КОД ИБ ИТОГИ
МОСКВА 05 ДЕК'19

DeviceLock DLP
Proactive Endpoint Security

Как развивались DLP-системы в 2019 году?

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

Что такое DLP?

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.*

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

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

Мониторинг перемещения данных

Защита от утечки по сети и через устройства

КОГДА ОБНАРУЖИВАТЬ ПЕРСОНАЛЬНЫЕ и другие важные ДАННЫЕ?

КОНТЕНТНЫЙ АНАЛИЗ И ФИЛЬТРАЦИЯ ДАННЫХ

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 содержимому)

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 в реальном времени для всех каналов 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*
  ЛИБО
- *Мониторинг каналов передачи данных без возможности предотвратить утечку*

Основные функциональные группы для анализа

Обнаружение хранимых данных

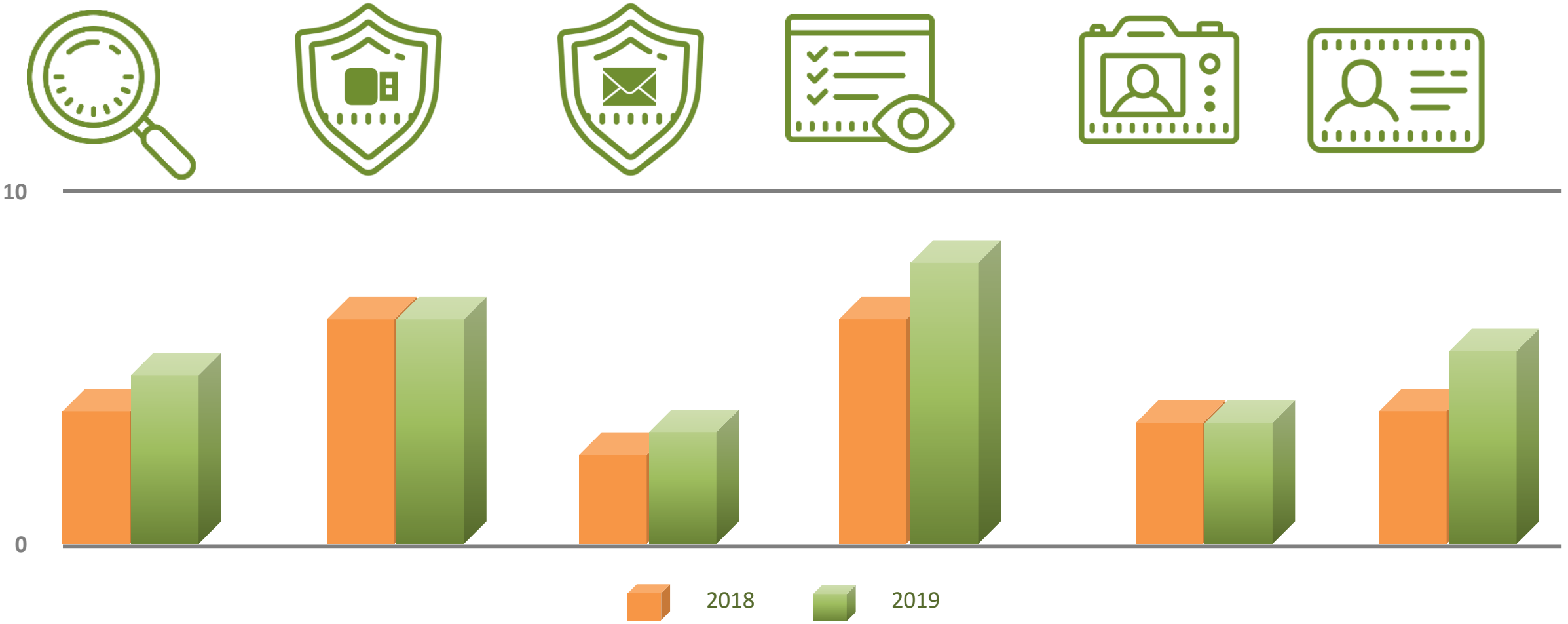
Защита от утечки через устройства

Защита от утечки по сети

Мониторинг перемещения данных

Мониторинг активности (UAM)

Аналитические функции (отчеты, UBA)



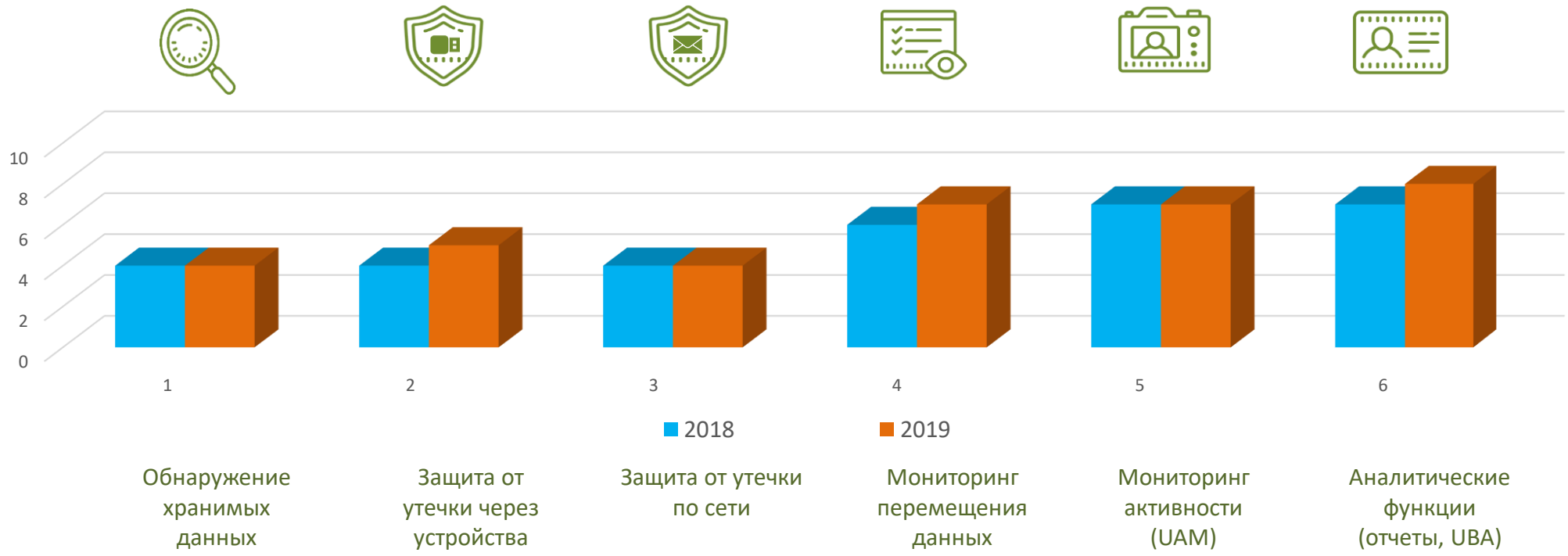
Новинки 2019. Система 1.

Март 2019

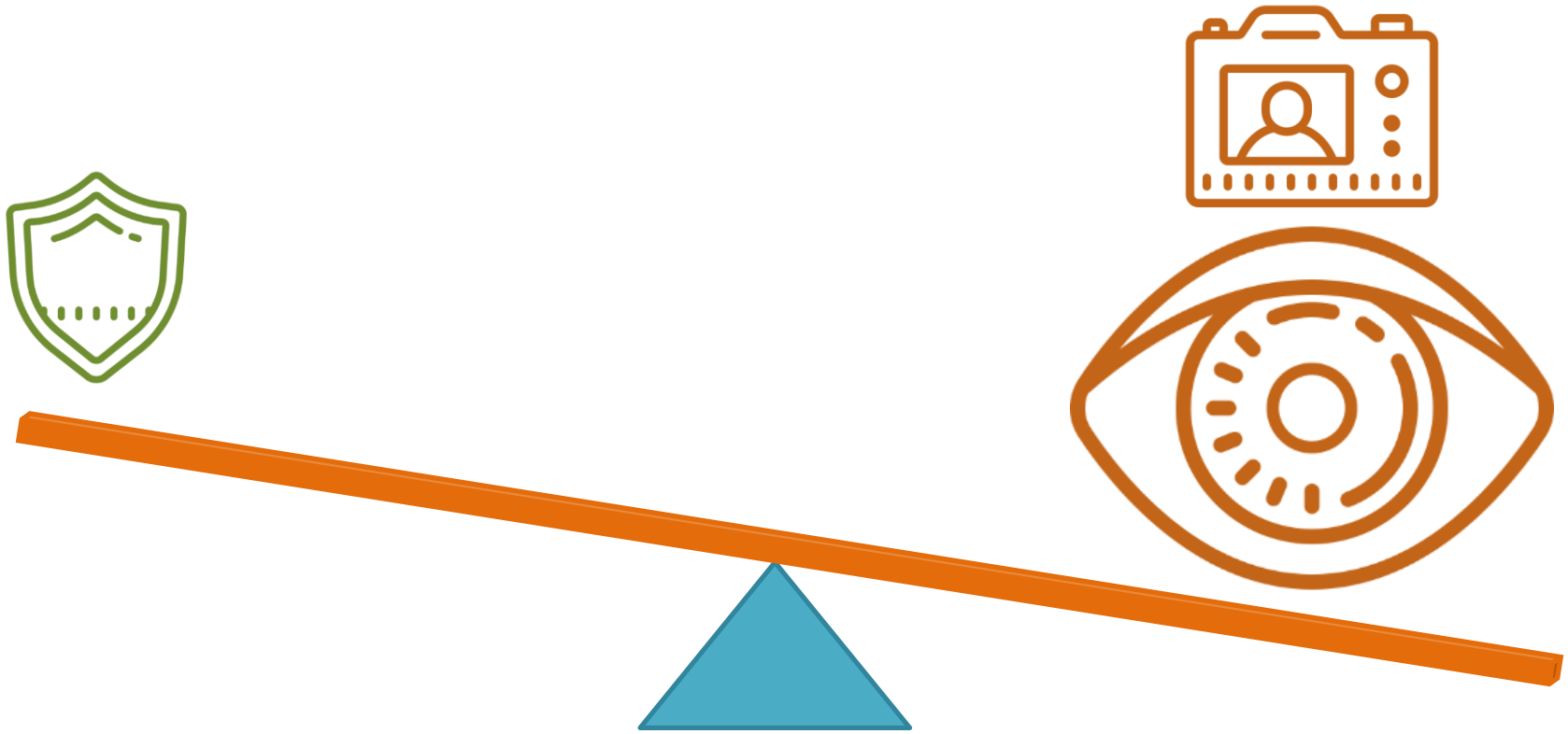
- Улучшение алгоритмов поиска по архиву

Август 2019

- Контроль RDP и TeamViewer
- Мониторинг Bitrix, Microsoft Teams и Slack



Система 1



Защита данных
от утечки

Мониторинг
и анализ инцидентов
Мониторинг активности
пользователей

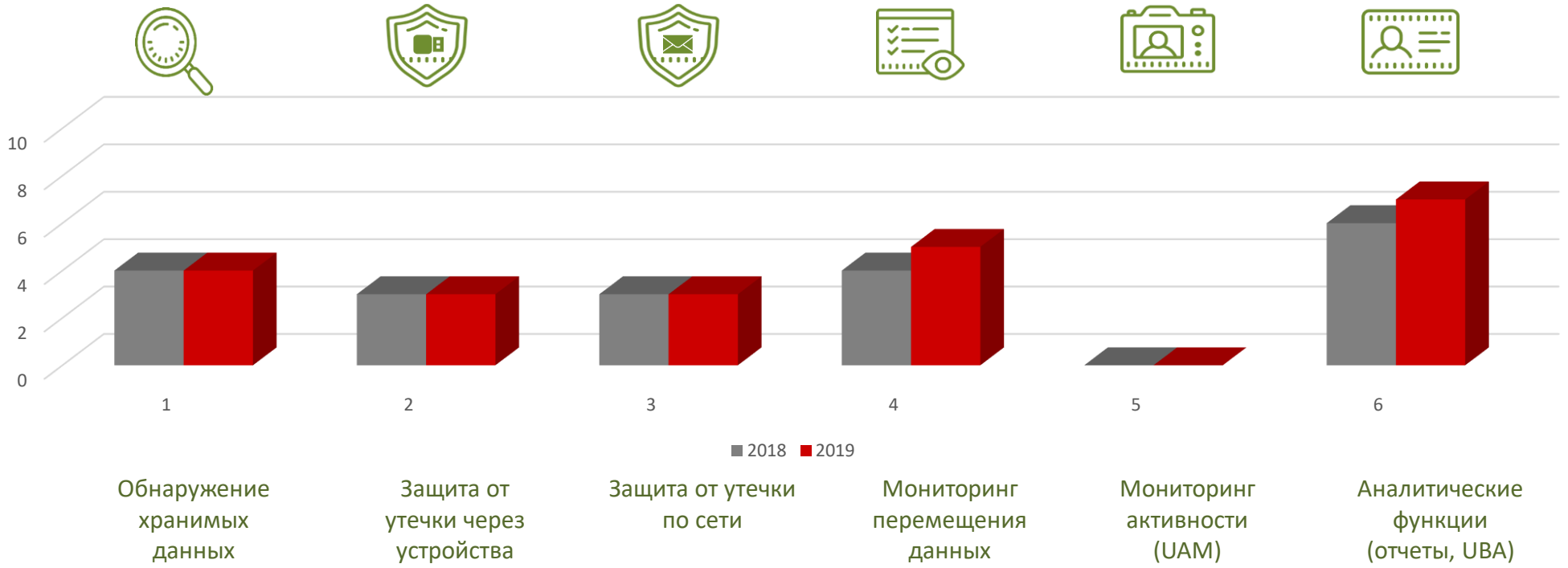
Новинки 2019. Система 2.

Май 2019

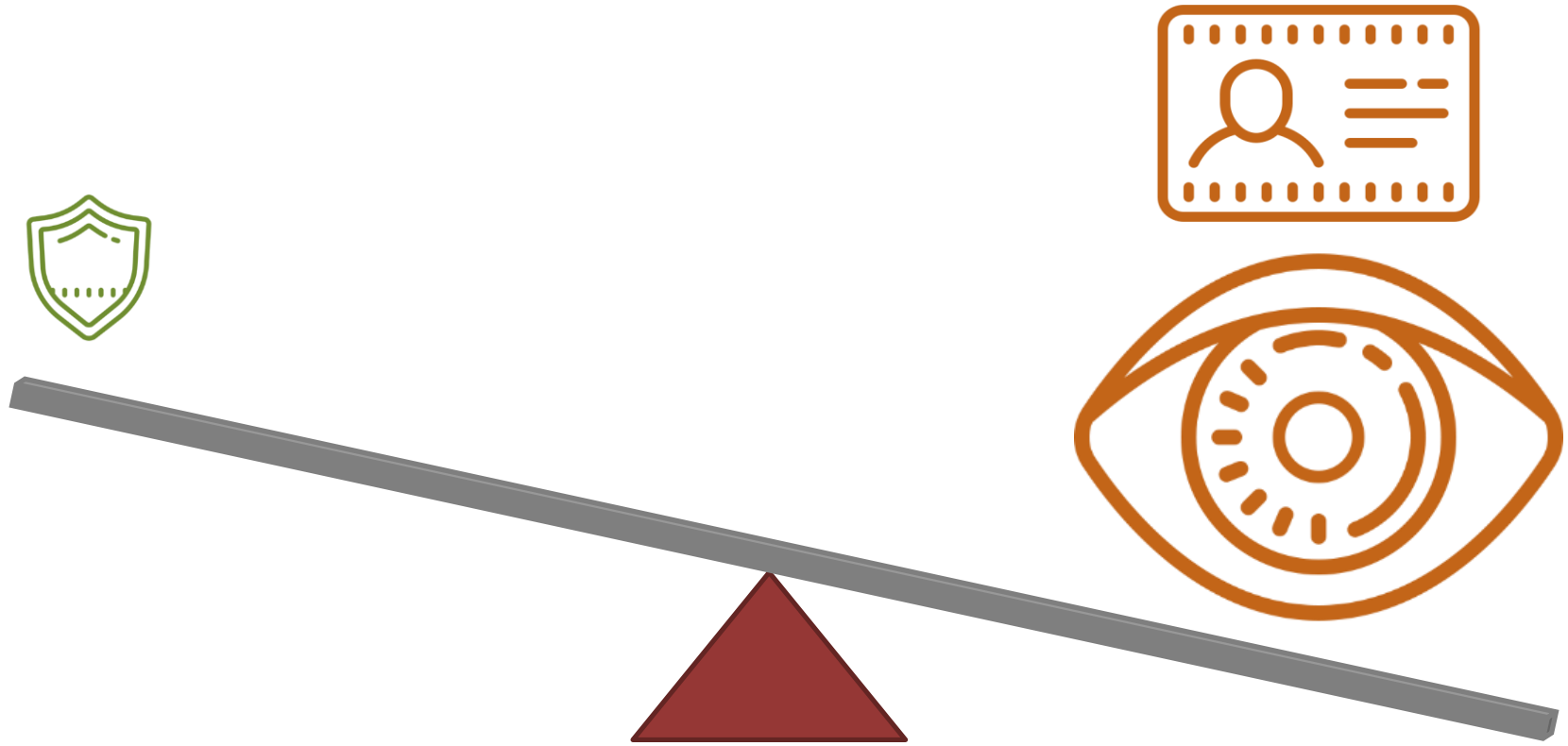
- Контроль Viber
- Анализ трафика от ICAP-агентов
- Извлечение данных из конструкторских документов
- Расширение возможностей поиска и досье

Октябрь 2019

- Добавление модуля UBA



Система 3



Защита данных
от утечки

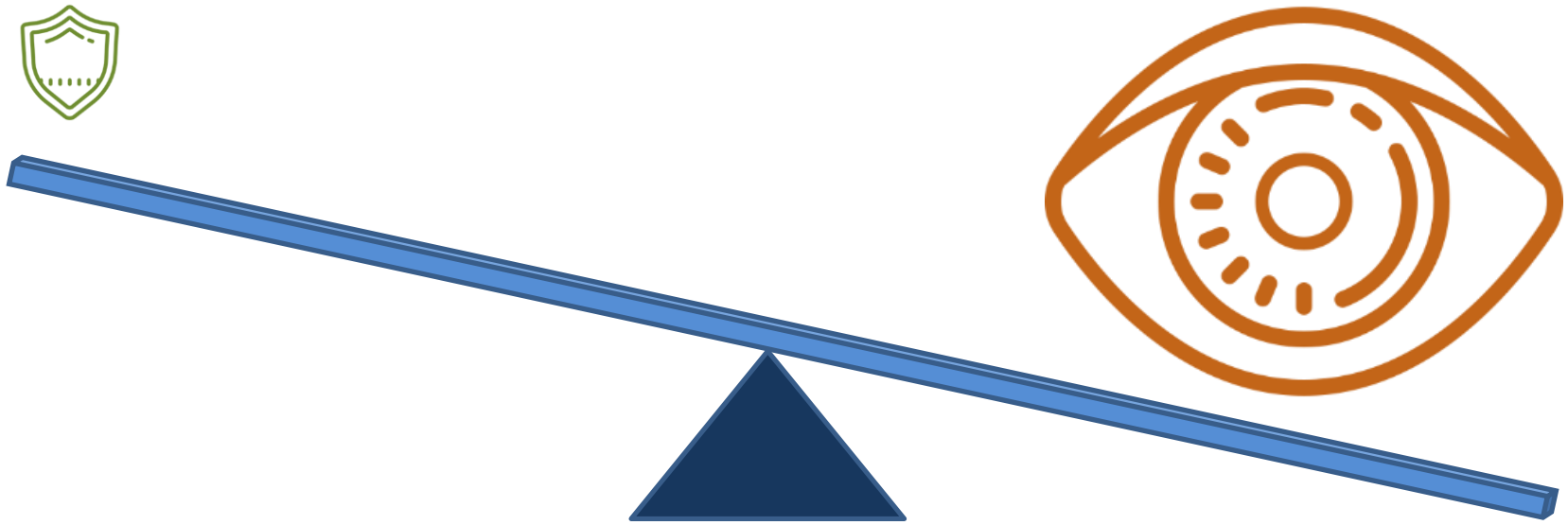
Мониторинг
и анализ инцидентов
Анализ поведения
пользователей

Новинки 2019. Система 3.

Май 2019

- Добавление модуля UBA
- Контроль Slack

Система 3



Защита данных
от утечки

Мониторинг
и анализ инцидентов

Новинки 2019. Система 4.

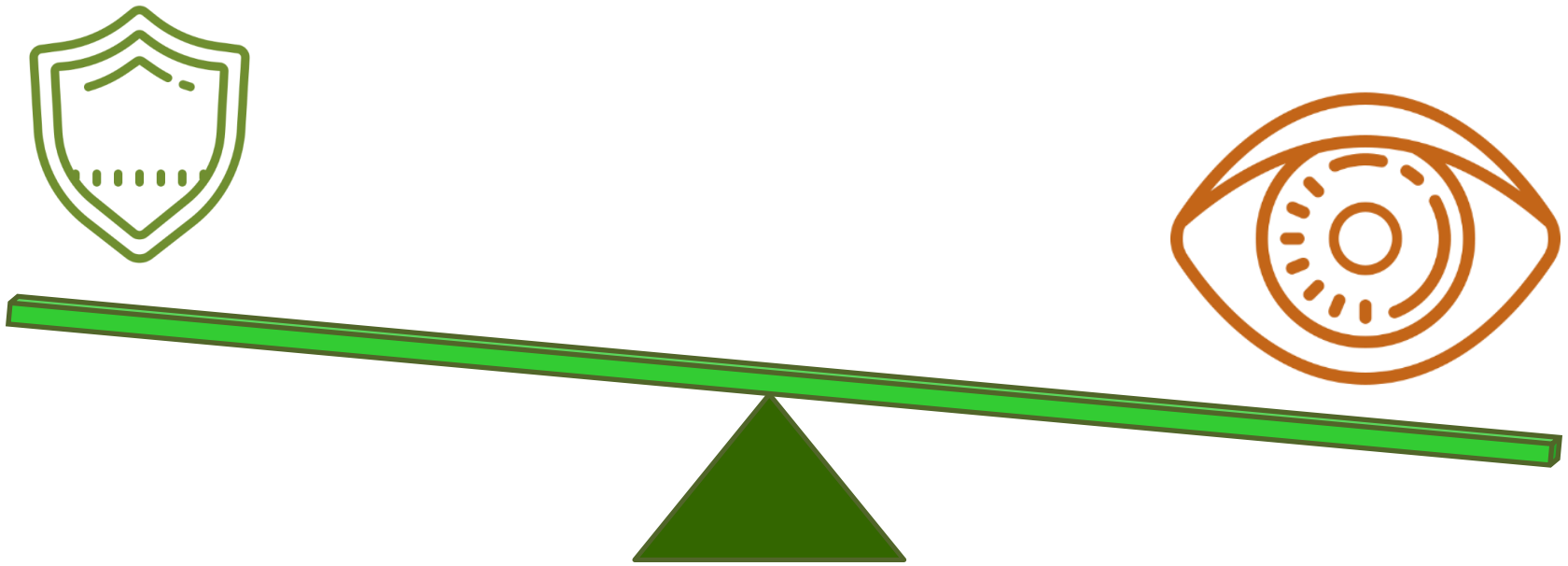
Август 2019

- Новая версия системы визуальной аналитики

Сентябрь 2019

- Анализ векторных изображений в чертежах AutoCAD

Система 3



Защита данных
от утечки

Мониторинг
и анализ инцидентов
Мониторинг
пользовательской
активности

РЕАЛИЗАЦИЯ КОНТРОЛЯ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ В СИСТЕМАХ 1-4

Контроль устройств: БЕЗ анализа содержимого,
Контроль сетевых коммуникаций: блокировка некоторых каналов передачи данных на уровне контекста

Мониторинг каналов передачи данных с ретроспективным анализом архива

Новинки 2019. DeviceLock DLP.

Апрель 2019

- Полноценный контроль Skype for Business и Lync, контроль частных бесед в Skype с контентной фильтрацией
- Полноценный контроль сервисов поиска работы
- Полноценный контроль сервиса Zoom
- Контентный анализ входящих данных для задач обнаружения

Июль 2019

- Контентный анализ для WhatsApp
- Контентный анализ в поисковом сервере

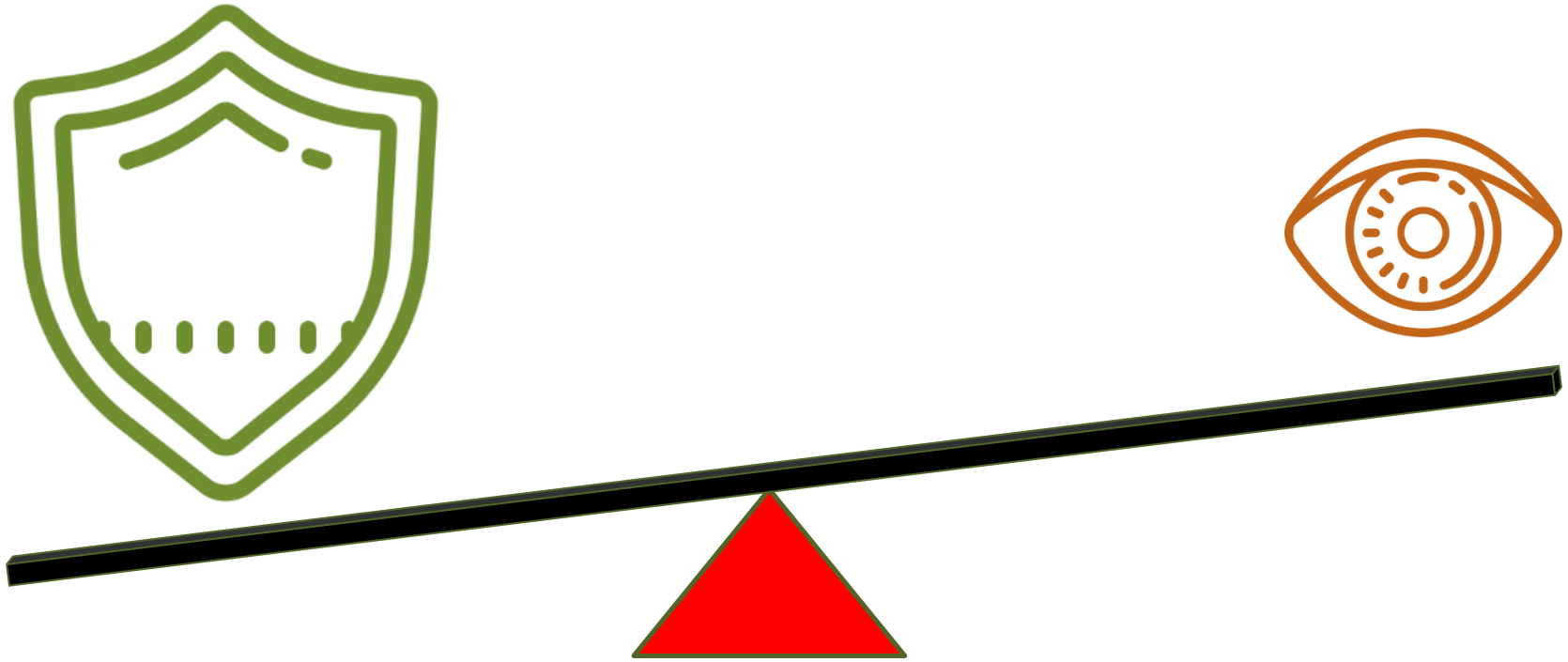
Октябрь 2019

- Поддержка PostgreSQL
- Блокировка любых сетевых сервисов

Ноябрь 2019

- Добавлен контроль ряда сетевых сервисов, поддержка MacOS Catalina

DeviceLock DLP

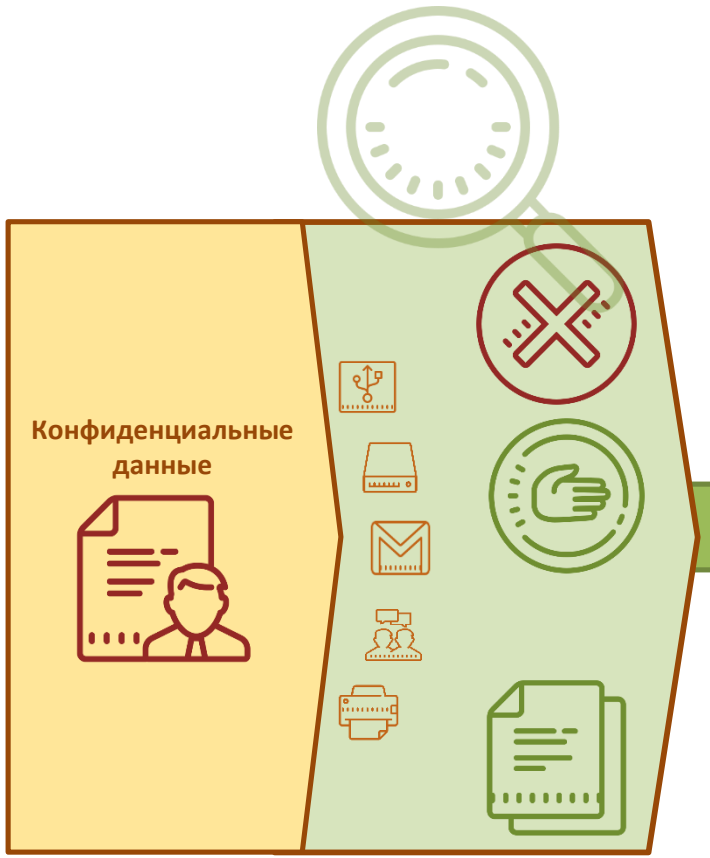


Защита данных
от утечки

Мониторинг
и анализ инцидентов

КОНТРОЛЬ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ В DEVICELOCK DLP

Полноценный контроль каналов передачи данных с анализом содержимого на каждом этапе



- Данные передаются после анализа содержимого с запретом передачи только данных ограниченного доступа:
- Нет данных ограниченного доступа – передача разрешена
- Возможность оперативной реакции по инциденту

- Создается копия переданных данных (как при блокировке, так и по факту разрешенной передачи данных)

Немедленное выявление инцидента в форме попытки утечки
Определение злоумышленника без ущерба для организации

Предотвращение утечки и дальнейшего бесконтрольного распространения данных

Выявление инцидента *(попытки передачи данных)*, Определение источника

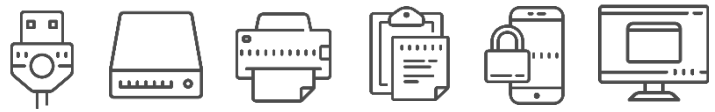
Сбор и хранение доказательной базы для расследования попыток хищения данных

Детектирование конфиденциальных данных в архиве –
Для проведения расследований и создания доказательной базы

DeviceLock® DLP

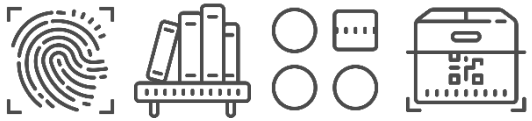
ПРЕДОТВРАЩЕНИЕ УТЕЧЕК ДАННЫХ

… 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

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.

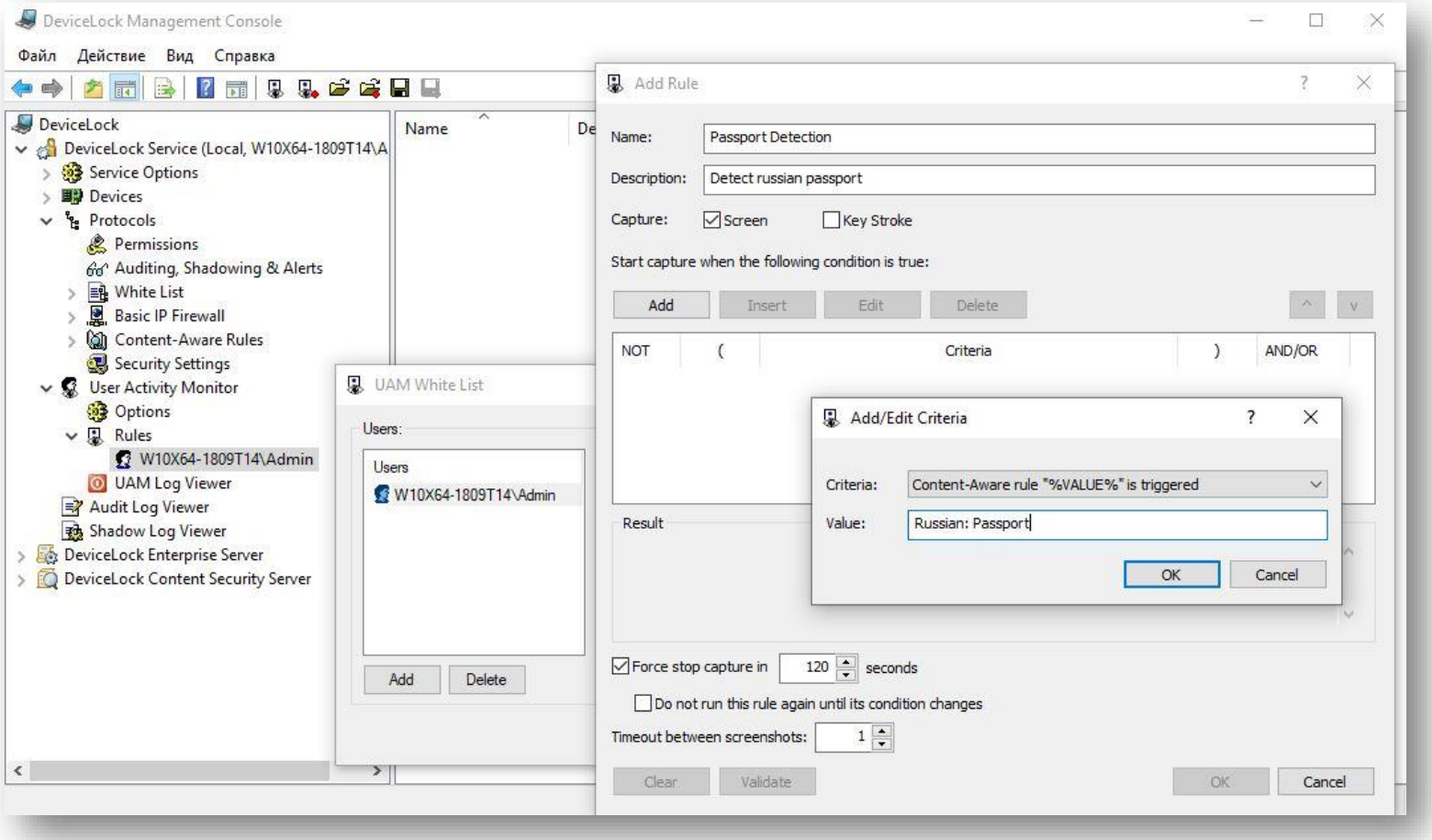
Развитие **DeviceLock Discovery** – сканирование и обнаружение данных на серверах SQL и noSQL, ElasticSearch баз с учетом накопленного опыта по нахождению незащищенных баз в Интернете...

Защита данных от фотографирования с экрана – возможность идентификации пользователя, компьютера и даты по фотографии экрана.

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

МОНИТОРИНГ ПОЛЬЗОВАТЕЛЬСКОЙ АКТИВНОСТИ (UAM)

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



КОД ИБ ИТОГИ
МОСКВА 05 ДЕК'19

СПАСИБО ЗА ВНИМАНИЕ!

СЕРГЕЙ ВАХОНИН
SV@DEVICELOCK.COM

www.DeviceLock.com

GET CONTACT