

# Решения IBM Trusteer для предотвращения финансового онлайн мошенничества

**Николай Поборцев**

IBM Security Sales Representative

[n.pobortsev@ru.ibm.com](mailto:n.pobortsev@ru.ibm.com)

*new threats, new thinking*

 Global	Сотни клиентов 100,000,000 ПК
 Solutions	Предотвращение мошенничества и защита от угроз
 Leader	Интеллект Технология Экспертиза

## Нам доверяют

<b>7/10</b> Top US Banks 	<b>9/10</b> Top UK Banks 
<b>4/5</b> Top Canadian Banks 	<b>Major</b> European Banks 

**Gartner**

Признал **IBM**

**Trusteer лидером** в  
2013 Magic Quadrant  
for Web Fraud  
Detection **второй год**  
**подряд**

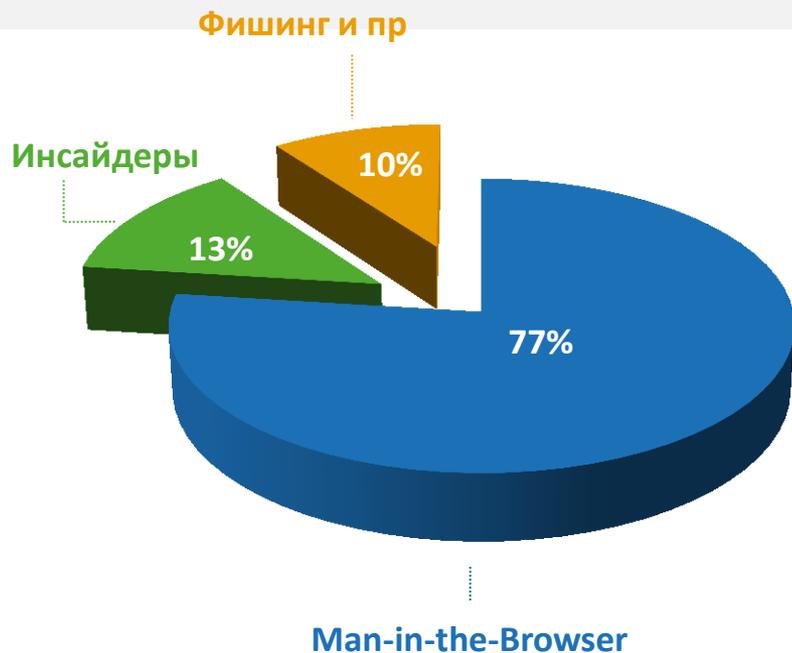
Цитаты Гартнера

“Все клиенты дали  
положительный отзыв о  
Trusteer Rapport и Trusteer  
Pinpoint Malware Detection”

“успешно предотвращает  
мошенничество с  
использованием зловредов”

“решение очень легко  
внедряется”

## Man-in-the-browser несет самый высокий риск



Source: McKinsey & Company

## Регуляторы



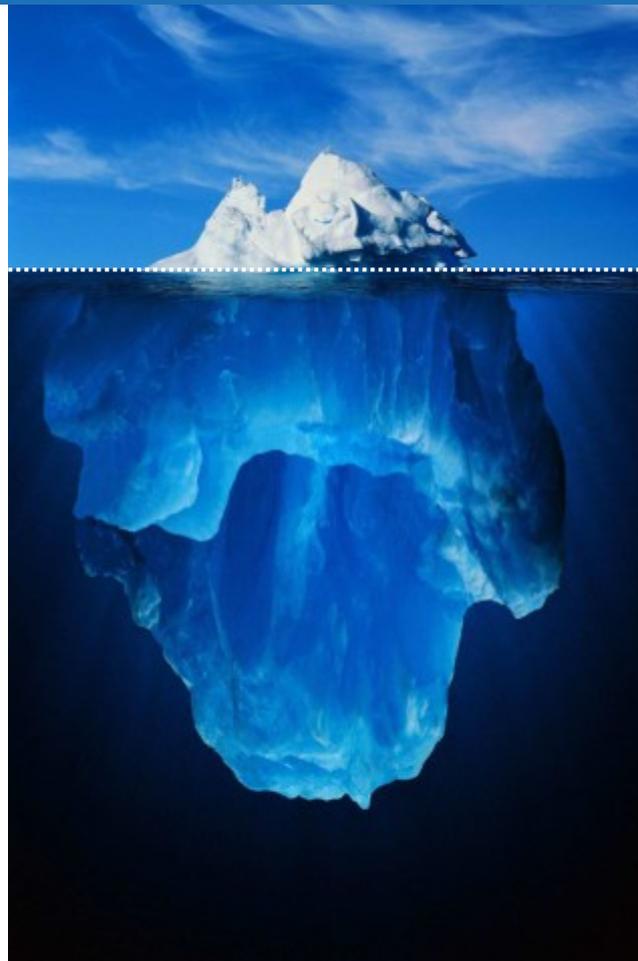
- Многоуровневая защита
- Отпечаток устройства
- Анализ рисков

“Our auditors have already told us the Trusteer solution is absolutely compliant with the new guidelines”

## В дополнение



## Онлайн мошенничество, прямые финансовые потери



### Дополнительные потери

- Чеки
- Карты
- Контакт центры

### Требования регуляторов

- Аудиты
- Инциденты
- Штрафы

### Непрямые потери

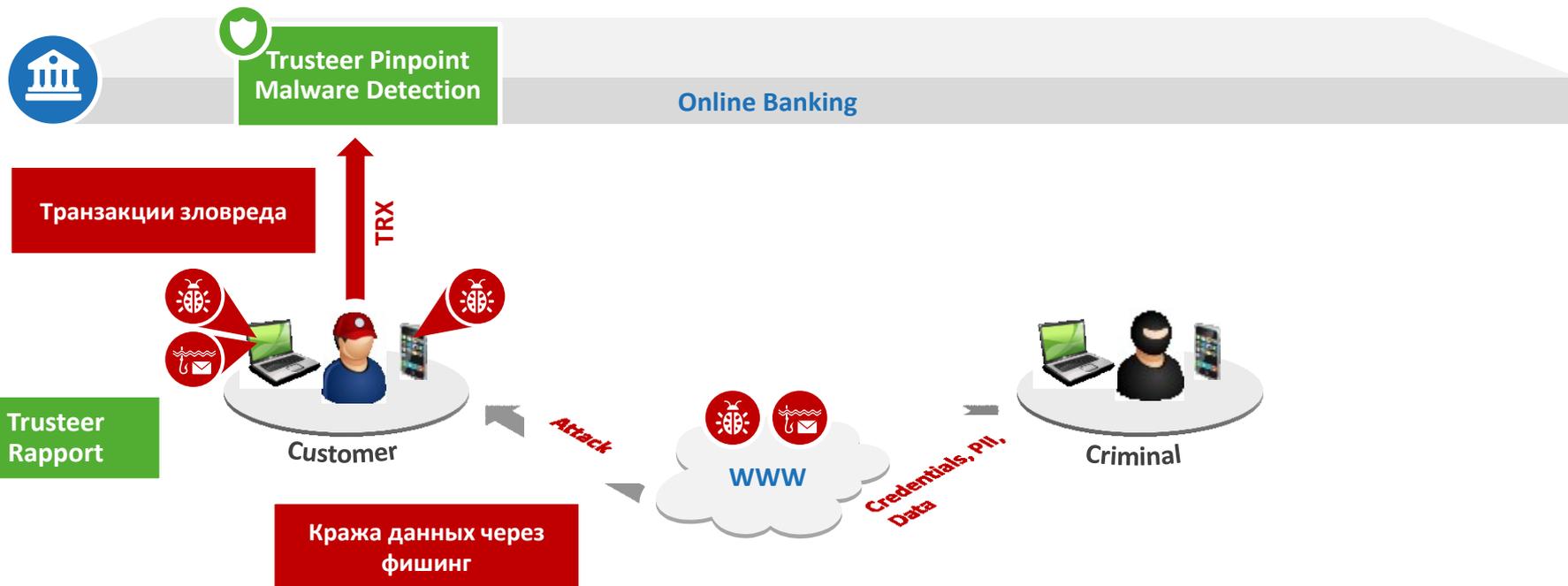
- Расследования
- Анализ транзакций
- Затраты на технологии

### Урон

- Бизнесу
- Потеря клиентов
- Потеря репутации

**Пример: фишинг и  
зловреды**

# Компрометация устройства, данных и транзакций



# Предотвращение атаки (Layer 1):

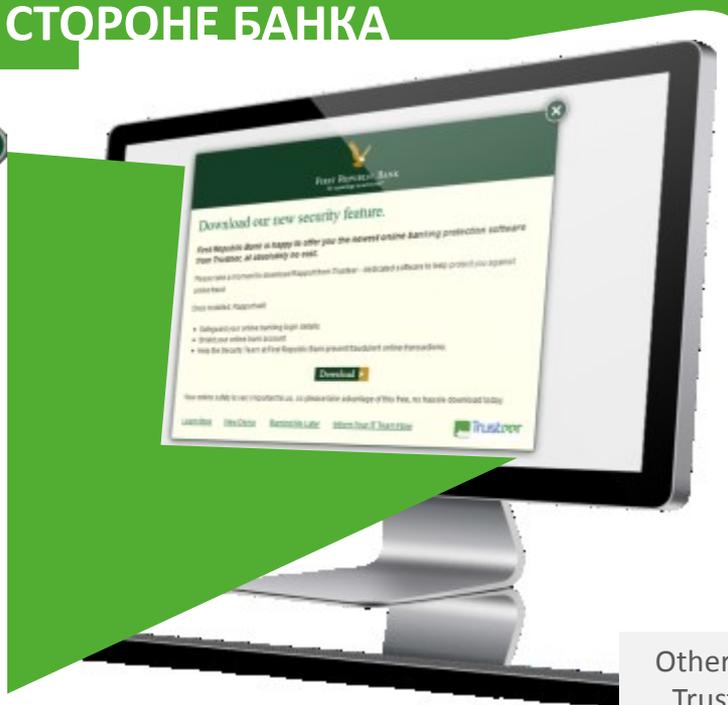
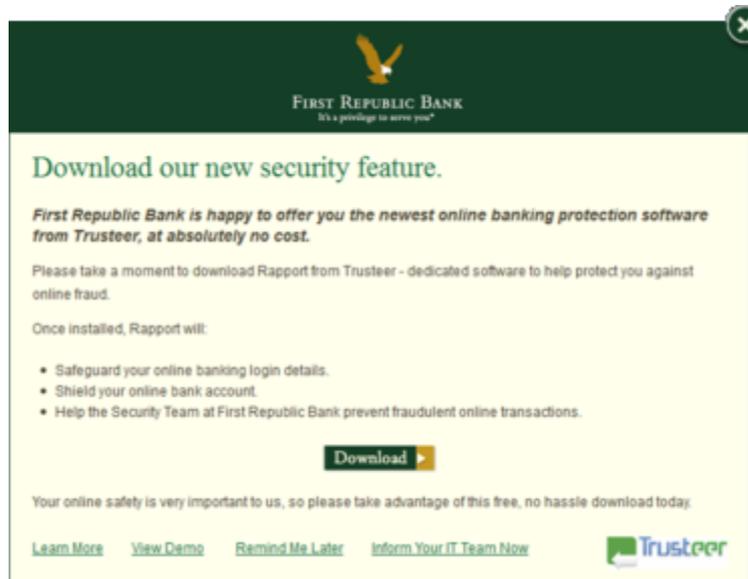


Online Banking



# Trusteer: Внедрение

- Добавляется на веб-сайт банка
- По желанию\принудительная установка
- Интегрируется с большинством систем онлайн-банкинга
- НИКАКОГО ЖЕЛЕЗА И ПО НА СТОРОНЕ БАНКА



intuit

FIS

S1

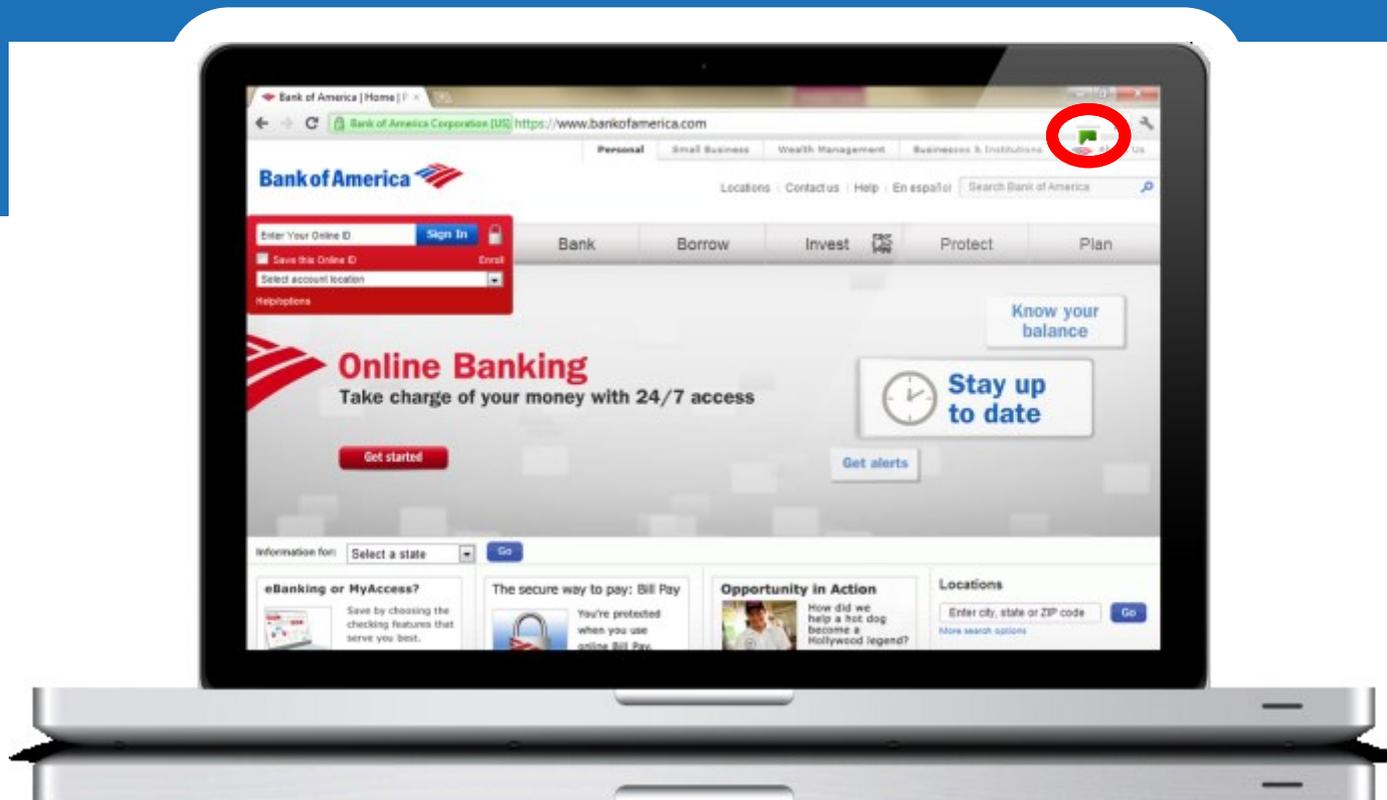
First Data

HARLAND

Other providers support  
Trusteer integration –  
please inquire

Прозрачно для  
пользователя

Не мешает  
повседневной работе





**Компактный  
агент для PC и  
Mac**

- Установка в один клик
- Никакого ПО и железа со стороны банка
- Минимальная нагрузка на ПК



**Защита от  
зловредов**

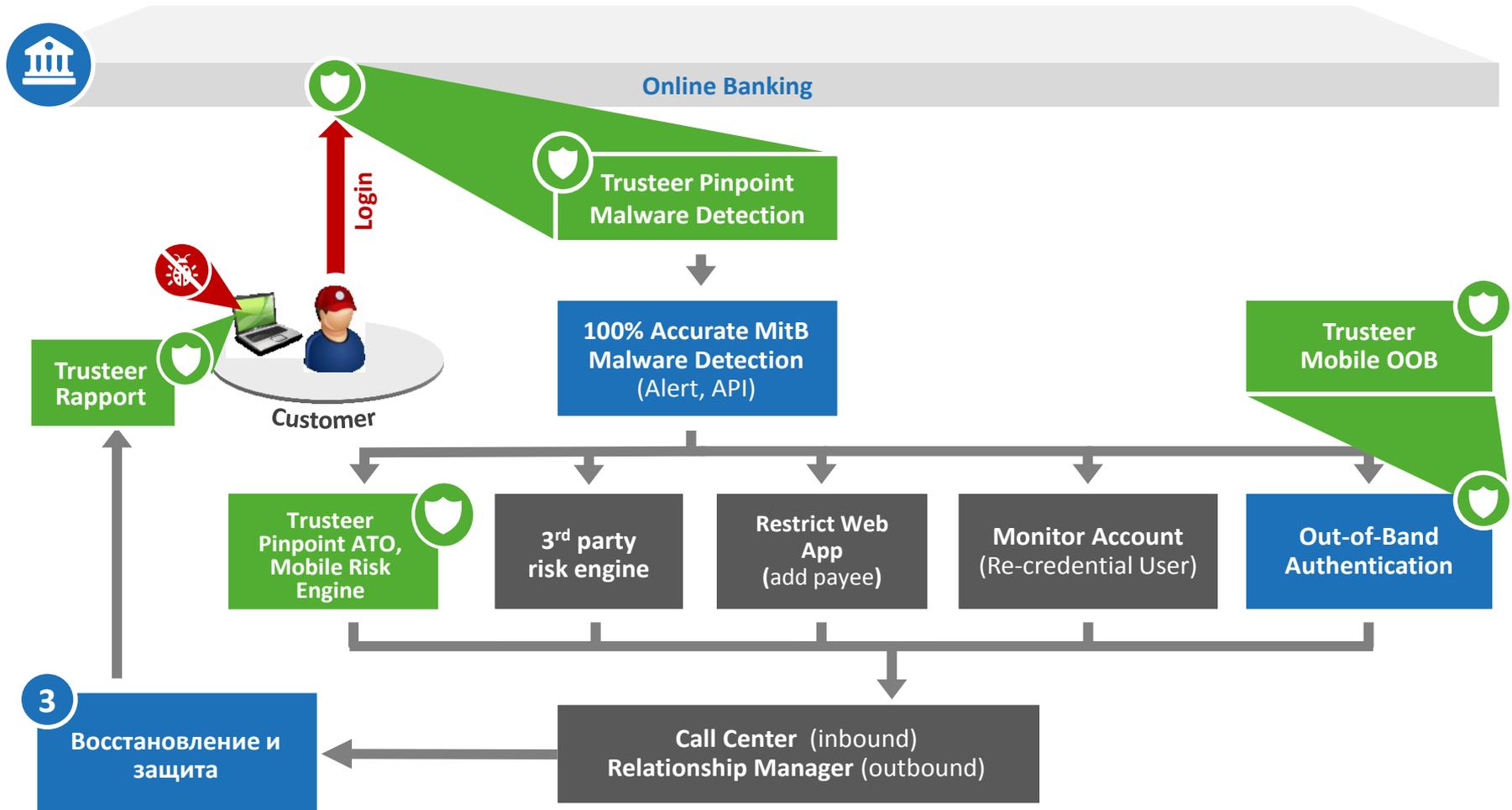
- Защищает данные пользователя и работу с приложением
- Предотвращает заражение
- Удаляет существующие зловреды



**Защита от  
фишинга**

- Оповещает команду безопасности в случае выгрузки данных пользователем на внешние ресурсы

# Предотвращение атаки (Layer 2):





### Защита от зловредов

- Безагентное детектирование Man-in-the-Browser Malware
- Zeus, Spyeye, Carberp, Citadel, Gozi, Tilon и др.



### Точная реакция

- Минимум ложных срабатываний
- Автоматизация принятия решений



### Простая интеграция

- Интеграция с Trusteer Pinpoint Account Takeover Detection и Trusteer Mobile Risk Engine
- API/Email для веб приложений Web App, системы анализа рисков и антифрода

**Пример: Account  
Takeover &  
New Account Fraud**

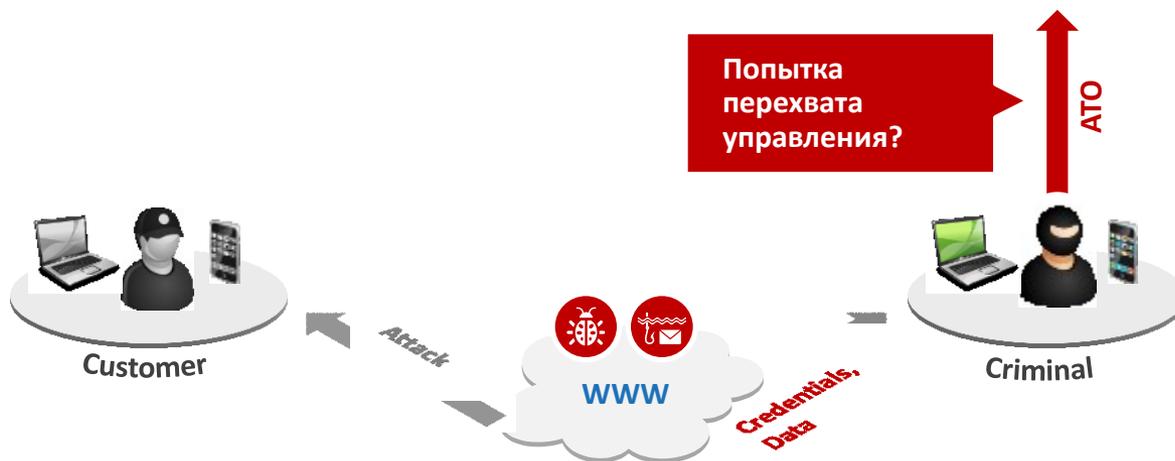
# Перехват управления аккаунтом

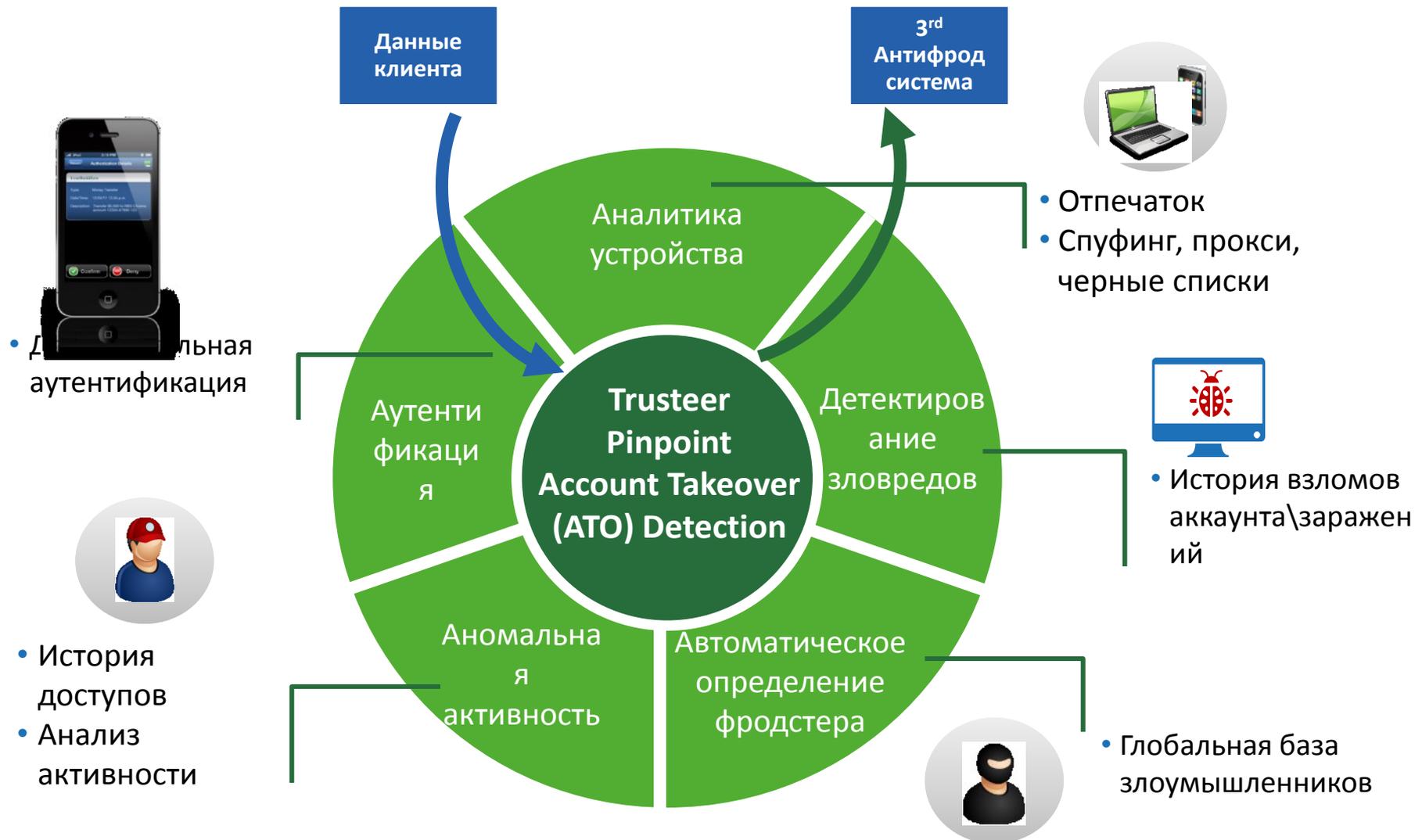


Online Banking



Trusteer Pinpoint  
Account Takeover  
(ATO) Detection





# Особенности IBM Trusteer Pinpoint Account Takeover (ATO) Detection

**Trusteer**  
an IBM Company



Корреляция информации о устройстве и аккаунте



Автоматизация детектирования устройства злоумышленника



Автоматическое создание правил по детектированию мошенничества



FFIEC Compliant Login and Transaction Anomaly Detection

**Пример:  
Фрод с мобильных  
устройств**

# #1 Работа с уязвимым устройством

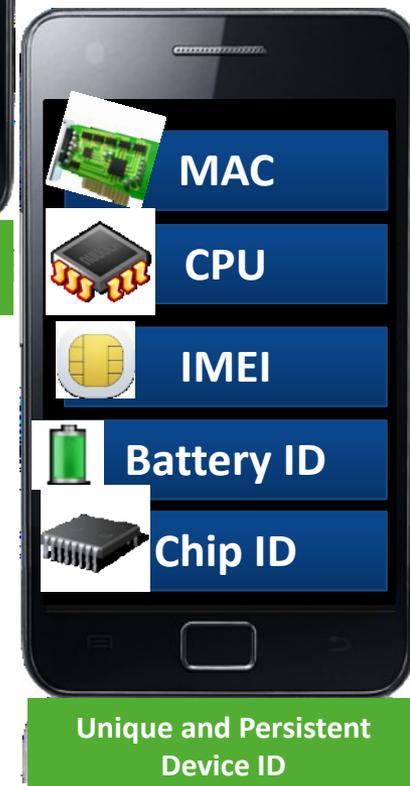


# #1 Работа с уязвимым устройством



# #2 Детектирование устройства злоумышленника

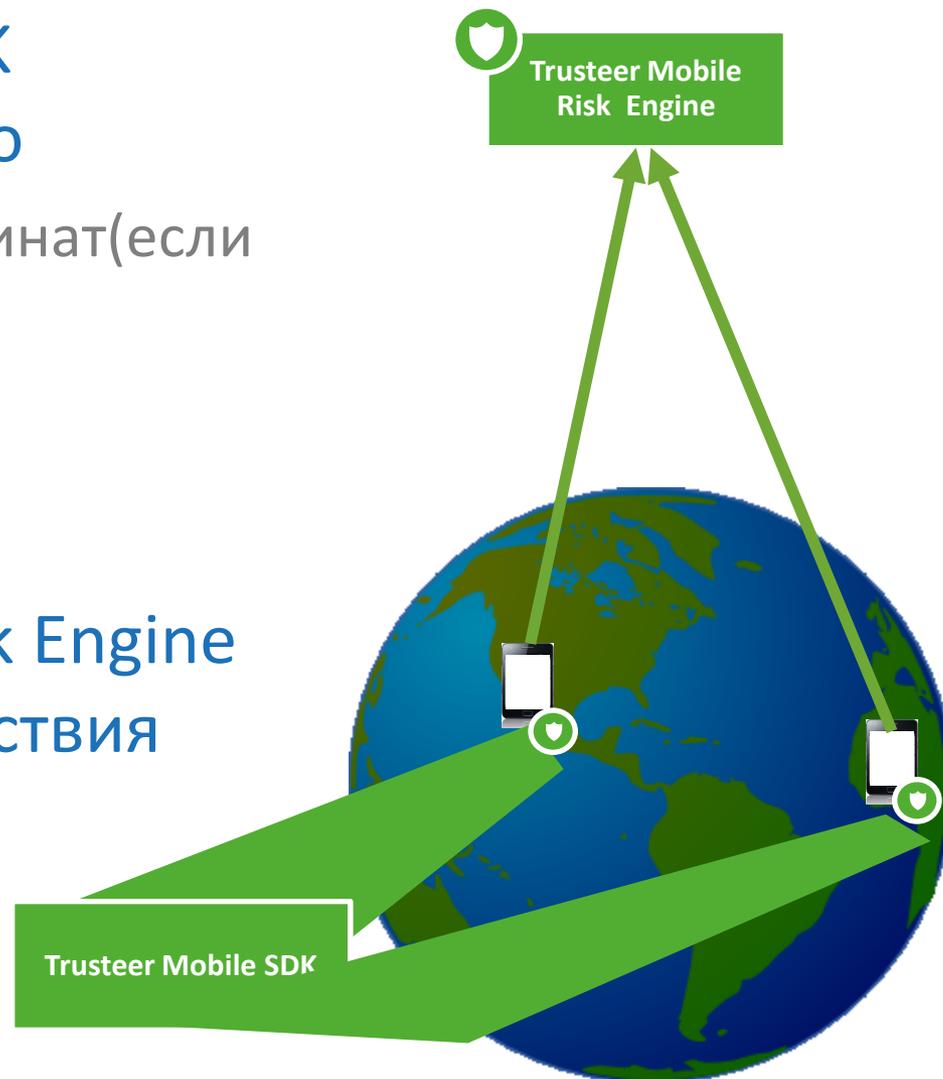
- Определить устройства без агента невозможно
  - Многие устройства идентичны
  - Злоумышленники могут подменять атрибуты
- IBM Trusteer Mobile SDK определяет все необходимые атрибуты устройства
  - Даже после переустановки OS
  - Точно детектирует устройство злоумышленника



\* Some limitation with iOS7

## #2 Детектирование устройства злоумышленника по геолокации

- IBM Trusteer Mobile SDK определяет геолокацию
  - На основании GPS координат(если разрешено)
  - На основании IP
- IBM Trusteer Mobile Risk Engine анализирует несоответствия





**Точно определяет параметры устройства и пользователя**

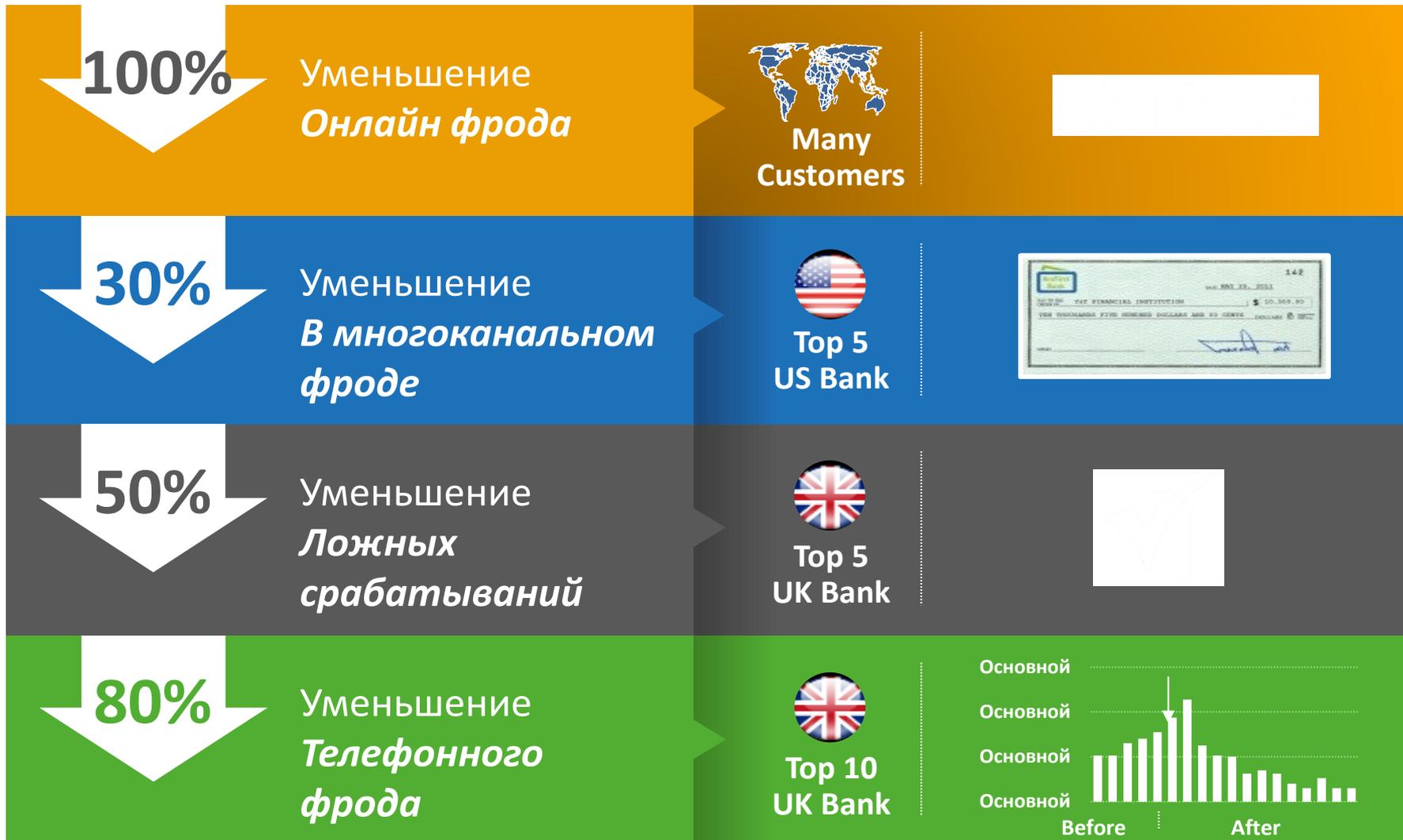


**Комплексная защита при работе через приложение и браузер**



**Коррелирует все доступные данные для точного определения мошенничества**







[ibm.com/security](https://ibm.com/security)

**Спасибо!**

**[n.pobortsev@ru.ibm.com](mailto:n.pobortsev@ru.ibm.com)**