



На **один** шаг ВПЕРЕДИ

Сергей Чекрыгин

Check Point

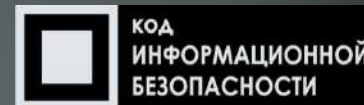
EMAIL

schekrygin@checkpoint.com



Check Point
SOFTWARE TECHNOLOGIES LTD.

Традиционный подход



Вирус

Антивирус (1984г)

Атаки

IPS, COB (IDS 1995г)

Вредоносные сайты

URL Фильтр (1995г)

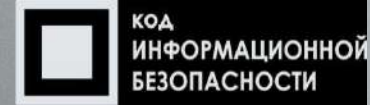
Опасные приложения

Контроль приложений

Бот-сети

Анти-бот (2007г)

Больше безопасности в одном устройстве



Межсетевой экран & VPN

Система предотвращения вторжений

Контроль приложений

Фильтрация по URL

Интеграция с AD

Антивирус

Антибот

Сетевой DLP





Check Point
SOFTWARE TECHNOLOGIES LTD.

Новые устройства Check Point Широкий диапазон для предотвращения угроз

Серии 3200 и 1400



Филиалы и небольшие
офисы

Серия 5000



Корпоративные
решения

Серия 15000



Крупные сети

Серия 23000



ЦОД и телеком

Неизвестные угрозы

не могут быть пойманы
традиционными технологиями ИБ

A person in silhouette stands in a dark, textured room, looking out through a bright, narrow doorway. The scene is dramatic, with strong contrast between the dark interior and the bright light from the doorway. The overall mood is one of anticipation and vigilance.

CHECK POINT

Мы защищаем

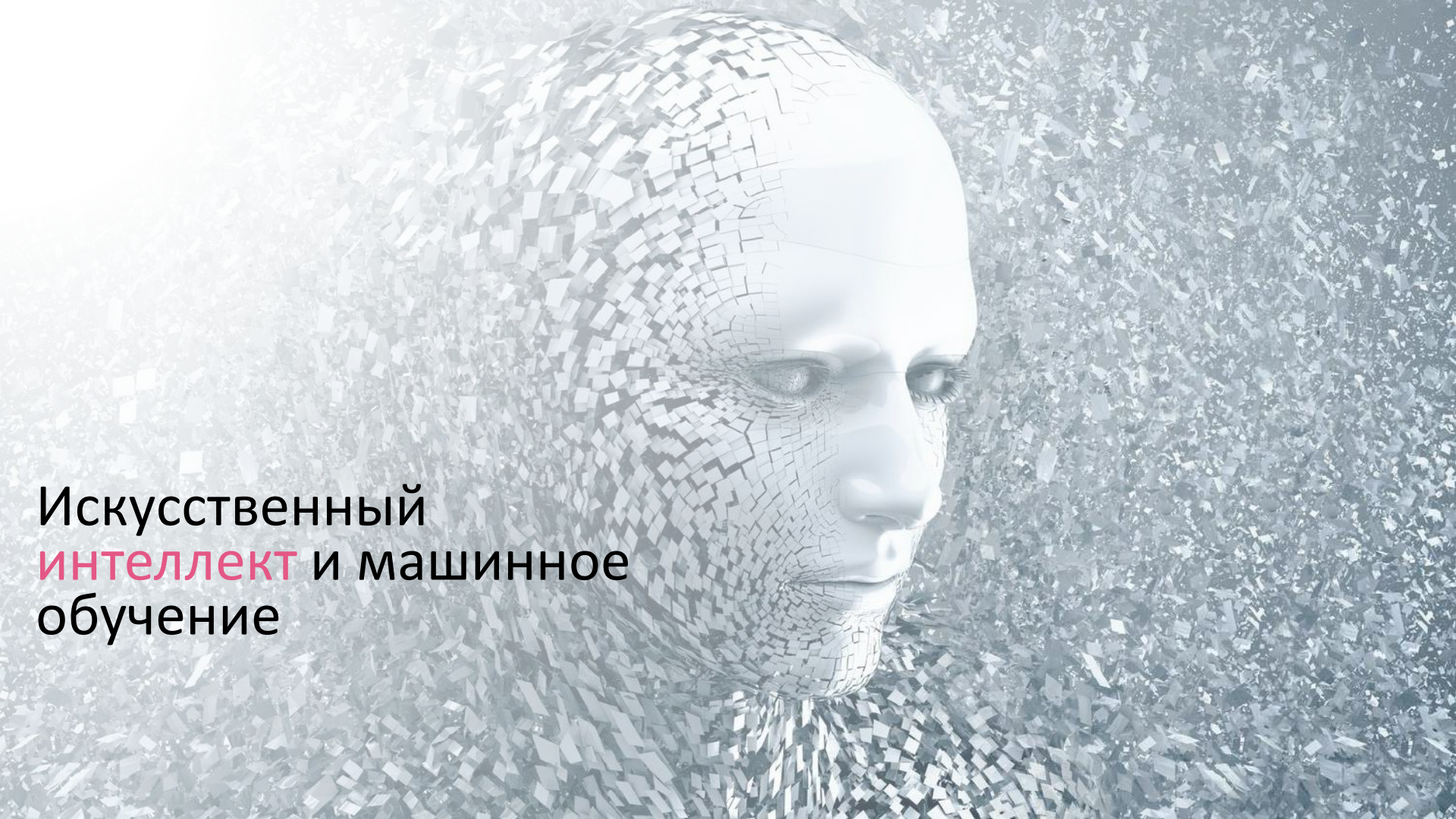
будущее

Беспилотные автомобили



Check Point
SOFTWARE TECHNOLOGIES LTD





Искусственный
интеллект и машинное
обучение

Новый
способ доставки



Новые модели бизнеса



Check Point
SOFTWARE TECHNOLOGIES LTD



UBER

Такси №1 в
мире не имеет
своих машин



 **airbnb**

Служба
размещения №1
не имеет
недвижимости



facebook

Провайдер
контента №1 не
создает контент



NETFLIX

Самая
быстрорастущая
ТВ сеть не имеет
кабелей



 **Alibaba.com**

Самый большой
ритейлер не
имеет склада



Предотвращение атак в гибридных облаках

Защита аккаунтов и данных



Office 365



Suite



Google Cloud Platform



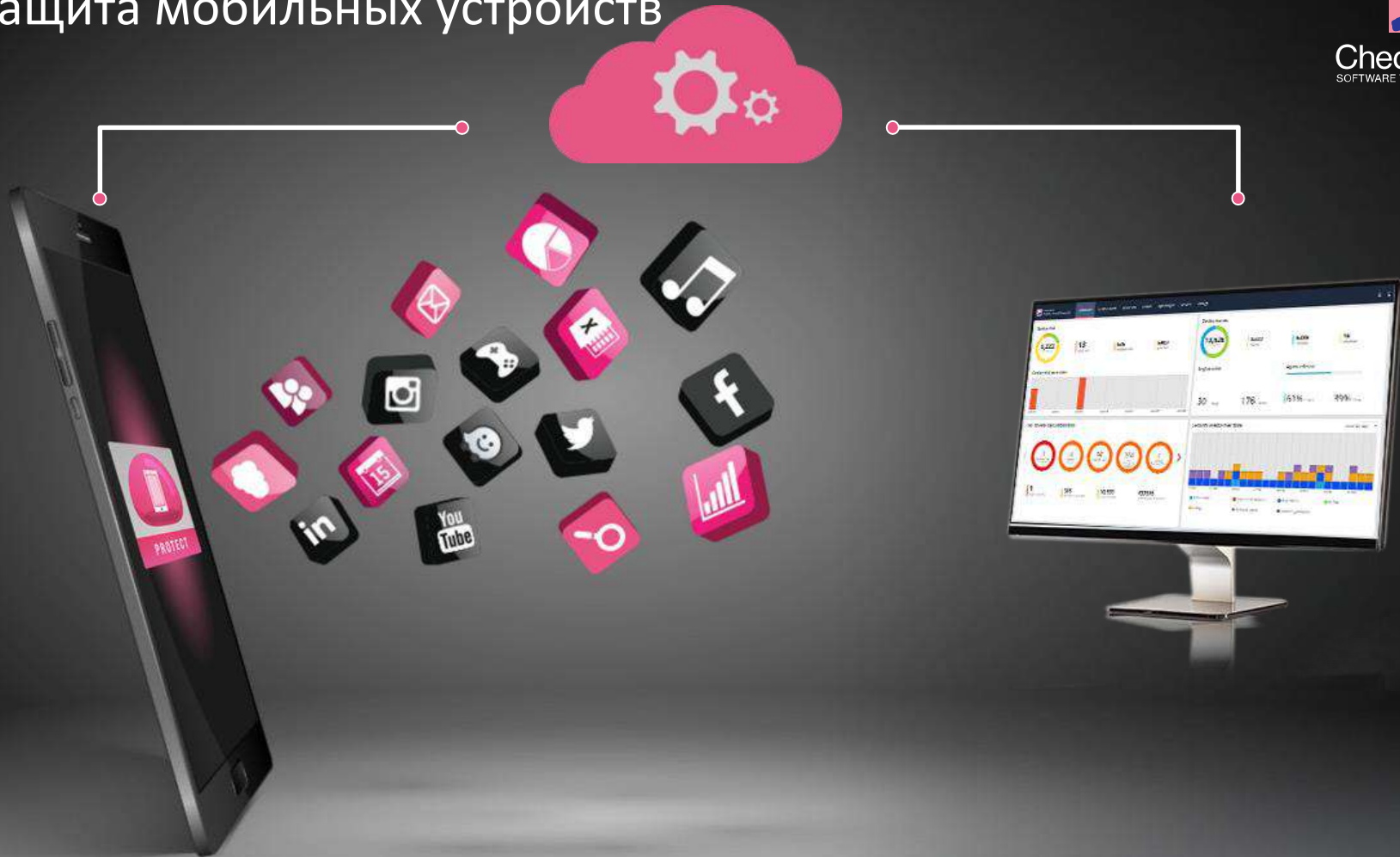
Microsoft
Azure



Защита мобильных устройств



Check Point
SOFTWARE TECHNOLOGIES LTD



Большинство зловредов видны только один раз

99% сигнатур видны 58 секунд или менее

Хакеры автоматически модифицируют код для избежания обнаружения

Verizon 2016 Data Breach
Investigations Report

Contributor

Оставаться на один шаг впереди



CHECK POINT

SandBlast

ZERO-DAY
PROTECTION



CHECK POINT

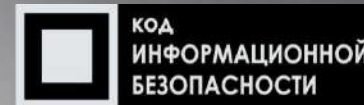
SandBlast™

ZERO-DAY
PROTECTION

Способ работы с тем,
что мы не знаем:

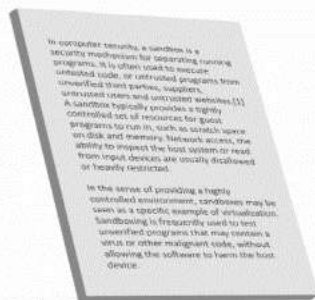
Песочница

Как работает защита от направленных атак



SANDBLAST

Как работает Песочница



- Системный реестр
- Сетевые соединения
- Файловая активность
- Процессы

Успешная стратегия защиты

Предовратить

Построить защиту для предотвращения

Обезвредить

Идентифицировать и восстановиться, если атака прошла

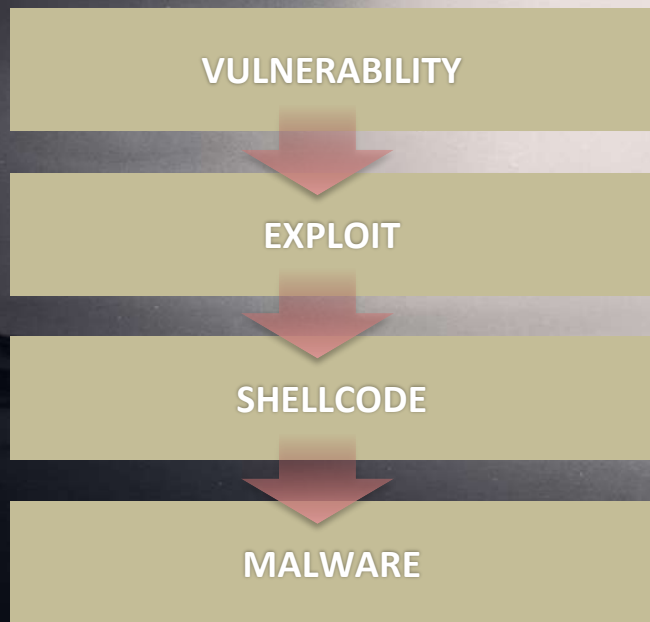


Check Point
SOFTWARE TECHNOLOGIES LTD

“ Разница между обнаружить и предотвратить как между 1 и бесконечностью.”

Предотвращение
держит Вас на шаг впереди

SandBlast – единственная песочница с обнаружением на уровне процессора



Песочница SANDBLAST

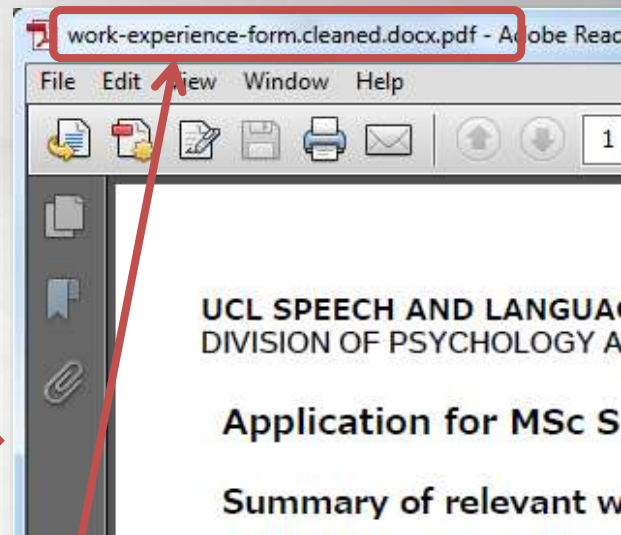
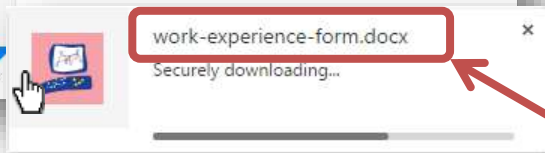
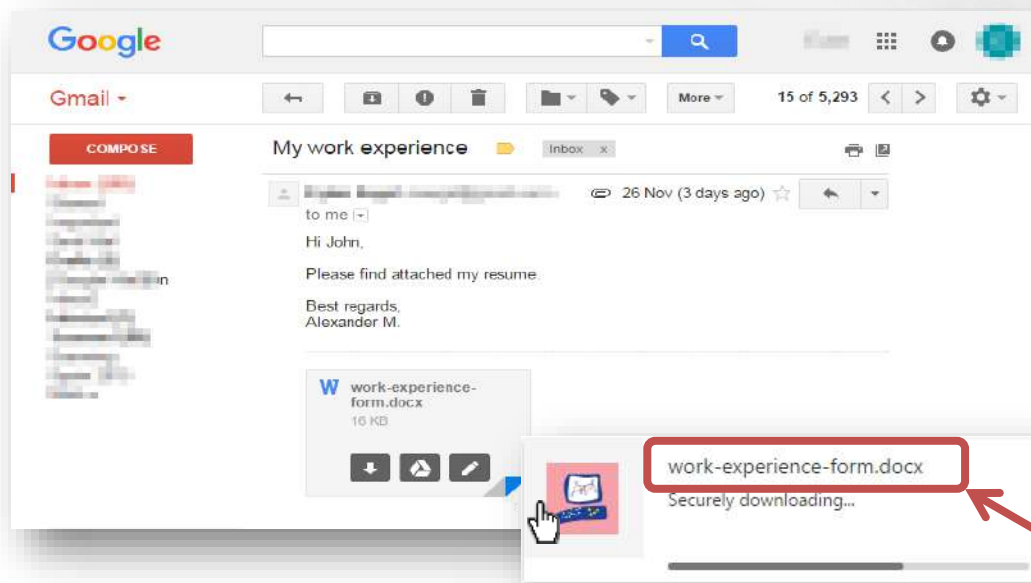
- Обнаружение на уровне процессора
- **Устойчивость к обходу**

Традиционная песочница

- Анализ поведения
- **Проверку можно обойти**

Мгновенная защита при загрузке из сети

Доставка безопасного файла

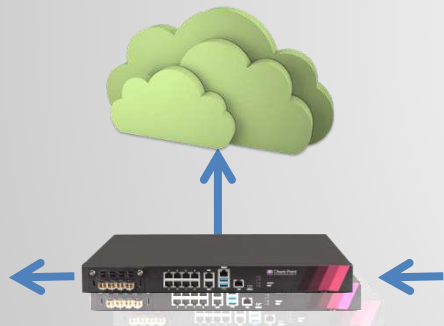


**Конвертация в PDF для защиты
или безопасная версия исходного файла**

Варианты установки

Облачный сервис
Шлюз + облачный сервис

Сервис в облаке Check Point



Шлюз безопасности в комплектации NGTX

У заказчика
Шлюз + песочница SandBlast

Выделенная песочница
SandBlast



Шлюз безопасности в комплектации NGTX

Выделенная песочница
Песочница в разрыве



Выделенная
песочница

Успешная стратегия защиты

Предовратить

Построить защиту для предотвращения

Обезвредить

Идентифицировать и восстановиться, если атака прошла

Представляем



CHECK POINT

SandBlast



...[redacted]... for designated
groups and individuals



**Интеграция
с SandBlast**

Обнаружение и
блокировка
неизвестных
угроз



**Удаление
угроз**

Очистка
документов за
секунды



**Анти-
фишинг**

Защита логинов
и паролей



**Расследова
ние**

Автоматическое
расследование и
восстановление




**Анти-
шифроваль
щик**

Защита и
восстановление
после
шифровальщиков




Интеграция с SandBlast

Обнаружение и блокировка неизвестных угроз




Удаление угроз

Очистка документов за секунды




Анти-фишинг

Защита логинов и паролей



Расследование

Автоматическое расследование и восстановление




Анти-шифровальщик

Защита и восстановление после шифровальщиков


При участии традиционных технологий ИБ



IPS



Анти-Вирус



Анти-бот

SANDBLAST Агент

SandBlast Агент **анализирует**

Единственное решение с автоматическим
анализом инцидентов и скриптом для
восстановления

Демонстрация и пилотирование

Отчет Security Checkup – проверка трафика в сети заказчика, бесплатно и конфиденциально.

- Выявление опасных приложений,
- доступ к опасным сайтам,
- коммуникации бот-сетей,
- вирусные атаки,
- утечка данных,
- IPS атаки,
- объяснение выявленных угроз,
- рекомендации по устранению

Обратить к партнеру
для заказа услуги



CHECK POINT

Мы защищаем
будущее



Сергей Чекрыгин
schekrygin@checkpoint.com



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ