только на защищаемых рабочих станциях все DLP-функции (контроль доступа, протоколирование, тревожные оповещения) и только для указанных пользователей и групп пользователей. Сетевая активность пользователей и групп, которым для выполнения бизнес-задач требуется свободный доступ к различным каналам сетевых коммуникаций, отслеживается сервером EtherSensor посредством перехвата и анализа сетевого трафика на уровне периметра.

Наиболее продуктивный вариант для контроля так называемых групп риска, когда на агентах DeviceLock создаются специальные наборы политик для DLP-контроля различных учетных записей, а переключение применяемых политик выполняется в реальном времени путем включения таких пользователей в группу пользователей, соответствующих той или иной группе риска.

Демонстрация DeviceLock EtherSensor

Некоторые сценарии применения гибридной DLP-системы DeviceLock DLP

ИЛЬШАТ ЛАТЫПОВ

Инженер-аналитик

Смарт Лайн Инк

Мониторинг передачи данных по протоколам FTP и SMB

Использование FTP и SMB разрешено для всех пользователей

Задача: журналирование передачи файлов.

Доступ предоставляется всем пользователям и группам

Журналирование передачи файлов на серверном уровне

Ограничение доступа в социальные сети для группы риска

Допускается использование социальных сетей для всех пользователей, за исключением группы риска.

Задача: Селективный контроль доступа к социальным сетям.
Создание архива данных, передаваемых через социальные сети.

Запрет доступа к социальным сетям для пользователей группы риска

Создание теневых копий на уровне сервера

Контроль независимо от используемого браузера

Ограниченное использование Skype и web-почты

Использование сервисов web-почты разрешено всем без ограничений.
Использование Skype разрешено всем пользователям, но не допускается передача документов финансового характера.

Задача:

1. Блокировать передачу финансовых документов через Skype.
2. Журналирование всех фактов переписки и отправки файлов через Skype и web-почту, с созданием теневой копии.
3. Информирование пользователя о запрете передачи документа с конфиденциальным содержимым.

Доступ предоставляется всем пользователям

Контроль текстового содержимого (контентная фильтрация) передаваемых через Skype данных на агенте

Создание записи в логе, теневой копии
(Skype от агента, Web-почта на уровне сервера)

Вывод сообщения о запрете передачи файла в системном трее

Контроль почтовой переписки с мобильных устройств

Использование корпоративной почты на мобильных устройствах разрешено для всех пользователей, но должно журналироваться.

Задача: журналирование передачи сообщений электронной почты и вложений, отправляемых с корпоративных адресов.

Доступ предоставляется всем пользователям

Журналирование передачи файлов и сообщений на серверном уровне (интеграция с почтовым сервером)

Контроль электронной почты в зависимости от местонахождения ПК

Допускается использование SMTP для всех пользователей внутри корпоративной сети, за пределами организации почтовая переписка запрещена.

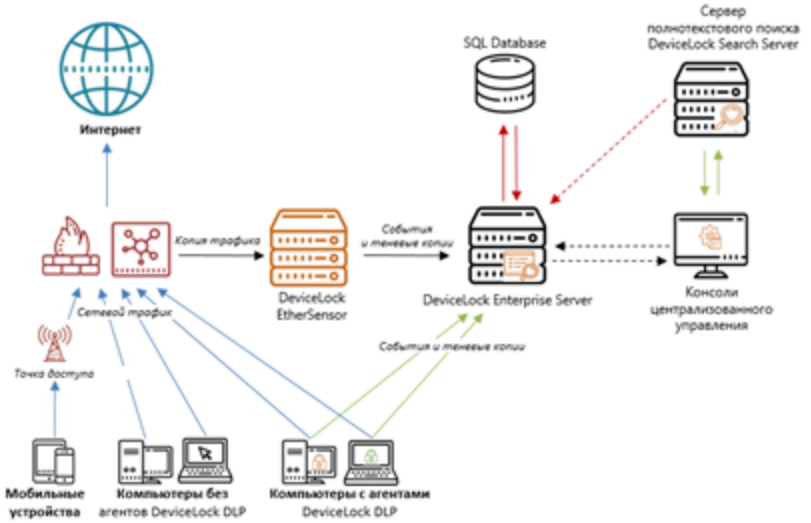
Задача: блокировка почтового протокола SMTP на ПК при отключении от корпоративной сети.

Контроль использования SMTP независимо от наличия подключения к корпоративной сети, с автоматической сменой политики контроля.

Создание теневой копии на уровне серверного перехвата

Контроль независимо от используемого почтового клиента

СПАСИБО
ЗА ВНИМАНИЕ!



www.DeviceLock.com