Check Point
SOFTWARE TECHNOLOGIES LTD.

На шаг впереди:
Как прекратить рассуждать об обнаружении новых угроз и начать их предотвращать?

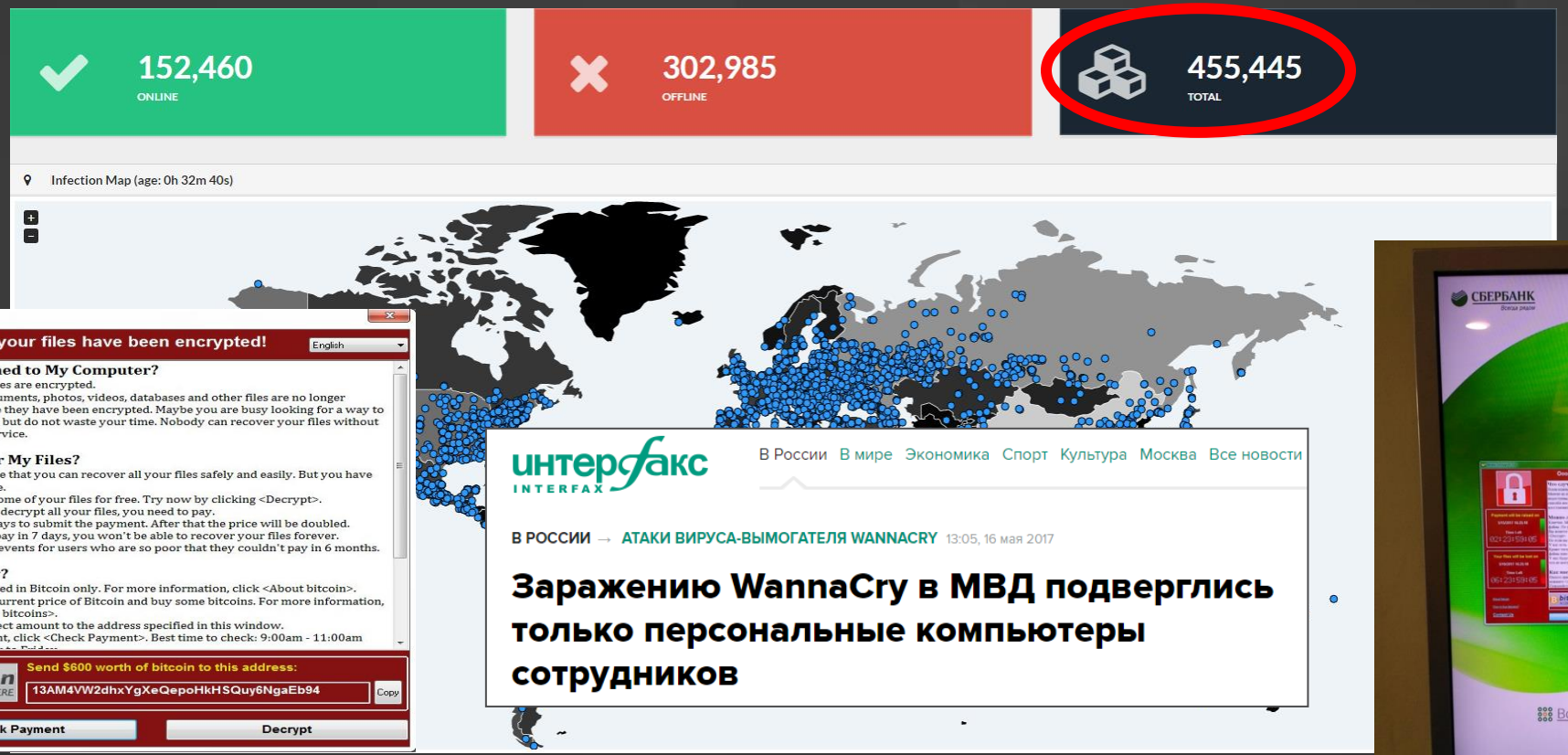
network, endpoint, mobile, cloud

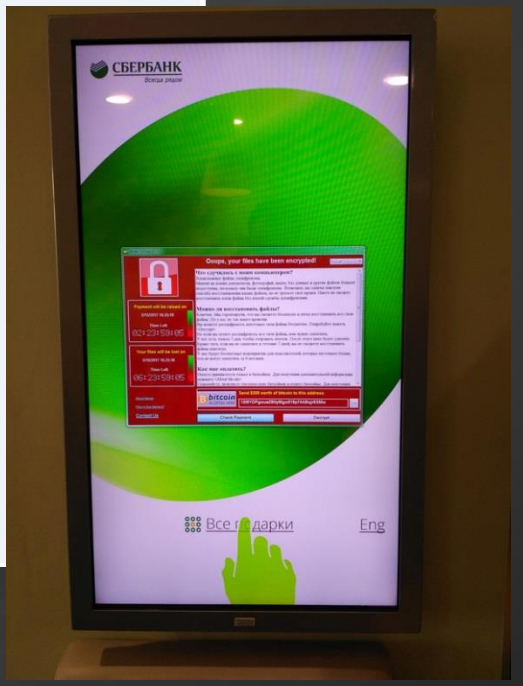
Алексей Белоглазов
Руководитель группы инженеров ИБ
abeloglazov@checkpoint.com
+79856478564

WannaCry: масштаб бедствия

MalwareTech (kill-switch domain sinkhole)

https://intel.malwaretech.com/botnet/wcrypt/





WannaCry 2.0: no kill-switch!

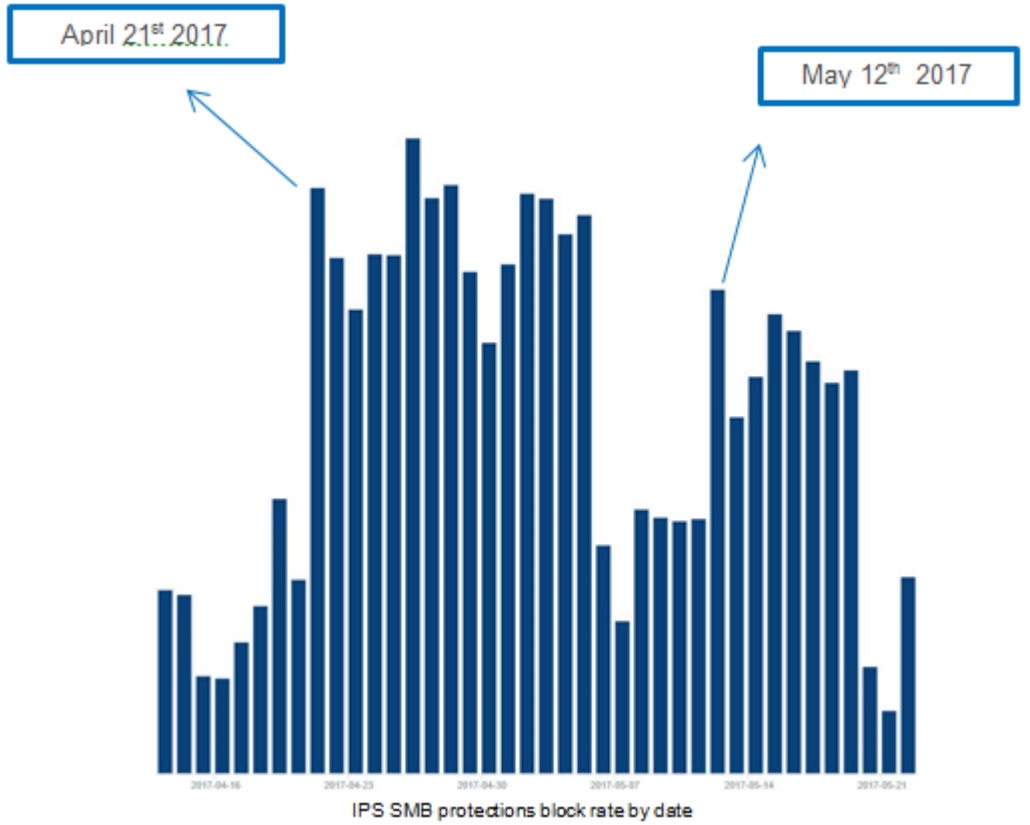
http://blog.checkpoint.com/2017/05/15/wannacry-new-kill-switch-new-sinkhole/

Пример: векторы атаки WannaCry

1. Червь WannaCryPTOR использует разработки АНБ (утечка через Shadow Brokers):
   - Поиск уязвимых хостов: SMBTouch, ArchiTouch
   - Эксплойты для SMB MS17-10: EternalBlue, EternalChampion, EternalSynergy, EternalRomance
   - Бэкдор: DoublePulsar

2. Фишинговая рассылка:
   - Ссылки в теле письма и документах PDF
   - Архивы ZIP с паролем с PDF

3. Атаки brute-force login на RDP-серверы и установка на них Ransomware



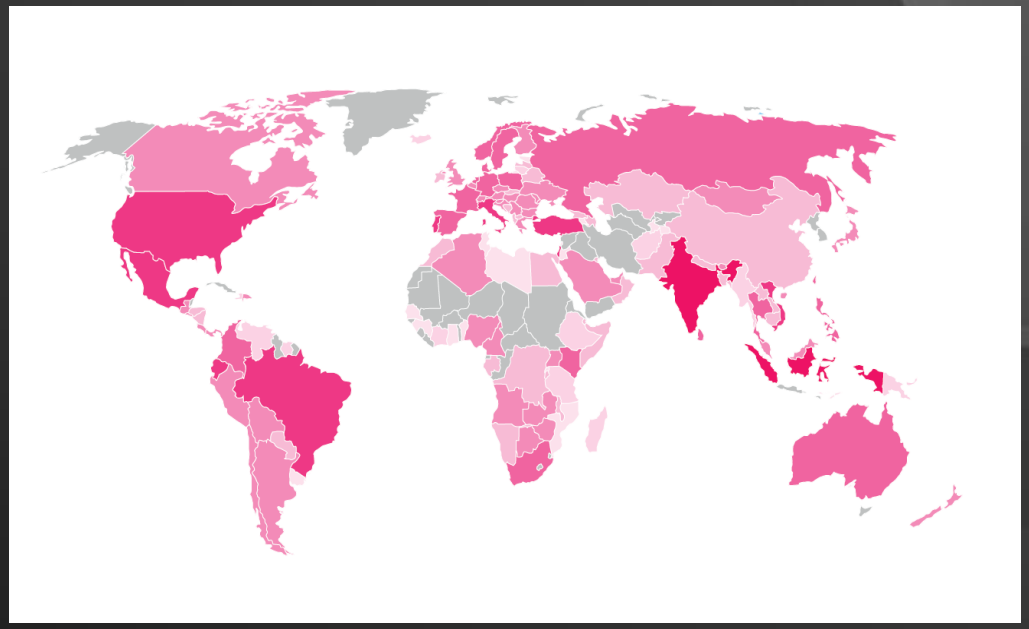
http://blog.checkpoint.com/2017/05/12/global-outbreak-wanacrypto/

http://blog.checkpoint.com/2017/05/25/brokers-shadows-analyzing-vulnerabilities-attacks-spawned-leaked-nsa-hacking-tools/

FIREBALL – новый китайский вредонос под управлением Rafotech marketing agency (Beijing) 250 млн. зараженний по веб!

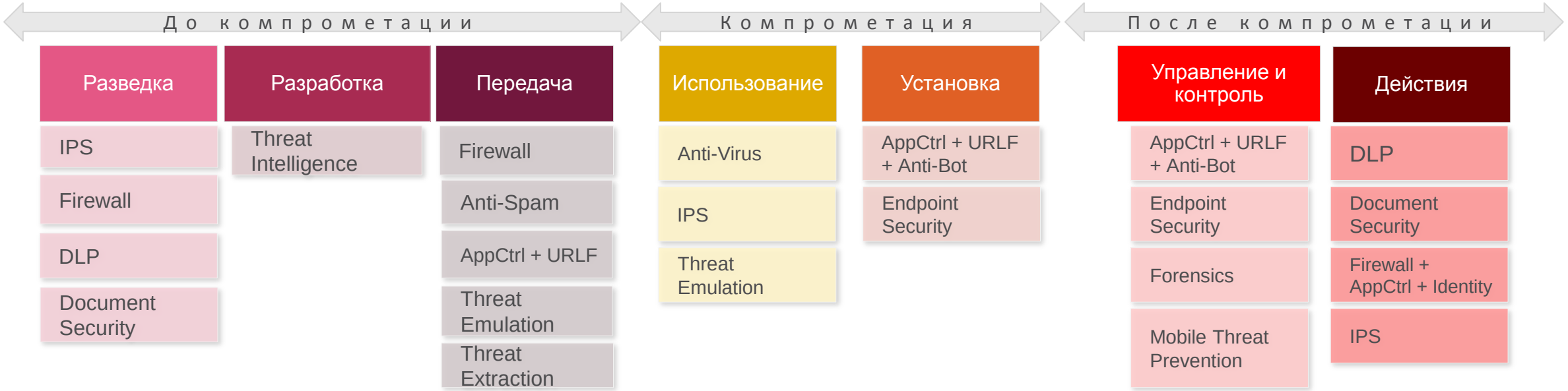
Browser hijacking через Wi-Fi / бесплатное ПО

- Фальшивый поисковик с редиректами на настоящие
- Кража данных пользователя, докачивание вредоносного ПО



УСПЕШНАЯ СТРАТЕГИЯ ЗАЩИТЫ
на всех этапах атаки для каждого вектора

Check Point
SOFTWARE TECHNOLOGIES LTD.



Предотвращение **ИЗВЕСТНЫХ** атак

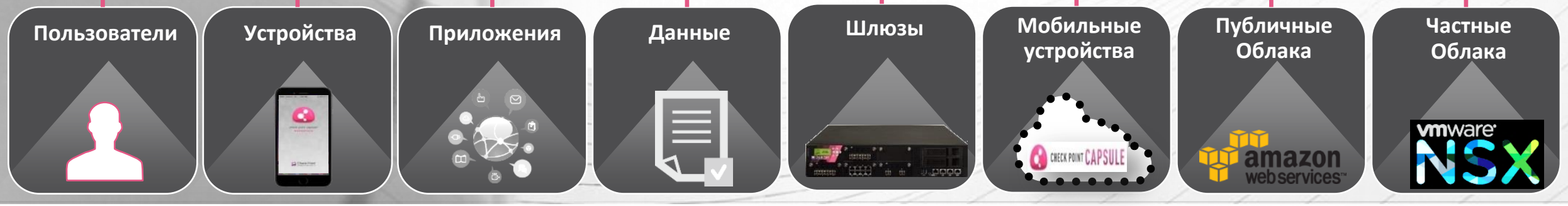
Применение защиты на основе сигнатур на каждом шаге для быстрого блокирования вторжений

Предотвращение **НЕИЗВЕСТНЫХ** атак

Блокировка даже новых и опасных атак с помощью технологий проактивной защиты

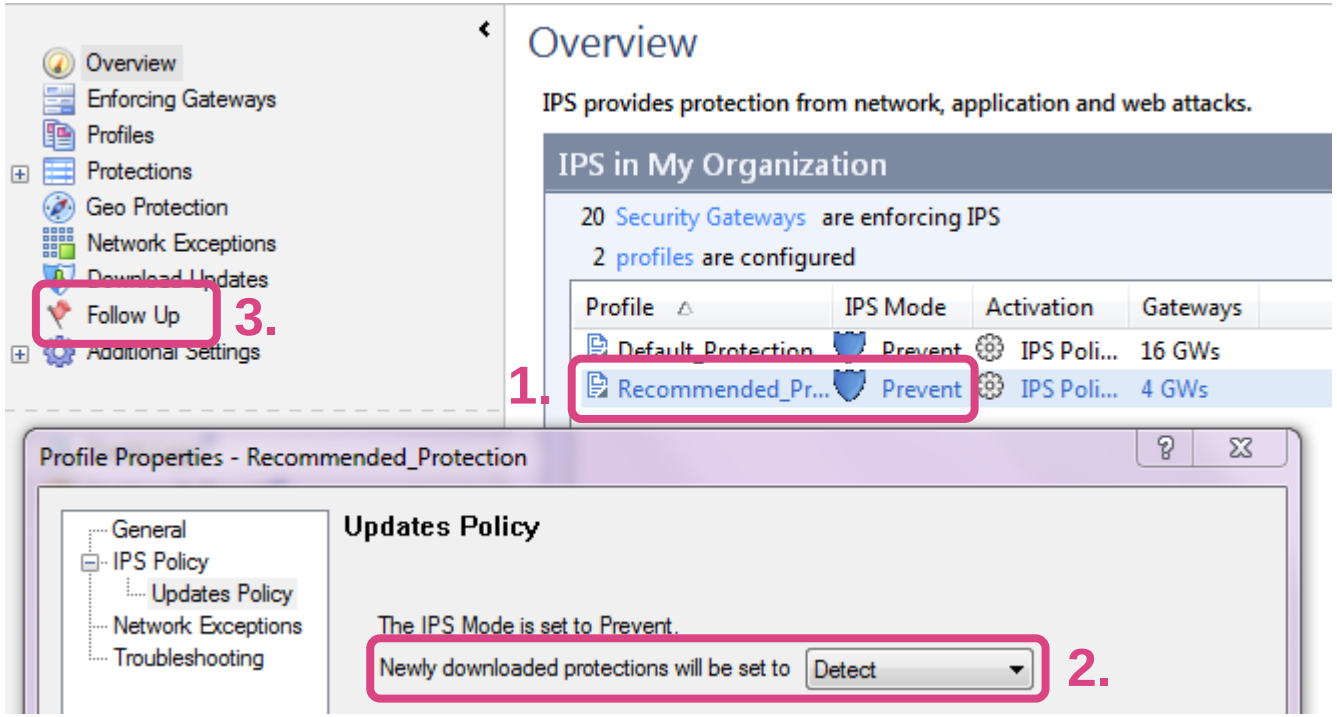
R80.10: единая политика контроля доступа

Name	Source	Destination	Services & Applications	Data	Action	Install On
Outbound access	production_net	Internet	Any	Any	AccessSubLayer	Policy Targets
Social media for marketing	marketing_role John	Internet	Twitter LinkedIn Instagram	Any	Accept	SG13800
Developers upload	developer_role	Internet	Dropbox Box	Any Direction Source Code - JAVA	Accept	SG13800 CapsuleCloud
Access Sensitive Servers	Any	Any	Any	Any	SensitiveServers	Policy Targets
Mobile Access	Mobile Devices	MailUS	MailServer	Any	Accept	Mobile
Access to Web Server	Any	WebServer	https	Any	Accept	AWS VMWare



Сокращение площади атаки

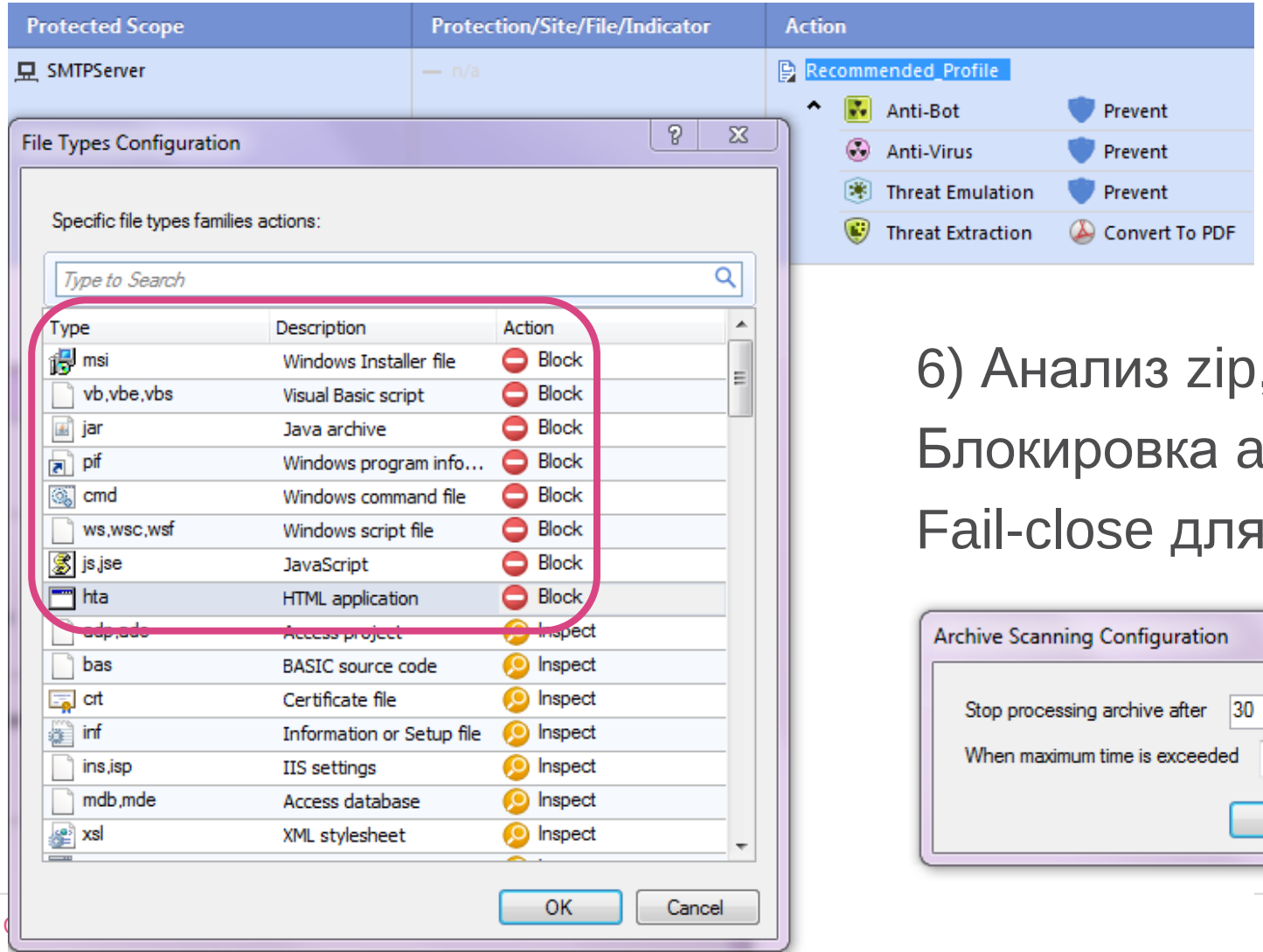
1) Next-Gen Firewall для сегментации и микросегментации, SDN (vSEC)
2) Строгая политика доступа на уровне приложений и групп пользователей
3) Расшифрование вх. и исх. SSL с исключениями по категориям
4) Предотвращение атак IPS без риска для доступности сервисов



Сокращение площади атаки

Check Point
SOFTWARE TECHNOLOGIES LTD.

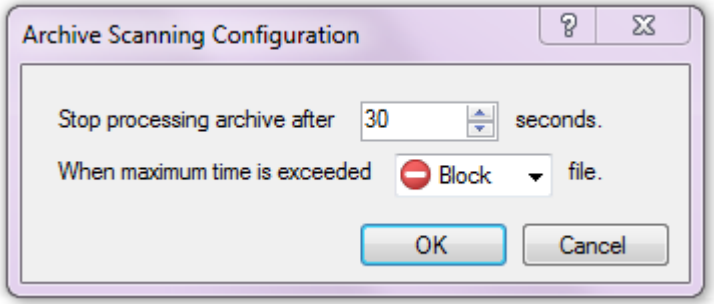
5) Блокировка опасного контента (exe, wsf, …) по формату и способу доставки



6) Анализ zip, rar, 7zip,…

Блокировка ace, arj, bz2, lzh,…

Fail-close для архивов с паролем



Zero Day Prevention vs. Detection

Большинство «песочниц» выборочно предотвращают в электронной почте и только детектируют в веб.

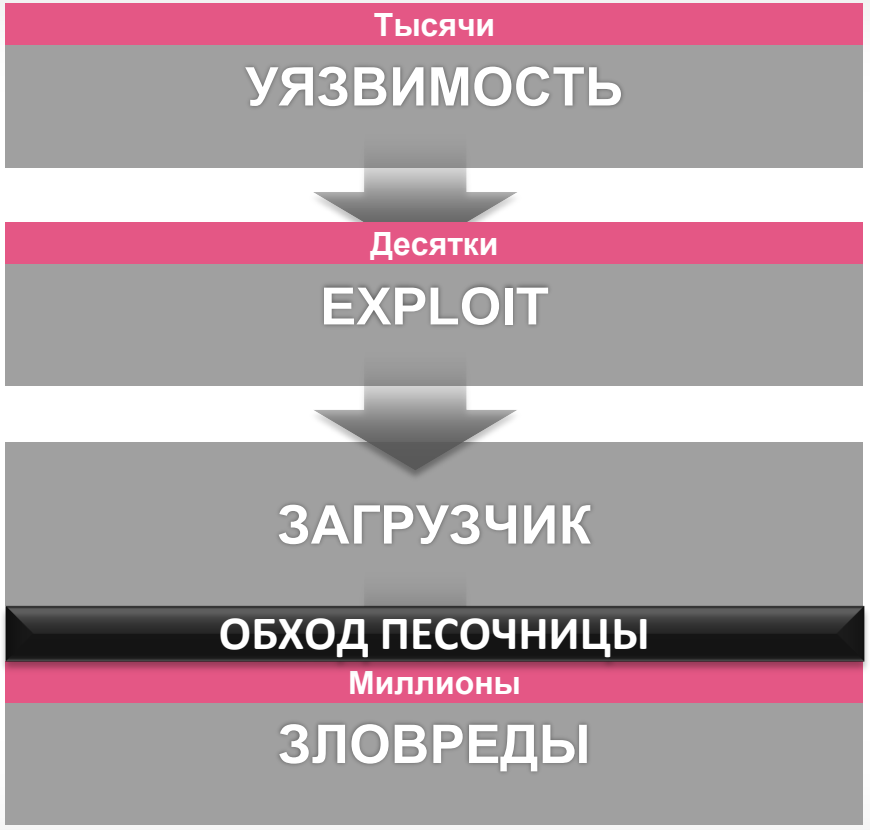
Они сообщают Вам плохие новости, **когда уже слишком поздно**, и создают много работы.

Сигнатура через X минут – это здорово, но уже не для Вас...

Обычную песочницу не так сложно обойти

Эмуляция в SandBlast всегда на шаг впереди

Check Point
SOFTWARE TECHNOLOGIES LTD.



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

Семейство ТЕХНОЛОГИЙ для защиты от таргетированных атак

THREAT EMULATION

Среда эмуляции (Уровни ЦП и ОС), устойчивая к методикам обхода

THREAT EXTRACTION

Проактивное удаление опасного контента при доставке

ENDPOINT FORENSICS

Быстрое понимание ситуации для лучшей защиты и исправления

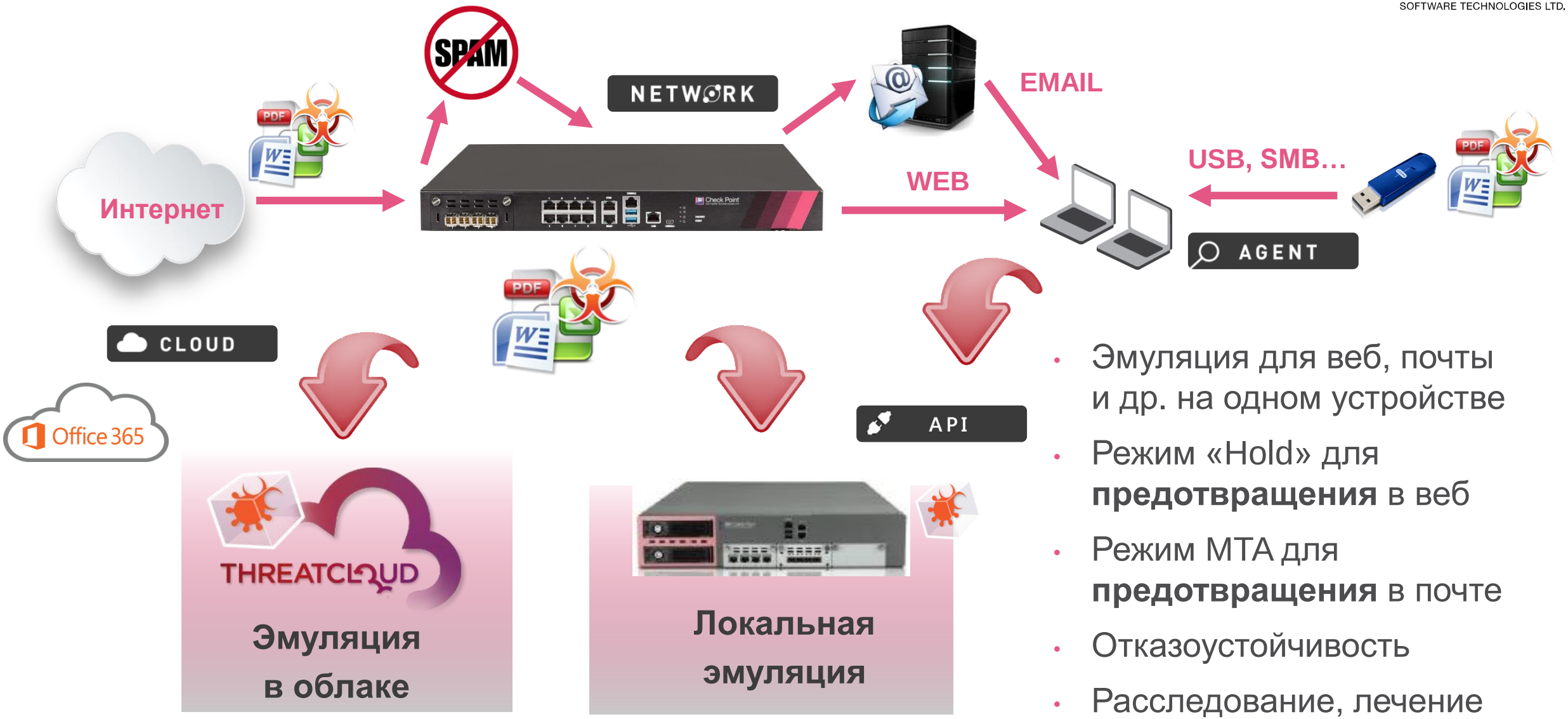
ZERO PHISHING

Защита учетных записей от кражи через фишинговые сайты

ZERO RANSOMWARE

Идентификация и восстановление после действий программы-вымогателя

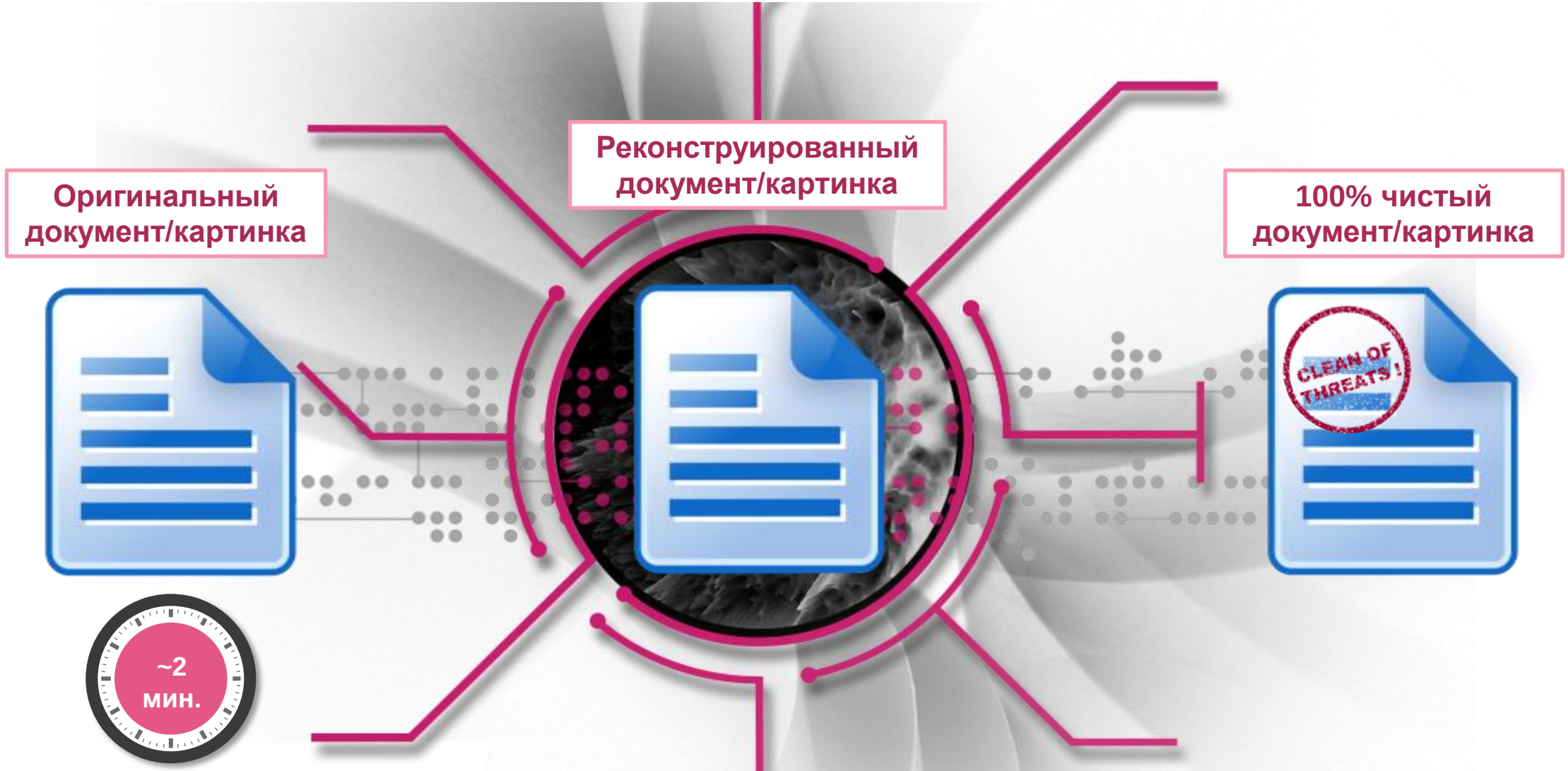
Предотвращение Zero Day с Check Point



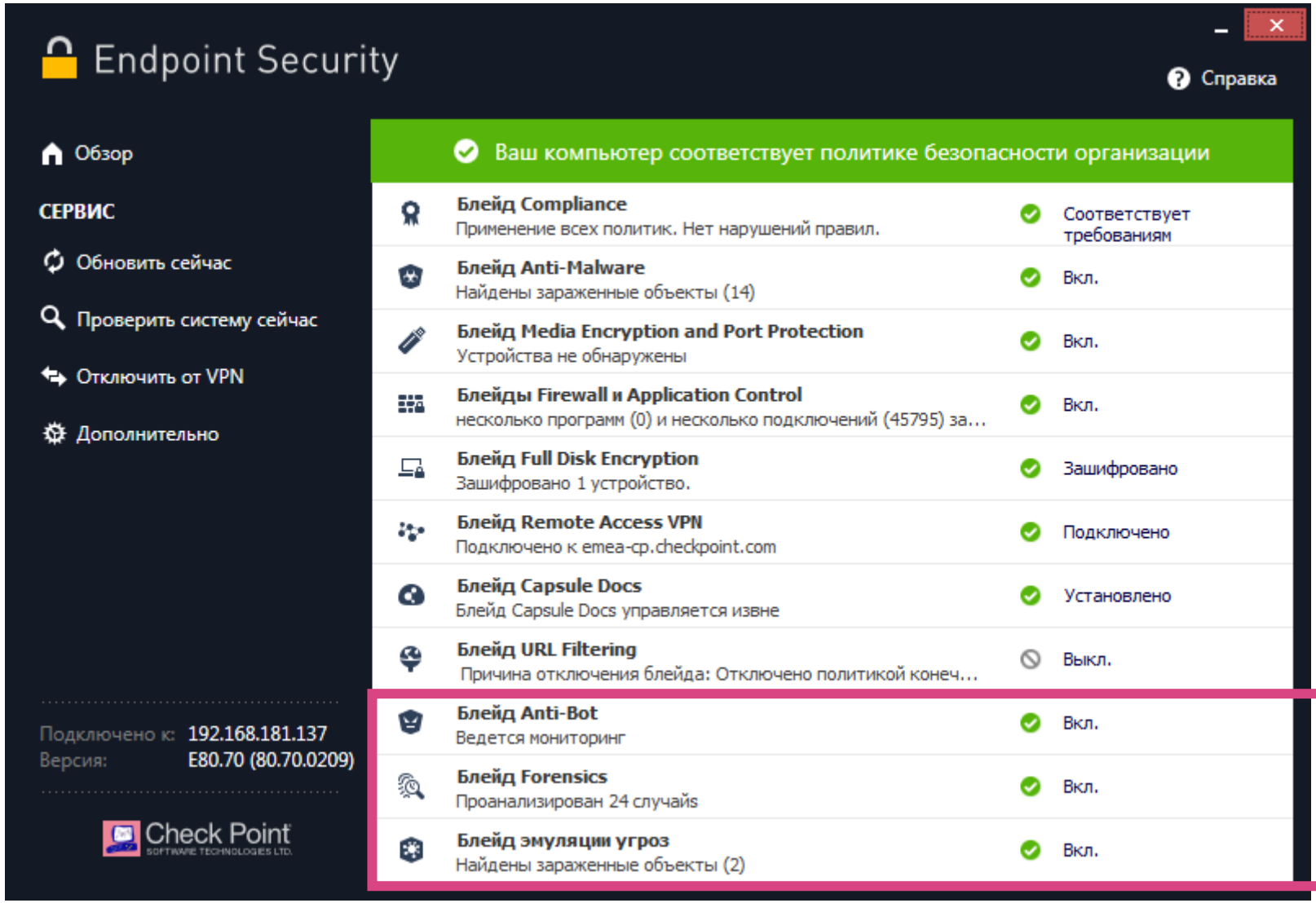
- Эмуляция для веб, почты и др. на одном устройстве
- Режим «Hold» для **предотвращения** в веб
- Режим MTA для **предотвращения** в почте
- Отказоустойчивость
- Расследование, лечение

Sandblast Threat Extraction

Доставка гарантированно безопасных документов и изображений



Защита конечных точек от Check Point

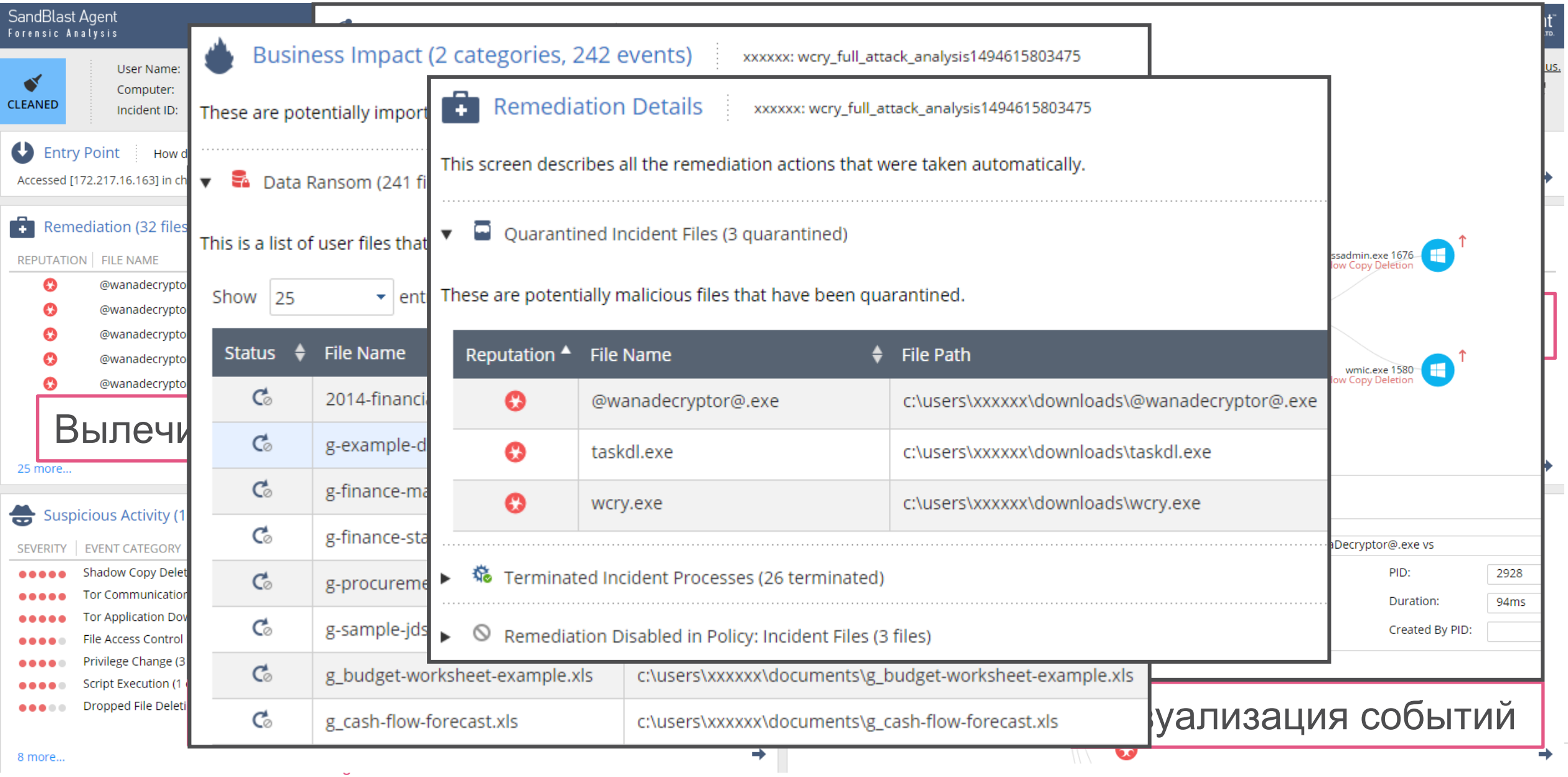


- Универсальный агент
- Модульная архитектура
- Замена AV или
- Совместимость и интеграция с AV
- Защита от APT

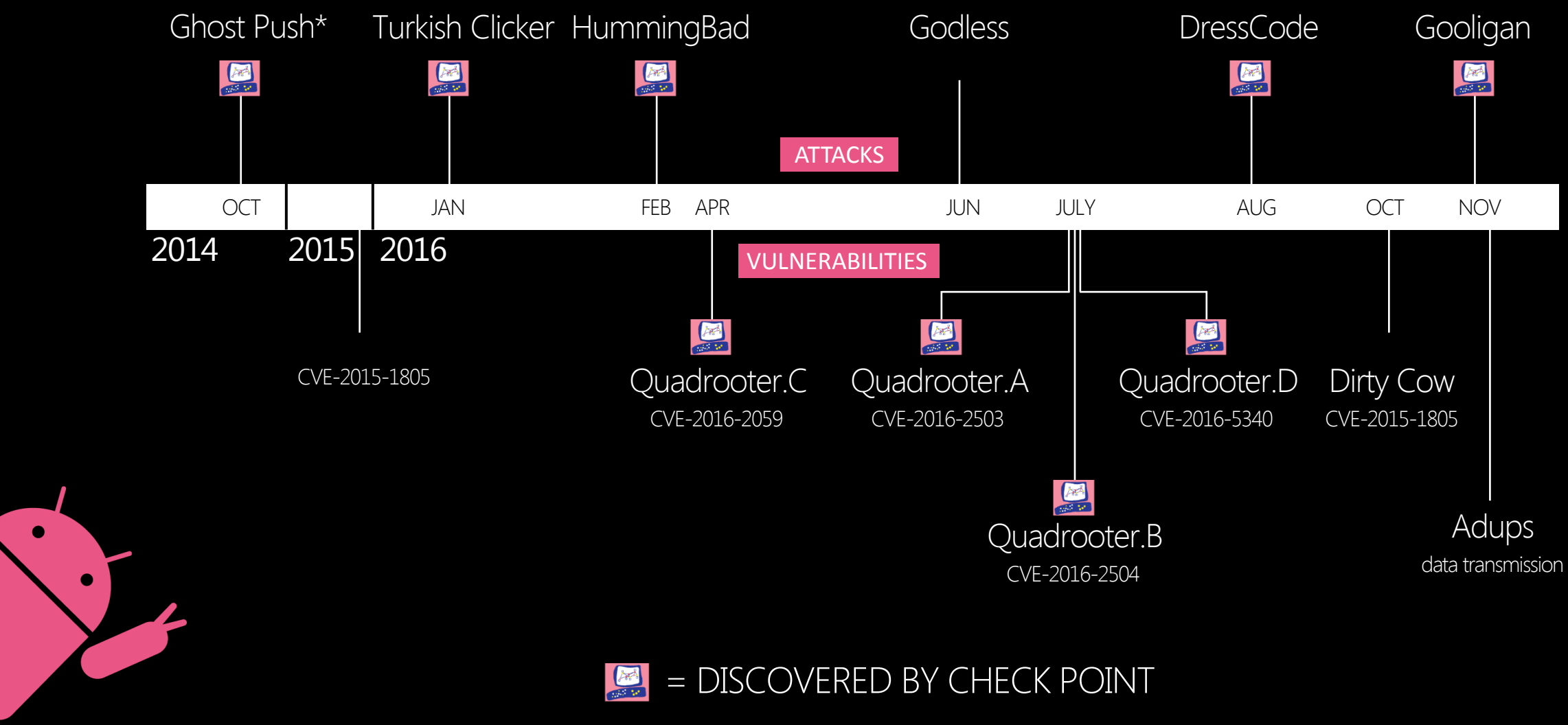
Check Point SandBlast AGENT


Recycle Bin
My Files
Wanna.xls
Cloud Folders
Google Chrome
My Files
My Files
Search My F...
Organize
Open
Share with
Accounts
Chrysanthemum
Desert
Family 2017
Finanace summary Dec 2016
Finanace summary Feb 2016
Hydrangeas
Jellyfish
Koala
Lighthouse
Maid with the Flaxen Hair
Payments
Penguins
private insurance
sceret password
Sleep Away
Sleep Away.rar
temp
Tomson
Tulips
This PC is protected by SandBlast Anti-Ransomware
Start
2:46 AM
5/15/2017

Песочница, AV, AB, AR, IoC → Отчет Forensics



GOOGLE ANDROID SECURITY 2016 REPORT:
CHECK POINT ПЕРВЫМ ОБНАРУЖИЛ 70% НОВЫХ УГРОЗ

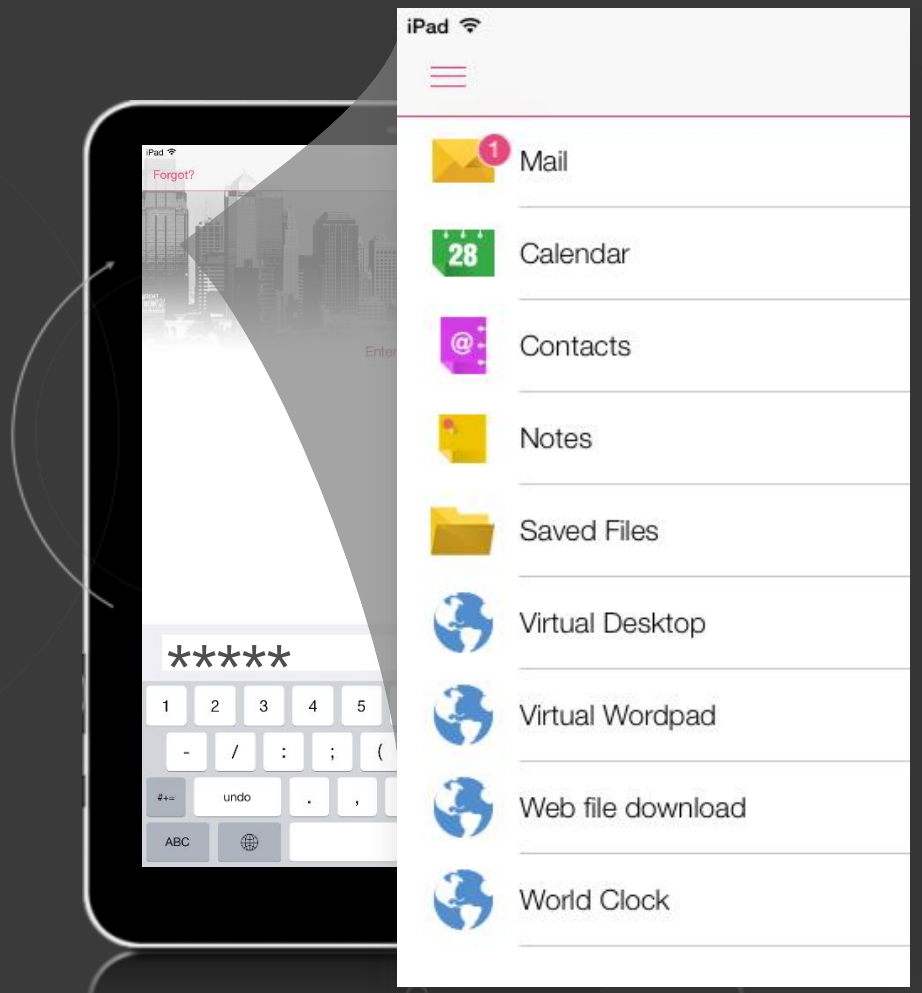


= DISCOVERED BY CHECK POINT

*Partially Check Point : BrainTest, Sept 2015

Source: Google Android Security 2016 Year In Review

Check Point Capsule: защищенная бизнес-среда



ЗАЩИЩЕННЫЙ вход (PIN, Touch-ID)

ПРОСТОЙ ДОСТУП
к опубликованным бизнес приложениям

ПЕРЕДАЙТЕ под IT контроль
ТОЛЬКО бизнес информацию (BYOD)

Корпоративные данные защищены **В Е З Д Е**

Miercom RATED BEST

Тест 2017:
100%

Check Point SOFTWARE TECHNOLOGIES LTD.

Check Point SOFTWARE TECHNOLOGIES LTD.

SandBlast Mobile

ПОВЕДЕНЧЕСКИЙ АНАЛИЗ УГРОЗ

ЗАЩИТА ОТ SMS-ФИШИНГА (ПРОВЕРКА ССЫЛОК)

СТАТИЧЕСКИЙ И ДИНАМИЧЕСКИЙ АНАЛИЗ В ПЕСОЧНИЦЕ ДЛЯ ВЫЯВЛЕНИЯ ИЗВЕСТНЫХ И НЕИЗВЕСТНЫХ УГРОЗ

ANDROID APP ON Google play

Available on the iPhone App Store

СЕТЕВАЯ ЗАЩИТА, MITM, SS7

ЗАЩИТА ОТ УЯЗВИМОСТЕЙ НА УРОВНЕ УСТРОЙСТВА (ОС)

airwatch

MaaS360

MobileIron

Good

http://blog.checkpoint.com/2017/02/09/smishing-threat-unraveling-details-attack/

http://pages.checkpoint.com/miercom-report-on-sandblast-mobile.html