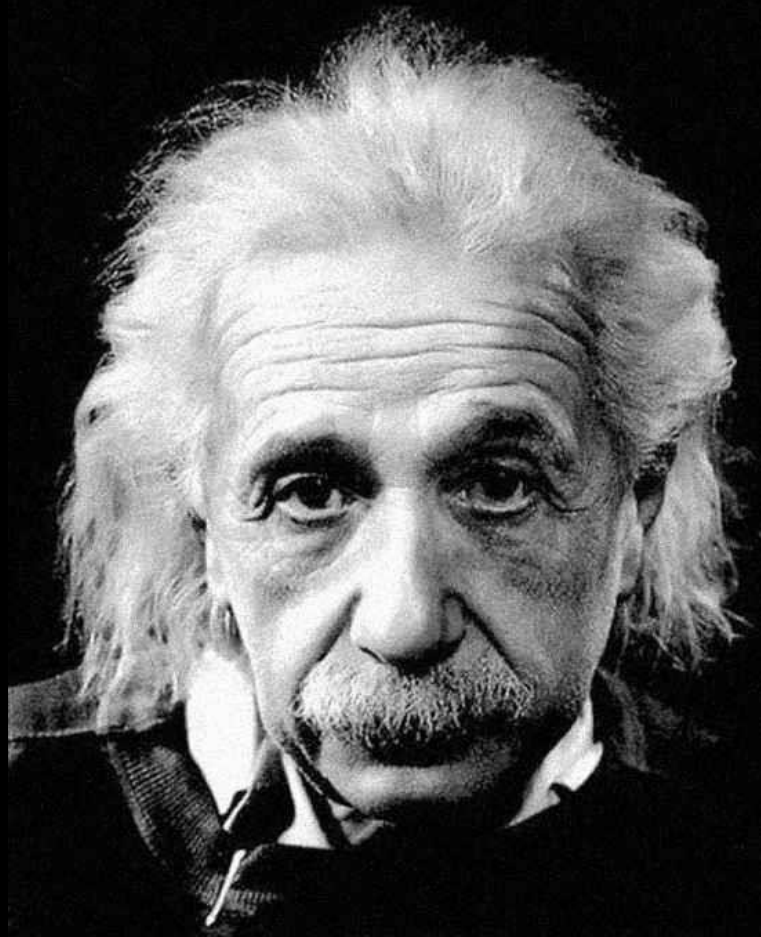




Check Point  
SOFTWARE TECHNOLOGIES LTD.

# 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*

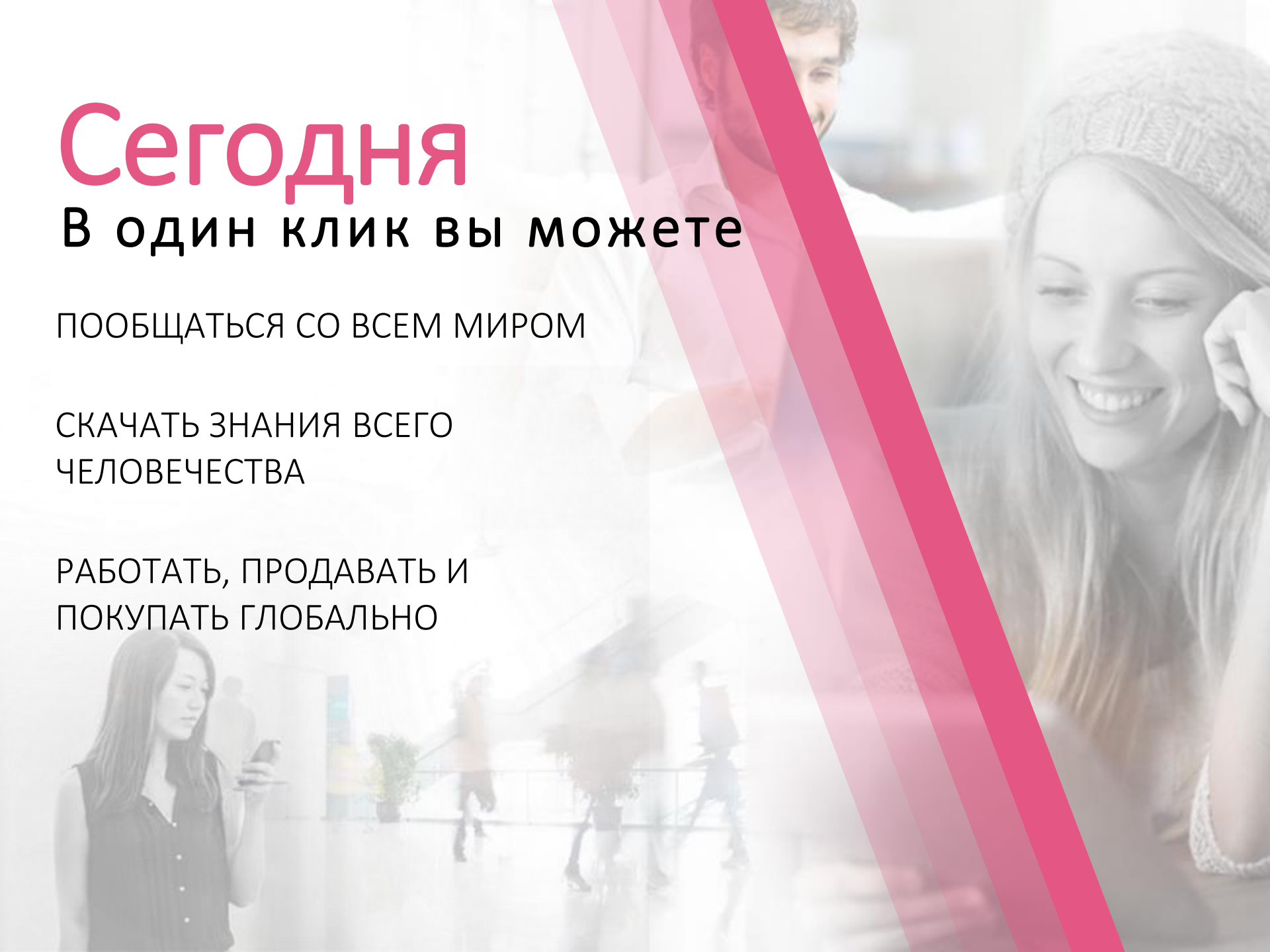
# Сегодня

## 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**

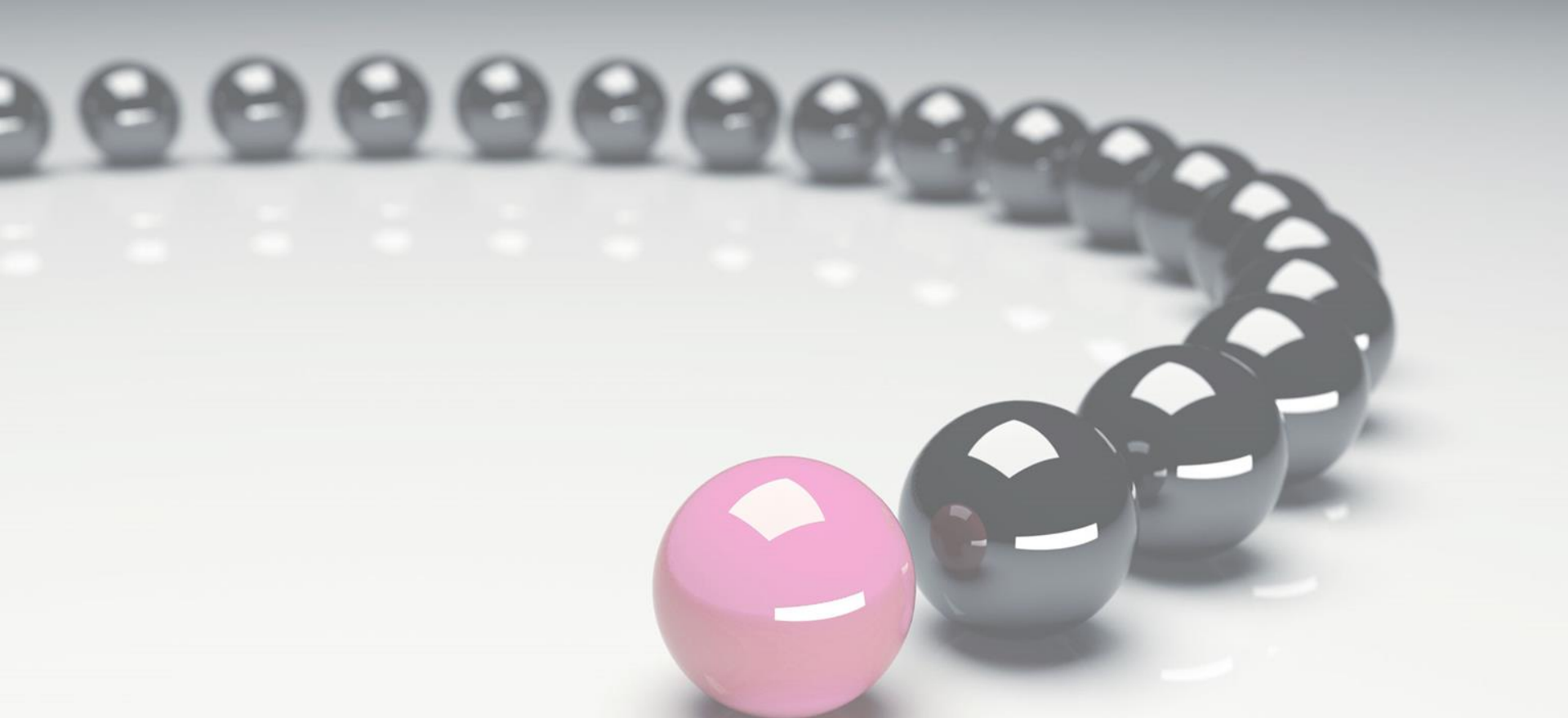
**High Risk Applications**

**Application Control**

A row of black spheres is arranged in a slightly curved line across the top of the image. In the foreground, a single pink sphere is positioned to the left of the black spheres, which are receding into the background.

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%

организаций скачивали незнакомый  
вредоносный код

# 200,000

уникальных угроз обнаруживается  
ежедневно

---

# E-mail От миссис Мира

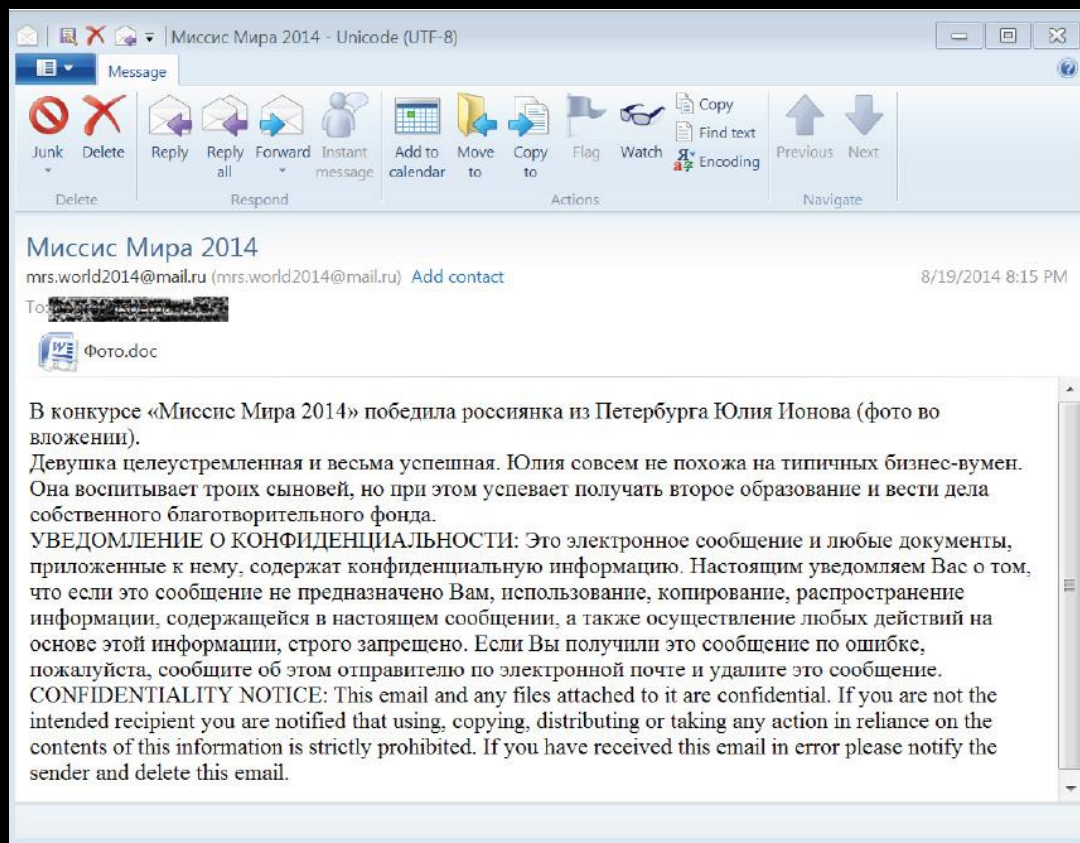
Таргетированная атака 2014 года

## ЦЕЛИ:

Российские и европейские организации

## МЕТОД:

Точечная фишинговая рассылка с эксплойтом в формате MS Word

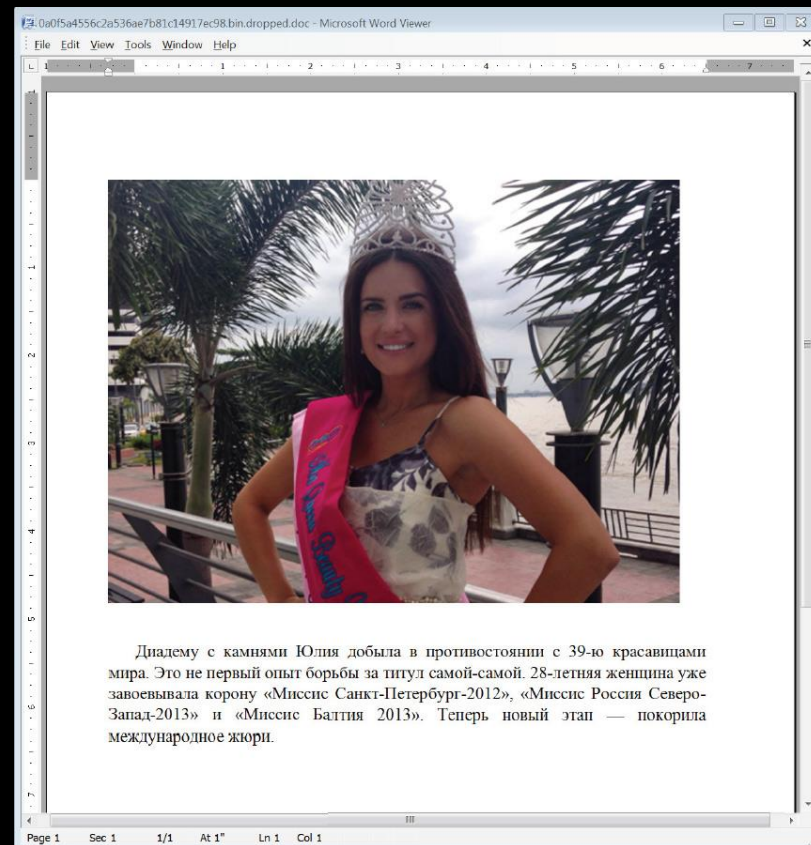


# Вредоносный документ

## 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

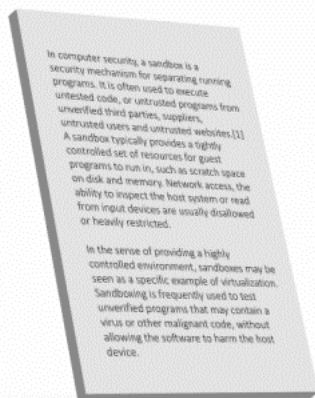


Один из способов защиты  
от неизвестного

**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 загрузки 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

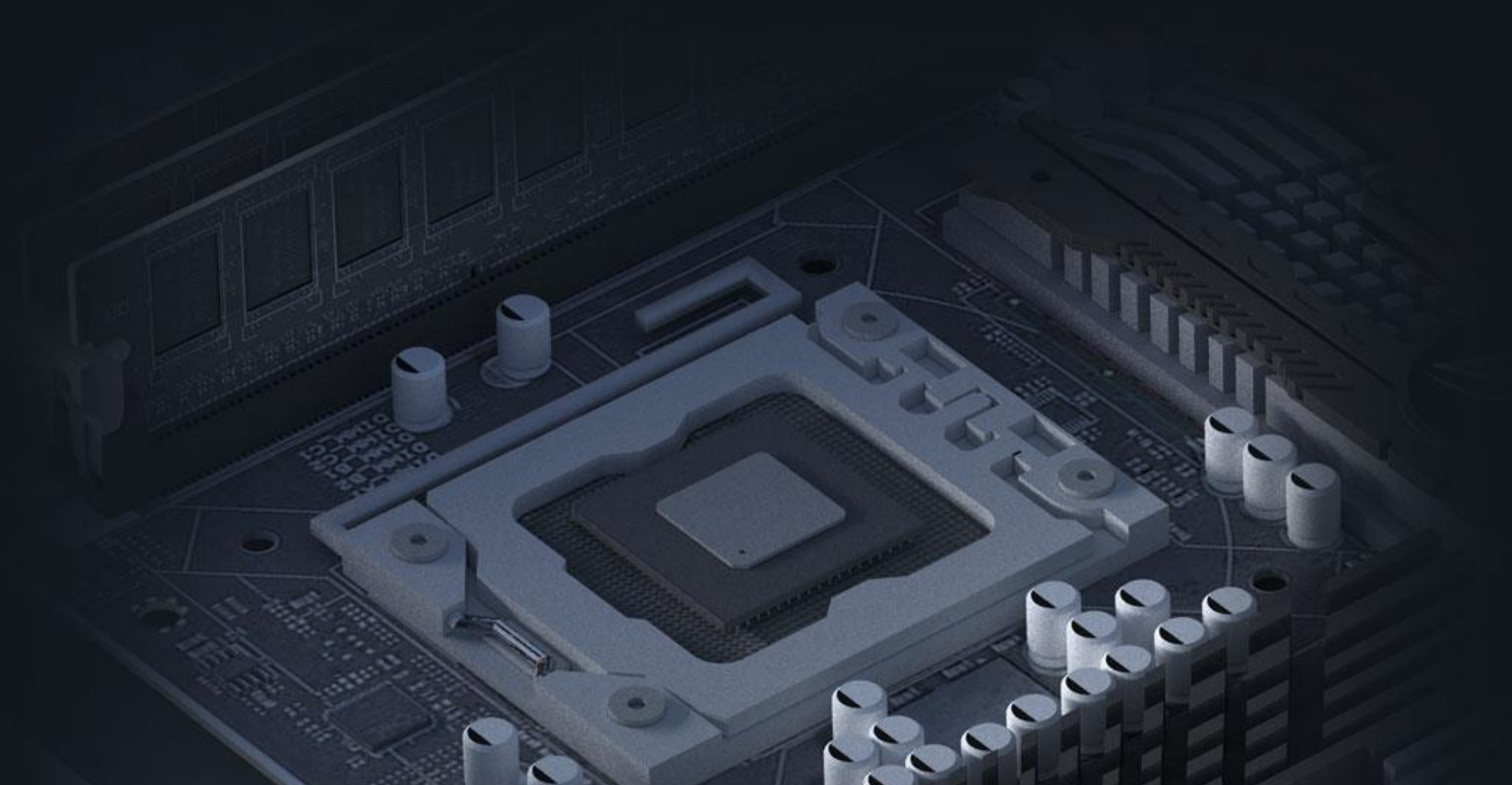
Уязвимость

Exploit

Shellcode

Malware





Опережая угрозы на **один** шаг

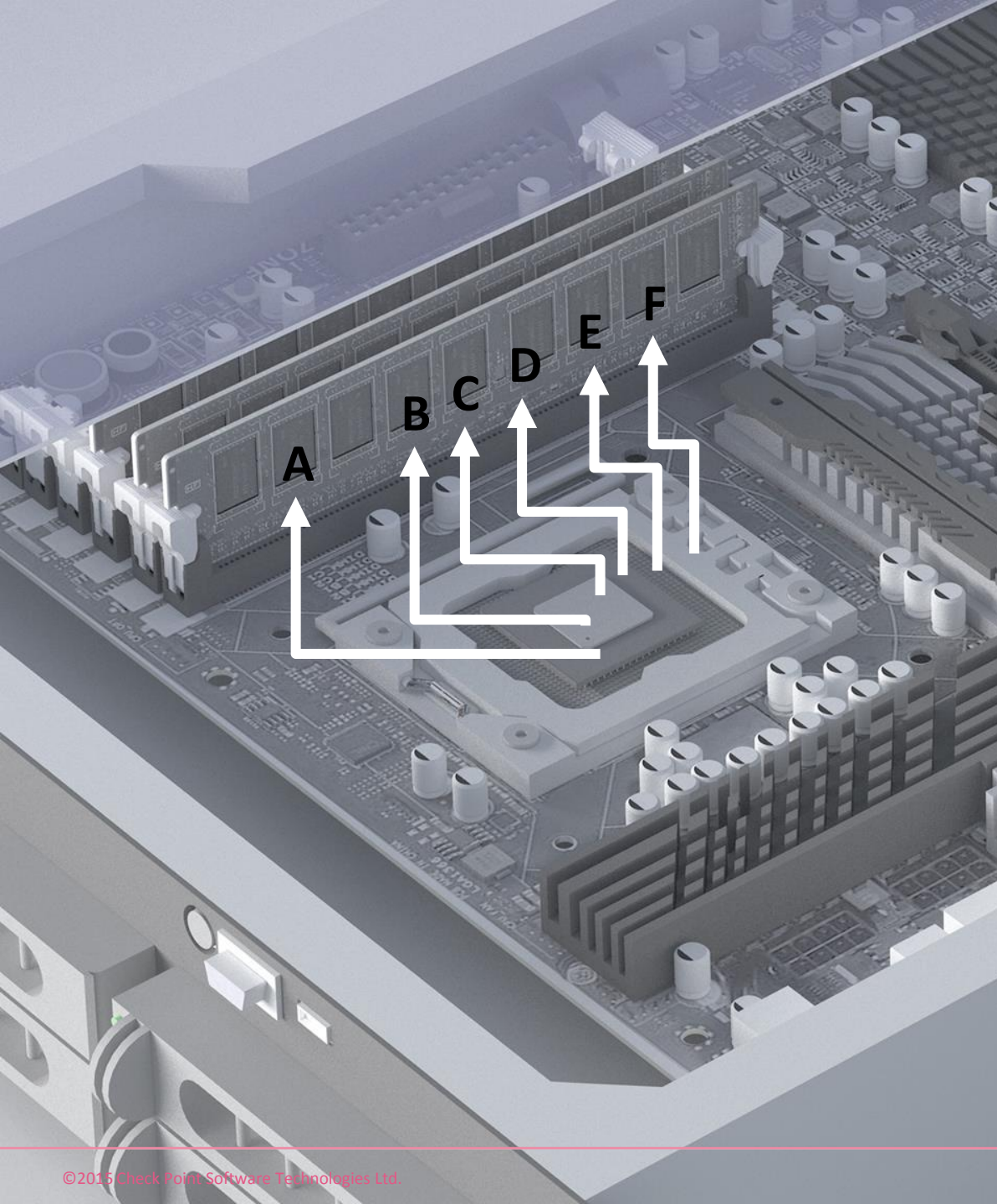
**CPU LEVEL THREAT PREVENTION**

Защита активностей на уровне CPU



# РАБОТА CPU

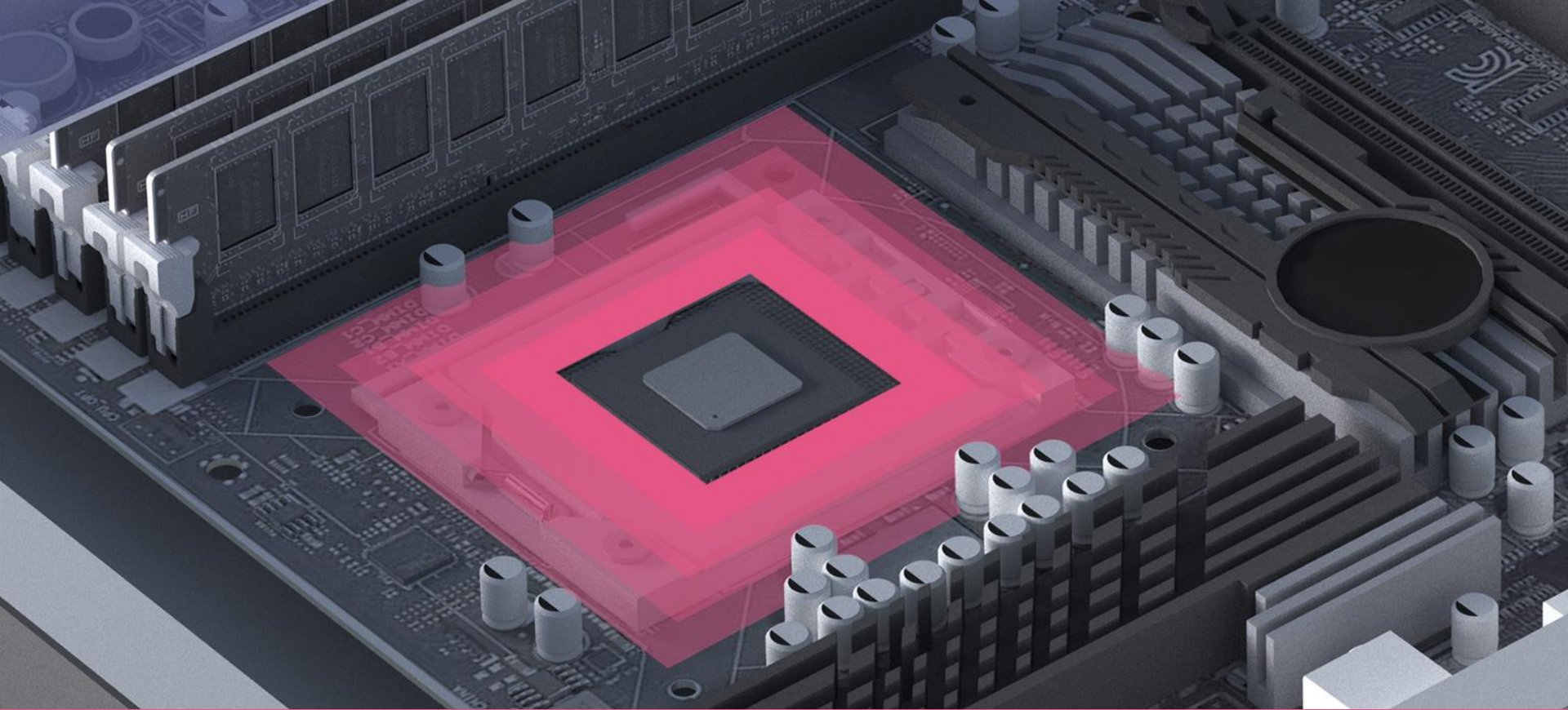
## Стандартный режим



# ROP EXPLOIT (Return Oriented Programming)

Перехватывает  
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



Check Point Threat Extraction eliminates malware contained in emailed and web-downloaded documents. Exploitable content including active content and various embedded objects are removed and files are reconstructed using known safe elements. Reconstructed files eliminate potential threats while providing zero malware documents with no delays.

## RECONSTRUCTED DOC

THREAT  
EXTRACTION





## ONE STEP AHEAD

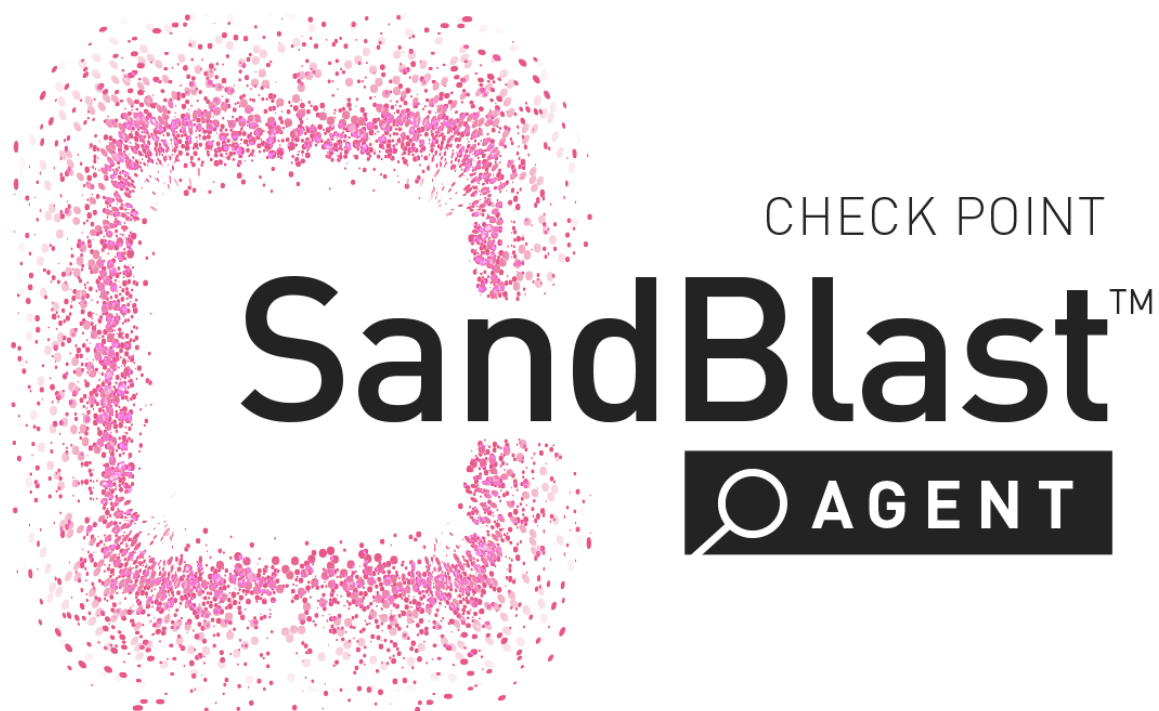
# ПРЕДОТВРАЩЕНИЕ ЗАРАЖЕНИЯ ПК

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

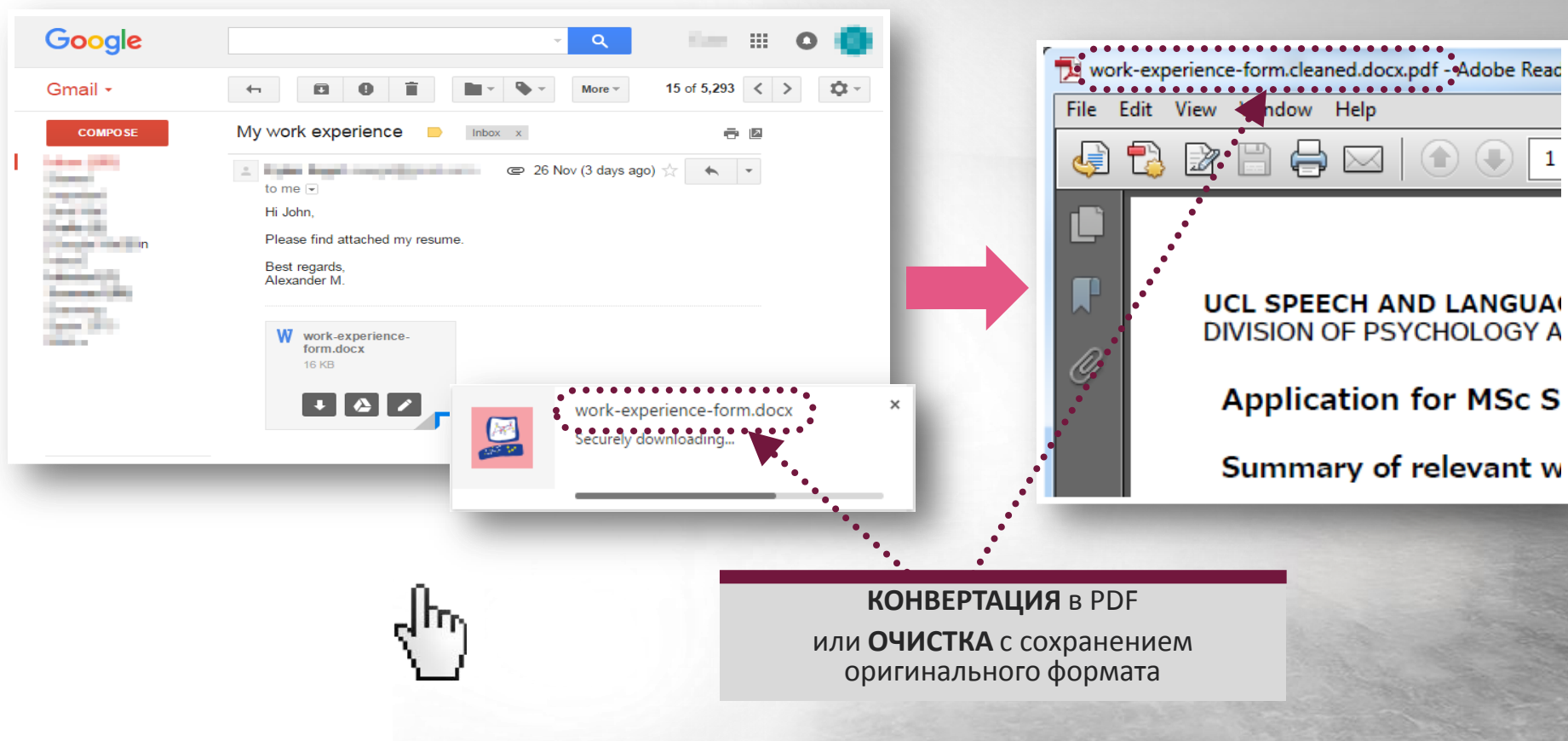
2

Очищенный файл  
доставляется  
немедленно

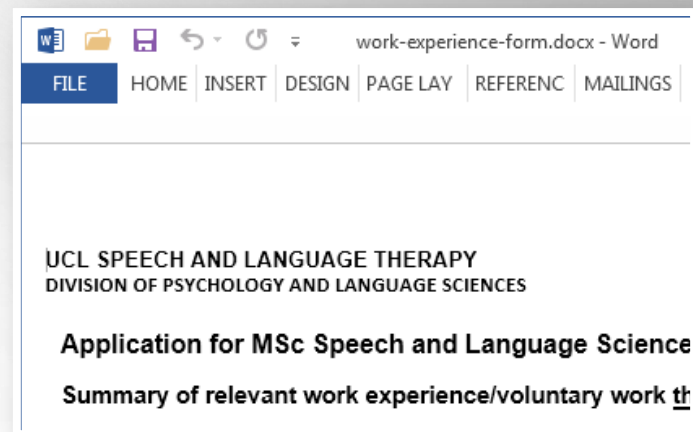
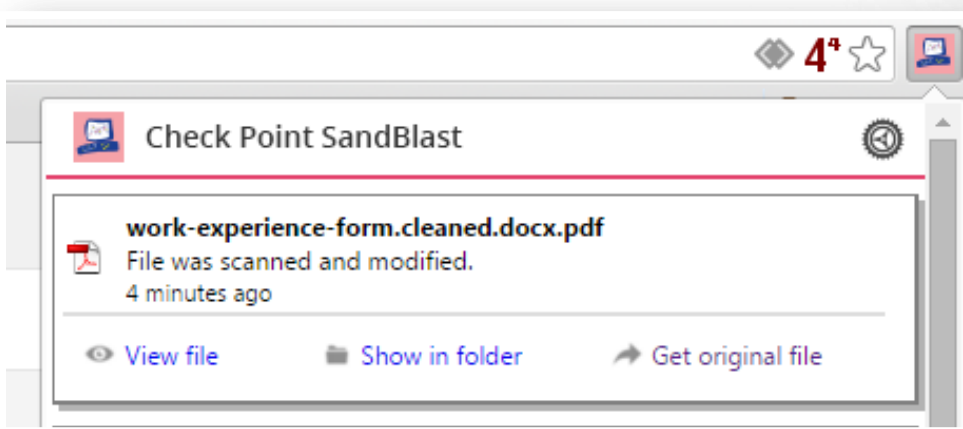
3

Оригинальный файл  
эмулируется в  
фоновом режиме

# Мгновенная защита для контента, загруженного из интернета

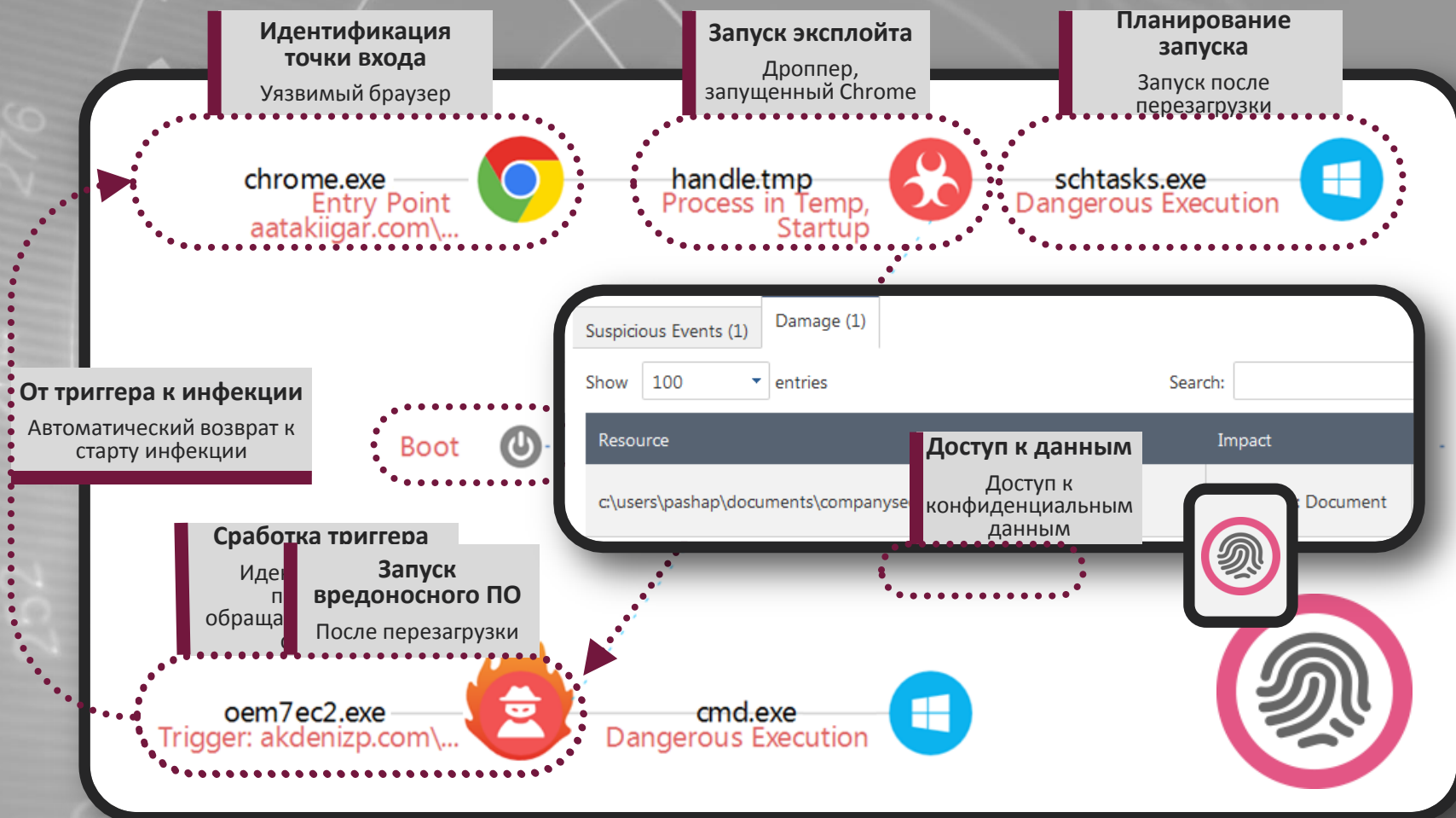


# Доступ к оригинальному файлу



**Только после эмуляции**  
если файл «чистый»

**Самообслуживание**  
Техподдержка не привлекается



Как защитить то,

# ЧТО ВНЕ НАШЕГО КОНТРОЛЯ



# МОБИЛЬНЫЕ УСТРОЙСТВА ТРУДНО КОНТРОЛИРОВАТЬ

A close-up photograph showing a hand holding a dark-colored smartphone. The phone is angled, showing its side profile with a visible earpiece. To the right of the phone is a white disposable coffee cup with a black lid. The background is dark and out of focus.

Нет фиксированного периметра

Смешивание личной и корпоративной информации

Невозможность установки сигнатурных AV на некоторых платформах

Тяжело предсказать поведение пользователя

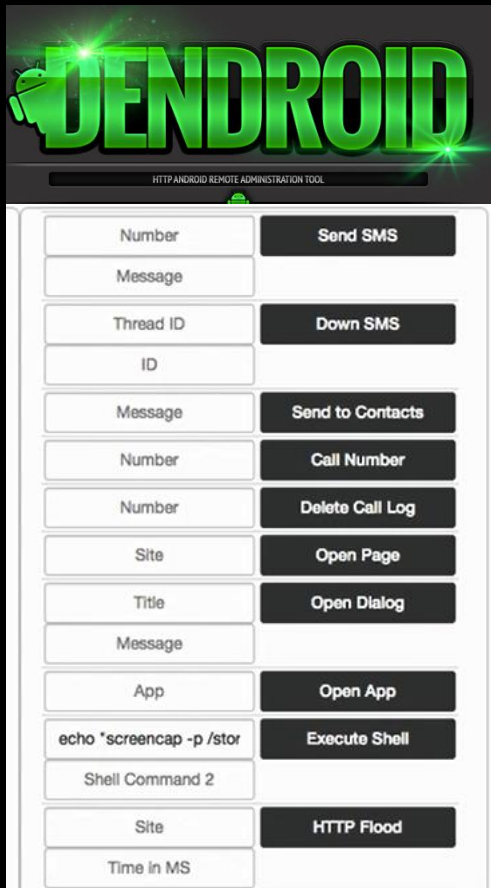


Существующие решения

# ОСТАВЛЯЮТ ДЫРЫ

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

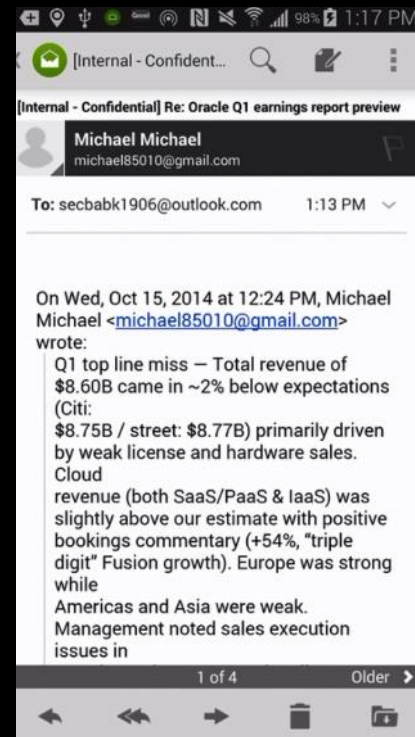
# ЭТО ПРОСТО



Геопозиция



Почта



Записи



Давайте думать иначе:

# ПРЕВЕНТИВНАЯ ЗАЩИТА ДЛЯ МОБИЛЬНЫХ

# Превентивная защита для мобильных

Мобильные приложения

INTERNET

Устройство



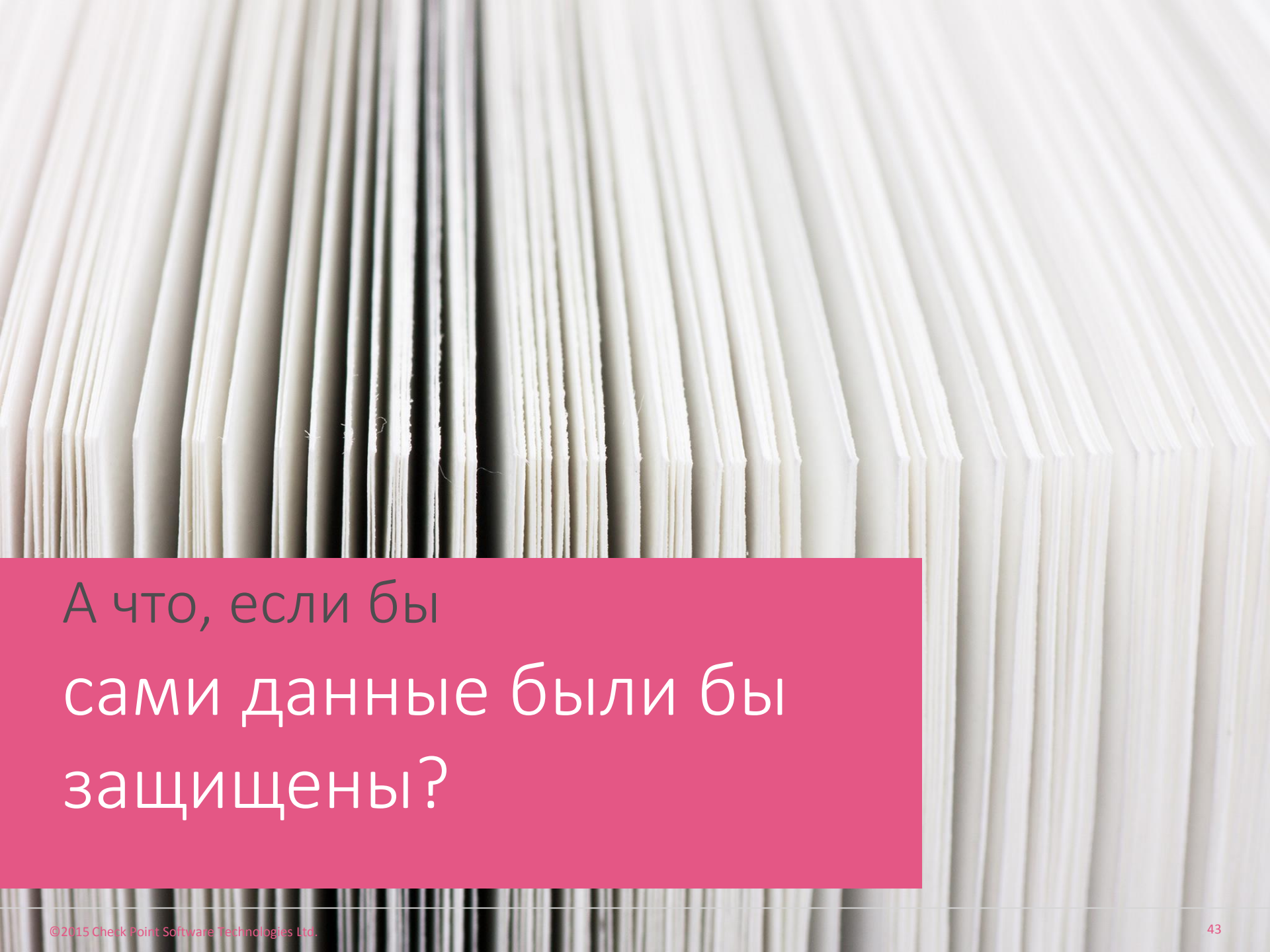
Check Point Capsule

# Защищая мобильное устройство



**ЕДИНОЕ РЕШЕНИЕ  
ДЛЯ МОБИЛЬНОЙ БЕЗОПАСНОСТИ**





А что, если бы  
сами данные были бы  
защищены?



...ced simi-  
was usually  
a written  
ence. In the  
cument is  
cribe a pri-  
ng with  
gn, such  
dditional

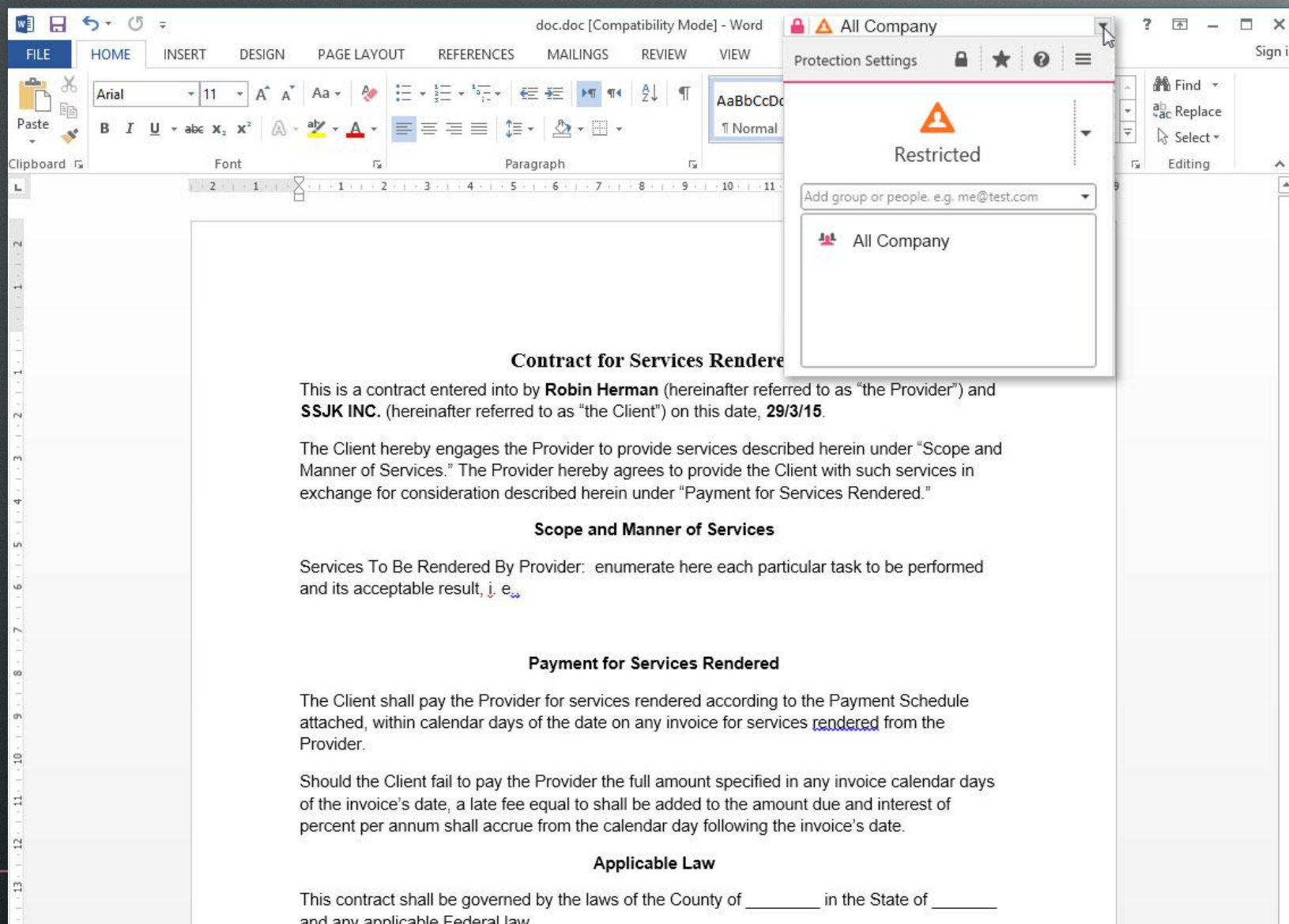
Оставаясь на один шаг впереди:

## CHECK POINT DOCUMENT SECURITY

Защита документов, где бы они не  
находились



# Защита документов в момент создания



The screenshot shows a Microsoft Word document titled "doc.doc [Compatibility Mode] - Word". The document is protected, as indicated by the "Protection Settings" pane on the right, which shows a lock icon and the text "Restricted". The document content is a contract for services rendered, with sections for "Contract for Services Rendered", "Scope and Manner of Services", "Payment for Services Rendered", and "Applicable Law". The "Protection Settings" pane also shows a list of groups with "All Company" selected.

**Contract for Services Rendered**

This is a contract entered into by **Robin Herman** (hereinafter referred to as "the Provider") and **SSJK INC.** (hereinafter referred to as "the Client") on this date, **29/3/15**.

The Client hereby engages the Provider to provide services described herein under "Scope and Manner of Services." The Provider hereby agrees to provide the Client with such services in exchange for consideration described herein under "Payment for Services Rendered."

**Scope and Manner of Services**

Services To Be Rendered By Provider: enumerate here each particular task to be performed and its acceptable result, i. e.,

**Payment for Services Rendered**

The Client shall pay the Provider for services rendered according to the Payment Schedule attached, within calendar days of the date on any invoice for services rendered from the Provider.

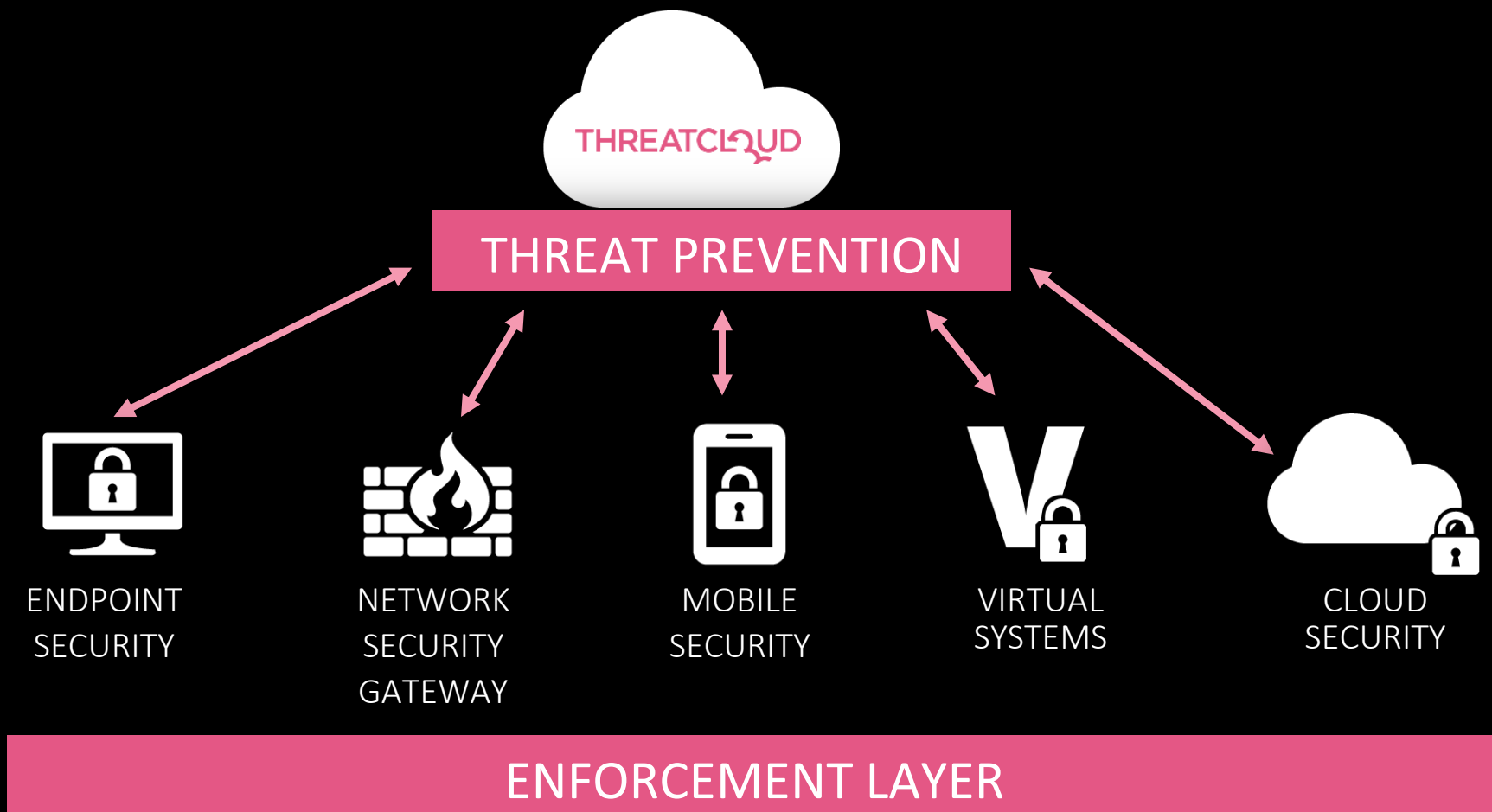
Should the Client fail to pay the Provider the full amount specified in any invoice calendar days of the invoice's date, a late fee equal to shall be added to the amount due and interest of percent per annum shall accrue from the calendar day following the invoice's date.

**Applicable Law**

This contract shall be governed by the laws of the County of \_\_\_\_\_ in the State of \_\_\_\_\_ and any applicable Federal law.

# Все основано на нашей архитектуре **SOFTWARE DEFINED PROTECTION (SDP)**

Архитектура, которая постоянно обновляет уровни защиты



# СПАСИБО!

