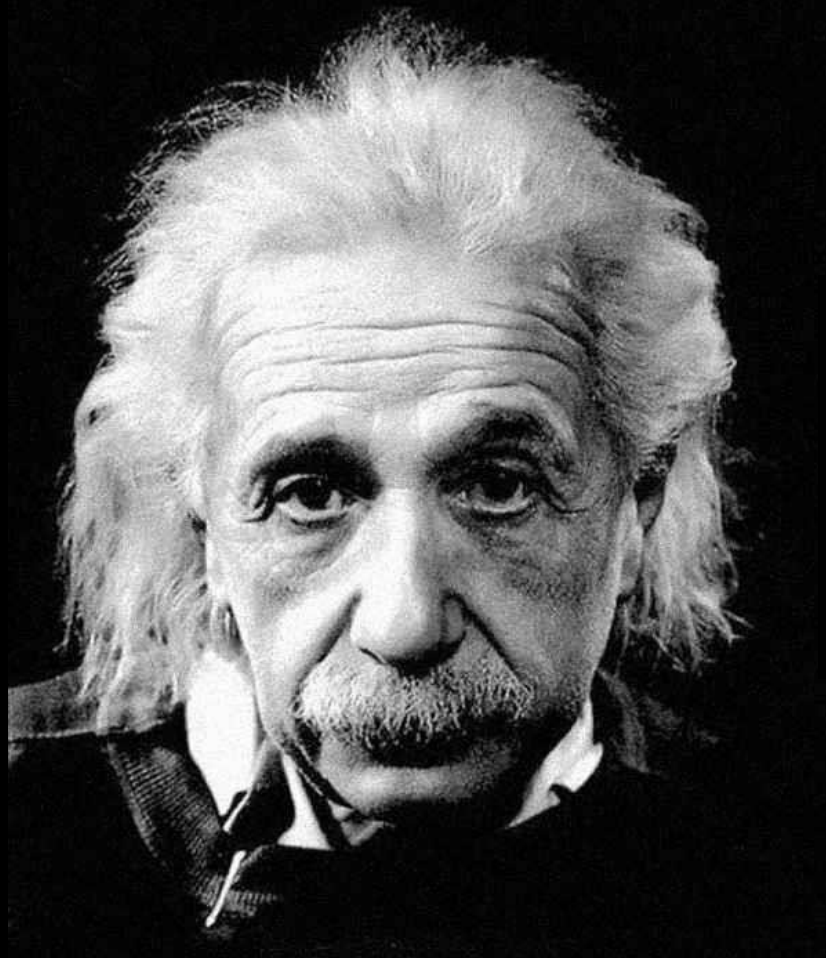
Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point
На шаг впереди



“Мир это опасное место для жизни; не из – за злых людей, а из-за тех, кто ничего не делает по этому поводу.”

– Albert Einstein

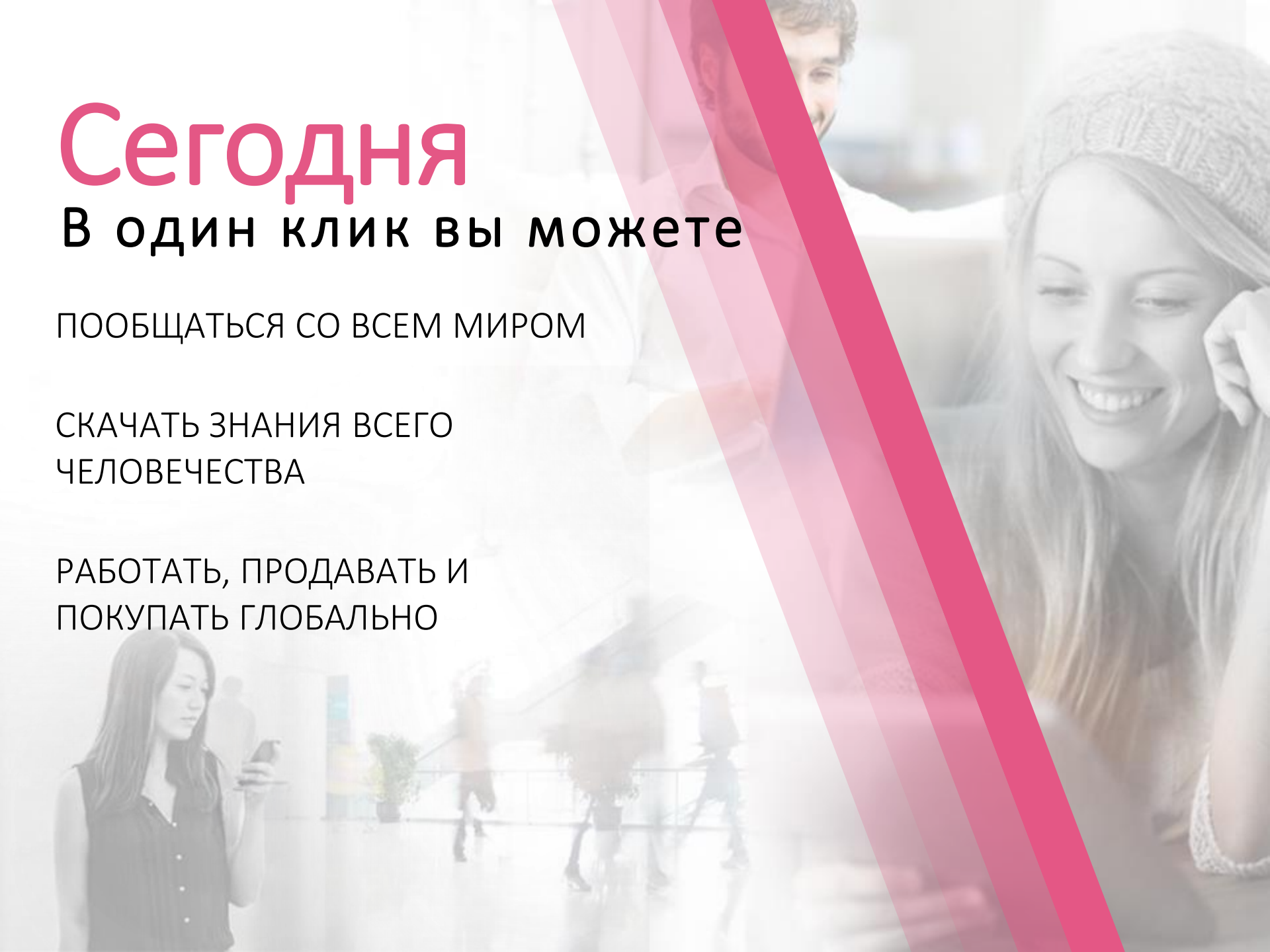
Сегодня

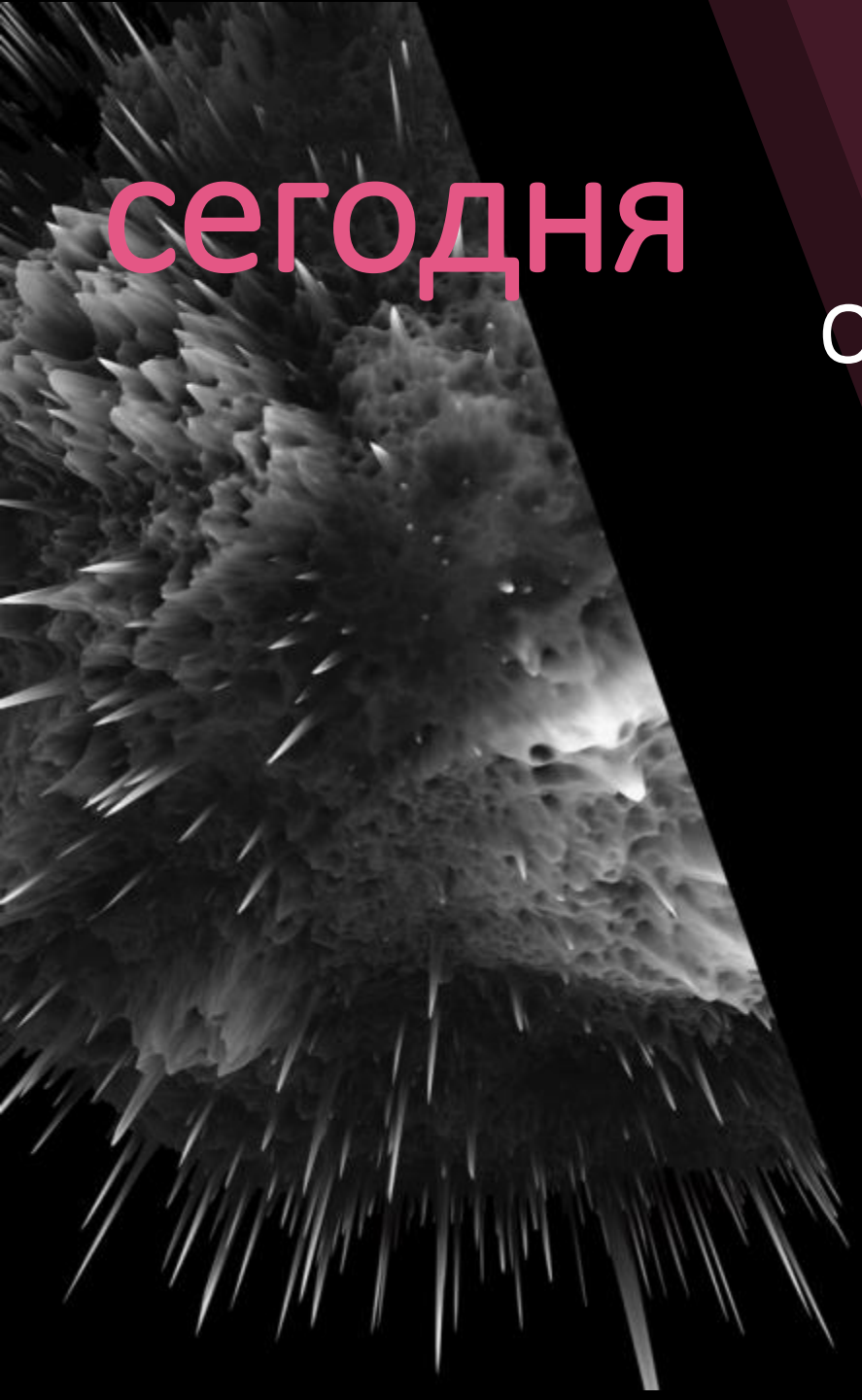
В один клик вы можете

ПООБЩАТЬСЯ СО ВСЕМ МИРОМ

СКАЧАТЬ ЗНАНИЯ ВСЕГО ЧЕЛОВЕЧЕСТВА

РАБОТАТЬ, ПРОДАВАТЬ И ПОКУПАТЬ ГЛОБАЛЬНО





сегодня

ОДНА АТАКА МОЖЕТ:

ОТКЛЮЧИТЬ ЭНЕРГЕТИЧЕСКУЮ СИСТЕМУ СТРАНЫ

ОСТАНОВИТЬ СИСТЕМЫ КОММУНИКАЦИЙ И ТРАНСПОРТНОГО КОНТРОЛЯ

УКРАСТЬ ЧАСТНЫЕ ДАННЫЕ МИЛЛИОНОВ

РАЗОРИТЬ ПРЕДПРИЯТИЯ С ВЕКОВОЙ ИСТОРИЕЙ

Гонка Вооружений Продолжается

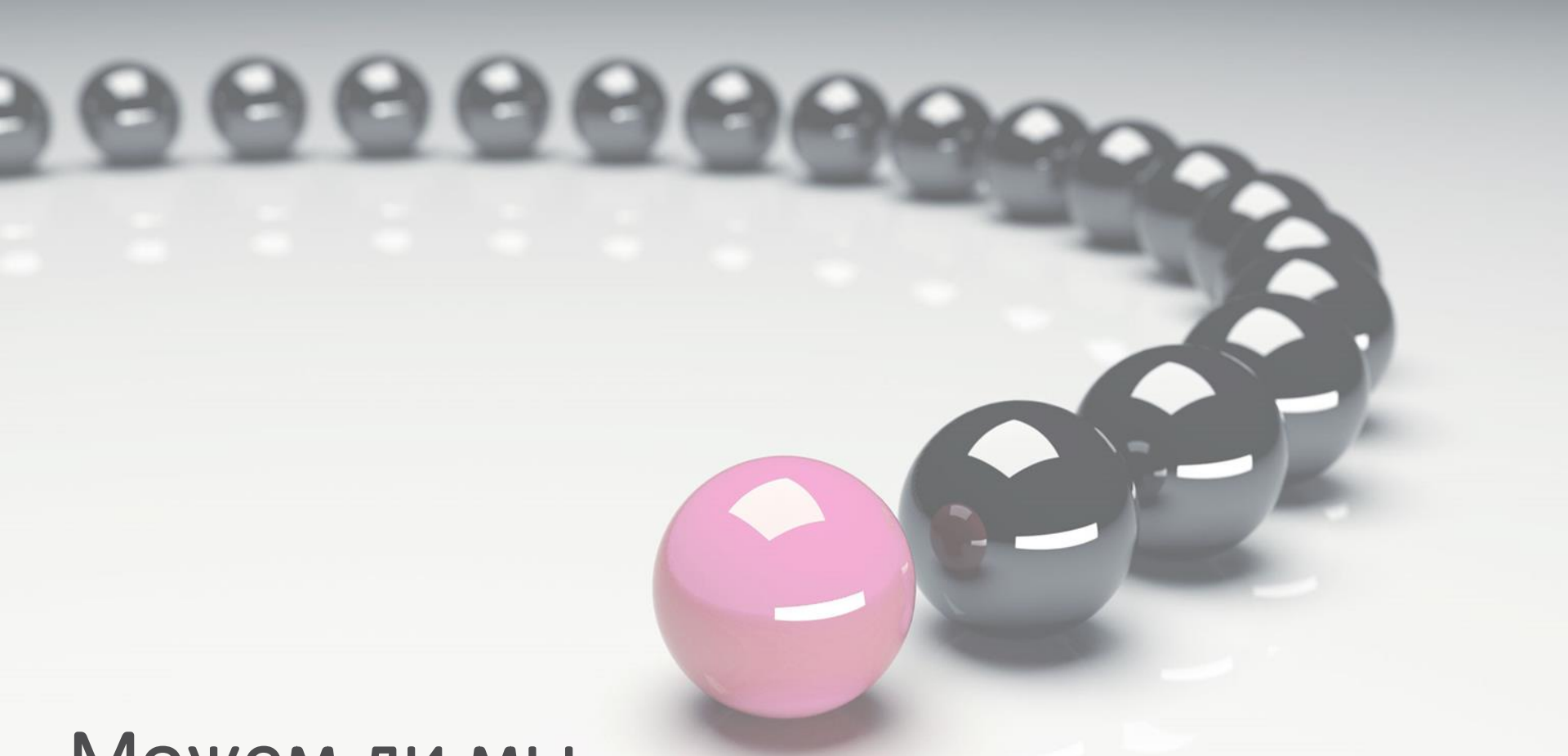
В 2014 году обнаружено больше угроз, чем за все предыдущие 10 лет

ТРАДИЦИОННЫЙ ПОДХОД К БЕЗОПАСНОСТИ

Virus	Anti -Virus
Malicious Web Sites	URL Filtering
Attacks	IPS
Botnet	Anti-Bot
High Risk Applications	Application Control

А что если бы

БЕЗОПАСНОСТЬ БЫЛА НА ОДИН ШАГ ВПЕРЕДИ?



Можем ли мы
ЗАЩИТИТЬ ОТ УГРОЗ
КОТОРЫЕ ЕЩЕ НЕ СУЩЕСТВУЮТ?

Нам нужно
ДУМАТЬ
ИНАЧЕ

ДЕЙСТВОВАТЬ
ИНАЧЕ

40%

органицаций скачивали незнакомый вредоносный код

200,000

уникальных угроз обнаруживается ежедневно

E-mail От миссис Мира

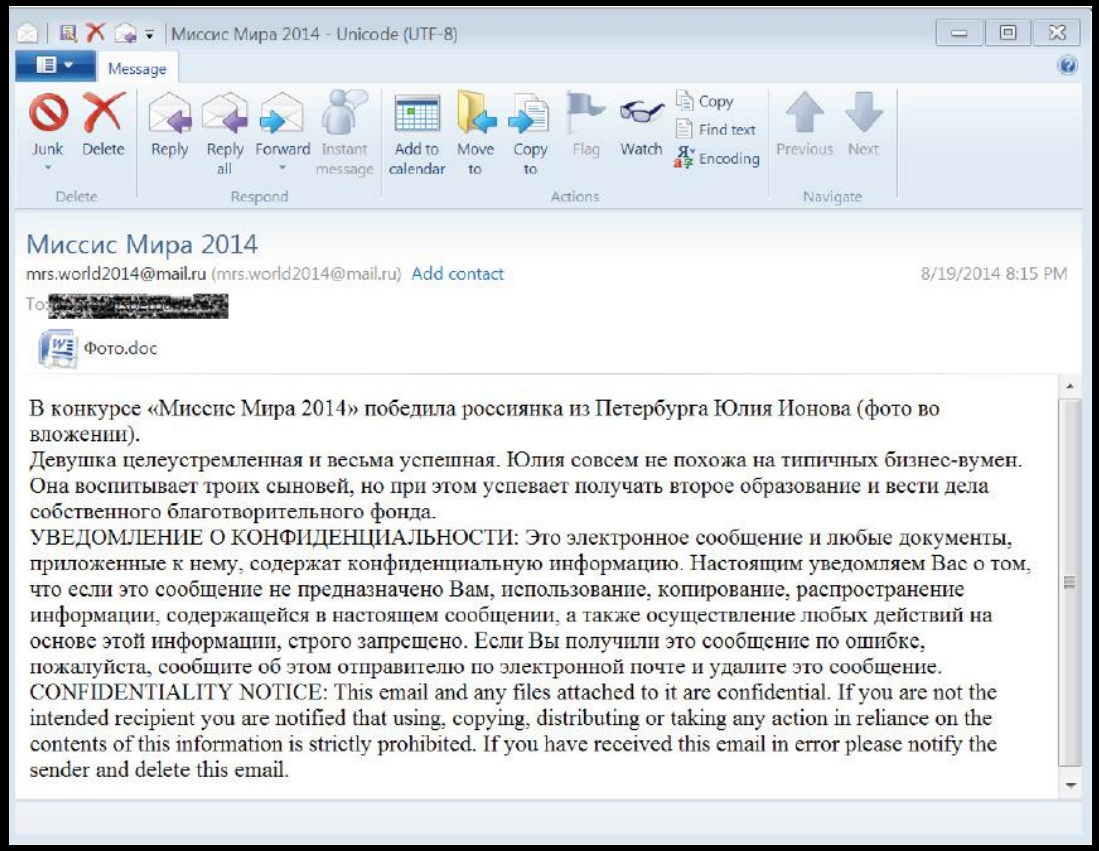
Таргетированная атака 2014 года

ЦЕЛИ:

Российские и европейские организации

МЕТОД:

Точечная фишинговая рассылка с эксплойтом в формате MS Word

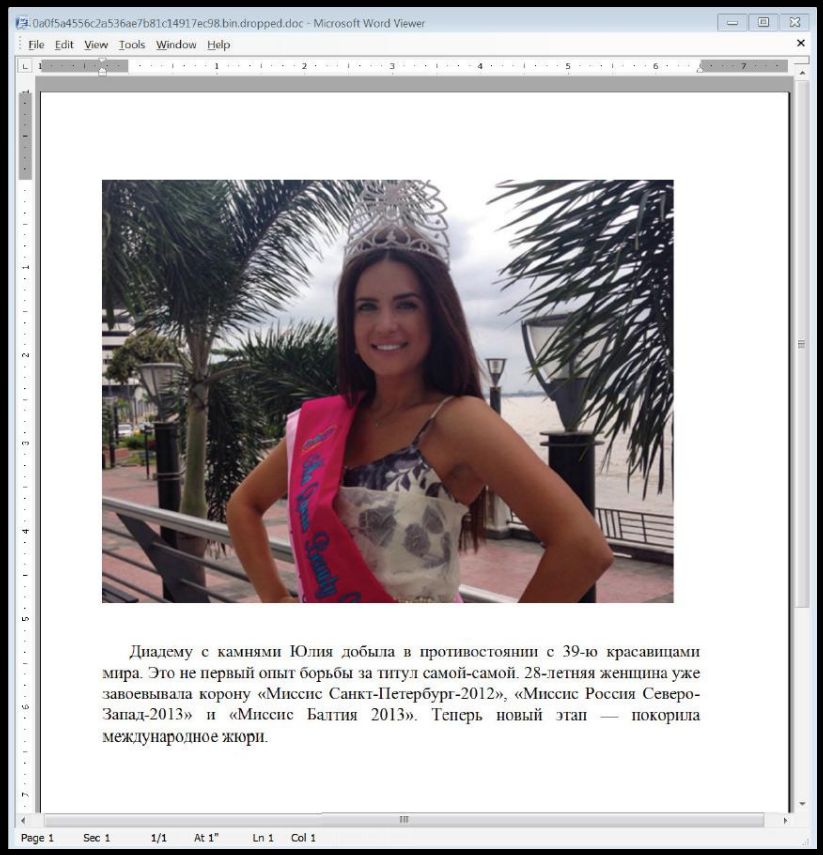


Вредоносный документ

RETURN ORIENTED PROGRAMMING (ROP) EXPLOIT

Использование
новой уязвимости
MS word (CVE-2012-0158)

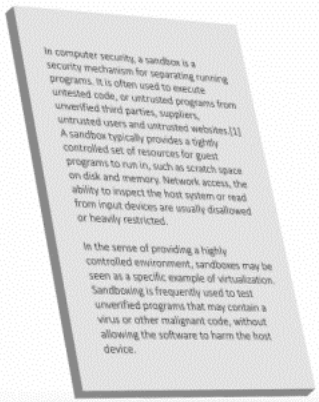
- Отсылал системную информацию в командный центр
- Скачивал и устанавливал дополнительные модули для управления
- Шифровал и отправлял конфиденциальные данные в командный центр



Один из способов защиты
от неизвестного

SANDBOXING
(песочница)

КАК SANDBOXING РАБОТАЕТ



Отслеживает изменения в:

- Системном реестре
- Сетевых подключениях
- Активности файловой системы
- Системных процессах

MALWARE МОЖЕТ ОБХОДИТЬ SANDBOX

Для примера:

- Разные версии ОС
- Запрет на запуск в виртуальной среде
- Задержка атаки
- Размер файла
- Активация по сценарию

КАК РАБОТАЕТ MALWARE

КАК РАБОТАЕТ MALWARE

Уязвимость

Дыра в системе

КАК РАБОТАЕТ MALWARE

Уязвимость

Exploit

‘вооруженный’ код использующий уязвимость для перехвата контроля над системой

КАК РАБОТАЕТ MALWARE

Уязвимость → Exploit → Shellcode

Набор инструкций, который добавляется в систему для загруки или запуска вредоносной программы

КАК РАБОТАЕТ MALWARE

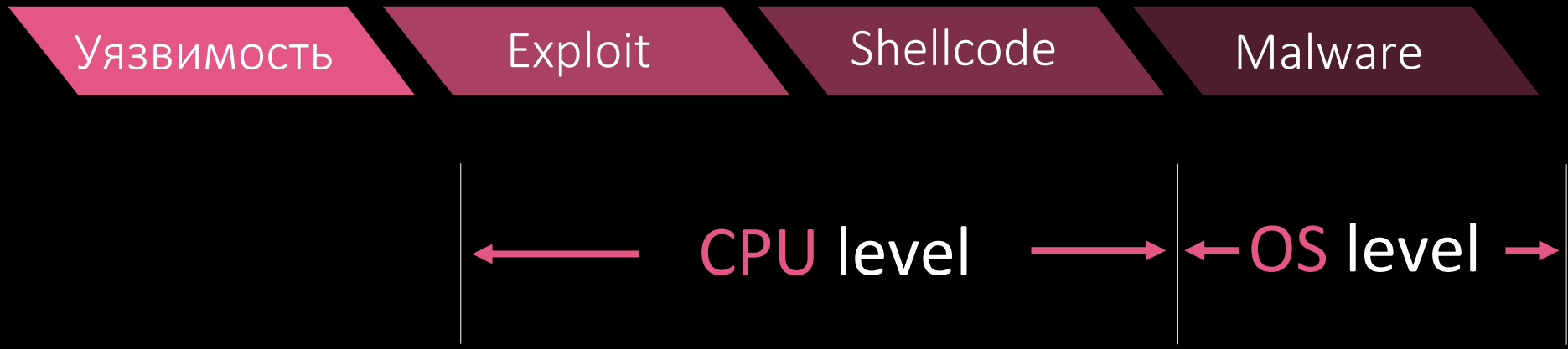
Уязвимость → Exploit → Shellcode → Зловред

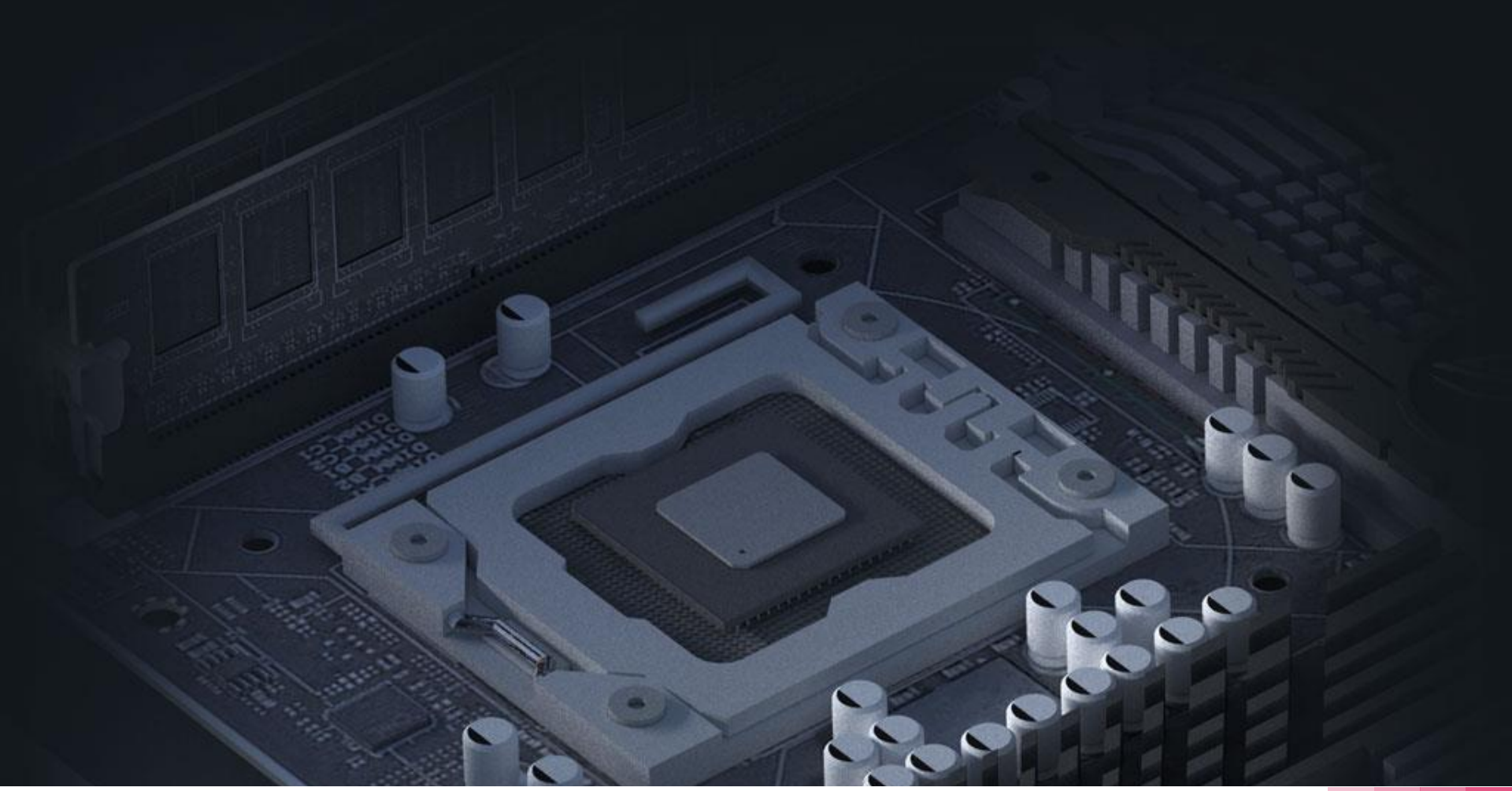
Зловредный код, который
шпионит либо
нарушает работу системы

А что если

Посмотреть ИНАЧЕ

КАК РАБОТАЕТ MALWARE





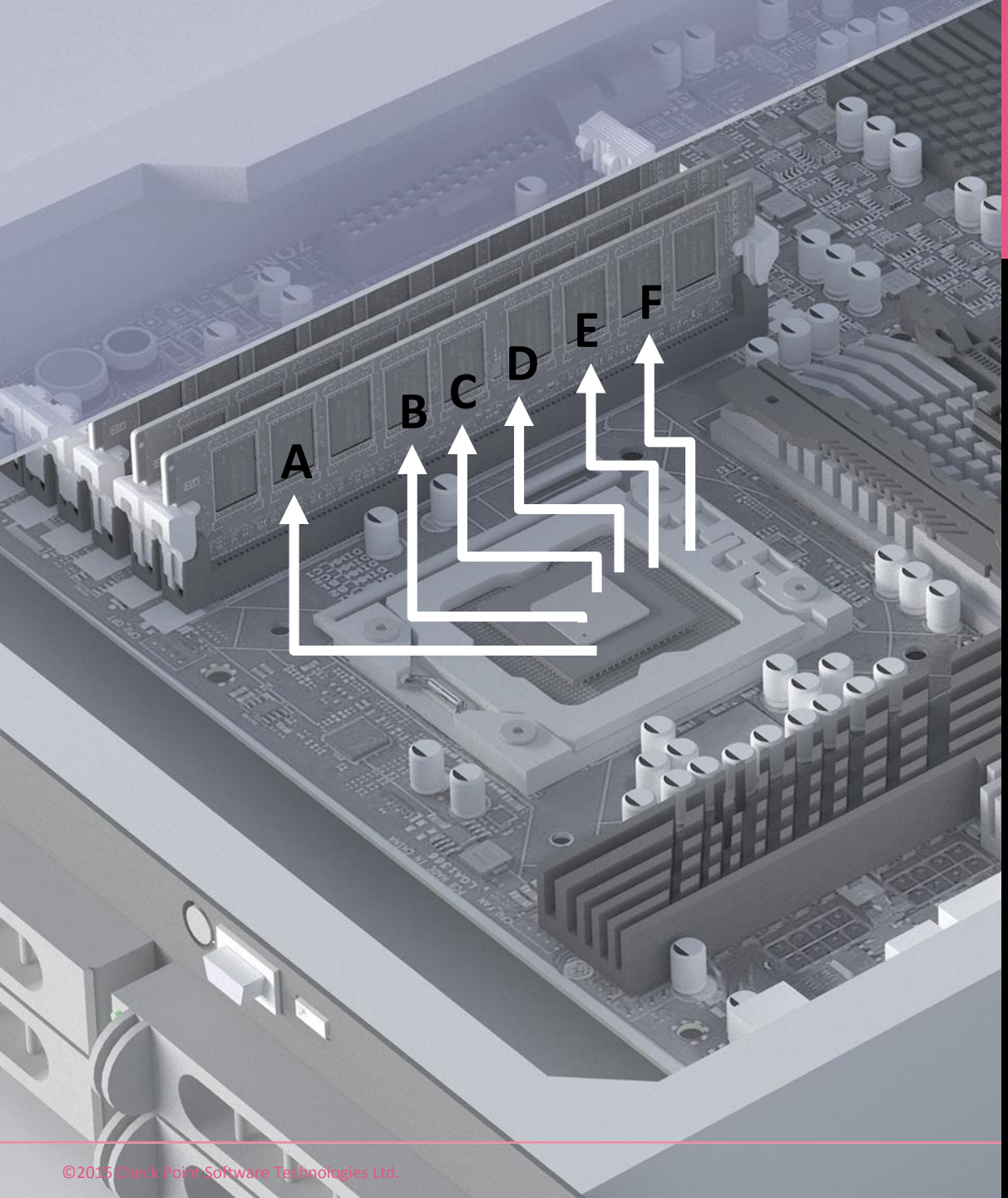
Опережая угрозы на один шаг

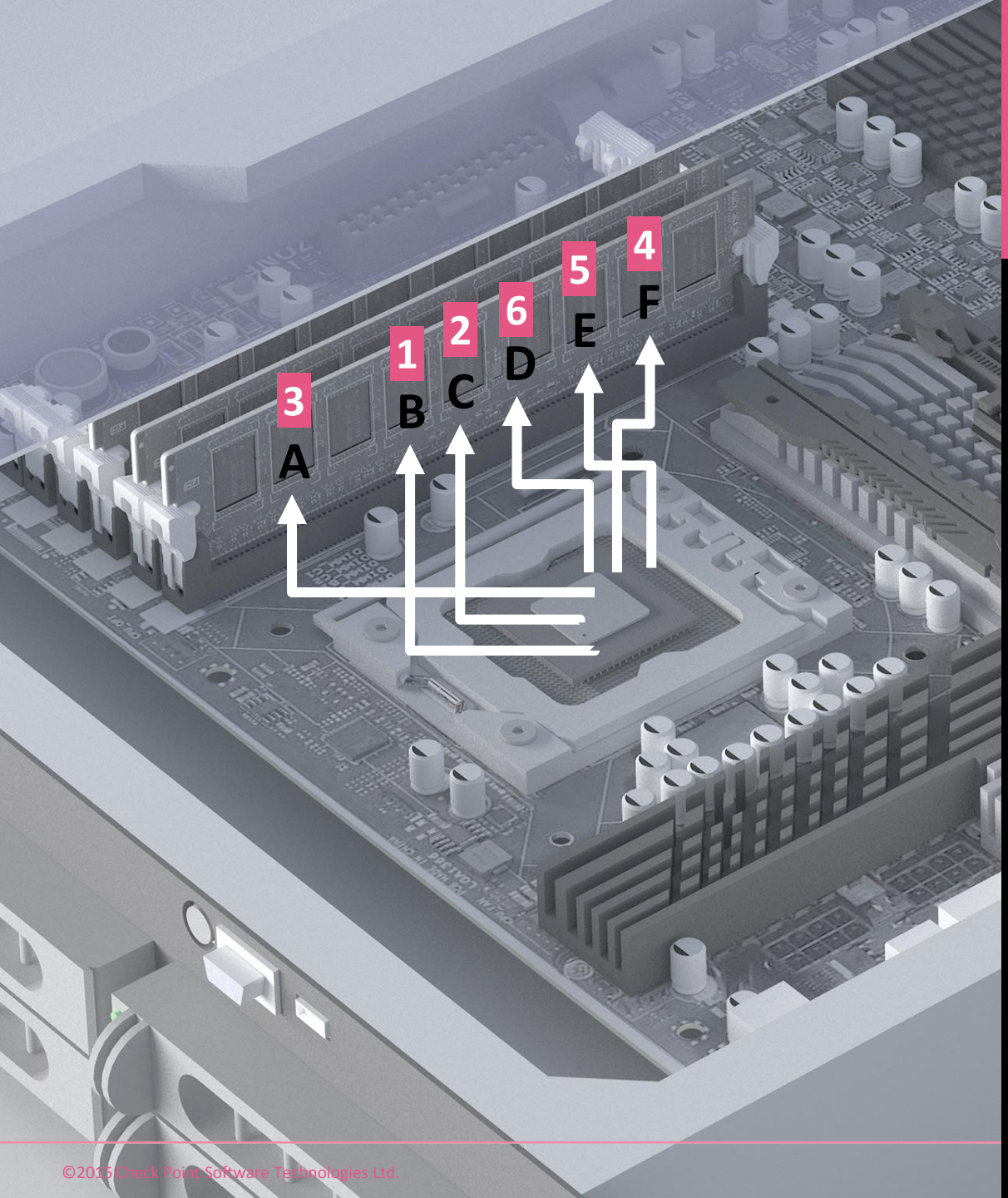
CPU LEVEL THREAT PREVENTION

Защита активностей на уровне CPU

РАБОТА CPU

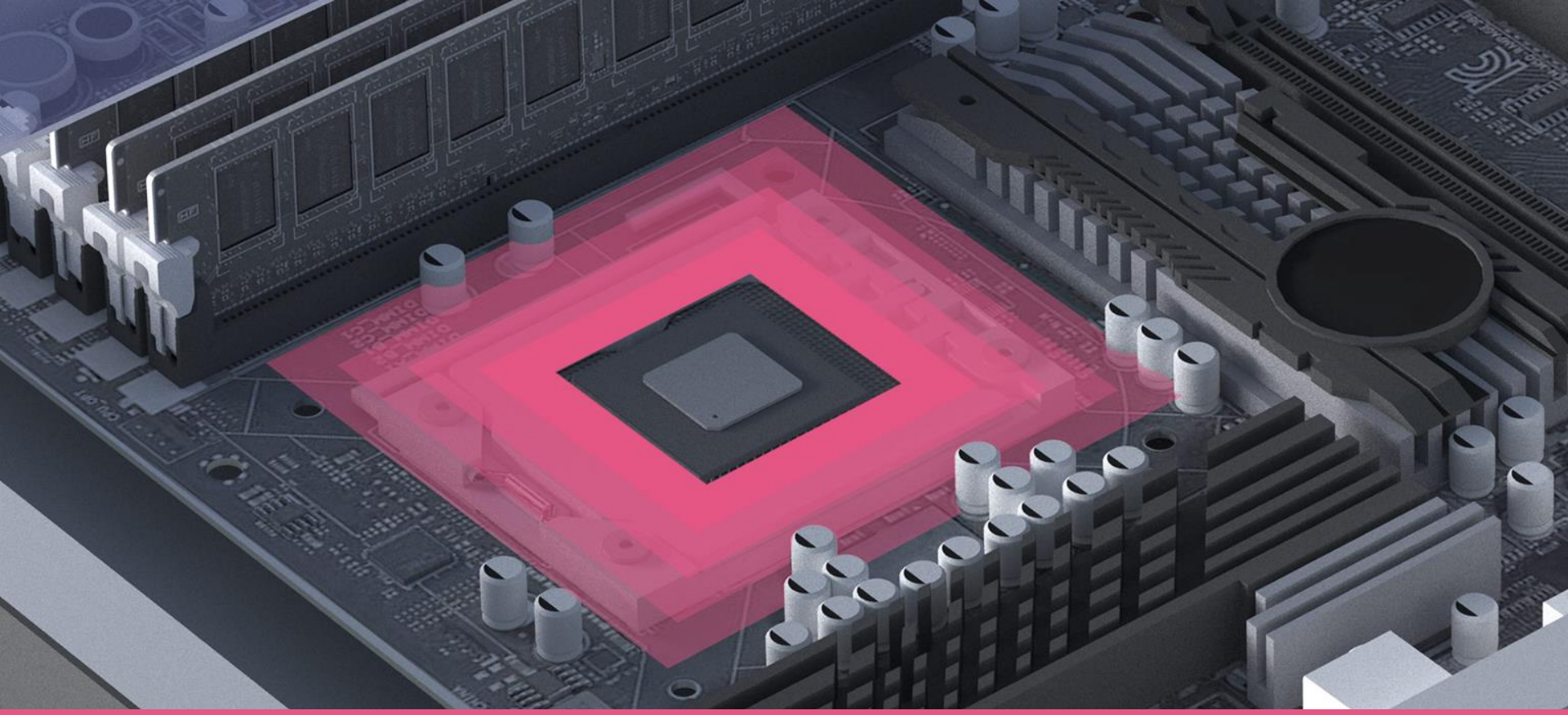
Стандартный режим





ROP EXPLOIT (Return Oriented Programming)

Перехватыет маленькие кусочки легитимного кода из памяти и заставляет CPU исполнять подменные команды



SANDBOX совмещенный с CPU LEVEL THREAT PREVENTION

- Определяет атаку до заражения
- Повышает уровень детектируемости
- На зависит от операционной системы
- Позволяет обойти недостатки песочницы

Посмотрим совершенно по новому?

Можем ли мы совершенно исключить угрозы?

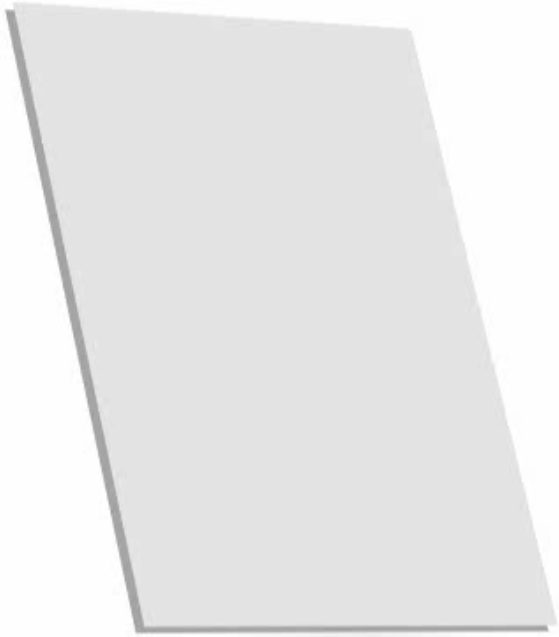
Опережая угрозы на один шаг

THREAT EXTRACTION

Реконструкция документов на лету, устранение источника угроз

ORIGINAL DOC

RECONSTRUCTED DOC



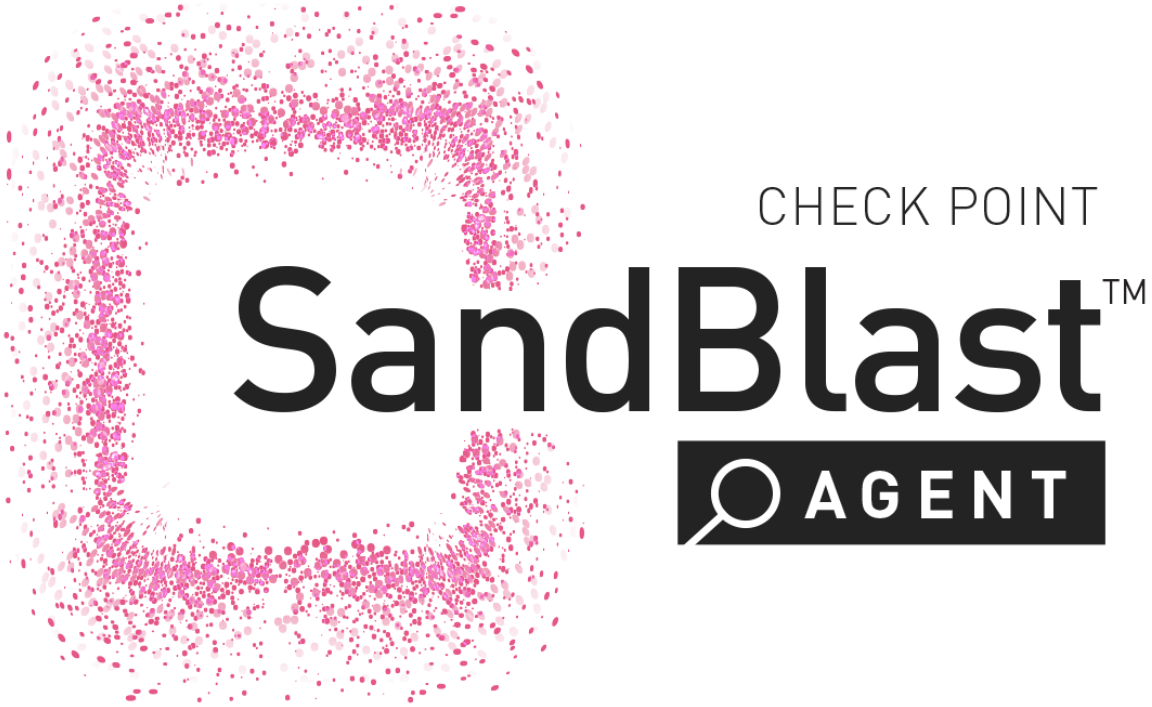
THREAT EXTRACTION

ONE STEP AHEAD

ПРЕДОТВРАЩЕНИЕ ЗАРАЖЕНИЯ ПК

детектирование и предотвращение попыток заражения и перехвата управления ПК

ПРЕДСТАВЛЯЕМ…



ЗАЩИТА И ИНСАЙД, ДАЮЩИЙ ПОНИМАНИЕ.

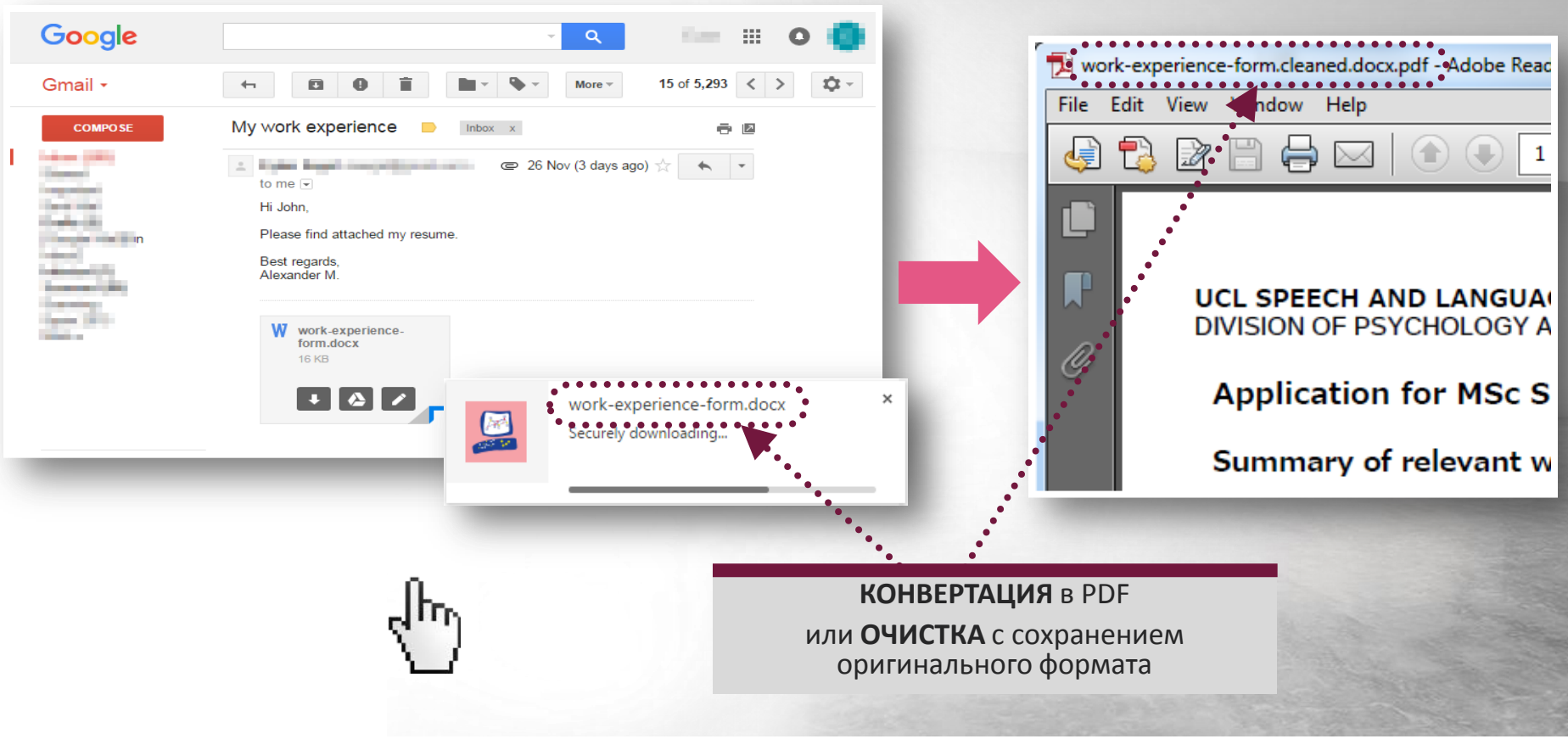
Предотвращение атаки – как работает...

1 Загрузки из интернет отправляются в облако SandBlast

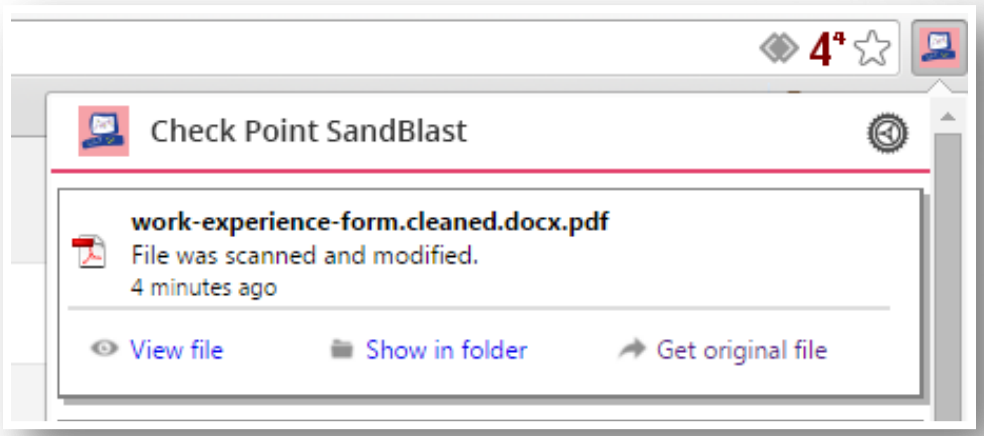
2 Очищенный файл доставляется немедленно

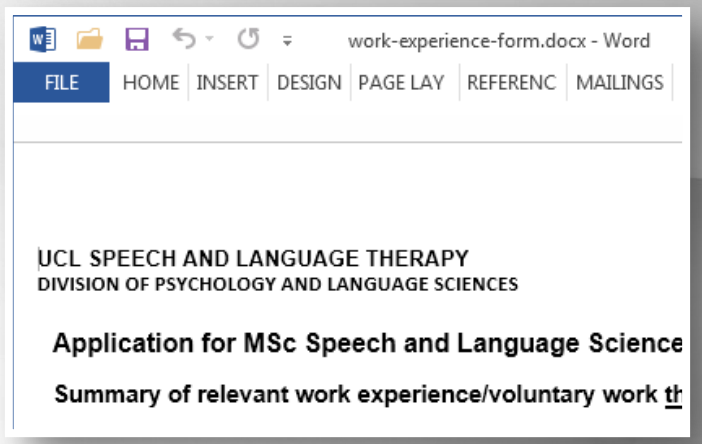
3 Оригинальный файл эмулируется в фоновом режиме

Мгновенная защита для контента, загруженного из интернета



Доступ к оригинальному файлу



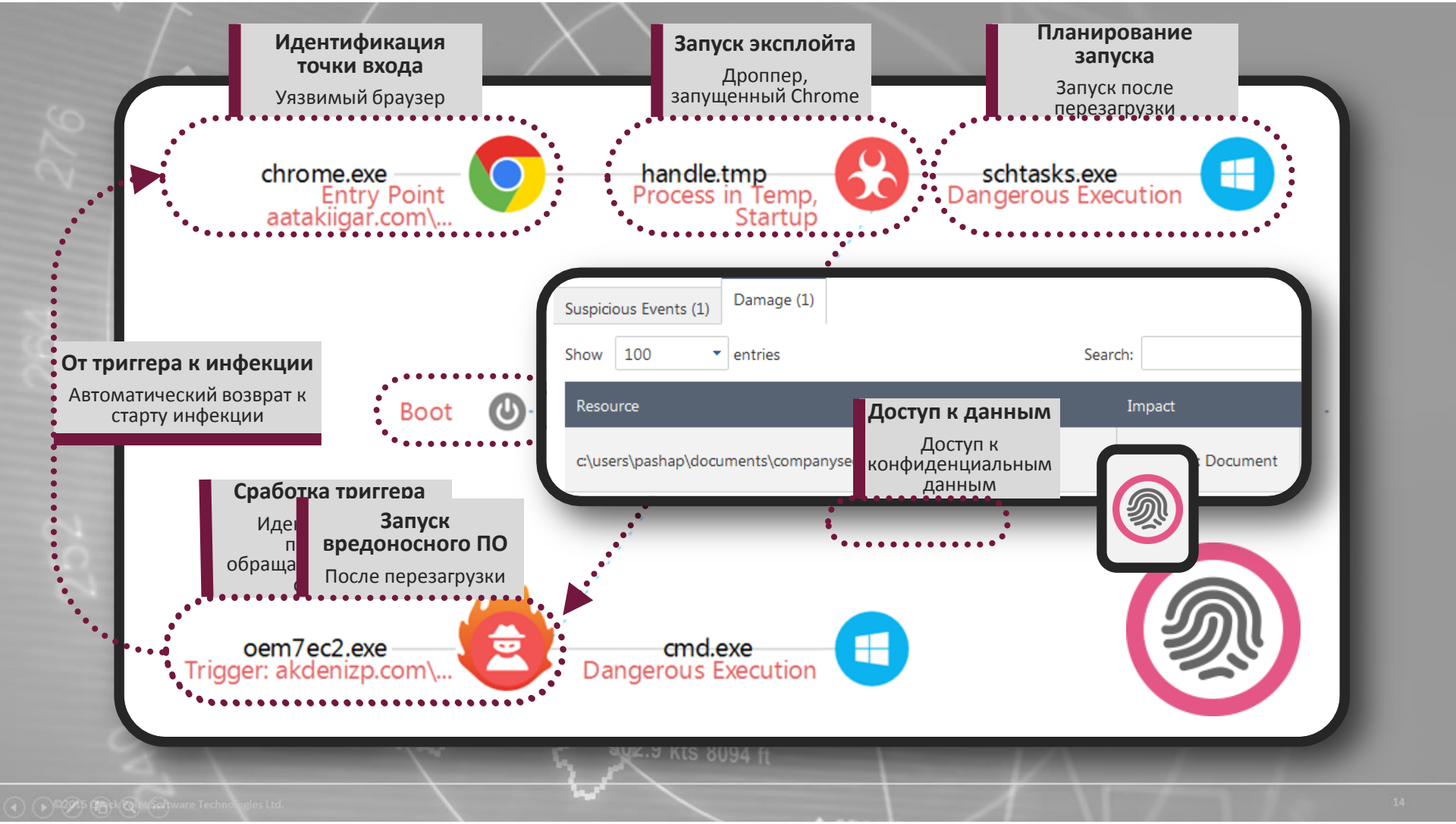


Только после эмуляции

если файл «чистый»

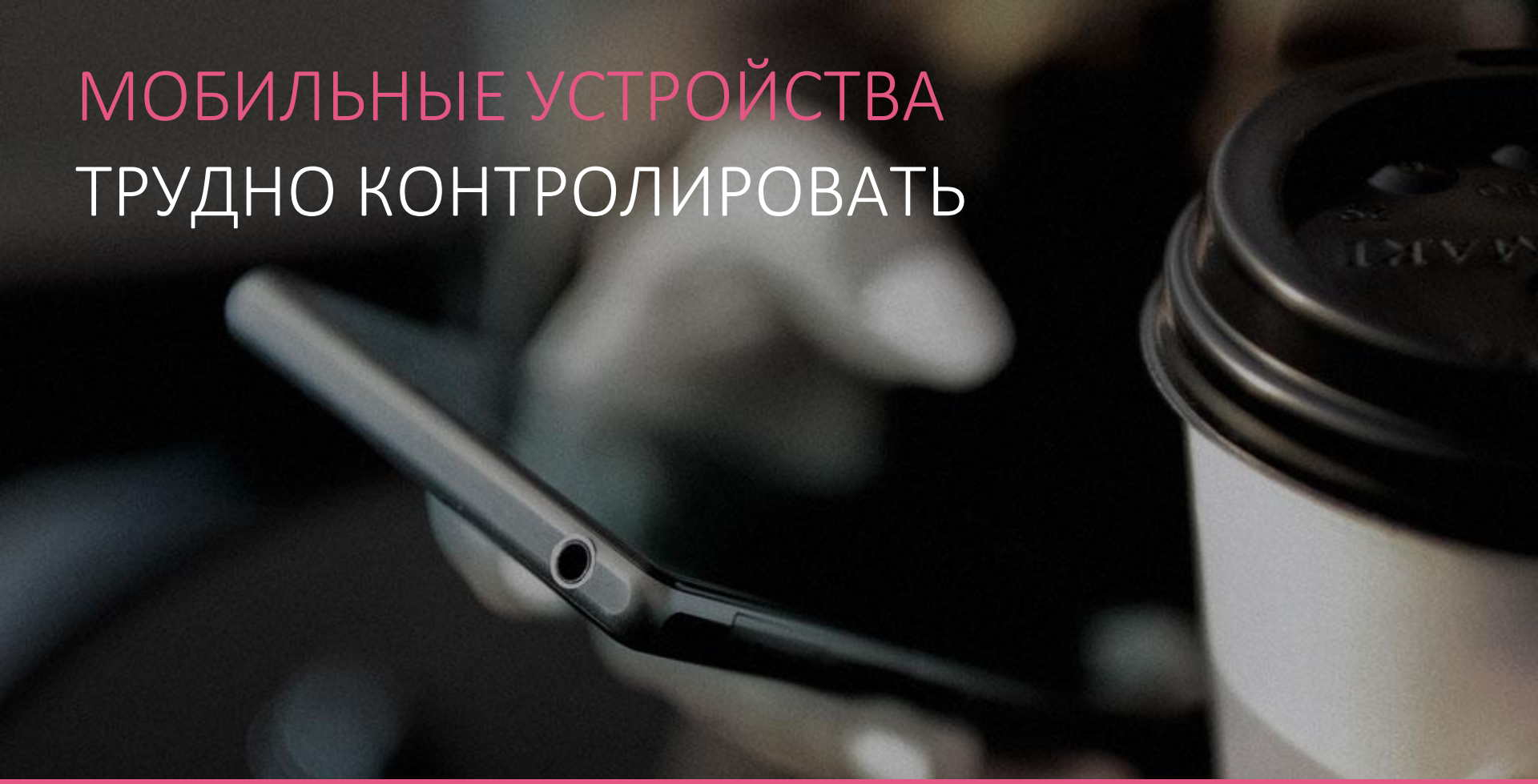
Самообслуживание

Техподдержка не привлекается


Идентификация точки входа
Уязвимый браузер
Запуск эксплойта
Дроппер, запущенный Chrome
Планирование запуска
Запуск после перезагрузки
chrome.exe
Entry Point
aatakiigar.com\...
handle.tmp
Process in Temp, Startup
schtasks.exe
Dangerous Execution
Suspicious Events (1)
Damage (1)
Show 100 entries
Search:
Resource
Impact
c:\users\pashap\documents\companyse
Document
Доступ к данным
Доступ к конфиденциальным данным
От триггера к инфекции
Автоматический возврат к старту инфекции
Boot
Сработка триггера
Запуск вредоносного ПО
После перезагрузки
oem7ec2.exe
Trigger: akdenizp.com\...
cmd.exe
Dangerous Execution

Как защитить то,

ЧТО ВНЕ НАШЕГО КОНТРОЛЯ



МОБИЛЬНЫЕ УСТРОЙСТВА ТРУДНО КОНТРОЛИРОВАТЬ

Нет фиксированного периметра

Смешивание личной и корпоративной информации

Невозможность установки сигнатурных AV на некоторых платформах

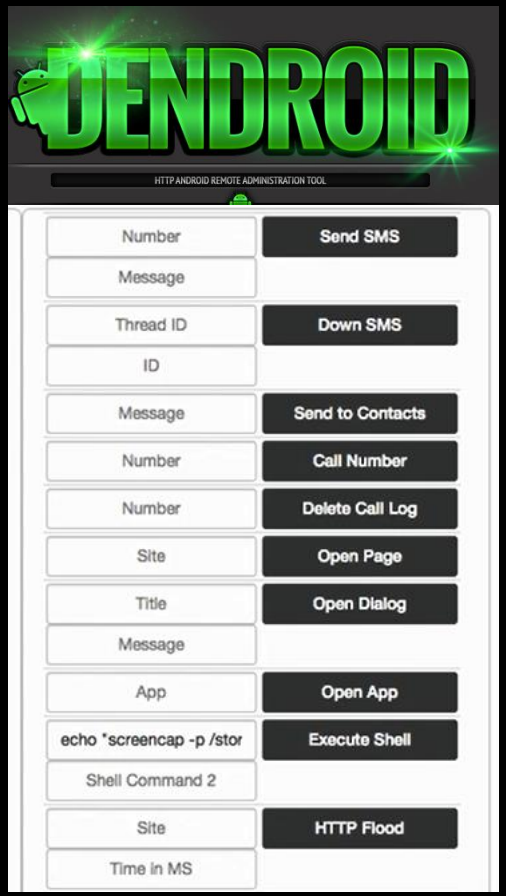
Тяжело предсказать поведение пользователя

Существующие решения

ОСТАВЛЯЮТ ДЫРЫ

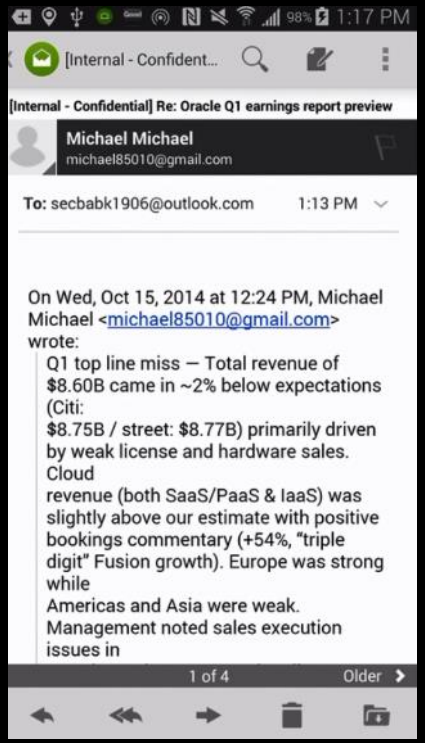
В большинстве своем они сфокусированы на управлении устройствами (MDM) и в меньшей степени на защите

ЭТО ПРОСТО



Геопозиция

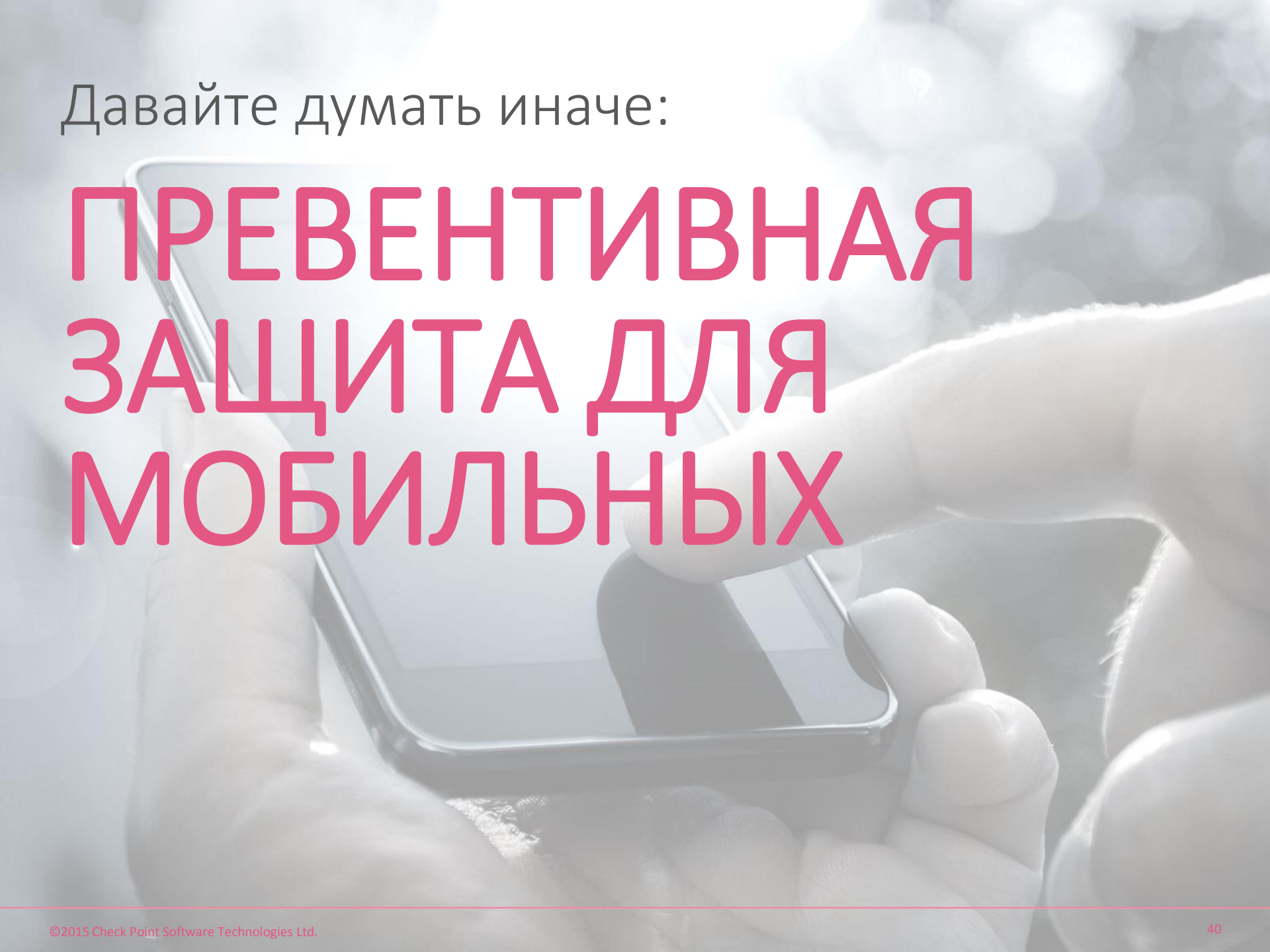
Почта



Записи

Давайте думать иначе:

ПРЕВЕНТИВНАЯ ЗАЩИТА ДЛЯ МОБИЛЬНЫХ



Превентивная защита для мобильных

Мобильные приложения

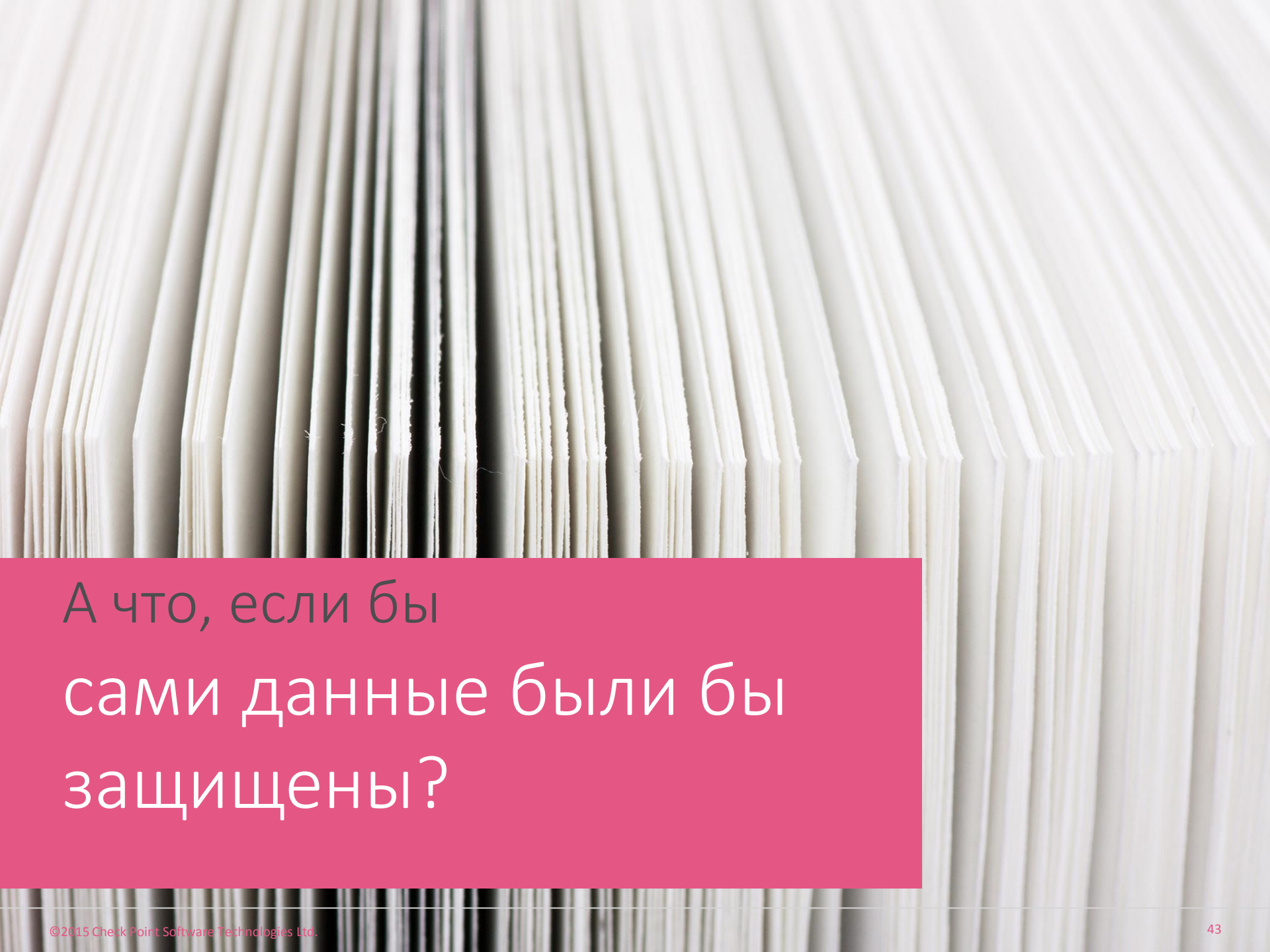
INTERNET

Устройство

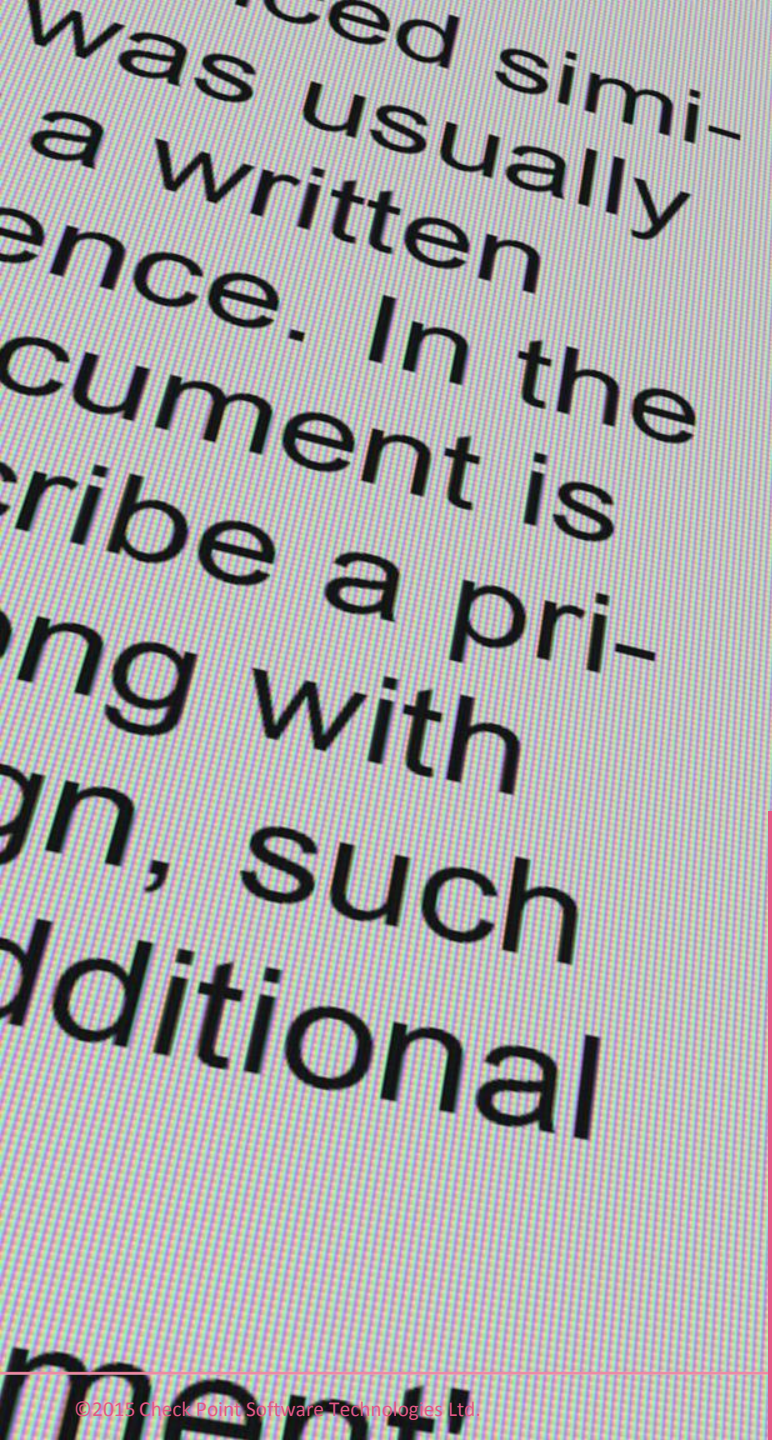
Check Point Capsule

Защищая мобильное устройсво

ЕДИНОЕ РЕШЕНИЕ
ДЛЯ МОБИЛЬНОЙ БЕЗОПАСНОСТИ



А что, если бы сами данные были бы защищены?

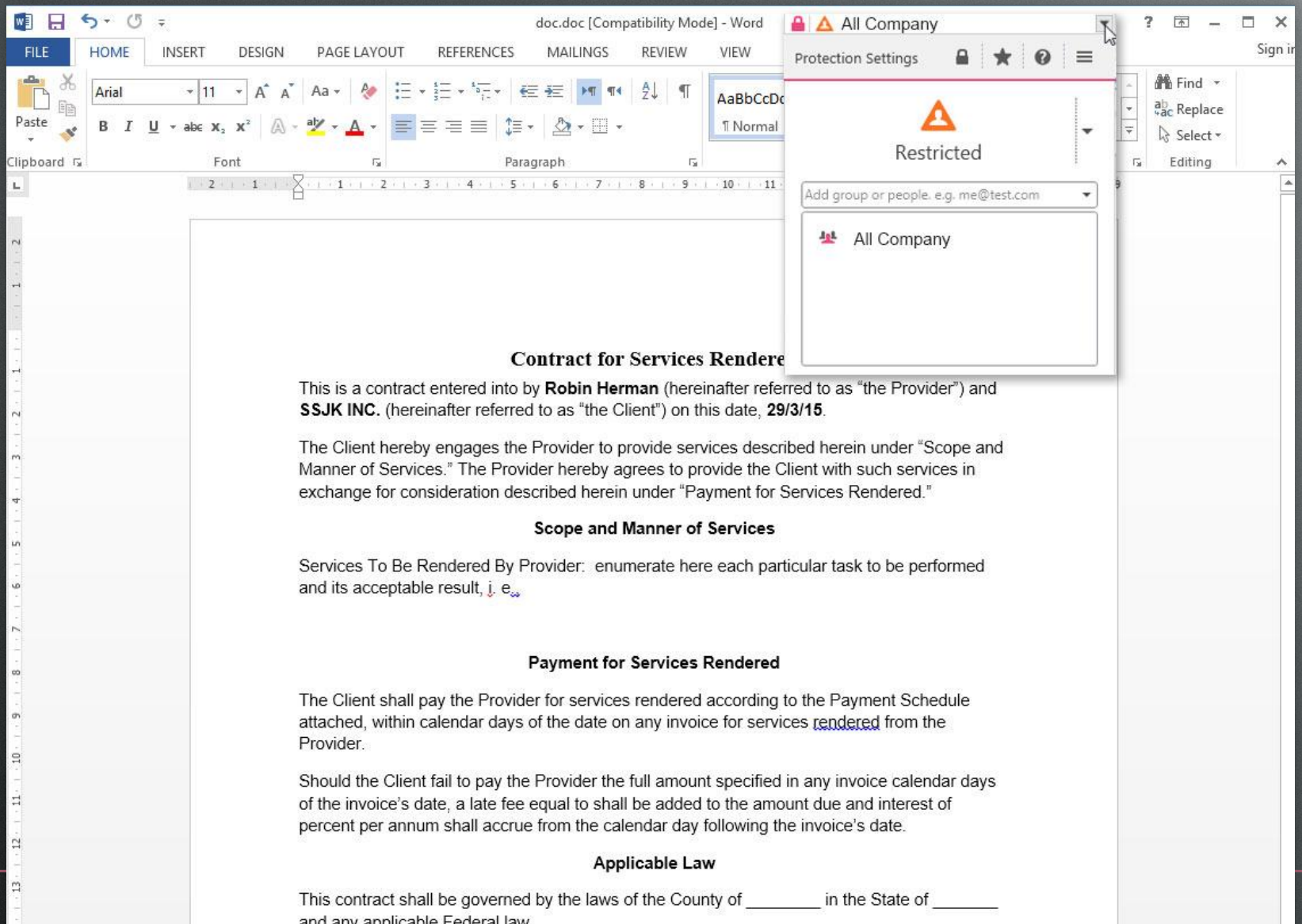


Оставаясь на один шаг впереди:

CHECK POINT DOCUMENT SECURITY

Защита документов, где бы они не находились

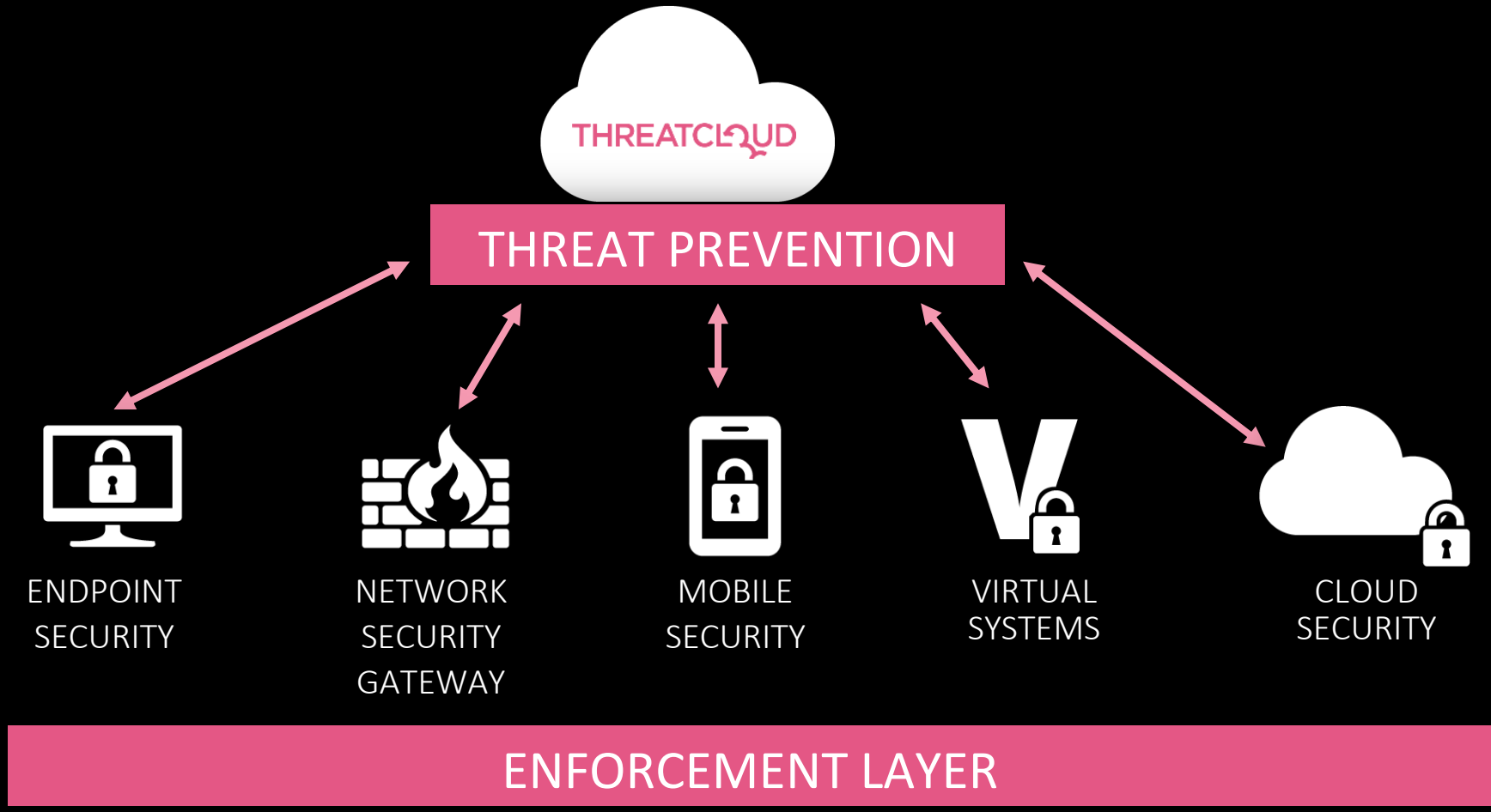
Защита документов в момент создания



Все основано на нашей архитектуре

SOFTWARE DEFINED PROTECTION (SDP)

Архитектура, которая постоянно обновляет уровни защиты



Check Point
SOFTWARE TECHNOLOGIES LTD.

СПАСИБО!