КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

DeviceLock DLP
Proactive Endpoint Security

Как защитить персональные * данные от утечки?

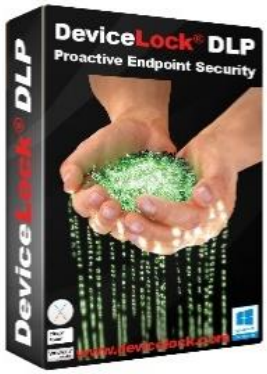
DeviceLock DLP - самый эффективный инструмент!

* … не только персональные!

СЕРГЕЙ ВАХОНИН
Директор по решениям
Смарт Лайн Инк
SV@DEVICELOCK.COM

АО Смарт Лайн Инк
2019

АО «Смарт Лайн Инк»



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 клиентов при более чем 7 000 000 инсталляций по всему миру за 20+ лет работы

DeviceLock – география использования

ЧТО ТАКОЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ?

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) *

Personally identifying information (PII) - имена и фамилии людей, даты рождения, места регистрации, адреса электронной почты, номер паспорта, налоговые идентификаторы (ИНН) и прочая подобная информация

Sensitive personal information (SPI) - конфиденциальные персональные данные, например медицинские записи и истории болезней, биометрические данные, финансовая информация, прочие чувствительные данные.

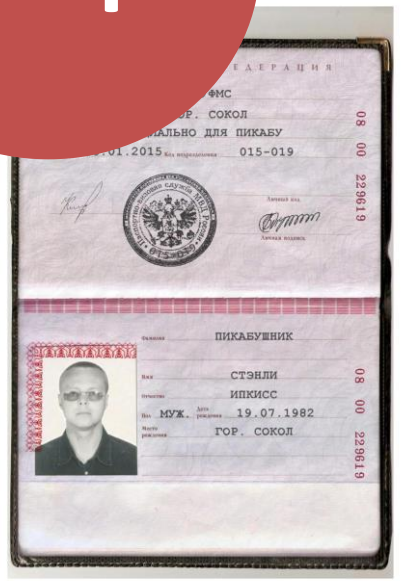
* Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ

ПРОДАЖА ПЕРСОНАЛЬНЫХ ДАННЫХ

«Базы персональных данных в формате Excel, содержащие ФИО, пол, телефон, полные паспортные данные, СНИЛС, адрес регистрации и проживания за 2017-2018 гг. реализуются **по 20-25 копеек за одну запись**.

Скан паспорта и фотография владельца паспорта с паспортом продаются по цене от 150 рублей за комплект, а комплект из сканов паспорта, СНИЛС, прав и ИНН - по цене **от 300 рублей**.

300 р.



«Ценность персональных данных без сканов документов невелика, так как они применяются в основном для спама и телефонного мошенничества»

«Сканы документов могут быть использованы для получения онлайн-займов и поэтому весьма востребованы криминальными элементами»

«**Пробив**» - «Выписки по счету клиентов банков из Топ-10 предлагаются по цене **от 8 000 рублей за месяц**»

Источник: Исследование инсайдерских утечек данных, Смарт Лайн Инк
https://www.devicelock.com/ru/press/issledovanie-insajderskih-utechek-dannyh.html

ВИДЫ УТЕЧКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Утечки через фотографирование рабочих экранов составляют 10% от инсайдерской утечки персональных данных (зарегистрированные инциденты)

Источник: Исследование инсайдерских утечек данных, Смарт Лайн Инк
https://www.devicelock.com/ru/press/issledovanie-insajderskih-utechek-dannyh.html

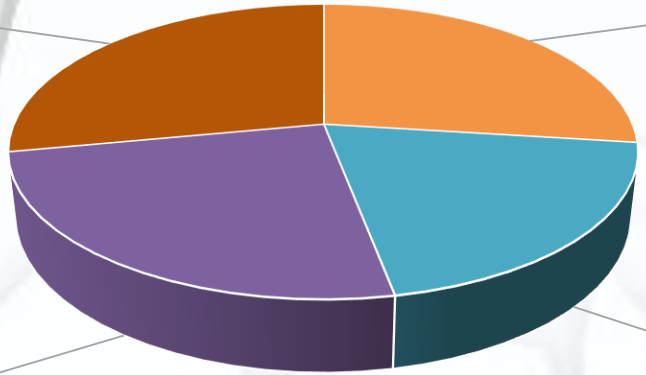
БОЛЬШИНСТВО УТЕЧЕК ДАННЫХ - ИНСАЙДЕРСКИЕ

Аналитический отчет Ponemon Institute : “2018 Cost of Data Breach Study”

- Ошибки сотрудников являются причиной около 27% утечек данных
- Большинство из 48% уязвимостей, связанных с вредоносным ПО или криминальными атаками, используют злоумышленников-инсайдеров или фишинг и социальную инженерию

Опрос “Data Protection Risks & Regulations in the Global Economy”

Недобросовестные сотрудники и злоумышленники – ключевая причина утечек данных в 69% опрошенных организаций



Источники: - Ponemon Institute LLC, Июль 2018 :
Опрос “Data Protection Risks & Regulations in the Global Economy”, Отчет “2018 Cost of Data Breach Study: Global Overview”

«АЙСБЕРГ» УТЕЧЕК ДАННЫХ

Самая значительная по агрегатному ущербу часть утечек данных происходит там, где информация чаще всего **создается, используется и хранится**:
на персональных компьютерах, рабочих станциях и мобильных устройствах обычных пользователей корпоративных информационных систем.

ЧЕМ ПРОЩЕ СЦЕНАРИЙ УТЕЧКИ ДАННЫХ – ТЕМ БОЛЕЕ ОН ВЕРОЯТЕН

Использование сотрудниками любых ИТ-сервисов и устройств, доступных на персональном уровне и не требующих обслуживания корпоративными службами ИТ – наиболее простой и вероятный сценарий утечки данных

Отсутствие фокуса на безопасности

Практически все сетевые приложения (социальные сети, облачные хранилища, мессенджеры), созданные для удобства пользователей, для удовлетворения их социальных потребностей – функционируют абсолютно без какой-либо обратной связи с инструментарием корпоративной безопасности.

Решения принимаются пользователем

Модель информационной безопасности потребительских приложений основывается на том, что все решения о способах и уровне авторизации, аутентификации и уровне доступа к данным принимает конечный пользователь – который далеко не всегда является владельцем данных, будучи при этом сотрудником организации.

Про личные устройства и говорить нечего....

DATA LEAK (loss) PREVENTION (protection) = ПРЕДОТВРАЩЕНИЕ УТЕЧЕК ДАННЫХ

DLP-система - ИТ-решение, обеспечивающее **выявление**, **отслеживание** и **предотвращение неавторизованного использования, хранения и перемещения** данных ограниченного доступа и др., используемых в организации

Обнаружение данных в хранилищах

Отслеживание перемещения данных

Защита от утечки по сети и через устройства

Defining DLP

Even a decade on, there is still little consensus on what actually compromises a DLP solution. Some people consider encryption or USB port control to be DLP, while others limit the term to complete product suites focused on analyzing and enforcing content usage policies. Securosis defines DLP as:

Products that, based on central policies, identify, monitor, and protect data at rest, in motion, and in use, through deep content analysis.

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

Full-suite solutions provide complete coverage across your network, storage repositories, and endpoints, even if you aren't using their full capabilities.

Источник: 'Understanding and Selecting a Data Loss Prevention Solution', Securosis Whitepaper, 2018, v.3

ПРИНЦИПЫ ПОЛНОЦЕННОГО КОНТРОЛЯ КАНАЛОВ ПЕРЕДАЧИ ДАННЫХ

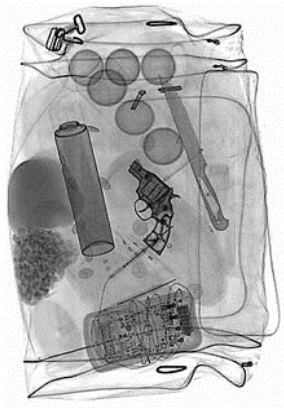
Автоматическое принятие решений о возможности передачи/печати/сохранения на основе двух взаимодополняющих методов

Контекстный контроль

- Пользователь, его права, группы
- Дата и время
- Местонахождение
- Источник / адресат
- Тип файла / данных
- Использование шифрования данных
- Направление передачи данных
- Информация об устройстве / веб-сервисе

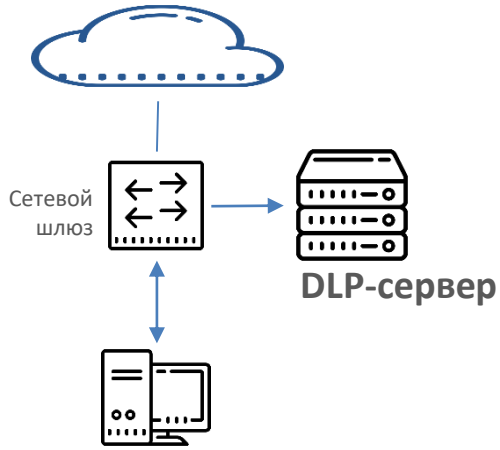
Контентный анализ и фильтрация (проверка содержимого)

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



СЕТЕВЫЕ АРХИТЕКТУРНЫЕ РЕШЕНИЯ DLP-СИСТЕМ

Мониторинг сетевого трафика



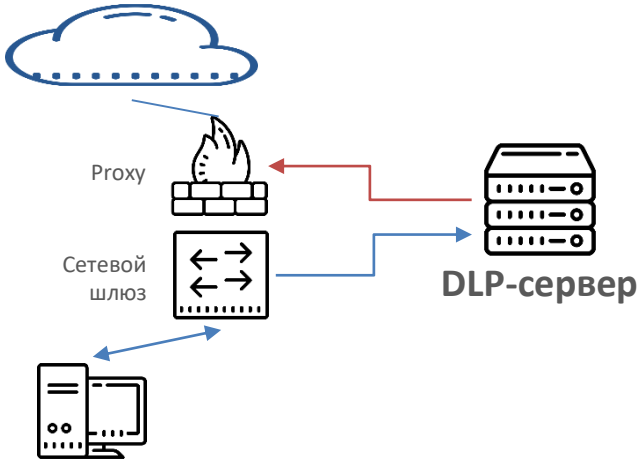
Плюсы

- Высокая производительность
- Возможность интеграции с почтовыми серверами
- Возможность анализа трафика с мобильных устройств

Минусы

- Невозможность анализа «закрытых» протоколов
- Перехват всего трафика целиком без разбора
- Риск позднего выявления утечки чувствительной информации
- Ограниченность внутренней сетью

Фильтрация сетевого трафика



Плюсы

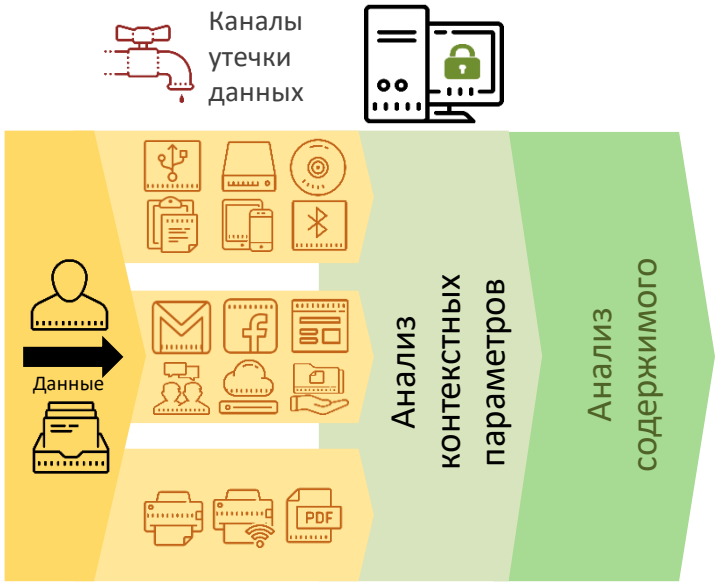
- Возможность фильтрации данных
- Возможность интеграции с почтовыми серверами
- Возможность анализа трафика с мобильных устройств

Минусы

- Проблема задержки трафика, его потери
- Ограниченность внутренней сетью
- Невозможность анализа «закрытых» протоколов
- Перехват всего трафика целиком без разбора

ENDPOINT-АРХИТЕКТУРА DLP-СИСТЕМ

Endpoint-агенты – неотъемлемая часть любой полнофункциональной DLP-системы



Ключевые возможности полноценного DLP-агента

- Сканирование хранимых данных на защищаемой рабочей станции
- Защита данных при операциях с устройствами
- Защита данных в сетевых коммуникациях
- Защита данных при операциях с системными функциями

Сценарии, когда DLP-агент – единственное решение

- Защита рабочей станции вне корпоративной сети
- Контроль конфиденциальной информации для всех каналов утечки данных, мониторинг использования конфиденциального контента
- Регулярное сканирование локальной файловой системы

Плюсы

- Возможность предотвращения утечки чувствительной информации в реальном времени
- Контроль рабочих станций внутри и вне корпоративной сети
- Возможность сбора дополнительных доказательств инцидента
- Контроль «закрытых» протоколов и сервисов
- Адресный контроль пользователей
- Отсутствие необходимости интеграции с почтовыми и proxy-серверами

Минусы

- Невозможность анализа трафика с мобильных устройств
- Дополнительная нагрузка на рабочие станции
- Дополнительные процедуры управления

КОГДА МОЖЕТ ВЫПОЛНЯТЬСЯ АНАЛИЗ СОДЕРЖИМОГО ФАЙЛОВ И ДАННЫХ? КОГДА ОБНАРУЖИВАТЬ ПЕРСОНАЛЬНЫЕ ДАННЫЕ?

ДО

Анализ **хранимых** данных (discovery)

ВО ВРЕМЯ

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

ПОСЛЕ

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

Последствия отсутствия механизма контентной фильтрации для всех каналов 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

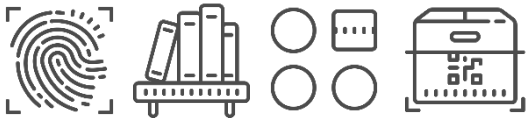
DeviceLock DLP

ПРЕДОТВРАЩЕНИЕ УТЕЧЕК ДАННЫХ

… все устройства и интерфейсы

…каналы сетевых коммуникаций

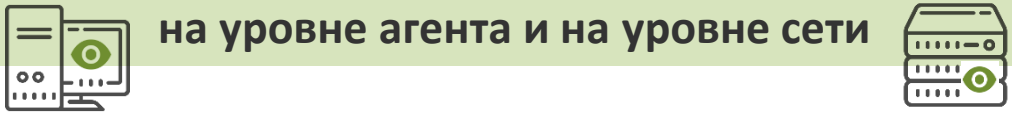
…с применением технологий контентной фильтрации



в режиме реального времени, в любых сценариях!

ДЕТАЛЬНЫЙ МОНИТОРИНГ СОБЫТИЙ

на уровне агента и на уровне сети



СКАНИРОВАНИЕ ХРАНИМЫХ ДАННЫХ

АНАЛИЗ АРХИВА: СЕРВЕР ПОЛНОТЕКСТОВОГО ПОИСКА

КОНТРОЛЬ КАНАЛОВ ПЕРЕДАЧИ ДАННЫХ В DEVICELOCK DLP

Контентная фильтрация данных и файлов <u>в реальном времени</u>:

- передаваемых в электронной почте и веб-почте; службах мгновенных сообщений, социальным сетях и передаваемых по сети файлов;
- в канале печати (печатаемых документах) и системном буфере обмена данными;
- в процессах сохранения данных на съемных носителях, в терминальных сессиях.

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 В РЕАЛЬНОМ ВРЕМЕНИ

Технологии контентной фильтрации

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

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

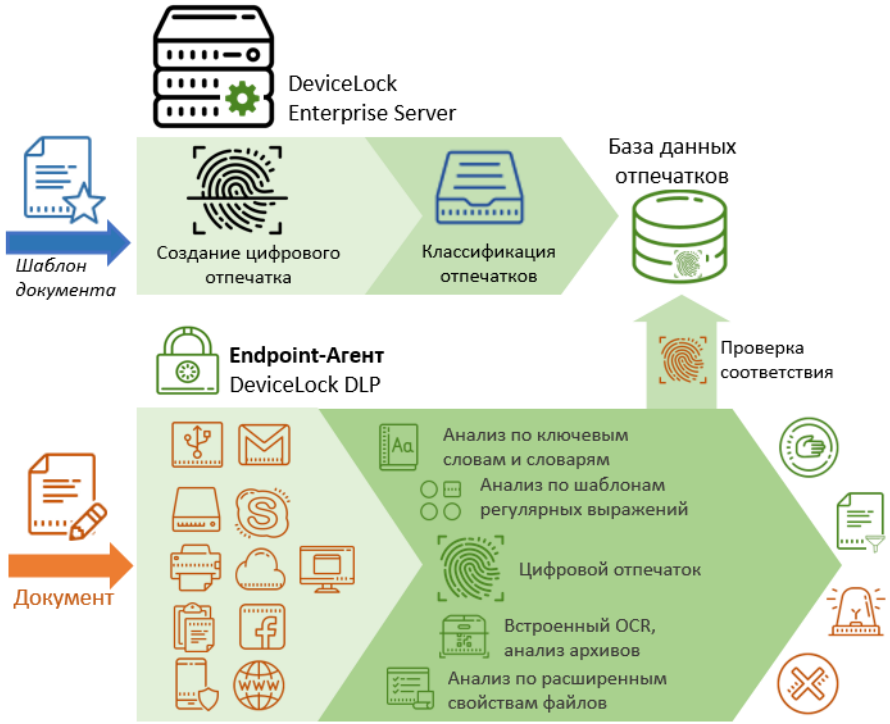
Встроенные промышленные и геоспецифичные терминологические словари.

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

Цифровые отпечатки (fingerprinting).

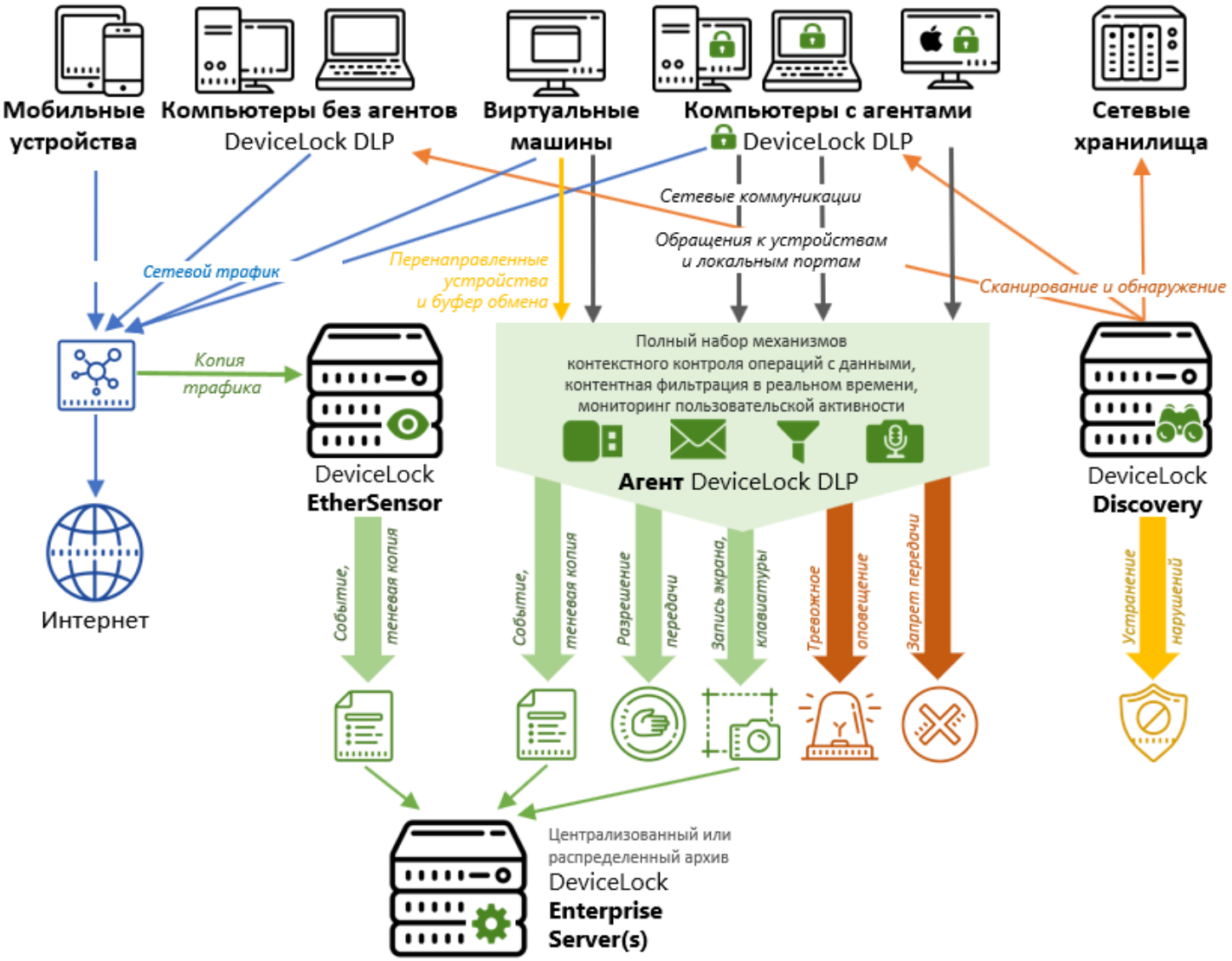
Встроенный модуль **оптического распознавания символов** (**OCR**).

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



КОГДА ОБНАРУЖИВАТЬ ПЕРСОНАЛЬНЫЕ и другие важные ДАННЫЕ?

DEVICELOCK DLP В ОДНОЙ КАРТИНКЕ



НОВОЕ В DEVICELOCK DLP - В БЛИЖАЙШЕМ БУДУЩЕМ

«**Карточки пользователей**», включая выявление аномалий для пользователя по его типичной активности в прошлом и текущей. Графики, связи и прочие UEBA-функции.

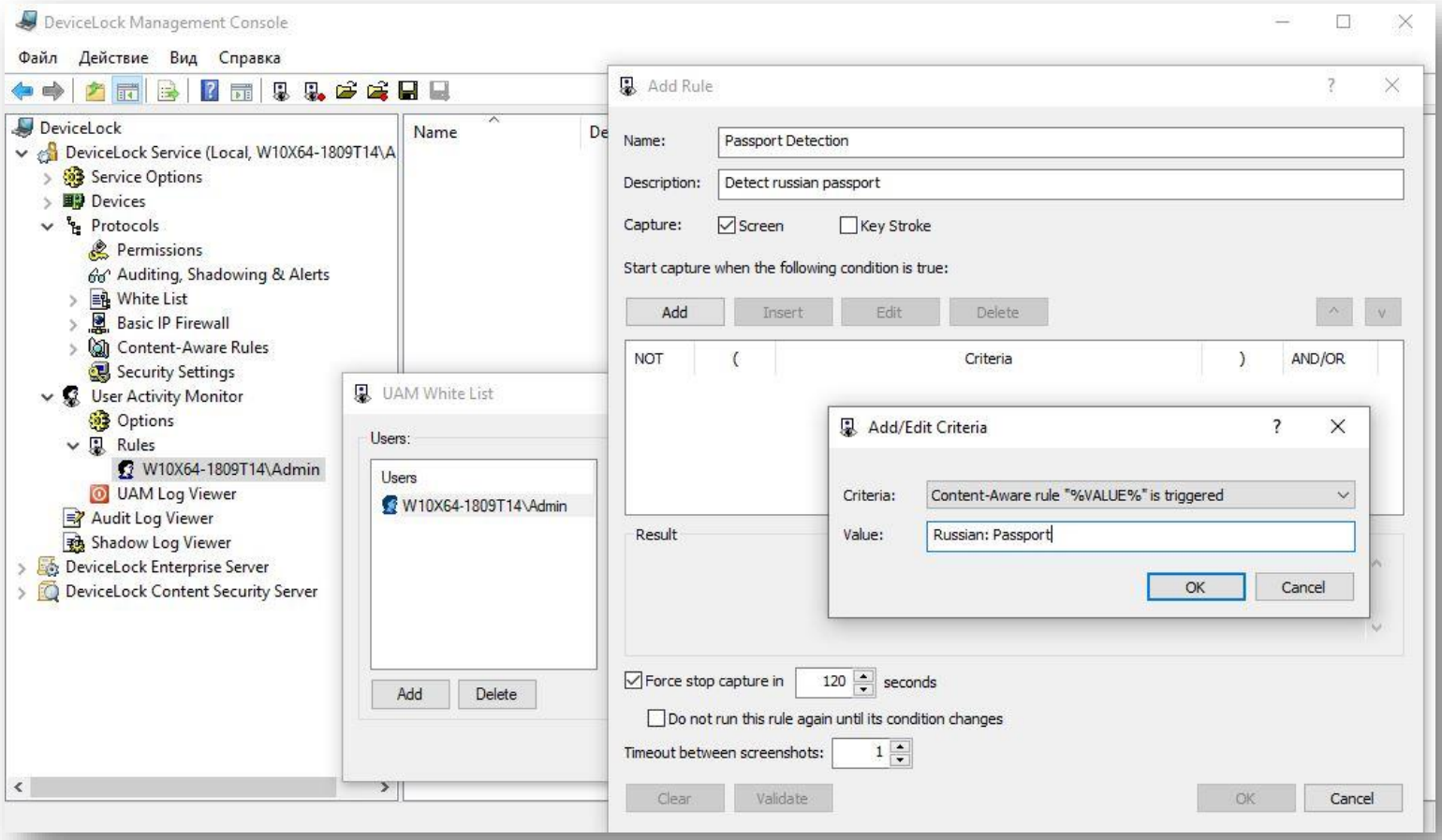
Развитие **DeviceLock Discovery** – сканирование и обнаружение данных на серверах SQL и noSQL, ElasticSearch баз с учетом накопленного нами опыта по нахождению незащищенных баз в Интернете...

Защита данных от фотографирования с экрана – возможность идентификации пользователя по фотографии экрана.

Модуль **User Activity Monitoring**: снимки и запись экрана, кейлоггер - **по триггерам**, включая правила анализа содержимого.

МОНИТОРИНГ ПОЛЬЗОВАТЕЛЬСКОЙ АКТИВНОСТИ

В ближайшей версии DeviceLock DLP 9 –
снимки и запись экрана, кейлоггер
- **по триггерам**, включая правила анализа содержимого!

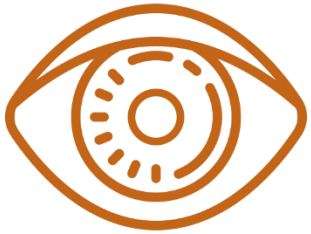


ЧТО В ИТОГЕ С ПЕРСОНАЛЬНЫМИ* ДАННЫМИ?

* И ДРУГИМИ ЗНАЧИМЫМИ ДЛЯ ОРГАНИЗАЦИИ ДАННЫМИ

Запрещать коммуникации и устройства?

Наблюдать за сотрудниками?



Защищать информацию!

Обнаружение данных в хранилищах

Отслеживание перемещения данных

Защита от утечки по сети и через устройства

#CODEIB

СПАСИБО
ЗА ВНИМАНИЕ!

СЕРГЕЙ ВАХОНИН
SV@DEVICELOCK.COM

www.DeviceLock.com