Check Point
SOFTWARE TECHNOLOGIES LTD.

Защита от угроз нулевого дня

Дмитрий Воронков
Консультант по безопасности
dvoronkov@checkpoint.com

Symantec Says Antivirus Is Dead, World Rolls Eyes

May 07, 2014 11:55 AM EST | 32 Comments

By Max Eddy

Технологии информационной защиты

- **Анти-Вирус**
  - Блокирует **файлы** с **известными** вирусами
- **IPS**
  - Анализирует трафик и блокирует его на основе **известных** шаблонов
- **Анти-Бот**
  - Обнаруживает подозрительный трафик по обновляемым шаблонам

*Эффективны, но против **ИЗВЕСТНЫХ** угроз*

СИГНАТУРЫ всегда ОТСТАЮТ

Насколько это серьезно?

99% контрольных сумм зловредов появляются на **58 секунд** ***или меньше***

Большинство вирусов встречаются **лишь раз**

Чтобы избежать детектирования, хакеры часто модифицируют код и схемы взаимодействия

Verizon 2016 Data Breach Investigations Report

Contributor

Source: Verizon 2016 Data Breach Investigations Report

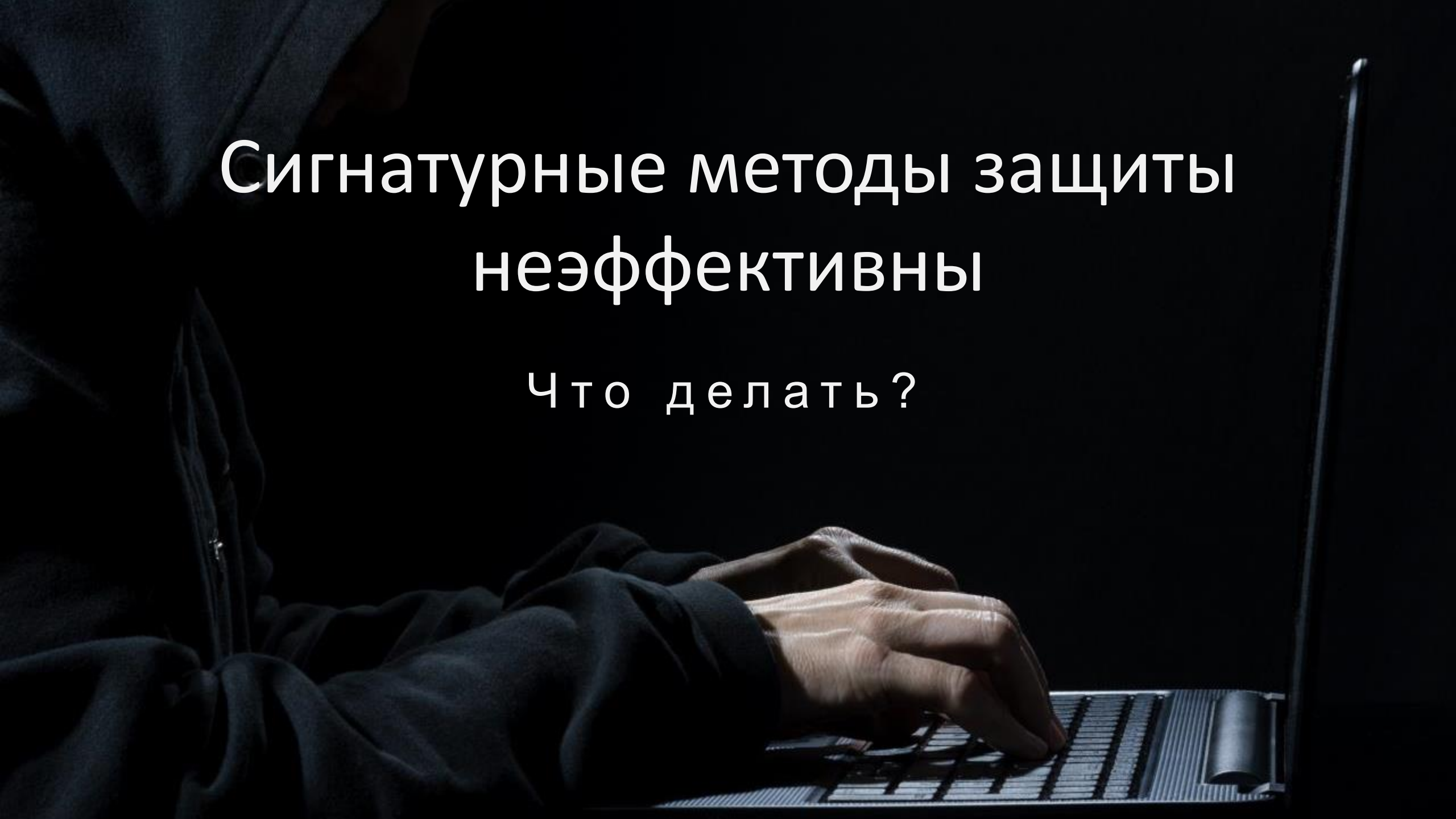
РОСТ НЕИЗВЕСТНОГО ВРЕДОНОСНОГО ПО

ВСЕ БОЛЬШЕ И БОЛЬШЕ

ТОГО, ЧТО ВЫ НЕ ЗНАЕТЕ

УГРОЗЫ НУЛЕВОГО ДНЯ, APT АТАКИ,

НЕИЗВЕСТНОЕ ВРЕДОНОСНОЕ ПО



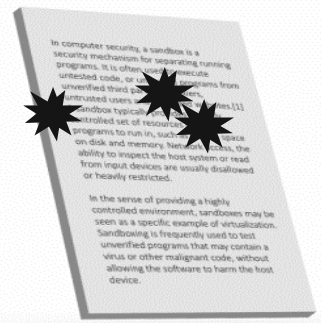
Сигнатурные методы защиты неэффективны

Что делать?

Эмуляция

Check Point
SOFTWARE TECHNOLOGIES LTD.

Откроем файл в безопасной среде



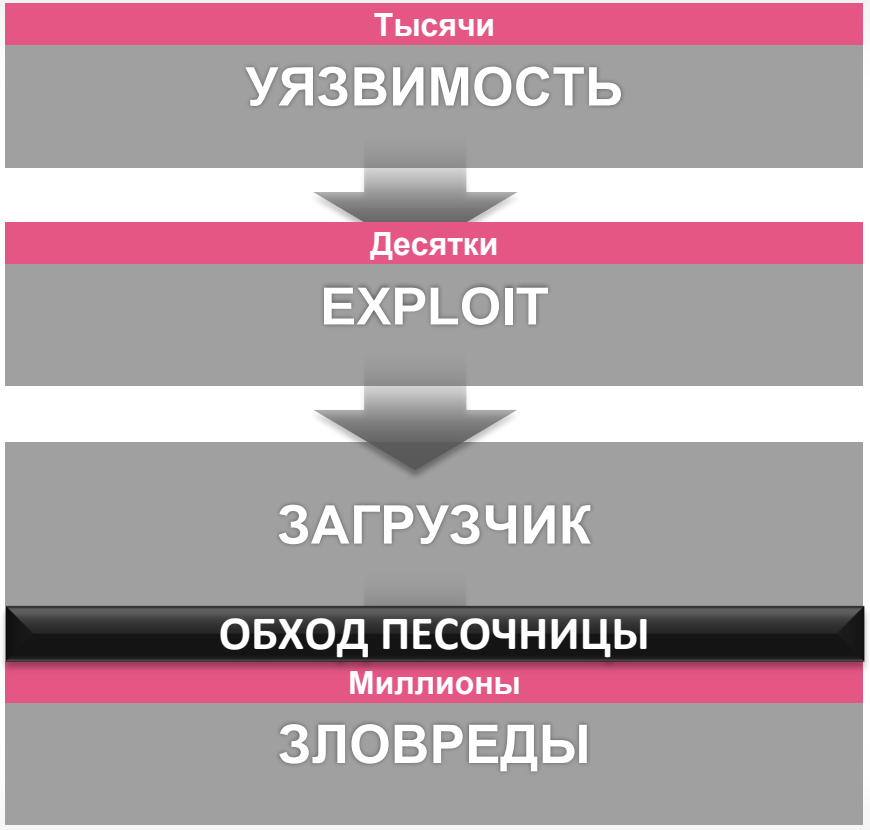
Наблюдаем:

- Реестр
- Сетевые соединения
- Действия с файлами
- Действия с процессами

Поведение – вот что выдает зловредное ПО. Однако...

Обычную песочницу не так сложно обойти

Эмуляция в SandBlast всегда на шаг впереди



CHECK POINT SandBlast™ ZERO-DAY PROTECTION

CPU Detection Engine

ДО того, как запустится код обхода…

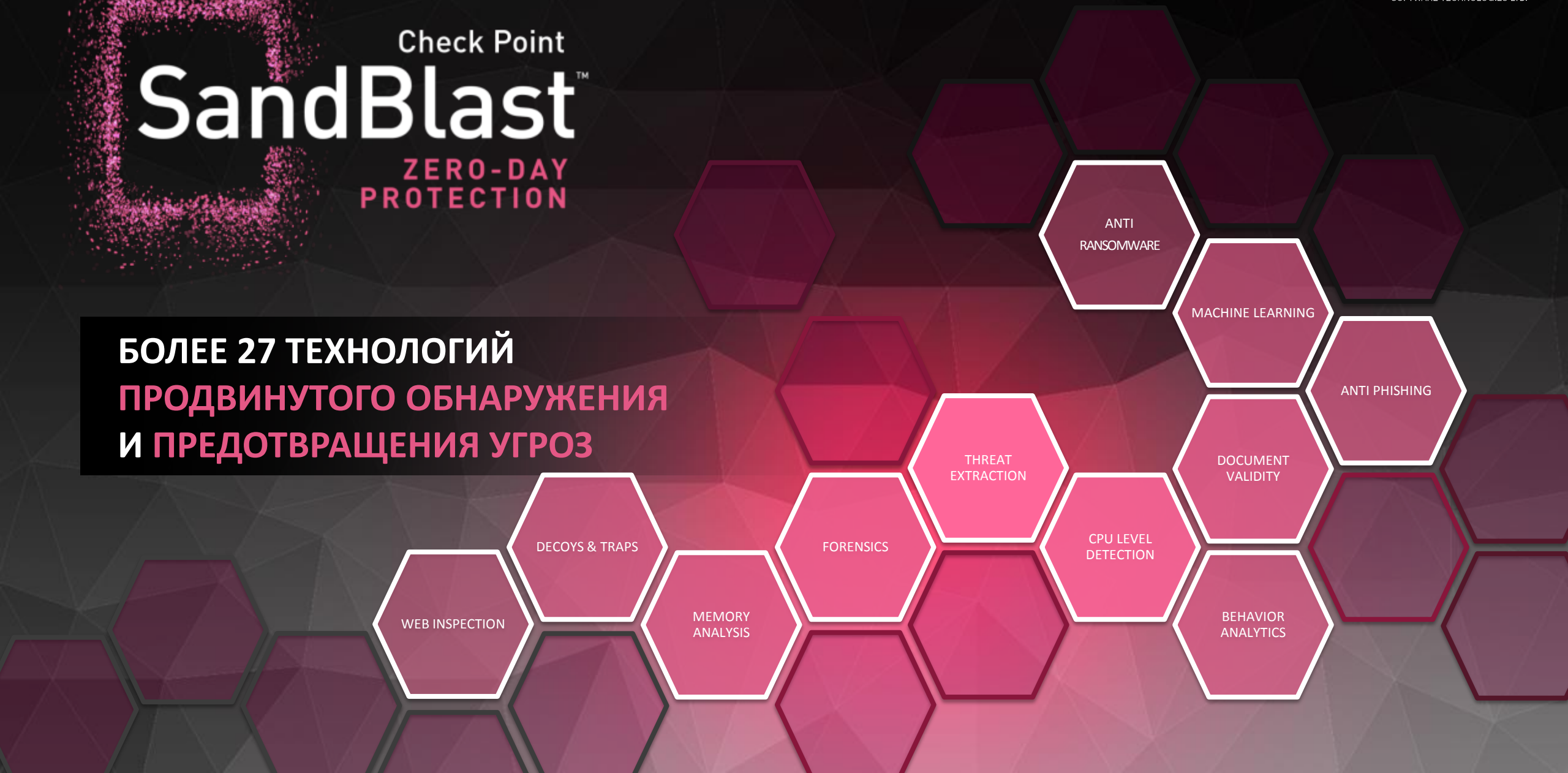
ДО загрузки зловреда….

Обычная песочница

Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point
SandBlast™
ZERO-DAY PROTECTION

БОЛЕЕ 27 ТЕХНОЛОГИЙ
ПРОДВИНУТОГО ОБНАРУЖЕНИЯ
И ПРЕДОТВРАЩЕНИЯ УГРОЗ



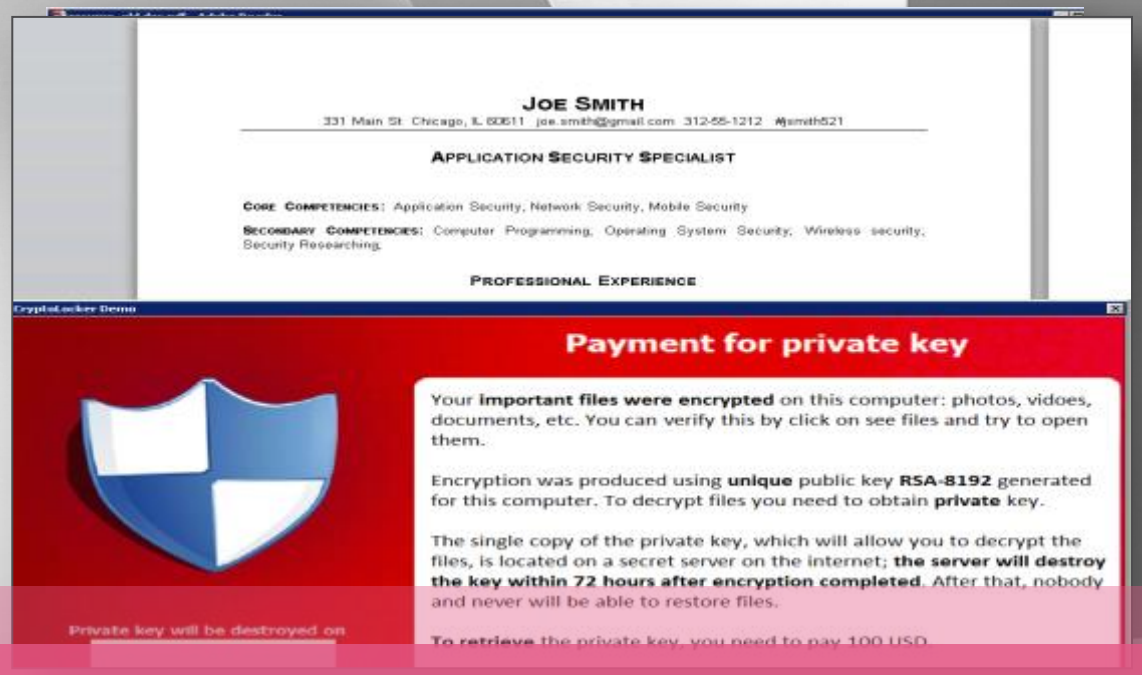
Sandblast Threat Extraction

Доставка гарантированно безопасных файлов

Check Point
SOFTWARE TECHNOLOGIES LTD.

ДО

Активация вредоносного ПО

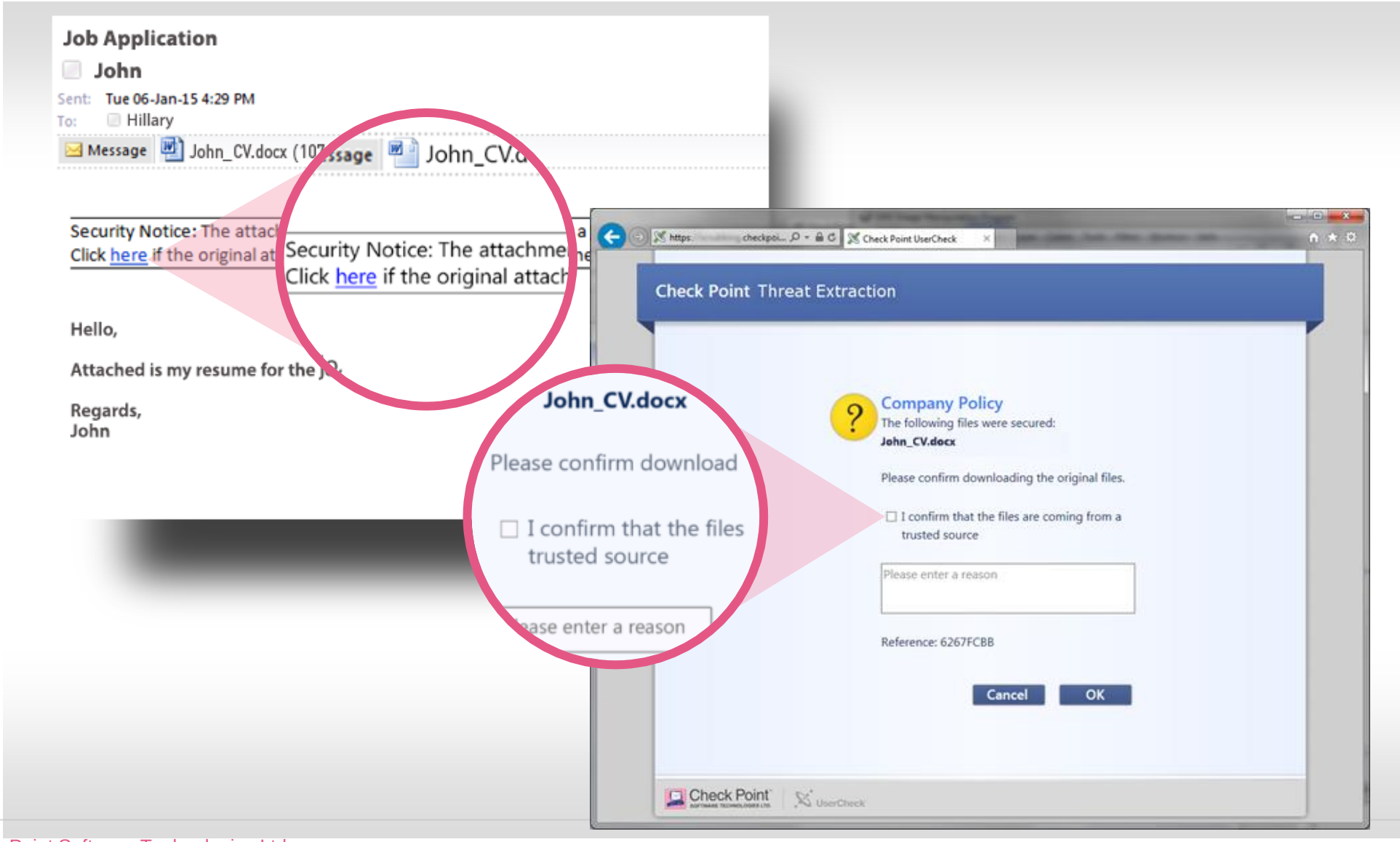


ПОСЛЕ

Вредоносное ПО удалено

Немедленный доступ. Проактивная защита.

Оригинальный файл доступен по ссылке



Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point SandBlast™ ZERO-DAY PROTECTION

ПРОДУКТЫ С ТЕХНОЛОГИЕЙ SANDBLAST

NETWORK

- Threat Emulation
- Threat Extraction

AGENT

- Threat Emulation
- Threat Extraction
- Zero Phishing
- Forensics

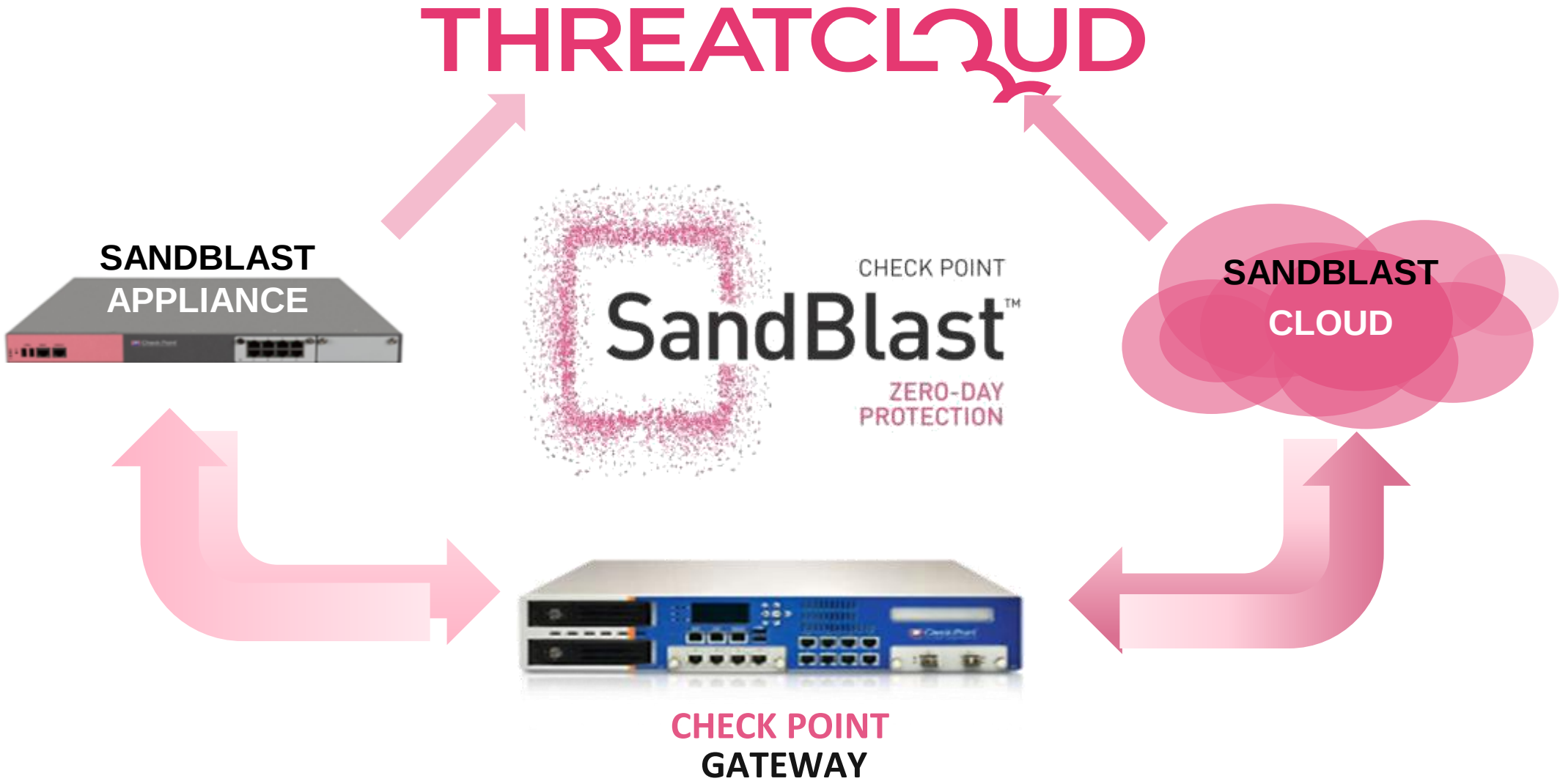
CLOUD

- Threat Emulation
- Threat Extraction

API

- Threat Emulation
- Threat Extraction

Быстрое и гибкое развертывание



Кто-то работает удаленно

Внешние накопители

Некоторые угрозы можно обнаружить только на рабочей станции

Архивы с паролем, HTTPS

Заражение от другого ПК

SandBlast Agent – защита рабочей станции

ЗАЩИТА
От атак
Нулевого дня

ЗАЩИТА
От фишинга

Быстрое
ОБНАРУЖЕНИЕ
и **ОСТАНОВКА**
атаки

Эффективная
ОЧИСТКА и
РАССЛЕДО-
ВАНИЕ

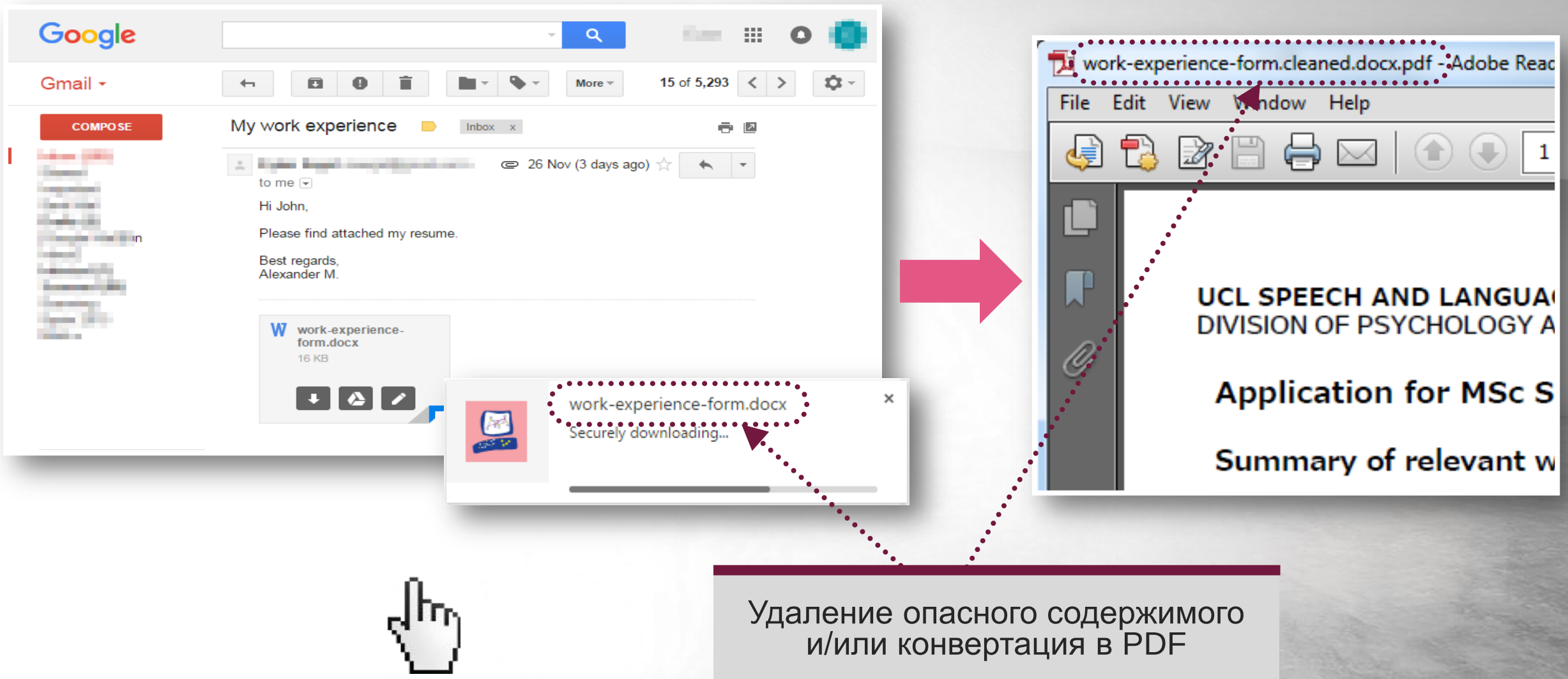
Анализ файлов на рабочей станции

1 Файл отсылается на устройство или облако SandBlast

2 Безопасная копия доставляется мгновенно

3 Оригинал эмулируется

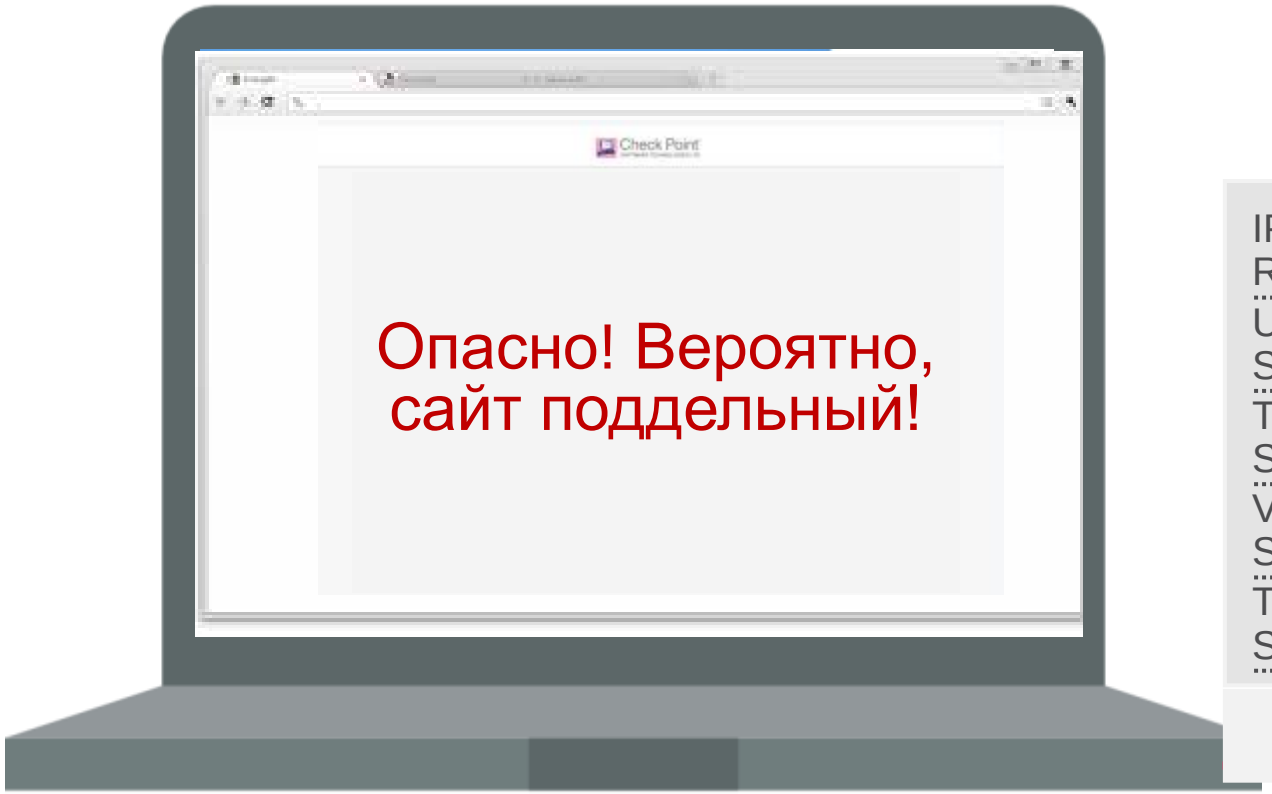
Защита скачиваемых файлов



Удаление опасного содержимого и/или конвертация в PDF

Предотвращение фишинга

Блокирует фишинговые сайты, в том числе новые



THREATCLOUD™

IP Reputation	✗	Domain Reputation	✗
URL Similarity	✓	Lookalike Characters	✗
Title Similarity	✗	Image Only Site	✓
Visual Similarity	✗	Multiple Top-Level Domain	✓
Text Similarity	✗	Lookalike Favicon	✗

PHISHING SCORE: 95%

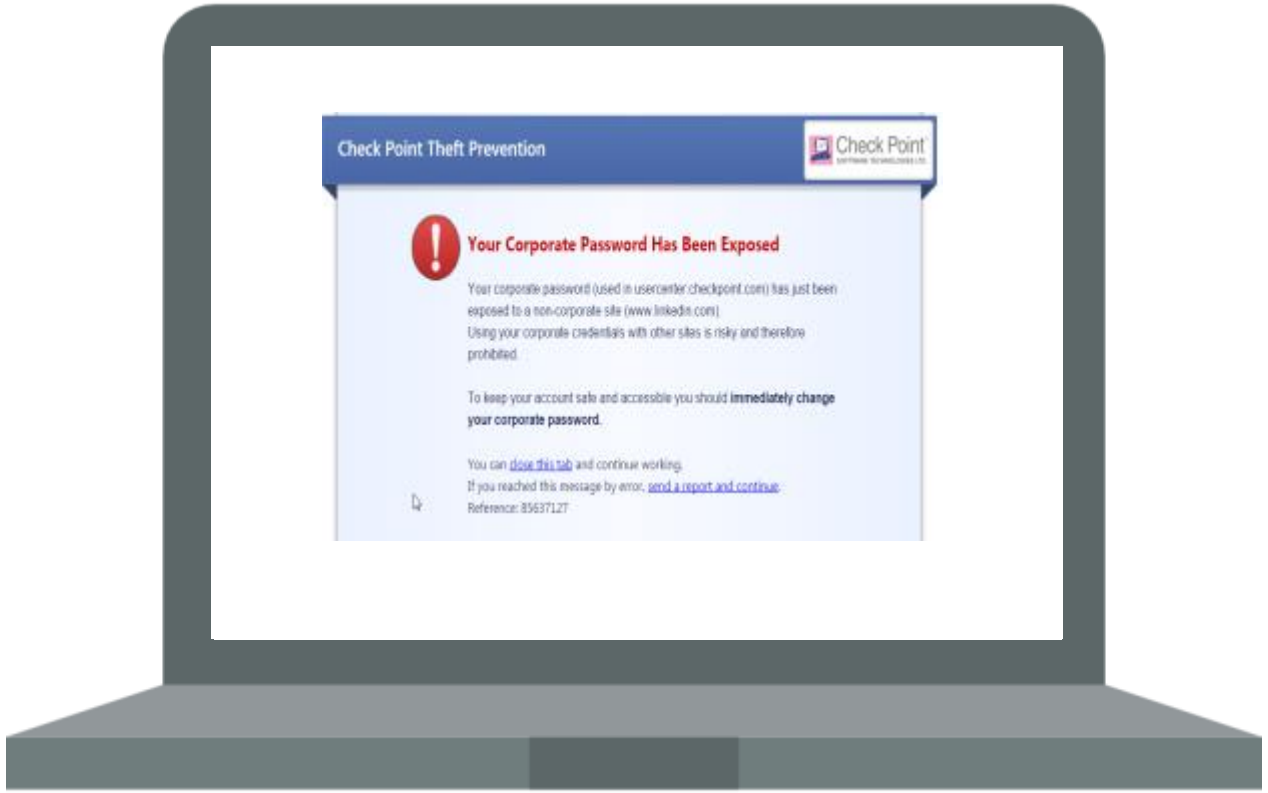
1 Новые сайты анализируются

2 Репутационный и эвристический анализ

3 Вердикт выносится за секунды

Предотвращение фишинга

Защита корпоративного пароля

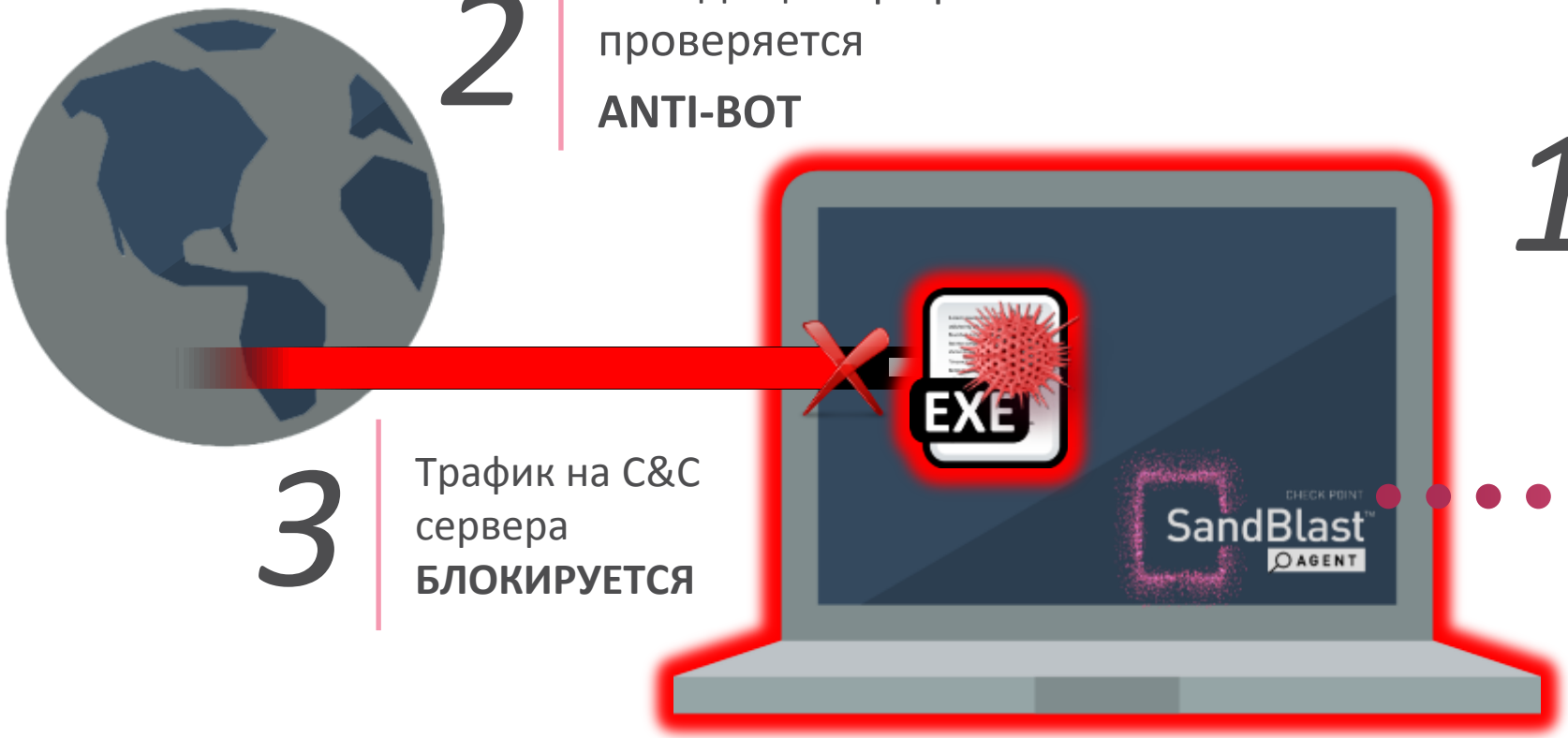


Предотвращает ошибочное или случайное использование корпоративного пароля на других ресурсах.

Обнаружение подозрительной активности

Check Point
SOFTWARE TECHNOLOGIES LTD.

2 Исходящий трафик проверяется **ANTI-BOT**



1 **ИНФОРМАЦИЯ ОБ УГРОЗАХ** постоянно обновляется

3 Трафик на C&C сервера **БЛОКИРУЕТСЯ**

4 **ОСТАНАВЛИВАЕТСЯ** подозрительный процесс либо **БЛОКИРУЕТСЯ** компьютер целиком

SandBlast Agent – Расследование инцидентов

АВТОМАТИЧЕСКИЙ сбор и анализ данных об инциденте

ПОНЯТНЫЕ ИНСТРУКЦИИ

Развернутый отчет об атаке

Только то, что необходимо

ФОРМИРУЕТСЯ АВТОМАТИЧЕСКИ

Инициируется от AV, AB или по команде

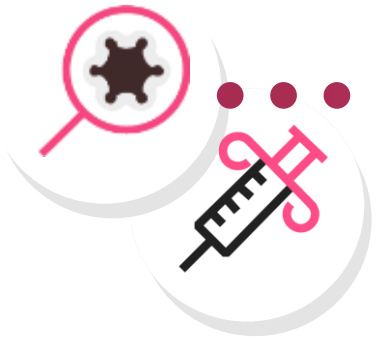
Анализ логов вручную не требуется

Сбор данных и формирование отчета

Check Point
SOFTWARE TECHNOLOGIES LTD.

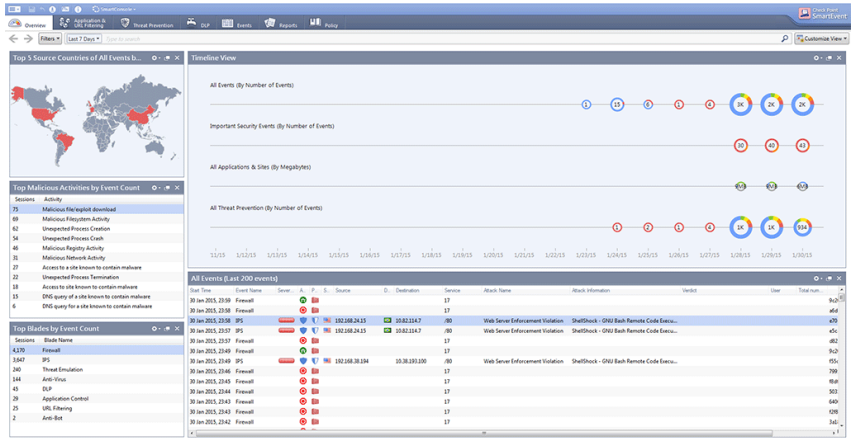
1 **ДАННЫЕ** о системе собираются постоянно от многих источников

2 **ОТЧЕТ** формируется автоматически по срабатыванию локального или внешнего триггера



3 Сырые данные анализируются с помощью сложных алгоритмов

4 **ПОДРОБНЫЙ** отчет формируется на SmartEvent



Начало атаки
Использование браузера Chrome

Эксплойт
Процесс-носитель вируса

Выполнение
Вредонос записывается на запуск после перезагрузки системы

chrome.exe
Entry Point
aatakiigar.com\...

handle.tmp
Process in Temp, Startup

schtasks.exe
Dangerous Execution

Триггеры атаки
Автоматическое обратное отслеживание атаки

Boot

Загруженный вредонос

Suspicious Events (1) | Damage (1)

Show 100 entries Search:

Resource	Impact
c:\users\pashap\documents\companysecret.doc	Data Loss: Document

Кража данных
Вредонос читает конфиденциальные данные

Триг
Иден
кот
соедин

Активация
Постоянные задачи запускаются после старта системы

oem7ec2.exe
Trigger: akdenizp.com\...

cmd.exe
Dangerous Execution

Одна система – единое управление

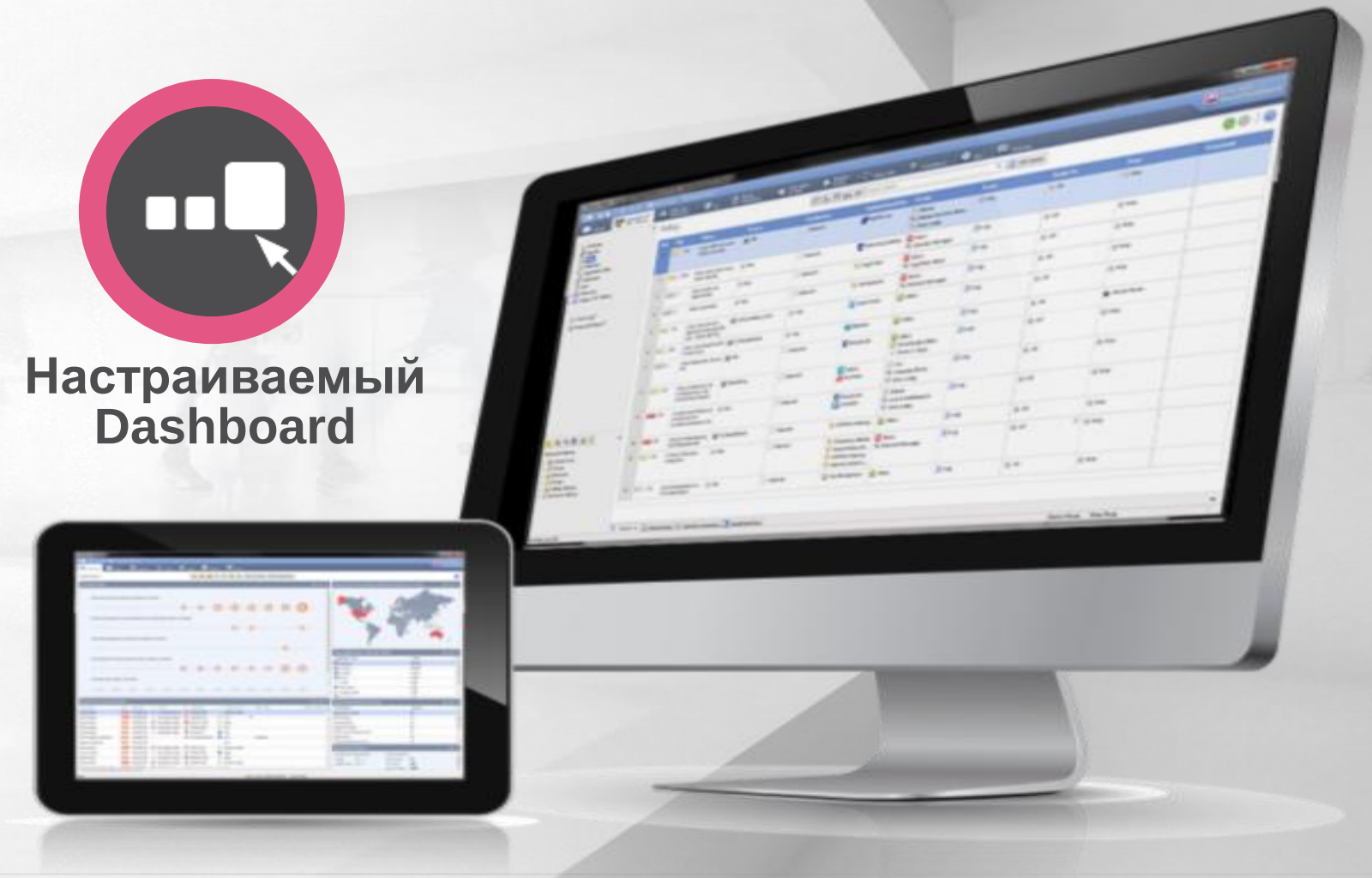
Удобная настройка, полная интеграция, абсолютная видимость

Интеграция и мониторинг

Общие политики

Настраиваемый Dashboard

CHECK POINT SandBlast™ ZERO-DAY PROTECTION



СПАСИБО!