AVSOFT

AVSOFT ATHENA

система выявления
и анализа
вредоносного ПО

О КОМПАНИИ

Компания «АВ Софт» существует с 2010 года. Основными направлениями деятельности являются разработка программного обеспечения в сфере информационной безопасности и ИТ-консалтинг.

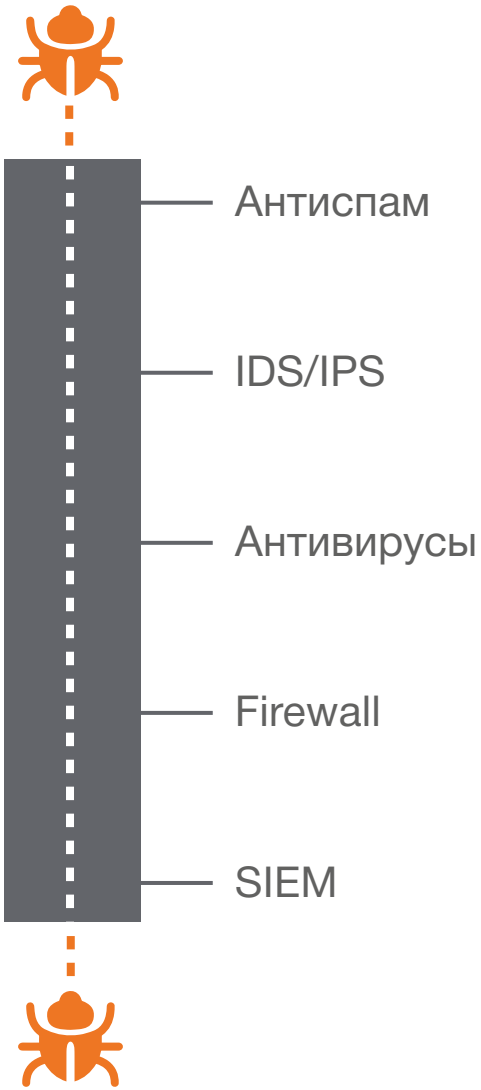
- Консалтинг в области ИБ
- Анализ вредоносного ПО
- Разработка ПО
- Расследование инцидентовв ИБ

ЦЕЛЕНАПРАВЛЕННЫЕ АТАКИ

Целенаправленные атаки (APT) являются одним из самых опасных видов атак и используются для осуществления шпионажа, сбора и передачи секретных данных, дестабилизации инфраструктуры, нанесения финансового ущерба

AVSOFT

МЕТОДЫ ЗАЩИТЫ ОТ APT



Для осуществления APT атак киберпреступники применяют вирусы нулевого дня (0-day), преодолевая все существующие способы защиты

НЕОБХОДИМОЕ РЕШЕНИЕ

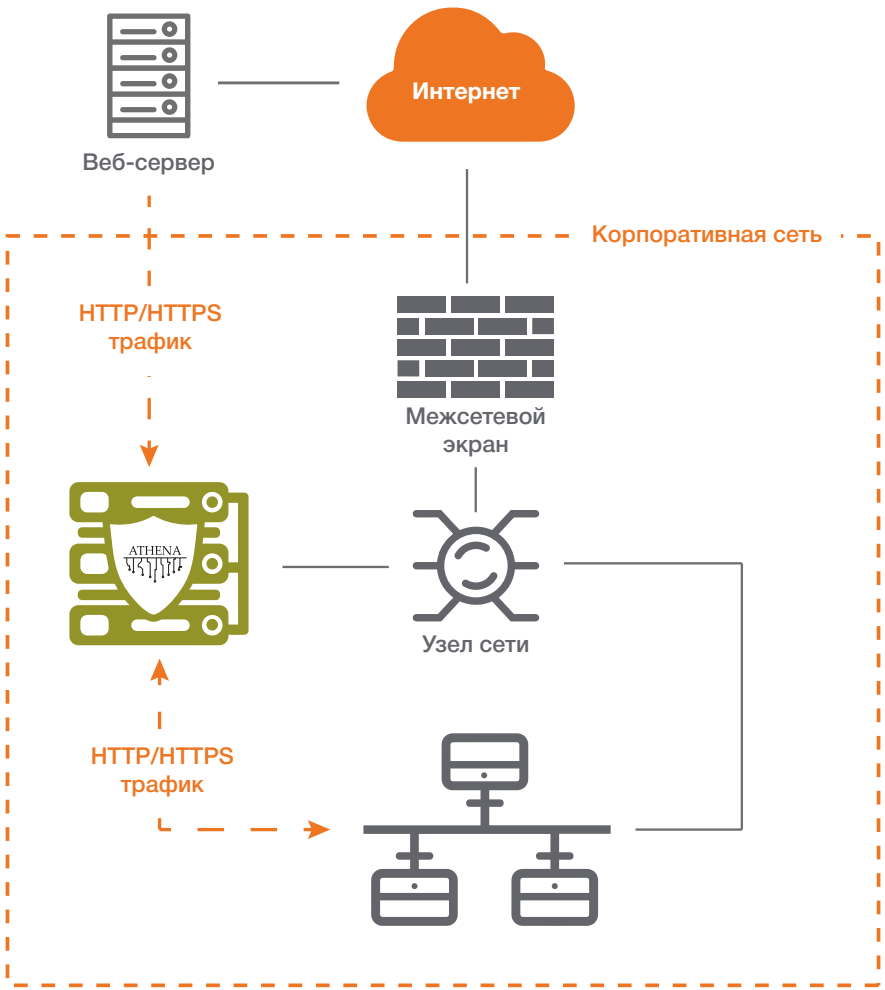
Для защиты от вирусов нулевого дня помимо традиционных антивирусных средств и средств анализа сетевого трафика необходимо использовать технологию изолированной исследовательской среды — «песочницы»

Компания «АВ Софт» предлагает систему «ATHENA» для проверки и анализа программного обеспечения множеством инструментов, включая технологию «песочницы»

AV SOFT

ВАРИАНТЫ ИНТЕГРАЦИИ

Проверка электронной почты



Проверка веб-трафика

РЕЖИМЫ ФУНКЦИОНИРОВАНИЯ

Автоматический режим

- Проверка, блокировка и обезвреживание файлов в автоматическом режиме
- Оповещение службы безопасности об угрозах и проблемах по различным каналам связи (Email, SIEM, Telegram…)
- Интеграция с другими системами по протоколу IMAP и через REST API

Экспертный режим

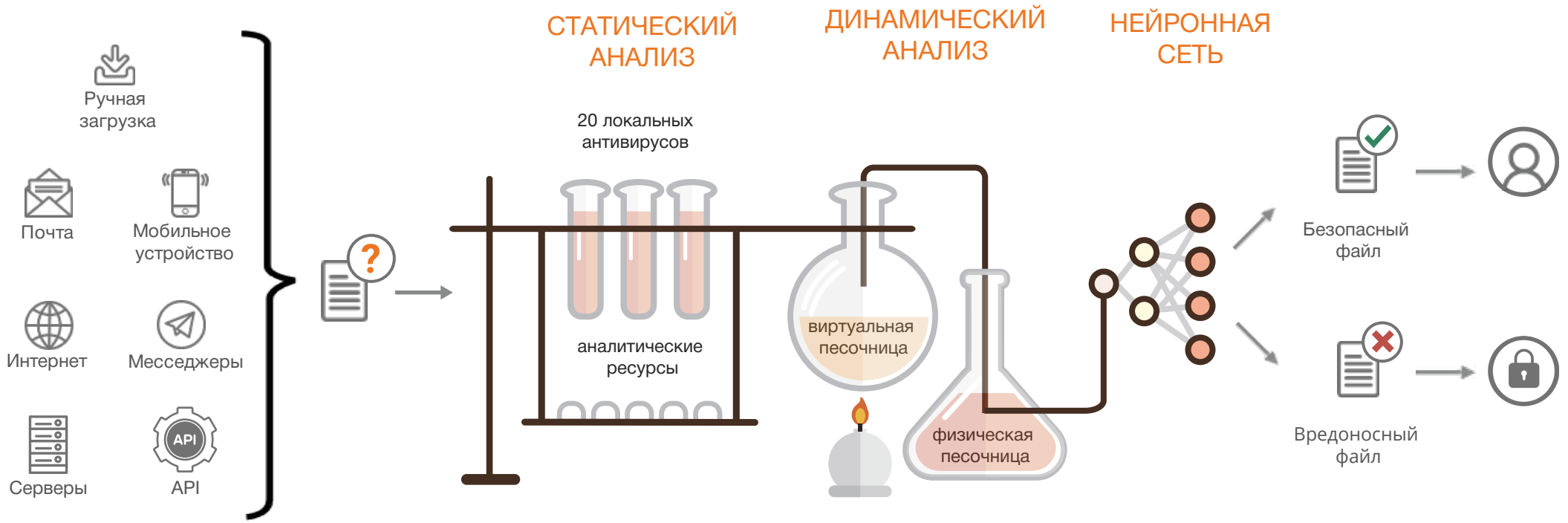
- Гибкая настройка среды исследования
- Возможность работы в исследовательской среде с проверяемым файлом
- Управление аналитическими инструментами и сигнатурами

ТЕХНОЛОГИЯ ПРОВЕРКИ

Прием файлов из множества источников

Лаборатория проверки файлов

Подробный отчет



СТАТИЧЕСКИЙ АНАЛИЗ

Любые типы файлов

Многоуровневая проверка

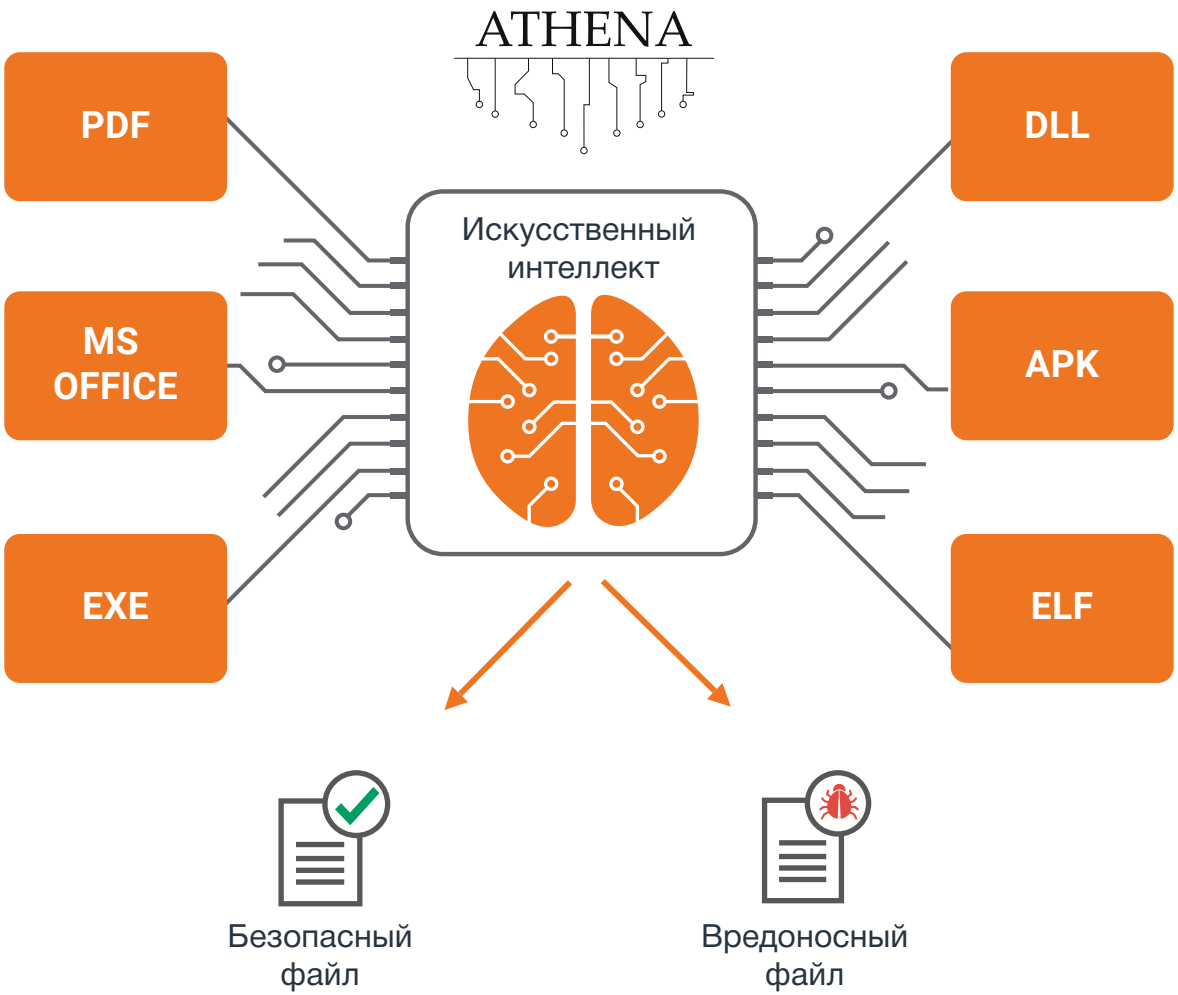
- Проверка в более 20 локальных антивирусах
- Статический анализ файлов
- Проверка во внешних аналитических ресурсах
- Использование нейронной сети

Результаты анализа

- Анализ офисных файлов на наличие активных элементов (макросы, скрипты и пр.)
- Анализ атрибутов, структуры и контента файлов на наличие подозрительных признаков (сжатие, обфускация и т.п.)
- Анализ манифестов мобильных приложений на требуемые разрешения

НЕЙРОННАЯ СЕТЬ

Использование нейронных сетей для проверки различных типов файлов



ДИНАМИЧЕСКИЙ АНАЛИЗ

Любые типы файлов на проверку

Исследование файлов в «песочнице»

Результаты анализа поведения

– события

– аналитики

– запись исследования и скриншоты

– сетевой трафик (проверка IP-адресов и доменов)

фиксация потребляемых ресурсов (майнинг)

AVSOFT

ЗАДАЧИ

ЗАЩИТА

защита серверов, мобильных устройств и рабочих мест от вредоносного ПО

ОБУЧЕНИЕ

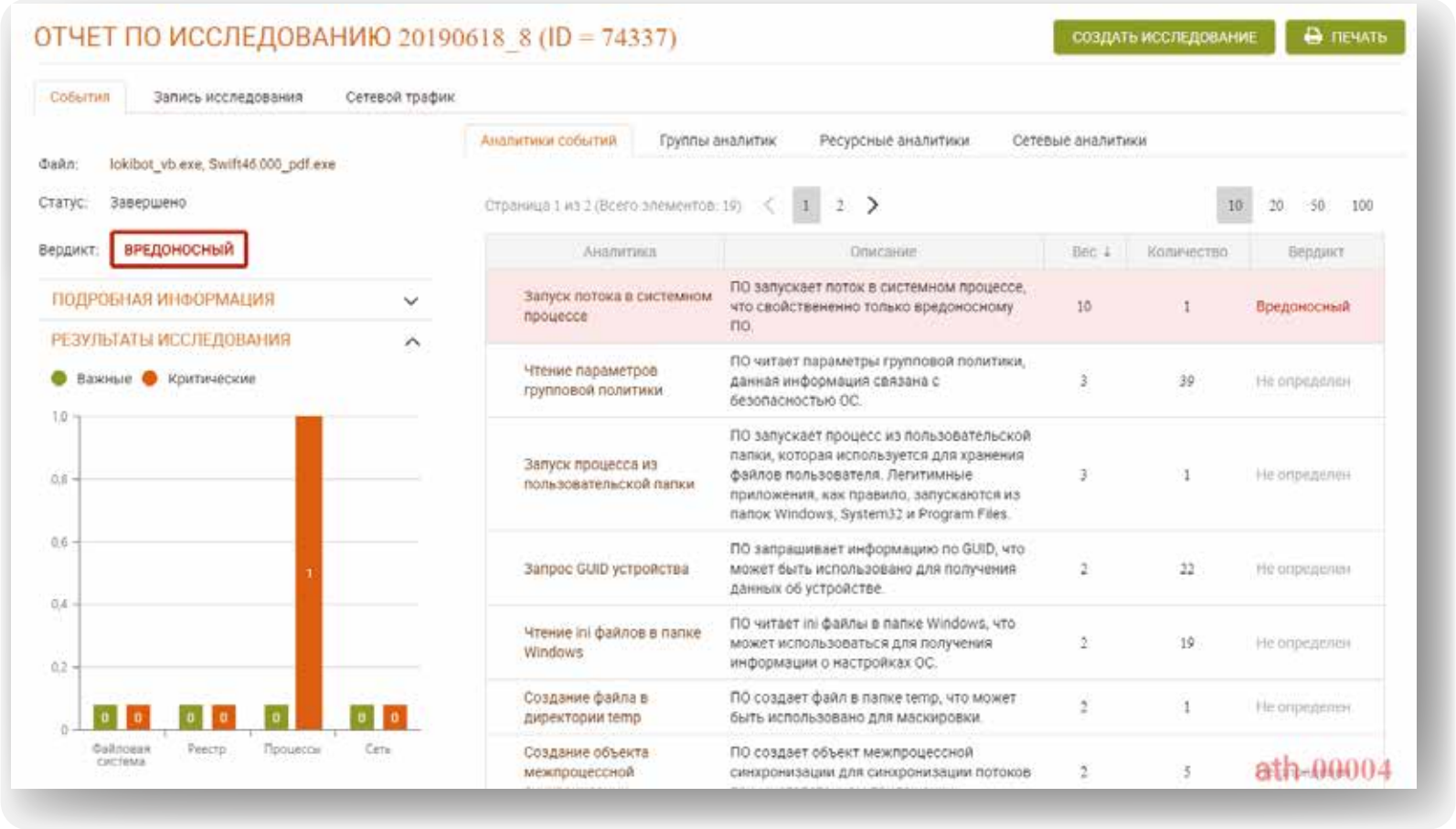
повышение компетенций специалистов в области информационной безопасности

РАЗРАБОТКА

создание новейших продуктов и базы знаний по анализу вредоносного ПО

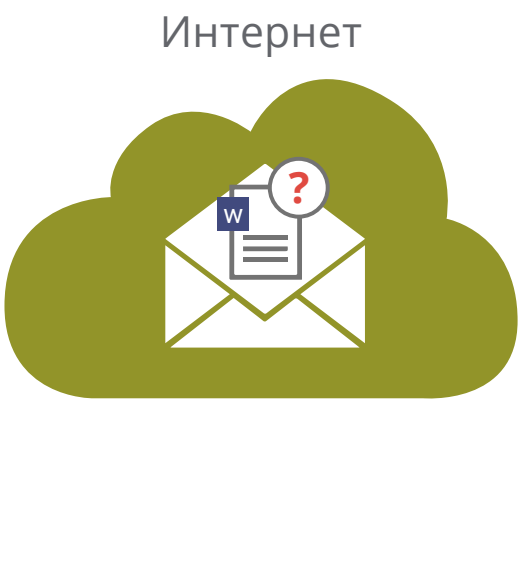
ОТЧЕТ ПО ФАЙЛУ

Система ATHENA предоставляет подробный
отчет с ключевой информацией
по результатам исследования файла



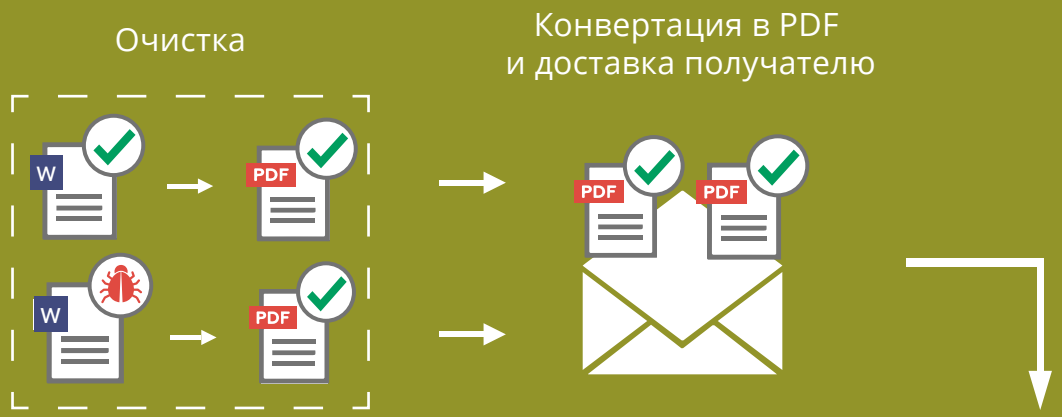
АНАЛИЗ ПОЧТОВОГО ТРАФИКА

Интернет



Очистка файлов от вредоносных элементов и доставка безопасного контента

В течение 1 минуты



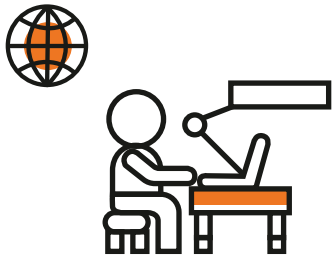
Получатель

Проверка вложений статическим и динамическим анализом

От 5 до 15 минут

АНАЛИЗ ВЕБ ТРАФИКА

Скачивание файла по ссылке



Скачивание файла по ссылке

Проверка файла в системе

ATHENA

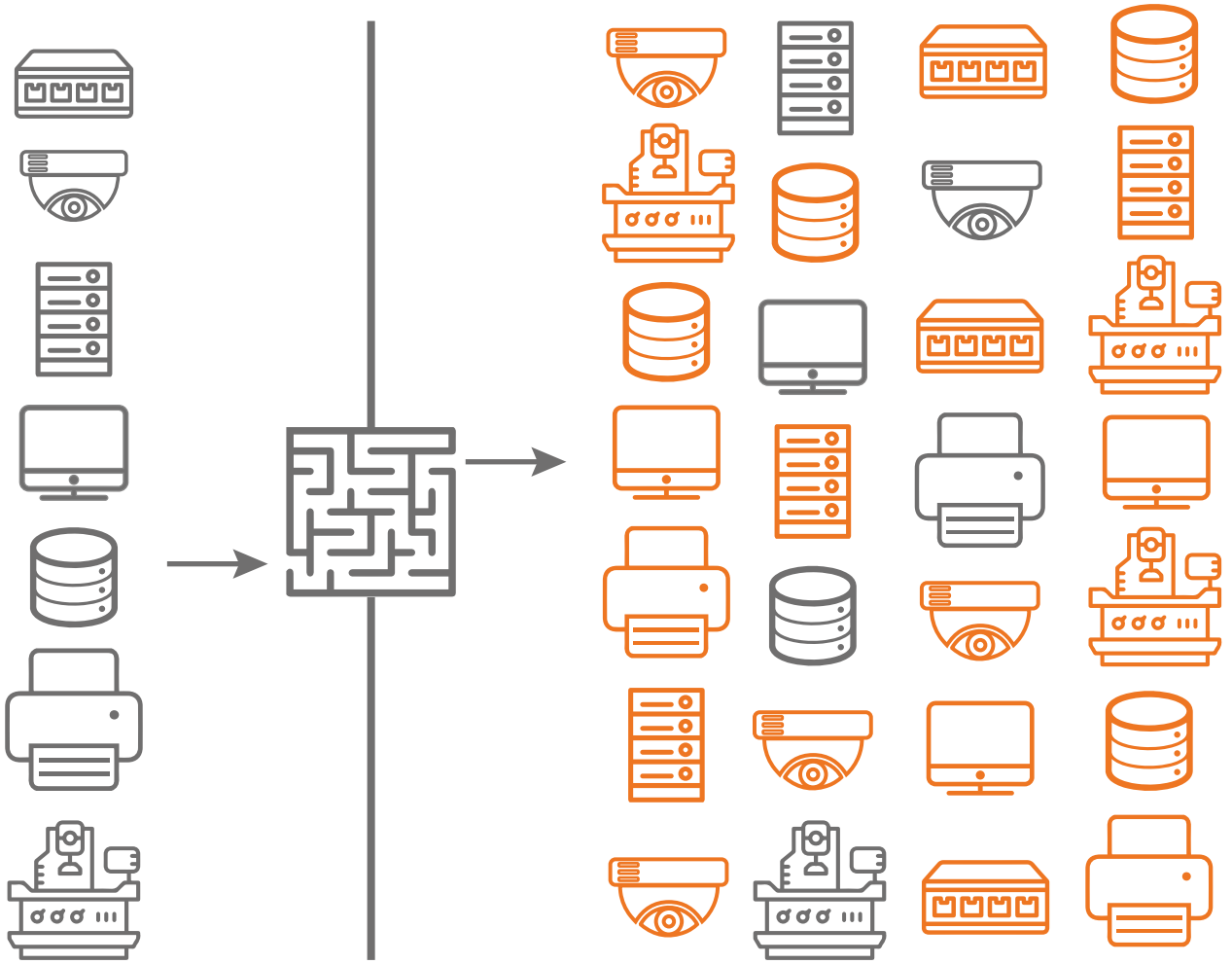
Поддерживаются протоколы: http, https, ftp, sftp

Результаты проверки

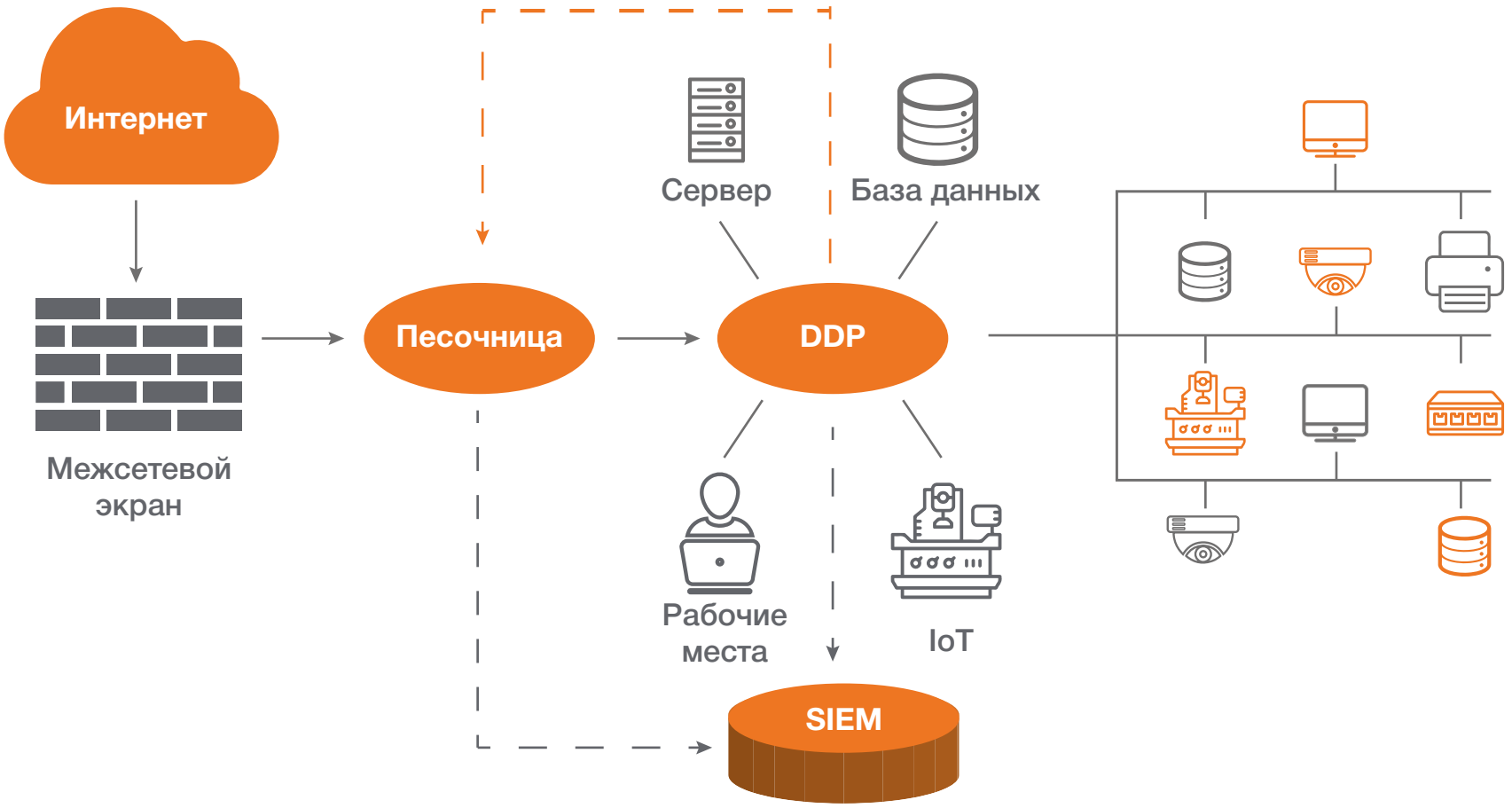
Составление черных и белых списков

ТЕХНОЛОГИЯ DECEPTION

Технология Deception позволяет имитировать реальную инфраструктуру



ИНТЕГРАЦИЯ ТЕХНОЛОГИЙ DECEPTION И SANDBOX



ПРЕИМУЩЕСТВА

- Более 20 антивирусов
- Кастомизация «песочницы»
- Проверка мобильных приложений
- Проверка файлов со съемных носителей
- Анализ ресурсов для выявления майнеров
- Проверка архивов (в т.ч. многотомных и запароленных)
- Нейронные сети
- Поддержка отечественных ОС

КОНТАКТЫ


office@avsw.ru


www.avsw.ru


+7 (495) 988-92-25


127106, г. Москва, ул. Гостиничная, д. 5

Спасибо, что нашли время
ознакомиться с презентацией!

AVSOFT