Check Point
SOFTWARE TECHNOLOGIES LTD.

THE NEXT ATTACK CAN BE PREVENTED

СЛЕДУЮЩУЮ АТАКУ МОЖНО ПРЕДУПРЕДИТЬ

Олександр Чубарук

Технический директор в Украине, Грузии и СНГ
ochubaruk@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

РОСТ НЕИЗВЕСТНОГО ВРЕДОНОСНОГО ПО

ВСЕ БОЛЬШЕ И БОЛЬШЕ

ТОГО, ЧТО ВЫ НЕ ЗНАЕТЕ

УГРОЗЫ НУЛЕВОГО ДНЯ, APT АТАКИ,

НЕИЗВЕСТНОЕ ВРЕДОНОСНОЕ ПО

Насколько это серьезно?

99% контрольных сумм зловредов видны **58 секунд** ***или меньше***

Большинство вирусов встречаются **лишь раз**

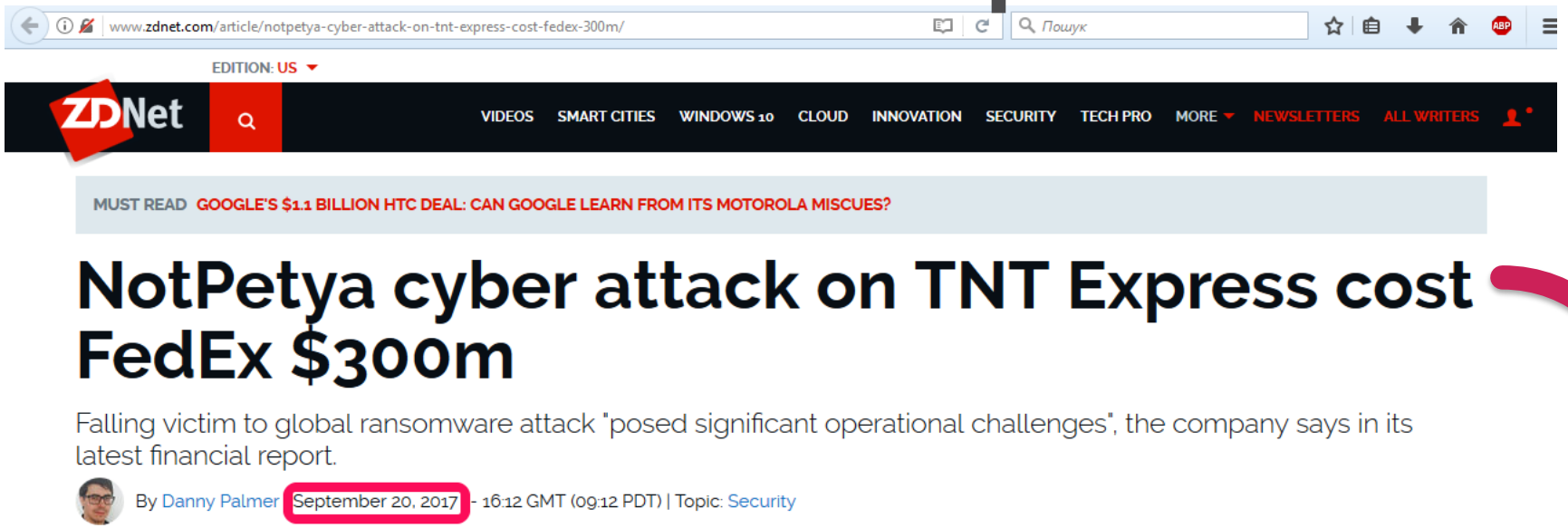
Чтобы избежать детектирования, хакеры часто модифицируют код и схемы взаимодействия

Verizon 2016 Data Breach Investigations Report

Contributor

Source: Verizon 2016 Data Breach Investigations Report

Насколько это серьёзно?



www.zdnet.com/article/notpetya-cyber-attack-on-tnt-express-cost-fedex-300m/

EDITION: US

ZDNet | VIDEOS | SMART CITIES | WINDOWS 10 | CLOUD | INNOVATION | SECURITY | TECH PRO | MORE | NEWSLETTERS | ALL WRITERS

MUST READ GOOGLE'S $1.1 BILLION HTC DEAL: CAN GOOGLE LEARN FROM ITS MOTOROLA MISCUES?

NotPetya cyber attack on TNT Express cost FedEx $300m

Falling victim to global ransomware attack "posed significant operational challenges", the company says in its latest financial report.

By Danny Palmer September 20, 2017 - 16:12 GMT (09:12 PDT) | Topic: Security

www.zdnet.com/article/petya-ransomware-cyber-attack-costs-could-hit-300m-for-shipping-giant-maersk/

EDITION: US

ZDNet | VIDEOS | SMART CITIES | WINDOWS 10 | CLOUD | INNOVATION | SECURITY | TECH PRO | MORE | NEWSLETTERS | ALL WRITERS

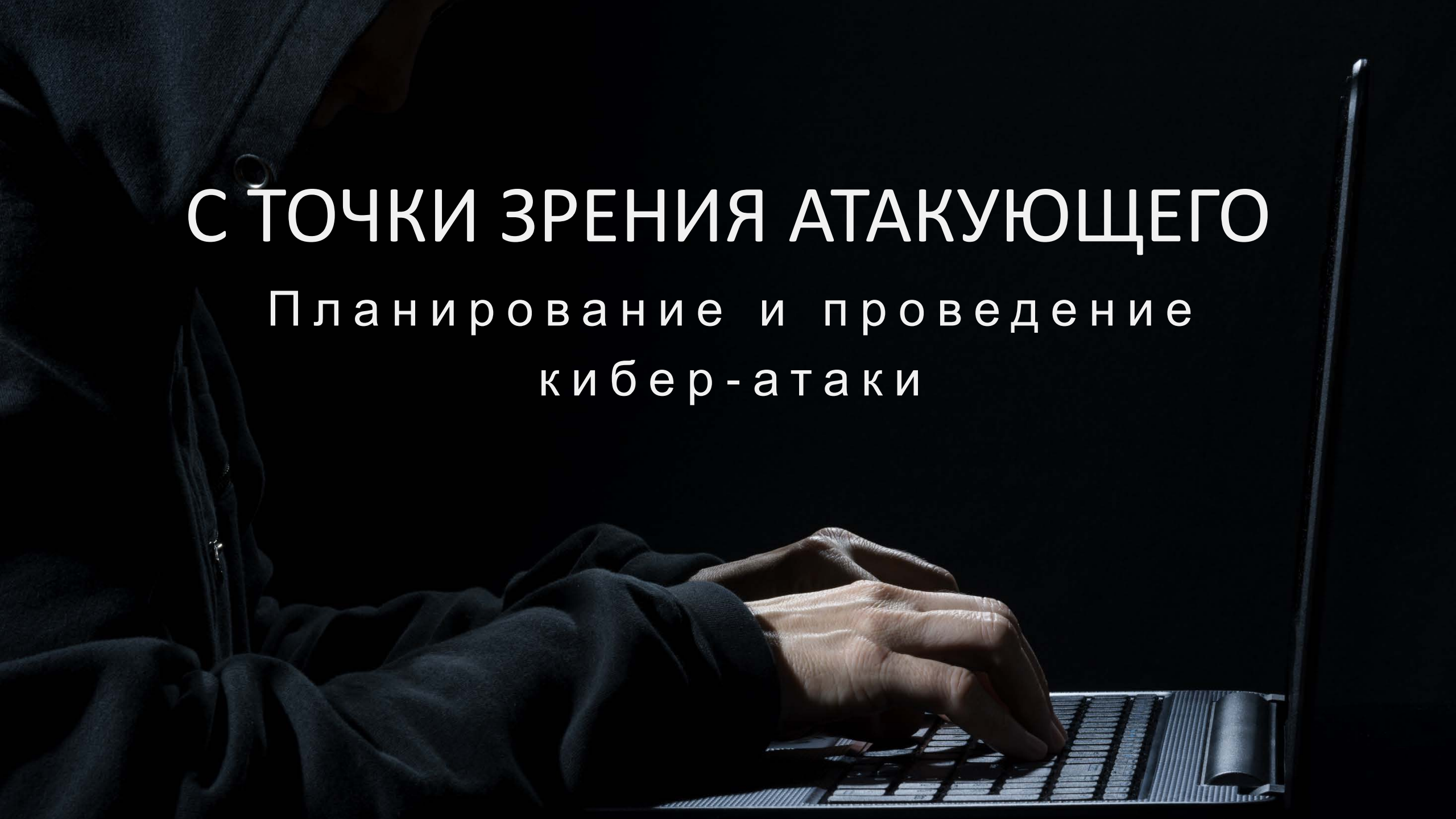
MUST READ GOOGLE'S $1.1 BILLION HTC DEAL: CAN GOOGLE LEARN FROM ITS MOTOROLA MISCUES?

Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk

June's cyberattack will cost the international shipping firm hundreds of millions of dollars in lost revenue.

By Danny Palmer August 16, 2017 - 11:28 GMT (04:28 PDT) | Topic: Security

Суммарные убытки** только двух компаний составили **600 млн долларов



С ТОЧКИ ЗРЕНИЯ АТАКУЮЩЕГО

Планирование и проведение кибер-атаки

The Cyber Kill Chain

Planning the attack

Weeks in advance

- *Look for potential victims*
- *Collect relevant social data*
- *Build, find or buy your weapon of choice*
  - *Exploit kit, Malware package*
- *Adapt to your specific needs*
- *Package for delivery*

Getting In

Within seconds

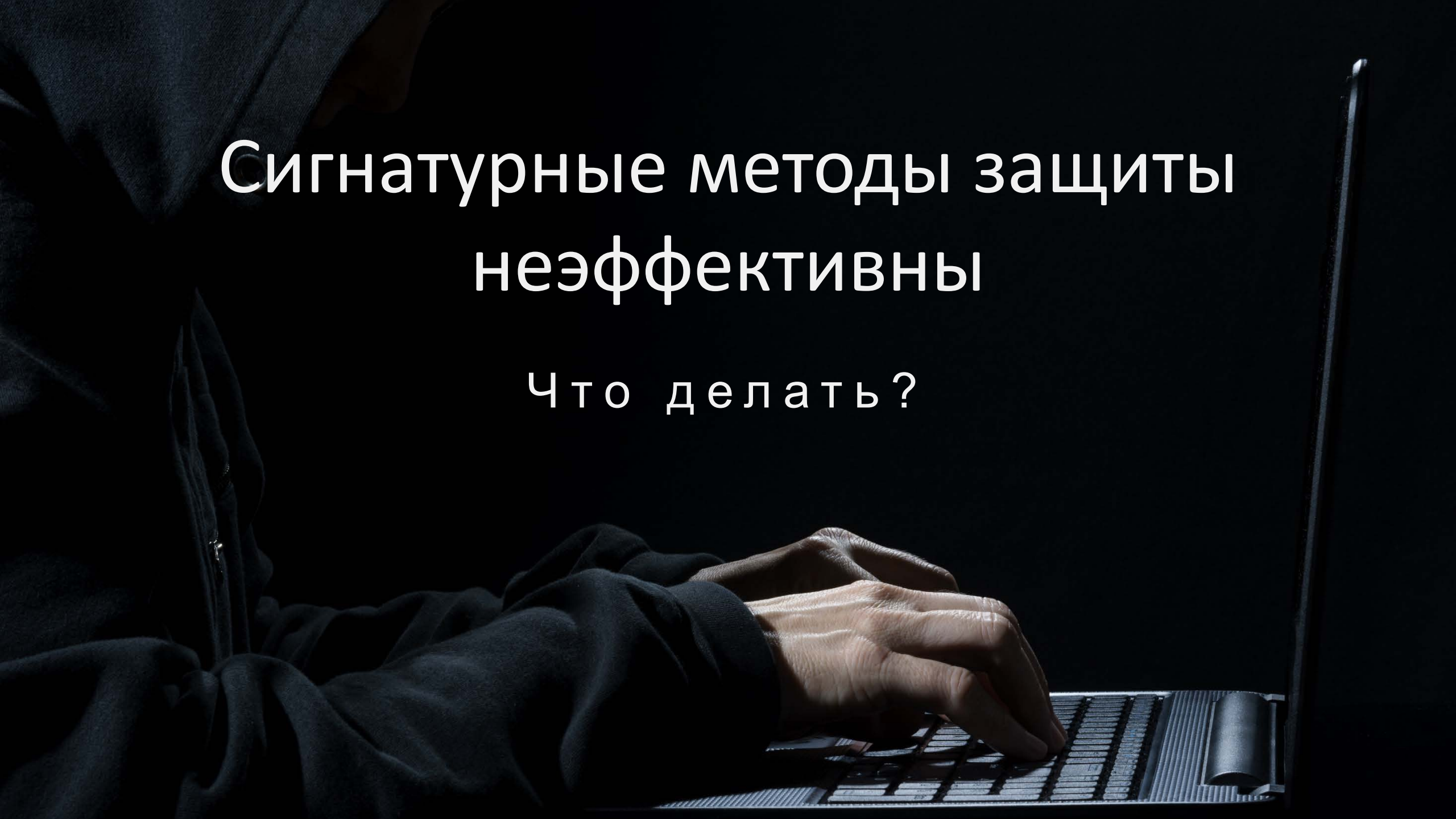
- *Bypass detection*
- *Convince the victim to open your crafted file*
- *Bypass system security control*
- *Install your malware*

Carrying out the attack

From here on…

- *Wait for your malware to "call home"*
- *Instruct it what to do on the victim's computer*
- *Continuously monitor its progress*

Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command & Control	Act on Objectives
Identify the target and exploitable weaknesses	Create/select attack vector	Deliver the malicious payload to the victim	Gain execution privileges	Install the malware on infected host	Establish a channel of communication	Data collection or corruption, Lateral movement and exfiltration

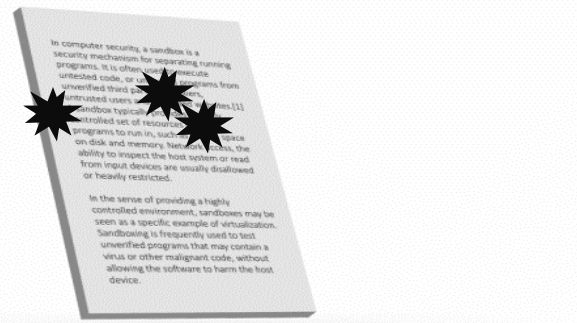


Сигнатурные методы защиты неэффективны

Что делать?

Эмуляция

Откроем файл в безопасной среде!



Наблюдаем:

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

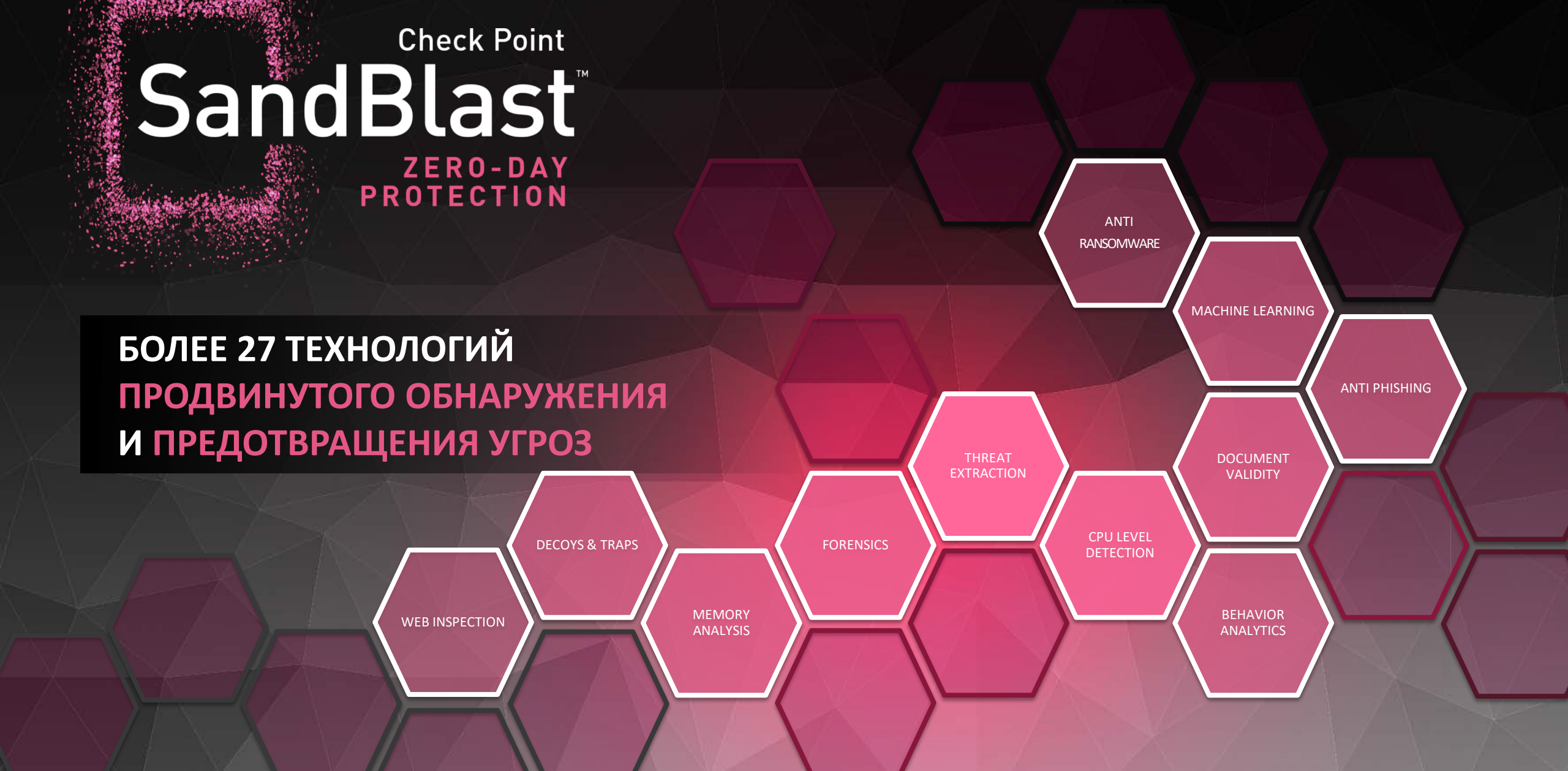
Поведение – вот что выдает зловредное ПО. Однако...

Обычную песочницу не так сложно обойти

Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point
SandBlast™
ZERO-DAY PROTECTION

БОЛЕЕ 27 ТЕХНОЛОГИЙ ПРОДВИНУТОГО ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ УГРОЗ



TRACK RECORD OF SECURITY LEADERSHIP AND EXCELLENCE

Check Point
SOFTWARE TECHNOLOGIES LTD.

IPS Recommended – Nov 2013
100% Mgt score; Best annual Mgt/Labor Cost (Upkeep / Tuning)!

NGFW Recommended – Feb 2013
Best Security + Management Score of 98.5%!

IPS Individual Test – Feb 2013 *
6100 IPS Security Score of 99%! 26.5G IPS

FW Recommended – Jan 2013
Best Security + Management score of 100%!

IPS Recommended – July 2012
Leading integrated IPS Security Score of 98.7%!

NGFW Recommended – Jan 2012
Continued NGFW Leadership and Excellence!

FW Recommended – April 2011
Only vendor to pass the initial test!

NGFW Recommended – April 2011
World's first NSS Recommended NGFW!

IPS Recommended – Jan 2011
Best integrated IPS Security Score of 97.3%!

NGIPS Recommended – Oct 2016
Leading Overall Security Effectiveness (99.9%) and TCO!

BDS Recommended – Aug 2016
2nd BDS Recommended! 100% Evasion Resistant!

NGFW Recommended – Feb 2016
99.8% Security Score! 5th NGFW Recommended and 11th NSS Recommended since 2011!

BDS Recommended – Aug 2015
Leading Security Effectiveness and TCO!

NGFW Recommended – Sept 2014
4th NGFW Recommended and 9th NSS Recommended since 2011!

NSS Labs

RECOMMEND

- Individual product test. NSS award "Recommended" only in Group Tests.

Check Point SandBlast

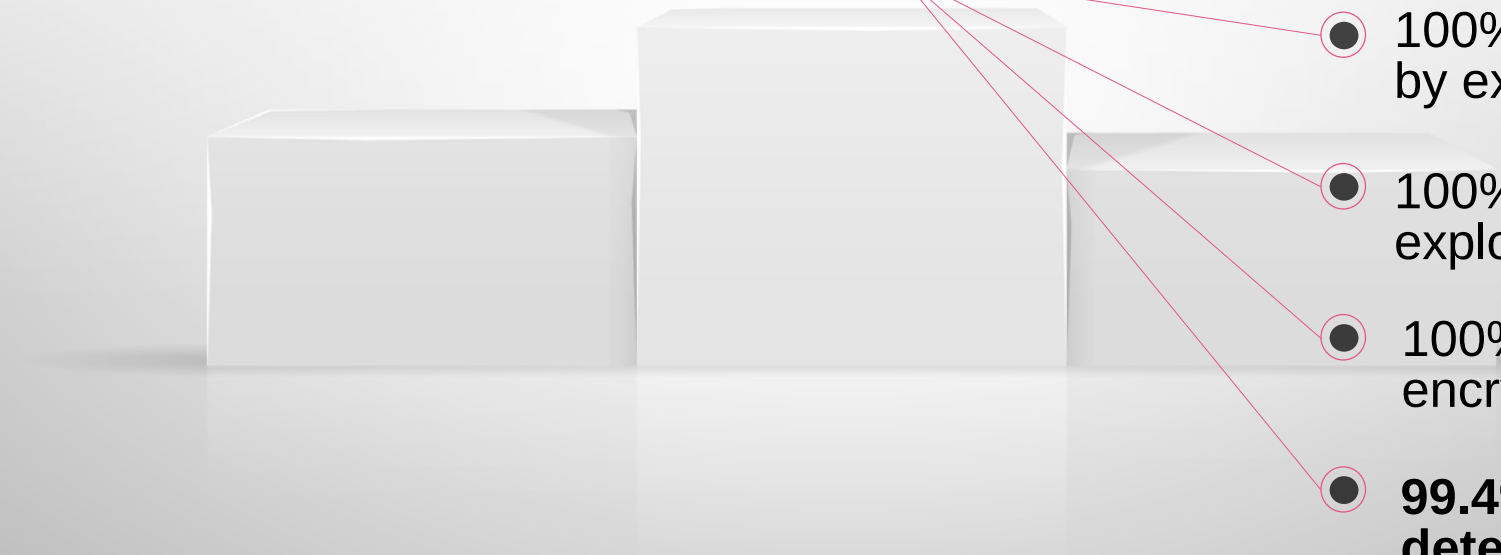
Recommended for Security Effectiveness and Value

2016 NSS Breach Detection Systems Test

Check Point SOFTWARE TECHNOLOGIES LTD.

NSS LABS RECOMMENDED

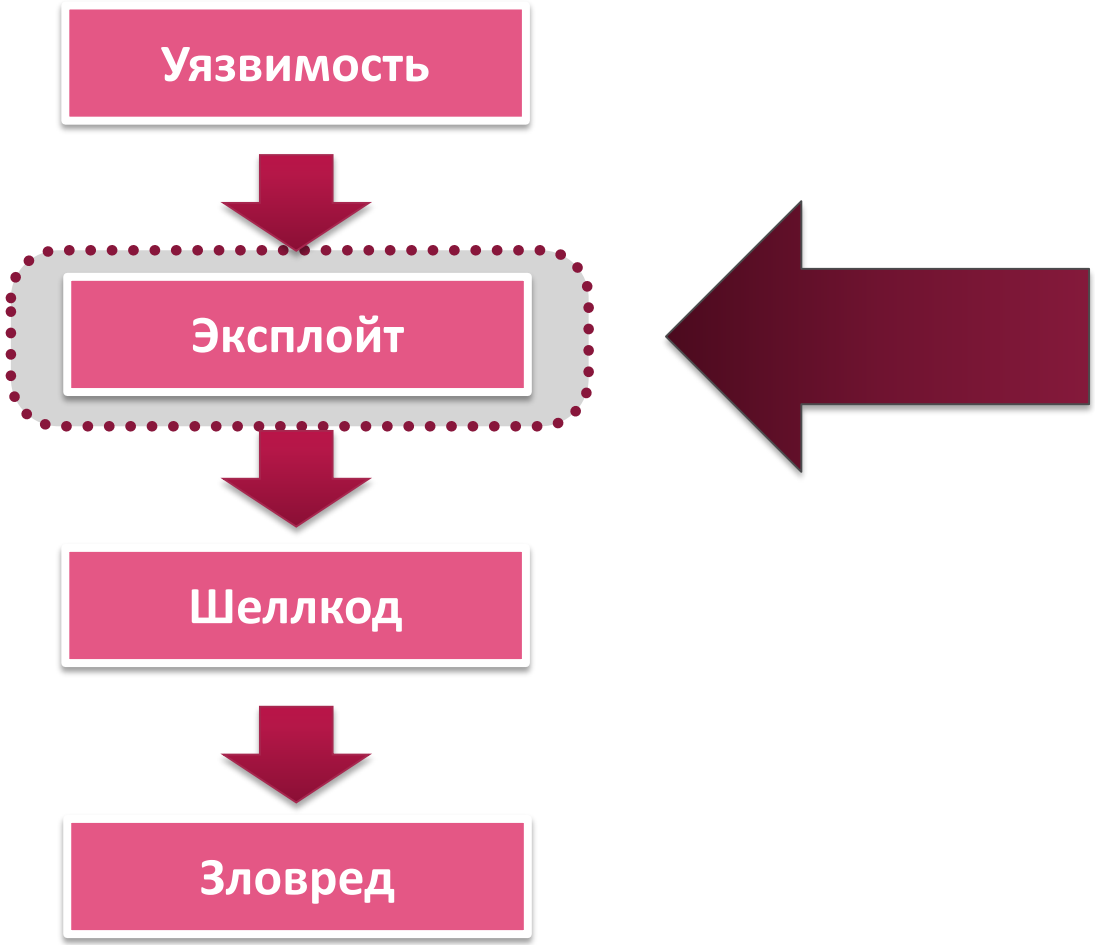
Check Point SandBlast™ ZERO-DAY PROTECTION



- 99.6% catch-rate of HTTP malware
- 100% catch-rate for Email unknown malware
- 100% evasion resistant sandbox
- 100% catch-rate for Drive-by exploits
- 100% catch-rate for Social exploits
- 100% catch-rate of SSL encrypted malware
- **99.4% overall breach detection rate**

Read the report: https://www.checkpoint.com/resources/nss-breach-detection-systems/

CPU-Level Detection



Фокус на обнаружении методов взлома

- **Обнаружение атаки до её начала**
  - Хакер не успевает запустить алгоритмы обхода
- **Узкое место для атаки**
  - Методов взлома существует всего несколько
  - Уязвимостей – тысячи, зловредов - миллионы

Threat Extraction: мгновенная очистка документов

Эмуляция всегда требует времени

- Большинство песочниц конкурентов работает в режиме обнаружения, а не предотвращения
- Они пропускают зловред в сеть, тем временем анализируют его в фоновом режиме

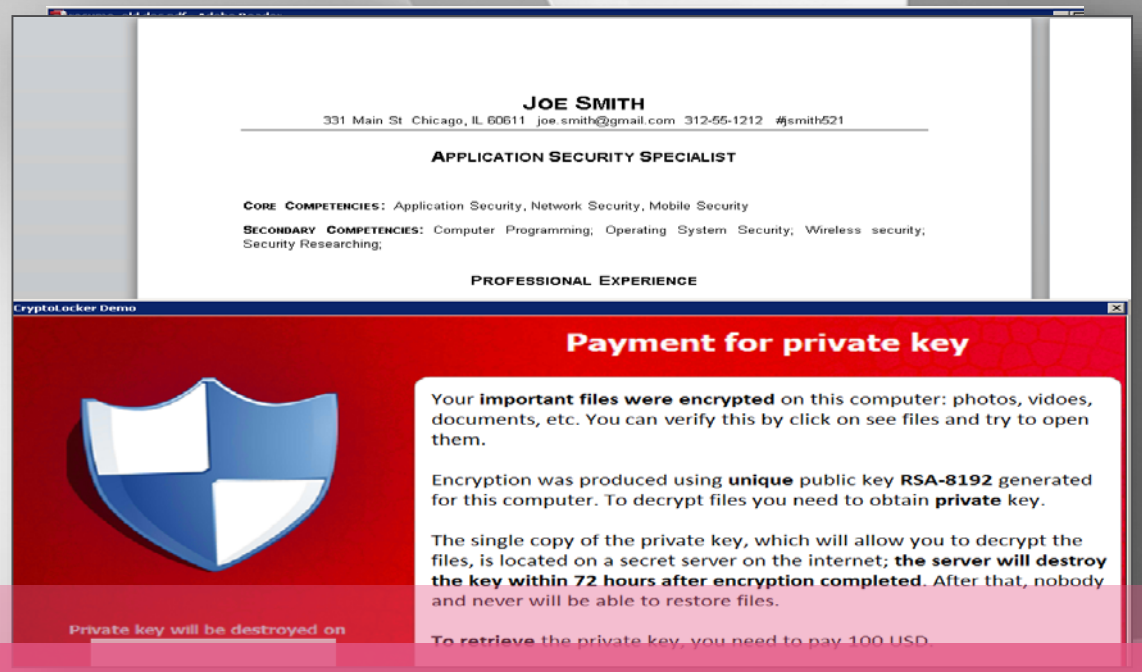
SandBlast Threat Extraction

Доставка гарантированно безопасных файлов

Check Point
SOFTWARE TECHNOLOGIES LTD.

ДО

Активация вредоносного ПО

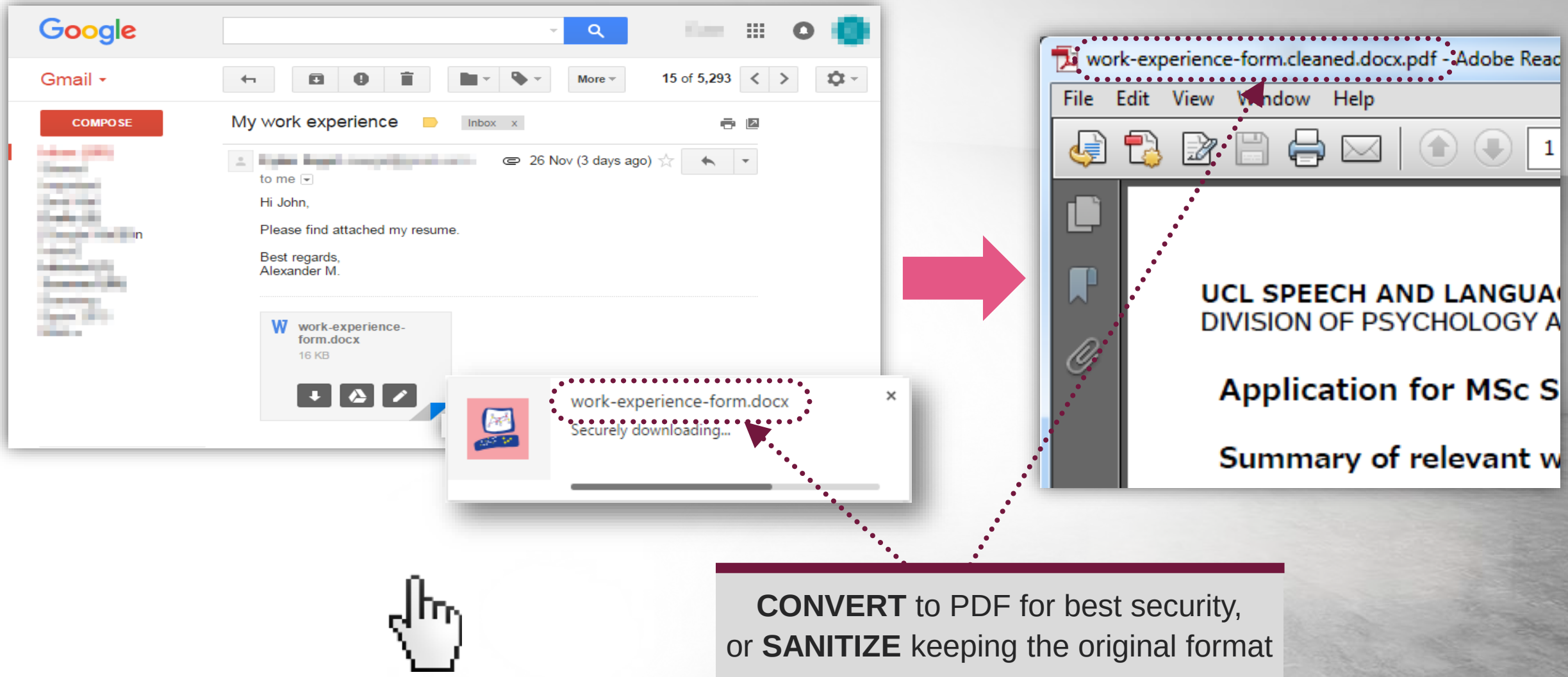


ПОСЛЕ

Вредоносное ПО удалено

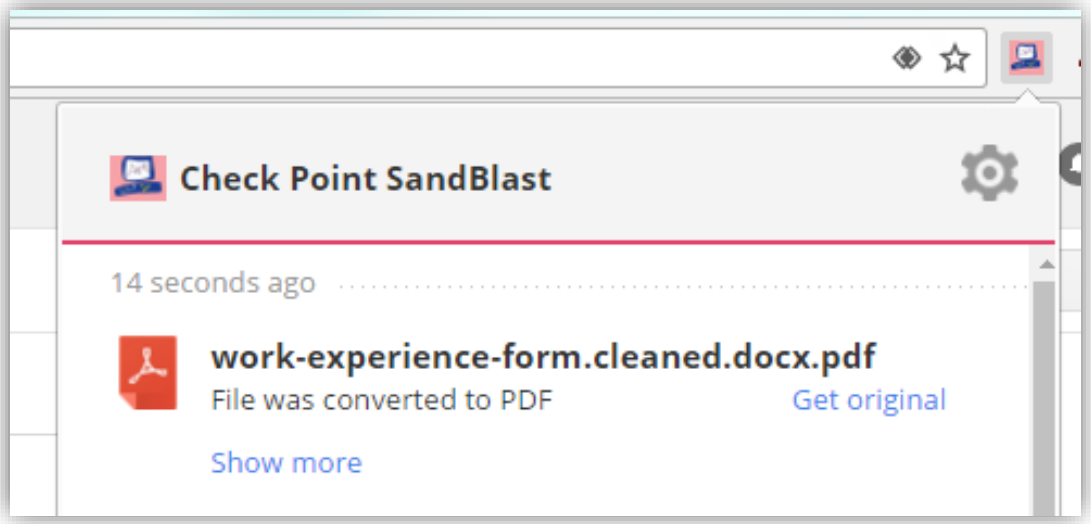
Немедленный доступ. Проактивная защита.

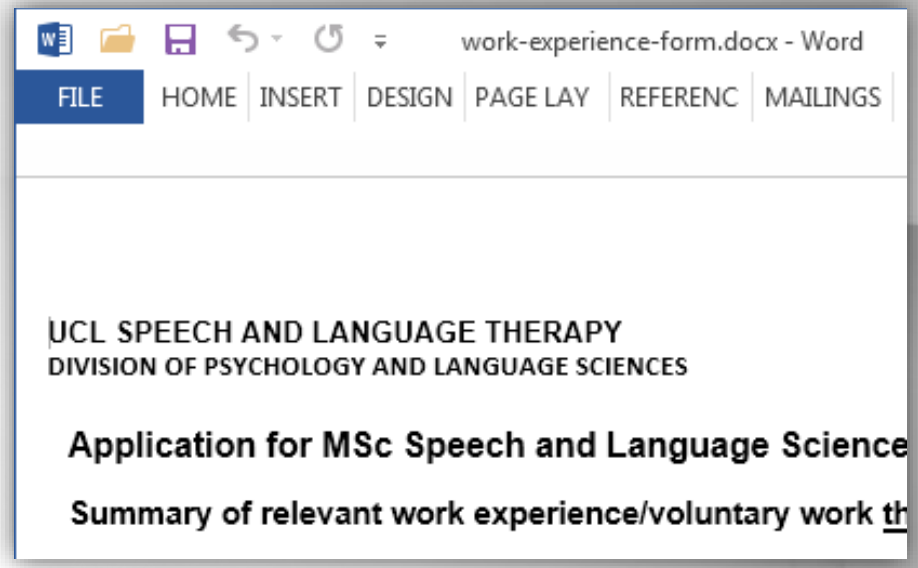
Как это работает при загрузке с Web



CONVERT to PDF for best security,
or **SANITIZE** keeping the original format

EASILY & SECURELY ACCESS THE ORIGINAL FILE





Only After Threat Emulation

when verdict is benign

Self-Catered

No Helpdesk Overhead

Кто-то работает удаленно

Внешние наколители

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

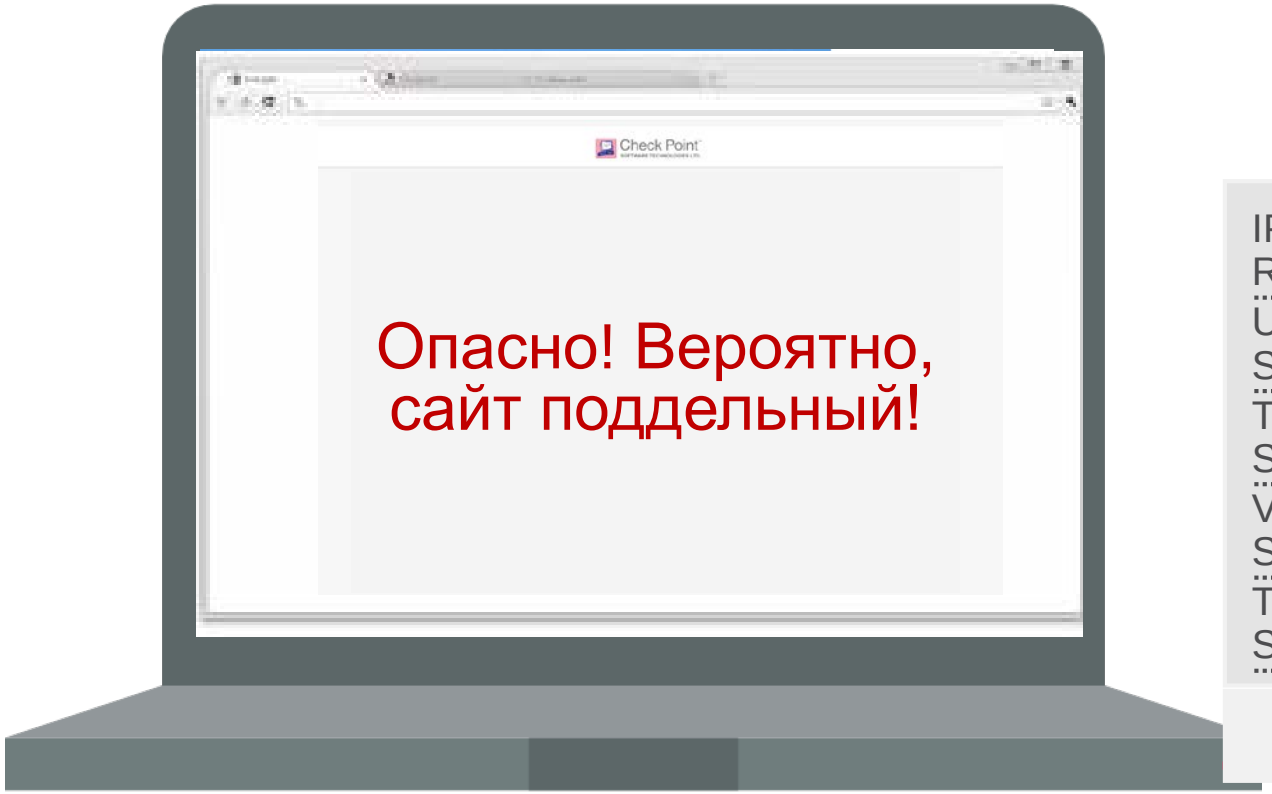
1 Файл отсылается на устройство или облако SandBlast

2 Безопасная копия доставляется мгновенно

3 Оригинал эмулируется

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%

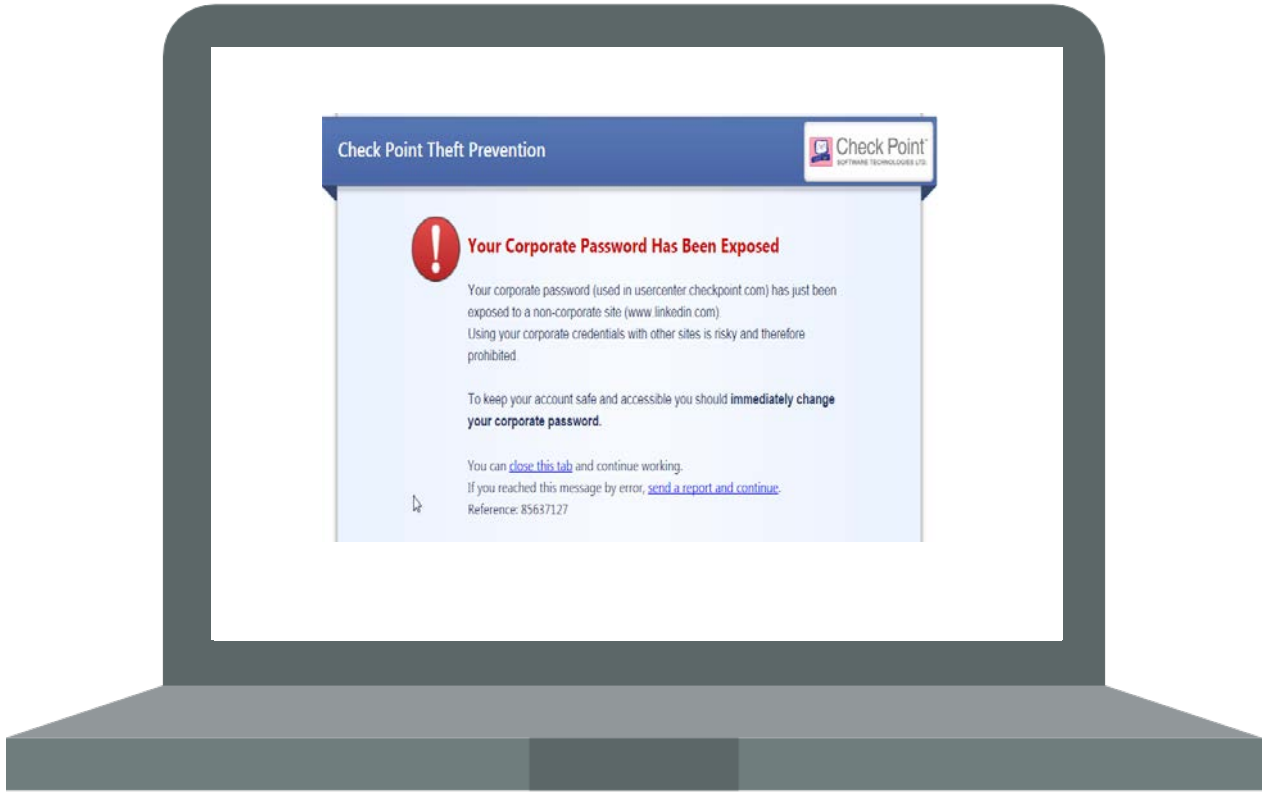
1 Новые сайты анализируются

2 Репутационный и эвристический анализ

3 Вердикт выносится за секунды

Предотвращение фишинга

Защита корпоративного пароля

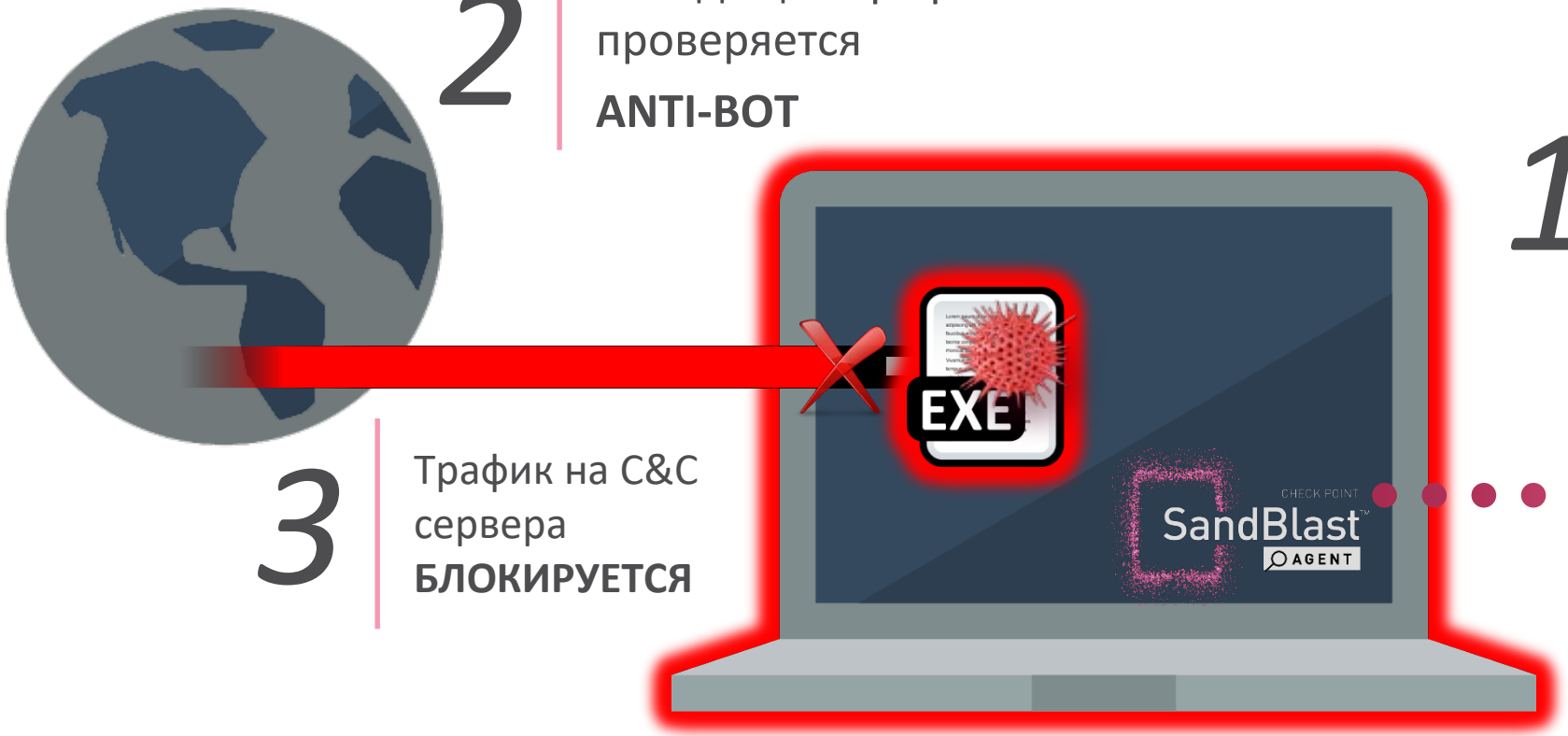


Предотвращает ошибочное или случайное использование корпоративного пароля на других ресурсах.

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**

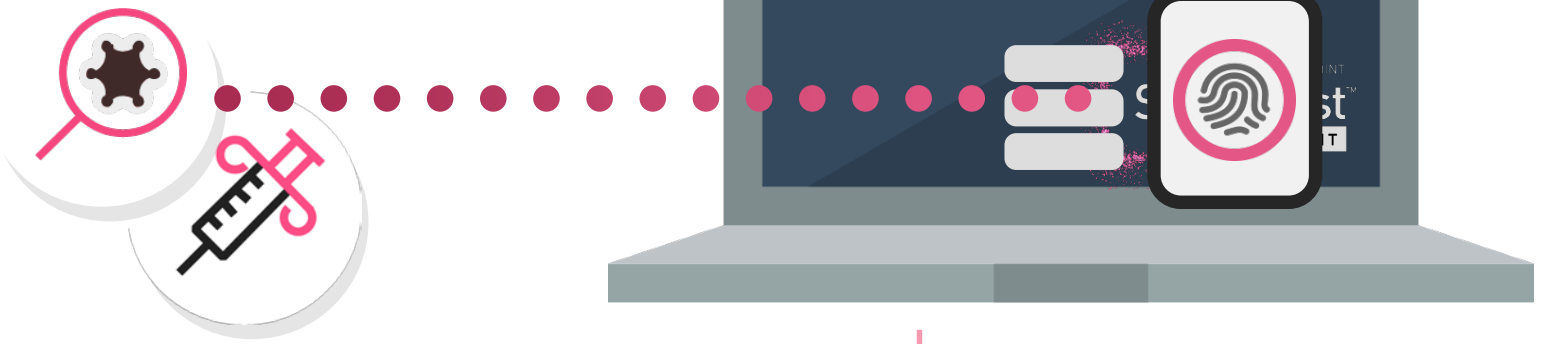
4 **ОСТАНАВЛИВАЕТСЯ** подозрительный процесс либо **БЛОКИРУЕТСЯ** компьютер целиком

Сбор данных и формирование отчета

Check Point
SOFTWARE TECHNOLOGIES LTD.

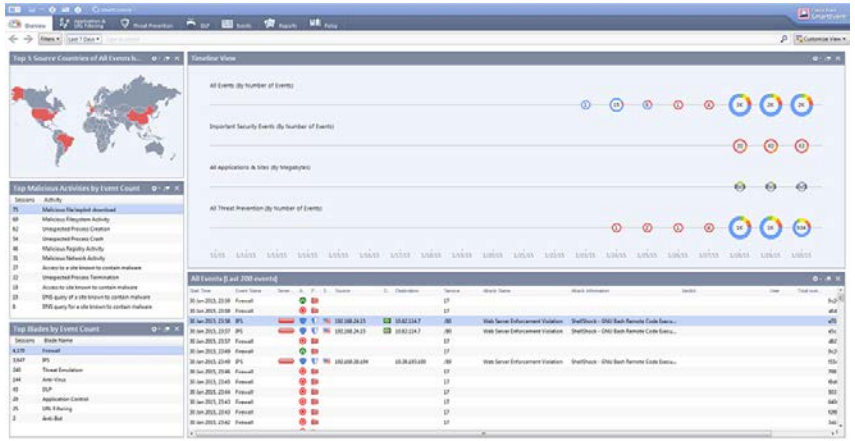
1 **ДАННЫЕ** о системе собираются постоянно от многих источников

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

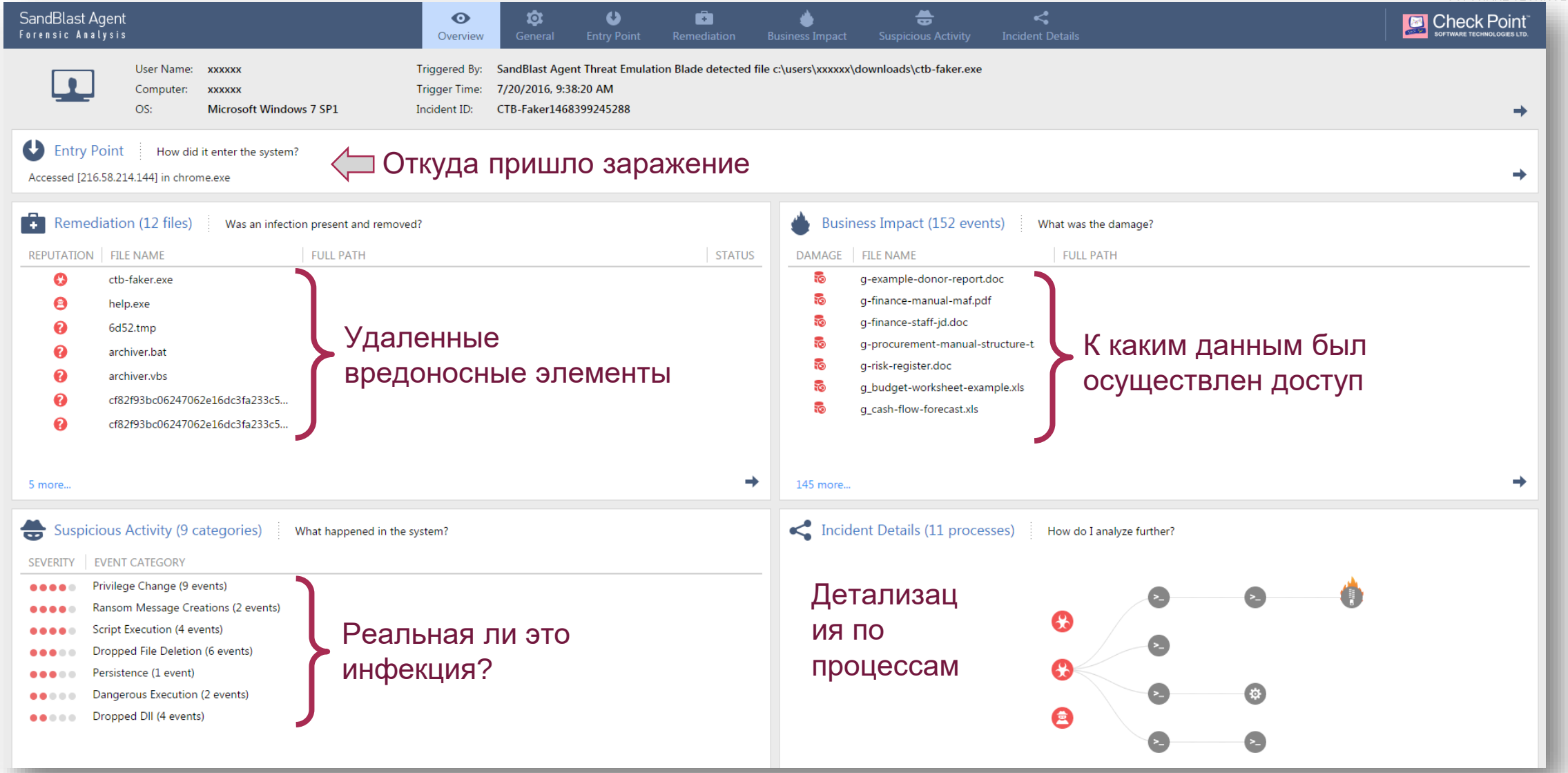


3 Сырые данные анализируются с помощью сложных алгоритмов

4 **ПОДРОБНЫЙ** отчет формируется на SmartEvent



ОБЗОР ОТЧЕТА: ЭФФЕКТИВНАЯ АНАЛИТИКА



Демонстрация работи:

блокирование Petya и восстановление зашифрованных данных

Как работает антишифрувальщик

Фоновый процесс

Анализ поведения

Постоянный мониторинг признаков работы шифрувальщика

Обнаружение шифрования

Идентификация нелигитимного шифрования

Снимки данных

Постоянное создание крактосрочных резервных копий файлов

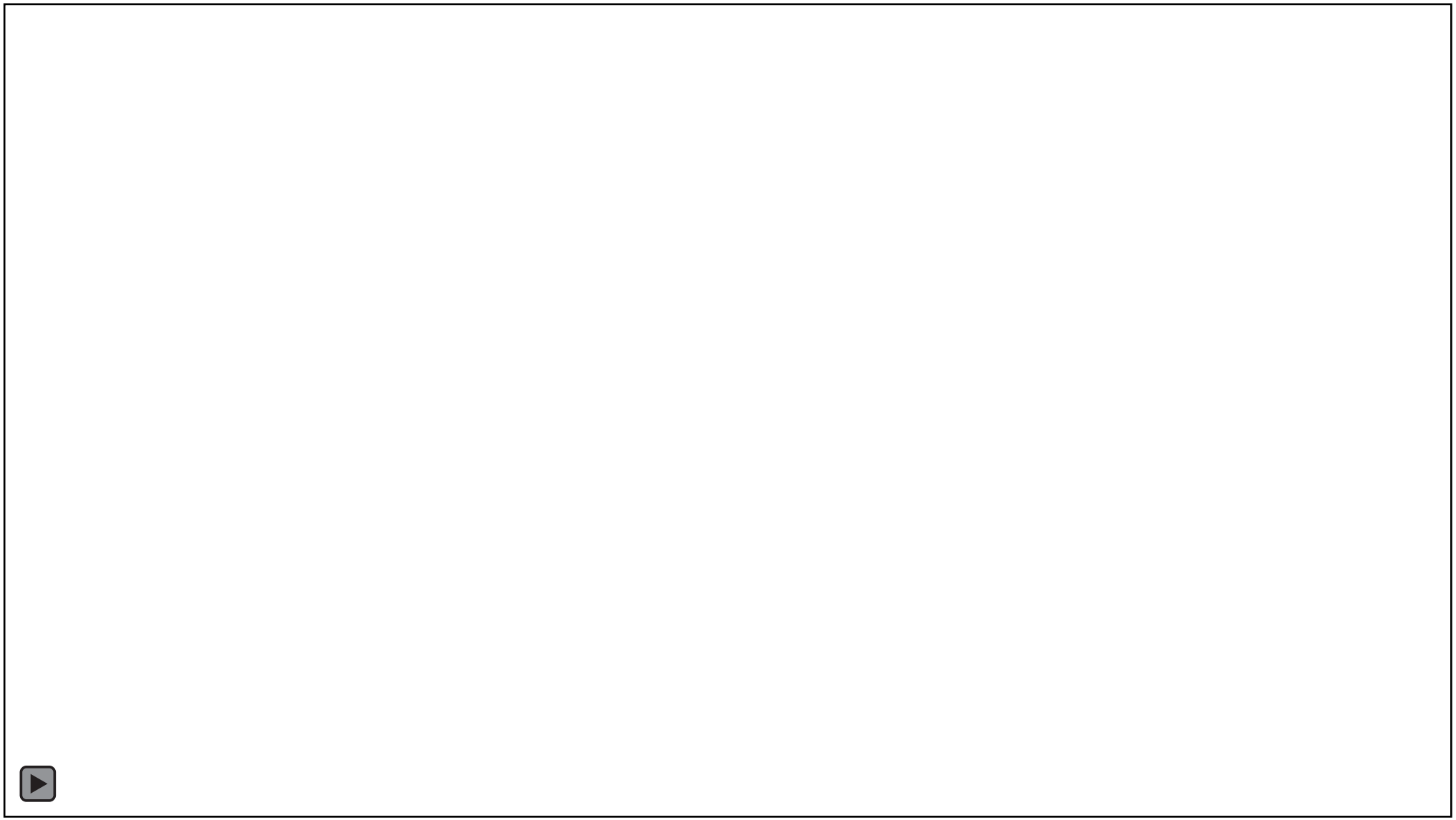
После обнаружения

Карантин шифрувальщика

Все элементы атаки идентифицируются процесоом анализа подозрительной активности и отправляются в карантин

Восстановление данных

Зашифрованные данные восстанавливаются из резервных копий



ЭФФЕКТИНОСТЬ ANTI RANSOMWARE

Тетсы только с технологией Anti-Ransomware

Без использования Антивируса, Антибота и Песочницы

| 6 месяцев | Свыше 200 копий в день

99.3% уровень детекта

*In real life you don’t have to turn those other protections off

“95% успешных атак можно было предотвратить, если бы существующие решения для защиты были бы настроены правильно”

Gartner

“Консоль управления Check Point остается де факто “золотым стандартом” с которым сравнивают остальных” Gartner

Одна система – единое управление

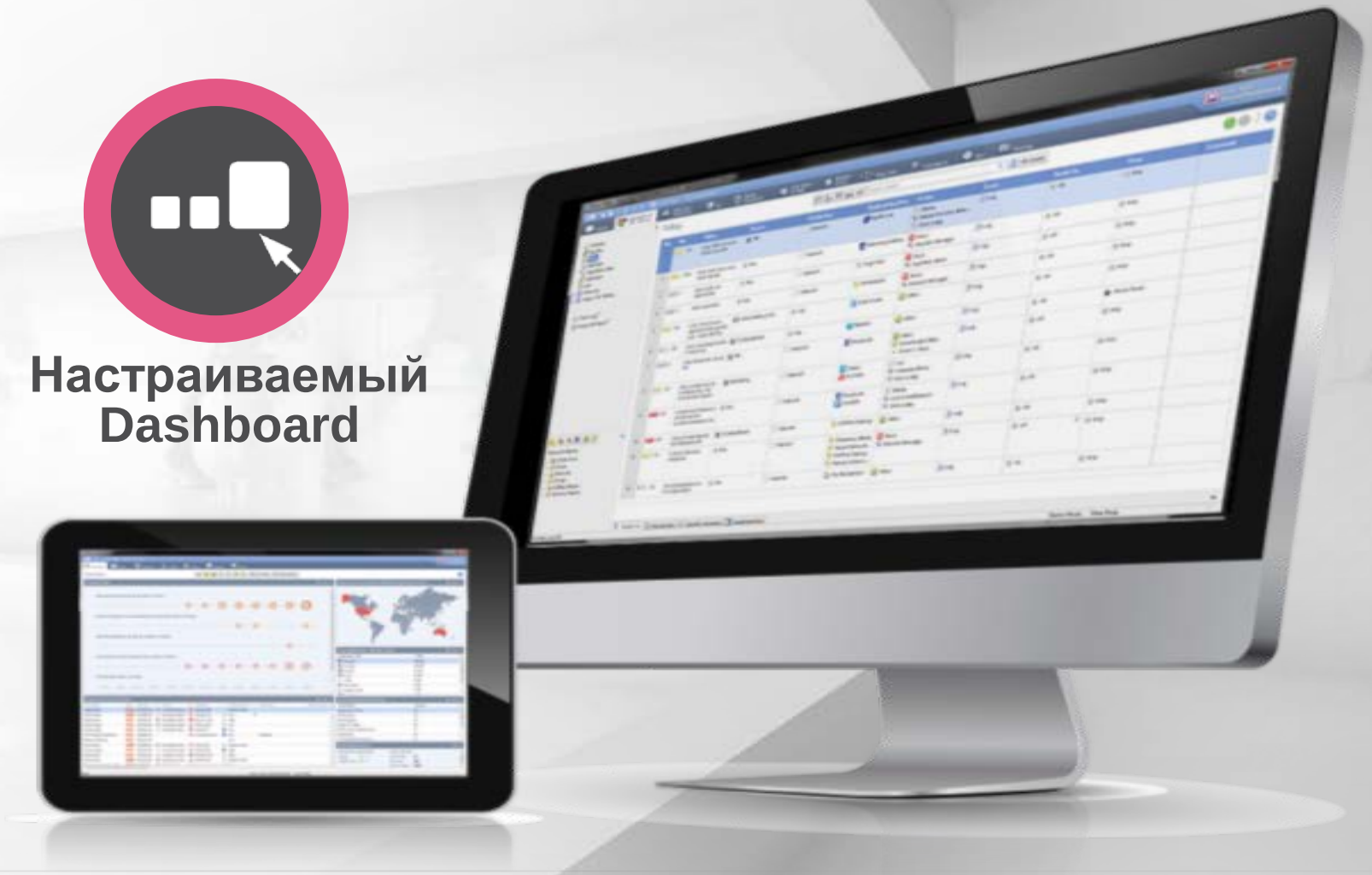
Удобная настройка, полная интеграция, абсолютная видимость

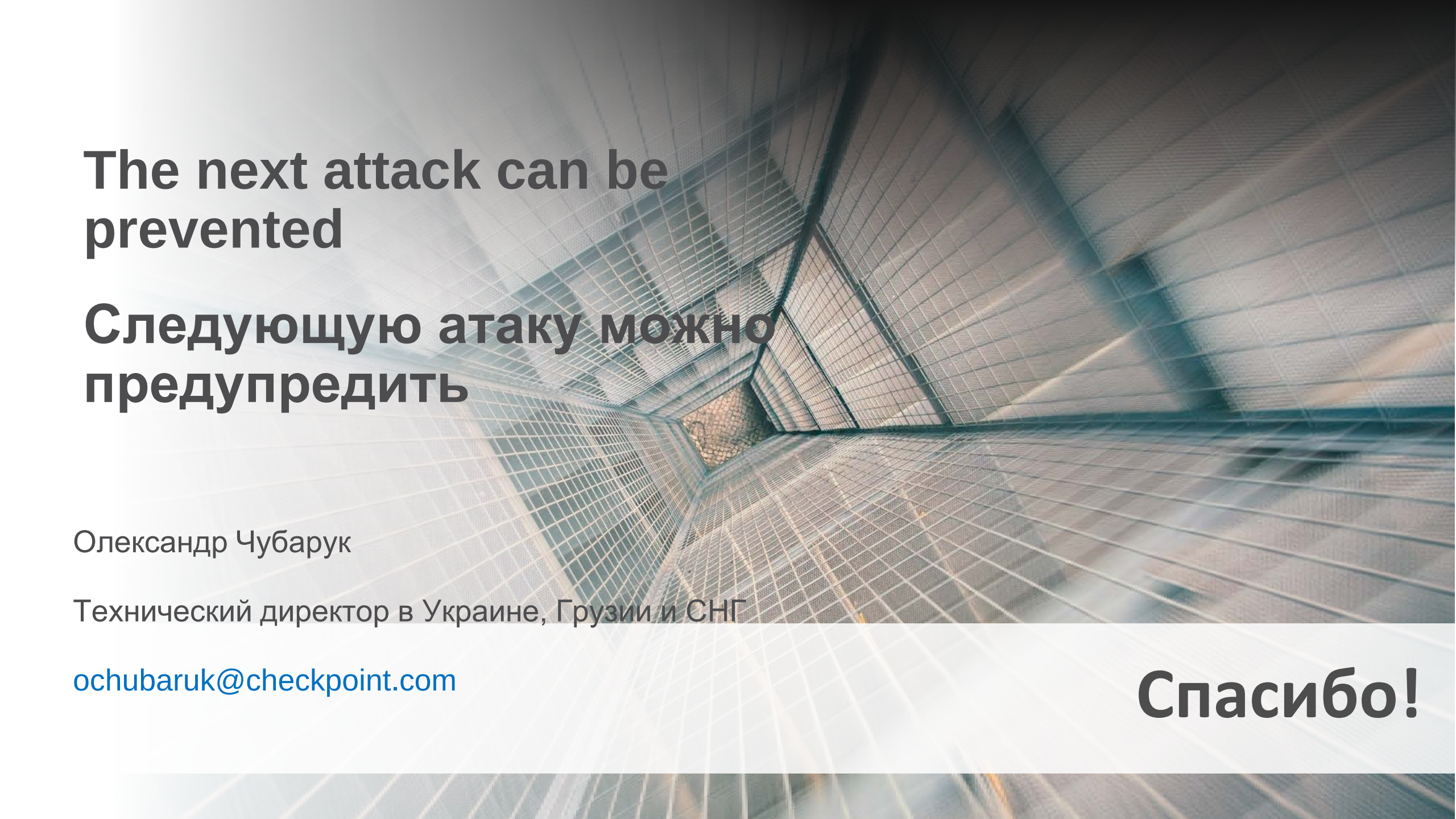
Интеграция и мониторинг

Общие политики

Настраиваемый Dashboard

CHECK POINT SandBlast™ ZERO-DAY PROTECTION





The next attack can be prevented

Следующую атаку можно предупредить

Олександр Чубарук

Технический директор в Украине, Грузии и СНГ

ochubaruk@checkpoint.com

Спасибо!