JETSECURITY
CONFERENCE 2018

IX ЕЖЕГОДНАЯ КОНФЕРЕНЦИЯ ЦЕНТРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

БОЛЬШЕ ЧЕМ БЕЗОПАСНОСТЬ

31 мая, 2018
Radisson Resort, Zavidovo

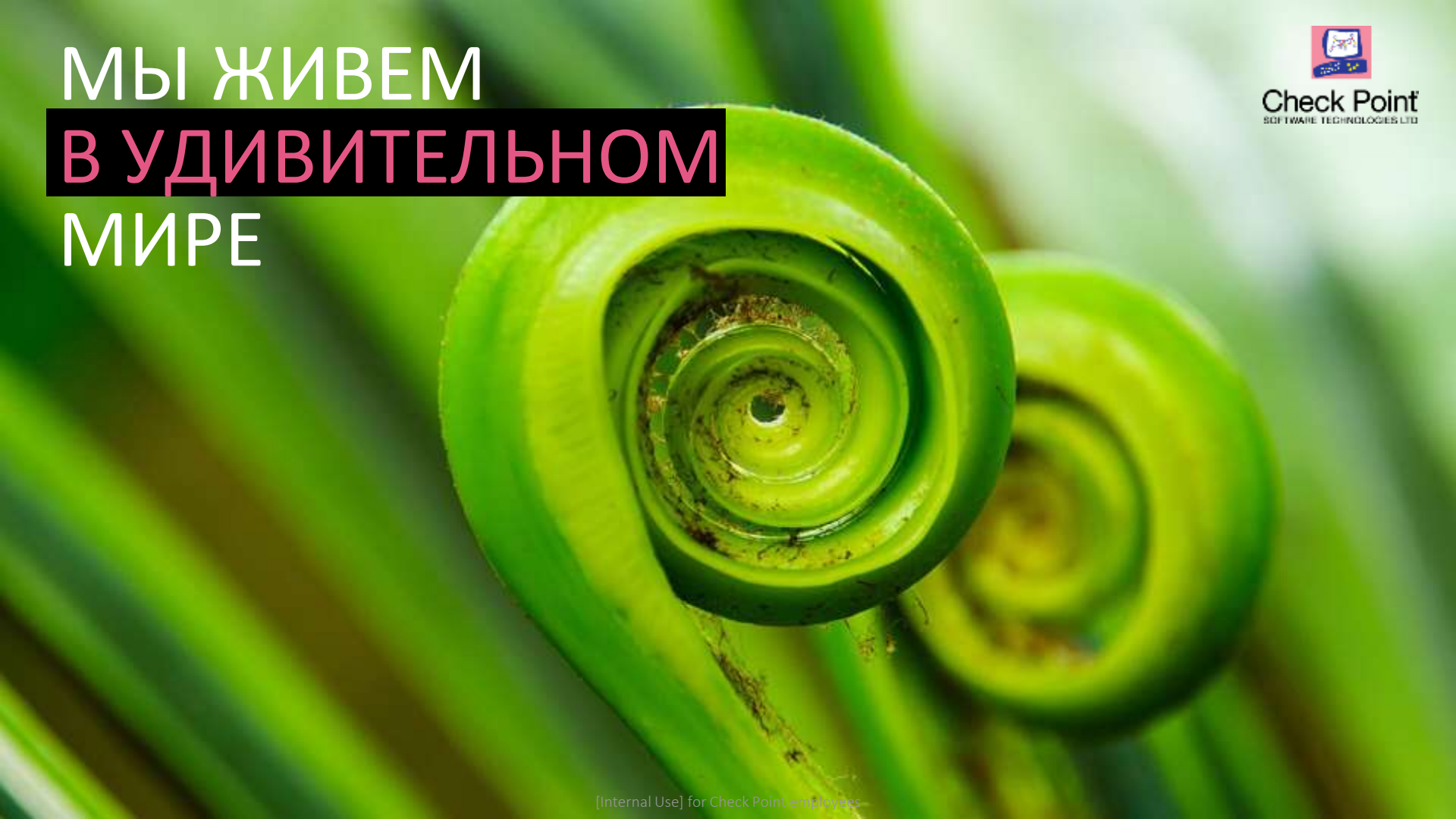
JETSECURITY
CONFERENCE 2018

Check Point:

Революция угроз 5-ого поколения.

Василий Дягилев
Генеральный Директор
Check Point Россия и СНГ

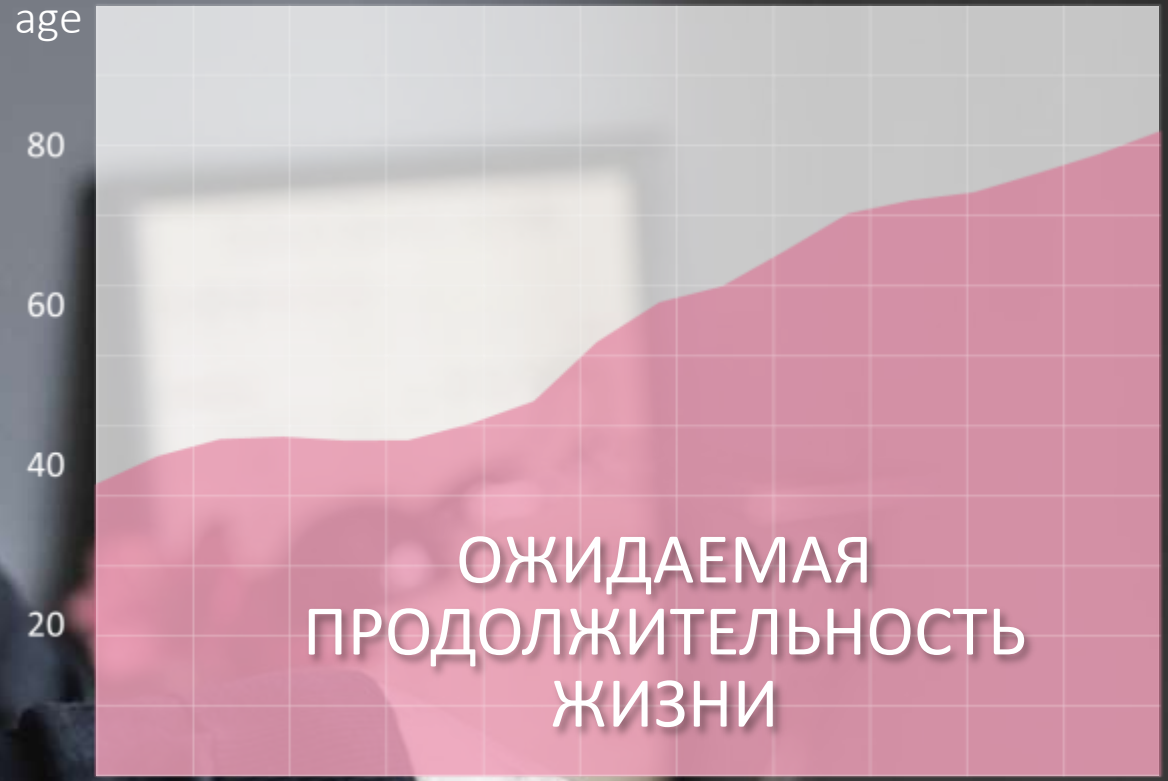
МЫ ЖИВЕМ В УДИВИТЕЛЬНОМ МИРЕ



Check Point
SOFTWARE TECHNOLOGIES LTD

Check Point
SOFTWARE TECHNOLOGIES LTD

МЫ ЖИВЕМ ДОЛЬШЕ



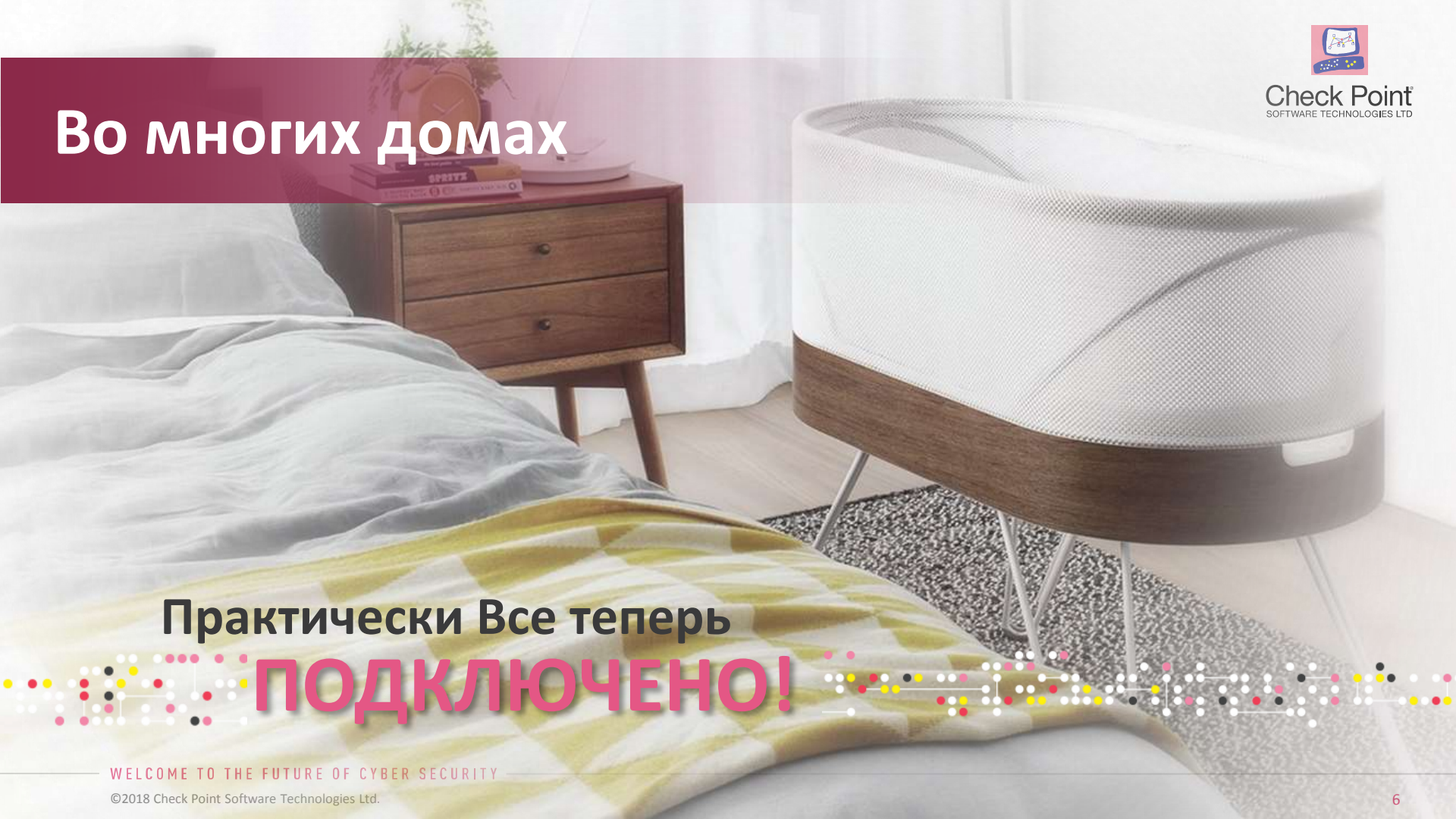
Source: ourworldindata.org

УСЛОВИЯ ЖИЗНИ СТАНОВЯТСЯ ЛУЧШЕ

Check Point
SOFTWARE TECHNOLOGIES LTD

Source: ourworldindata.org

Во многих домах



Практически Все теперь

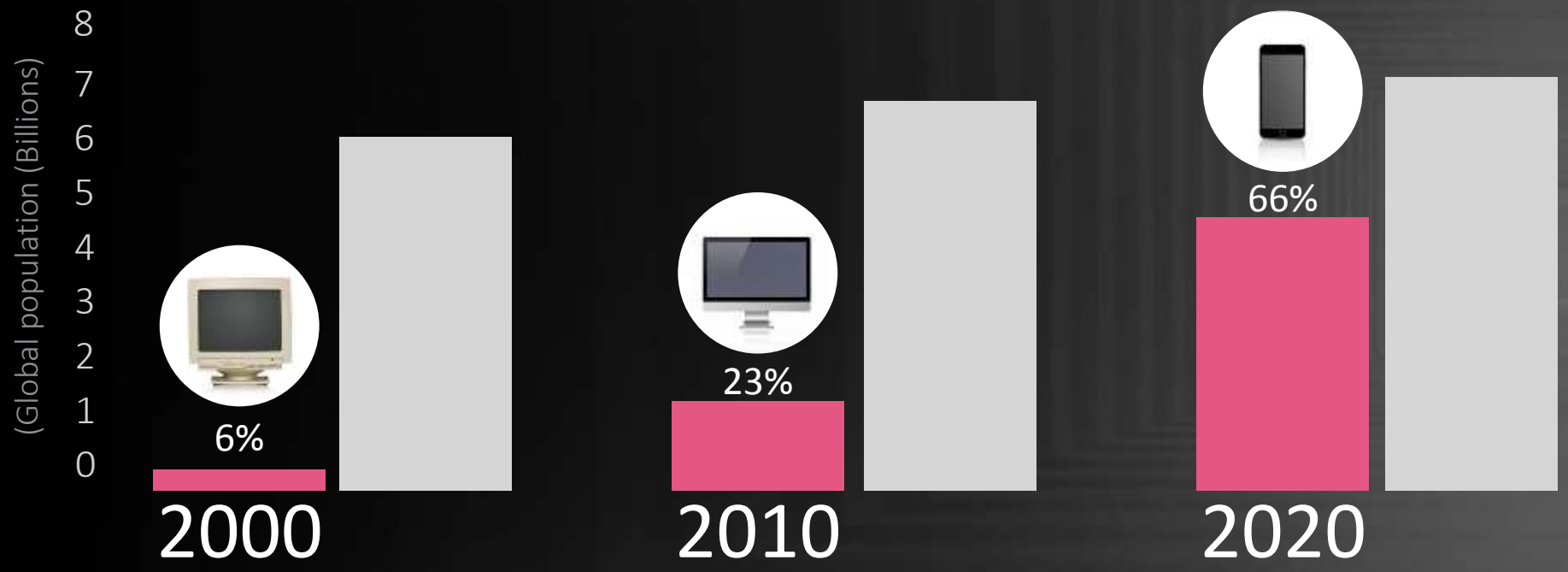
ПОДКЛЮЧЕНО!

Дроны провожают детей в школу

В ПОДКЛЮЧЕННОМ МИРЕ УЖЕ ЖИВЕТ 5 МИЛЛИАРДОВ НОВЫХ УМОВ

Check Point
SOFTWARE TECHNOLOGIES LTD

% Мирового населения подключенных к INTERNET



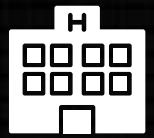
Источник: PHD Ventures, Inc.

СОВЕРШЕННО НОВЫЕ БИЗНЕС МОДЕЛИ

Check Point
SOFTWARE TECHNOLOGIES LTD

UBER

#1 Taxi компания в мире, у которой нет ни одного автомобиля



airbnb

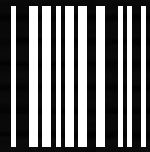
#1 Ресурс по аренде жилья, которые не владает ни 1 М2 площади

facebook

#1 В мире медиа провайдер, который не производит самостоятельного контента

NETFLIX

#1 быстро растущий телеканал, не имеющий стандартной сети вещяния



Alibaba.com

#1 Ритейлер в мире, не имеющий собственных складов и магазинов

АВТОНОМНЫЕ МАШИНЫ

TESLA, Яндекс, GOOGLE.
Cognitive Technologies

3D ПЕЧАТЬ ЕДЫ


Check Point
SOFTWARE TECHNOLOGIES LTD
НОВЫЕ
ВОЗМОЖНОСТИ

Эра ВЕЩЕЙ

новые возможности...

Как для хороших людей...

Так и для плохих...

А ЧТО ПРОИСХОДИТ В КИБЕР - БЕЗОПАСНОСТИ?

СТАЛ ЛИ 2017 ГОД ПЕРЕЛОМНЫМ ?

Check Point
SOFTWARE TECHNOLOGIES LTD

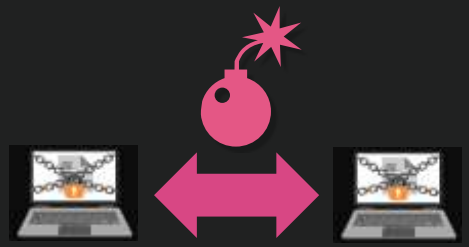
WannaCry

Тысячи предприятий в 99 странах

NotPetya

Полностью отключил целую Страну и поразил еще 60

ТРЕНДЫ КИБЕР-УГРОЗ ВТОРОЙ ПОЛОВИНЫ 2017



Горизонтальное распространение через эксплойты:
1) WannaCry, NotPetya, BadRabbit
2) IoT: IoTroop*, роутеры Huawei
3) Банковский троян TrickBot

Массивные DDoS атаки с IoT:
1) IoTroop* (использование кода Mirai)
2) Роутеры Huawei
3) Мобильные устройства на Android (Wirex)

Мобильные вредоносы открывают доступ в корпоративные сети:
1) Прокси (MilkyDoor)
2) Взлом роутеров на периметре

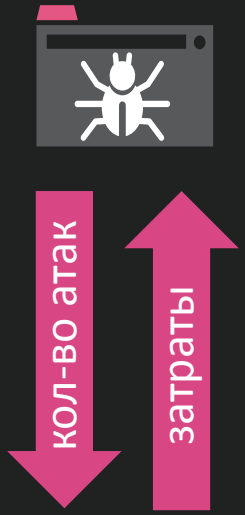
*Китайский ботнет из множества устройств: GoAhead, D-Link, TP-Link, AVTECH, NETGEAR, MikroTik, Linksys, Synology, ...

https://pages.checkpoint.com/global-cyber-attack-trends-2017

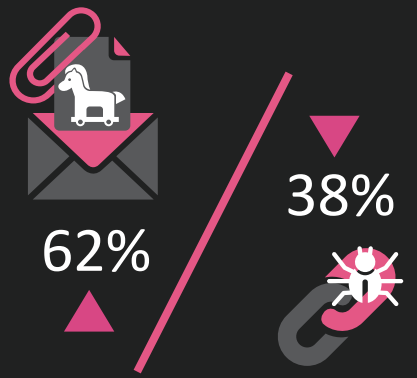
ТРЕНДЫ КИБЕР-УГРОЗ ВТОРОЙ ПОЛОВИНЫ 2017

в 20.5%
компаний

Криптомайнеры
+ онлайн на веб-сайтах
(Coin-Hive, Crypto Loot)



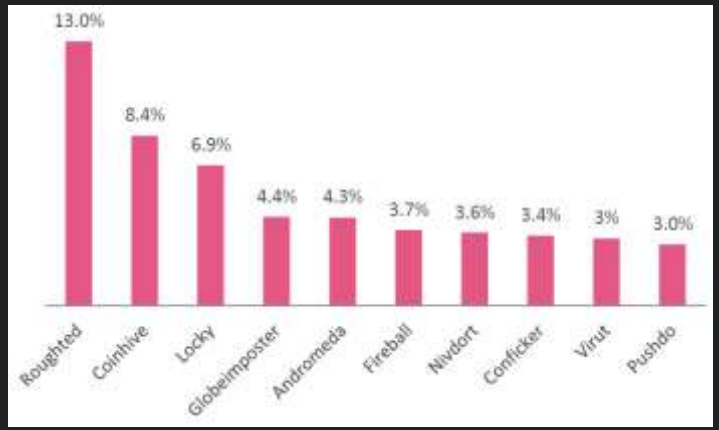
Exploit Kits
(Nuclear, Angler)



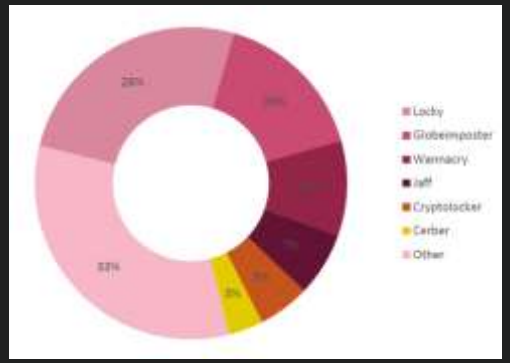
Целевой фишинг с
вредоносными
документами
Adobe, MS Office
(RTF, DDE, NEW: .xlam, .xlb)

https://pages.checkpoint.com/global-cyber-attack-trends-2017

ТРЕНДЫ КИБЕР-УГРОЗ ВТОРОЙ ПОЛОВИНЫ 2017



Наиболее активные вредоносы в РФ и СНГ

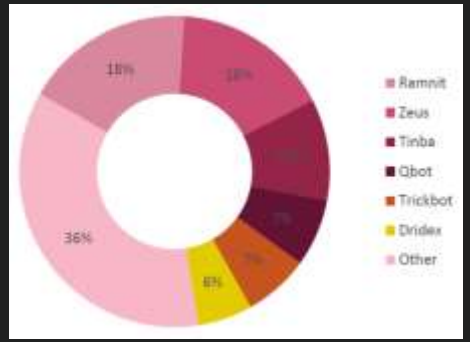


Топ шифровальщиков в РФ и СНГ

RoughTed – вредоносная реклама (malvertising)
CoinHive, Crypto Loot – онлайн криптомайнеры
TrickBot – банковский троян, использующий для распространения эксплойты SMB

Ожидания на 2018:

- Атаки на блокчейн (CryptoShuffler – криптовор)
- Атаки на облака (Microsoft +300%, Amazon, Google)
- Кросс-платформенные атаки (Windows, Mac OS X, Android)



Топ банковских троянов в РФ и СНГ

https://pages.checkpoint.com/global-cyber-attack-trends-2017

СТАЛ ЛИ 2017 ПЕРЕЛОМНЫМ?

WORLD ECONOMIC FORUM

Check Point
SOFTWARE TECHNOLOGIES LTD

Top 5 Global Risks in Terms of Likelihood

	2016	2017	2018
1st	Large-scale involuntary migration	Extreme weather events	Extreme weather events
2nd	Extreme weather events	Large-scale involuntary migration	Natural disasters
3rd	Failure of climate-change mitigation and adaptation	Major natural disasters	Cyberattacks
4th	Interstate conflict with regional consequences	Large-scale terrorist attacks	Data fraud or theft
5th	Major natural catastrophes	Massive incident of data fraud/theft	Failure of climate-change mitigation and adaptation

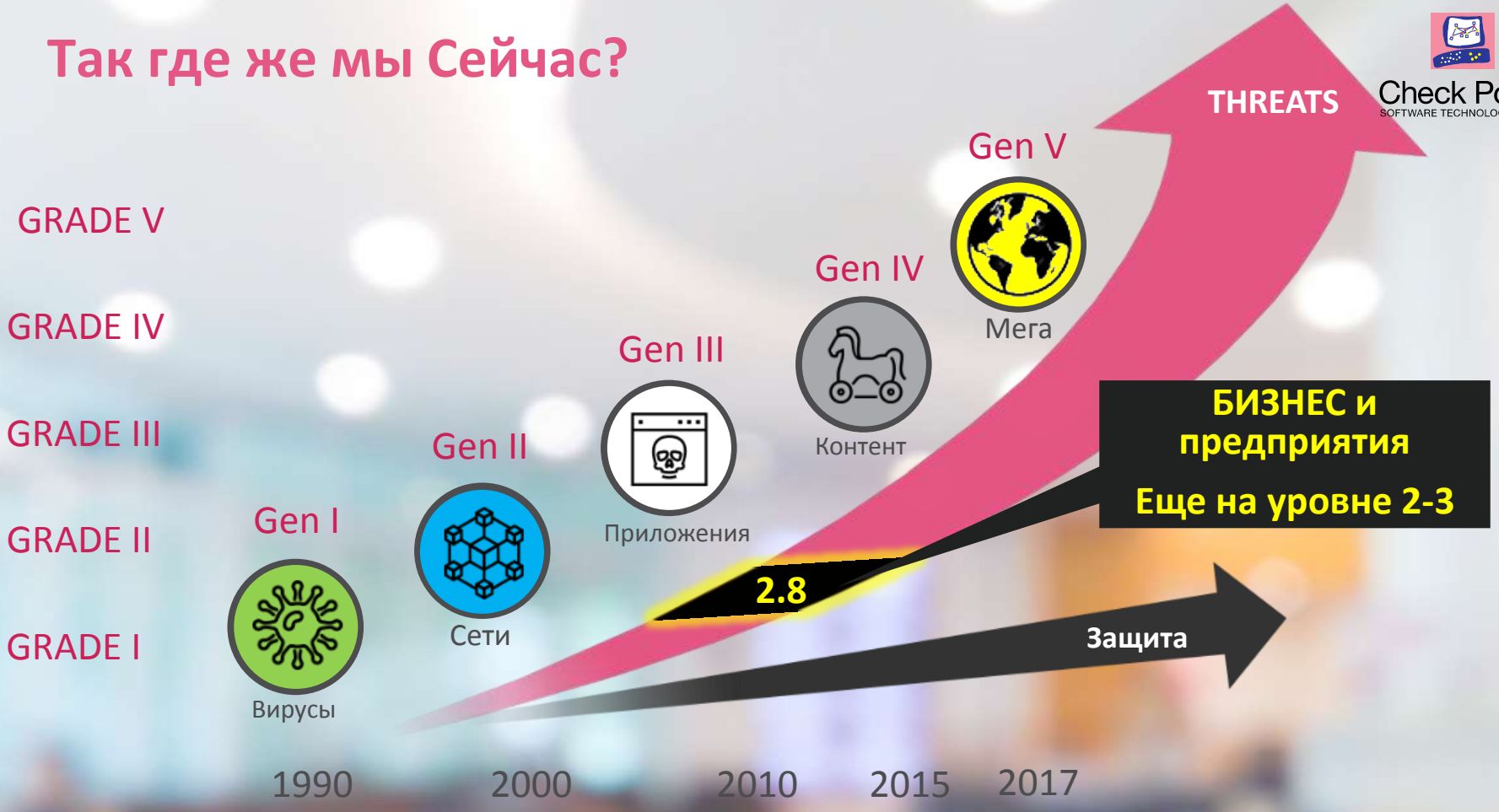
Сегодня – Переломный момент!
Мы достигли пятого поколения Угроз!

Check Point
SOFTWARE TECHNOLOGIES LTD

ДАВАЙТЕ ПОСМОТРИМ ЧТО ЭТО ЗНАЧИТ **В РЕАЛЬНОСТИ!**

Поколения Кибер Угроз и решения по защите

Так где же мы Сейчас?



2018- Год АТАК 5-ого ПОКОЛЕНИЯ GEN5

Крупный масштаб (Страна\индустрия)

Мульти- Вектор (Сеть,Облако,Мобильность)

Технологии Гос Уровня

Уже сейчас защита уровня 4 поколения не всегда достаточна!

Check Point
SOFTWARE TECHNOLOGIES LTD

Gen IV

Контент

ПРЕДОТВРАЩЕНИЕ (НЕ ДЕТЕКТ!!!!)

Работа в реальном Времени!

Закрытие всех векторов Сети, Мобильность, Облака

МЫ ОБЯЗАНЫ ДВИГАТЬСЯ ВПЕРЕД БЫСТРЕЕ!

НО ЧТО МЫ ВИДИМ?


“Со мной это не случится”
“Это очень дорого”
“Внедрение Каждой технологии это 6 месяцев
20 Техноло ну где-то к
“Это слишком сложно”

Вам нужна Армия технологий

Check Point
SOFTWARE TECHNOLOGIES LTD

Вам Нужна Армия Технологий

КАЖЕТСЯ НЕВОЗМОЖНЫМ?

Check Point
SOFTWARE TECHNOLOGIES LTD

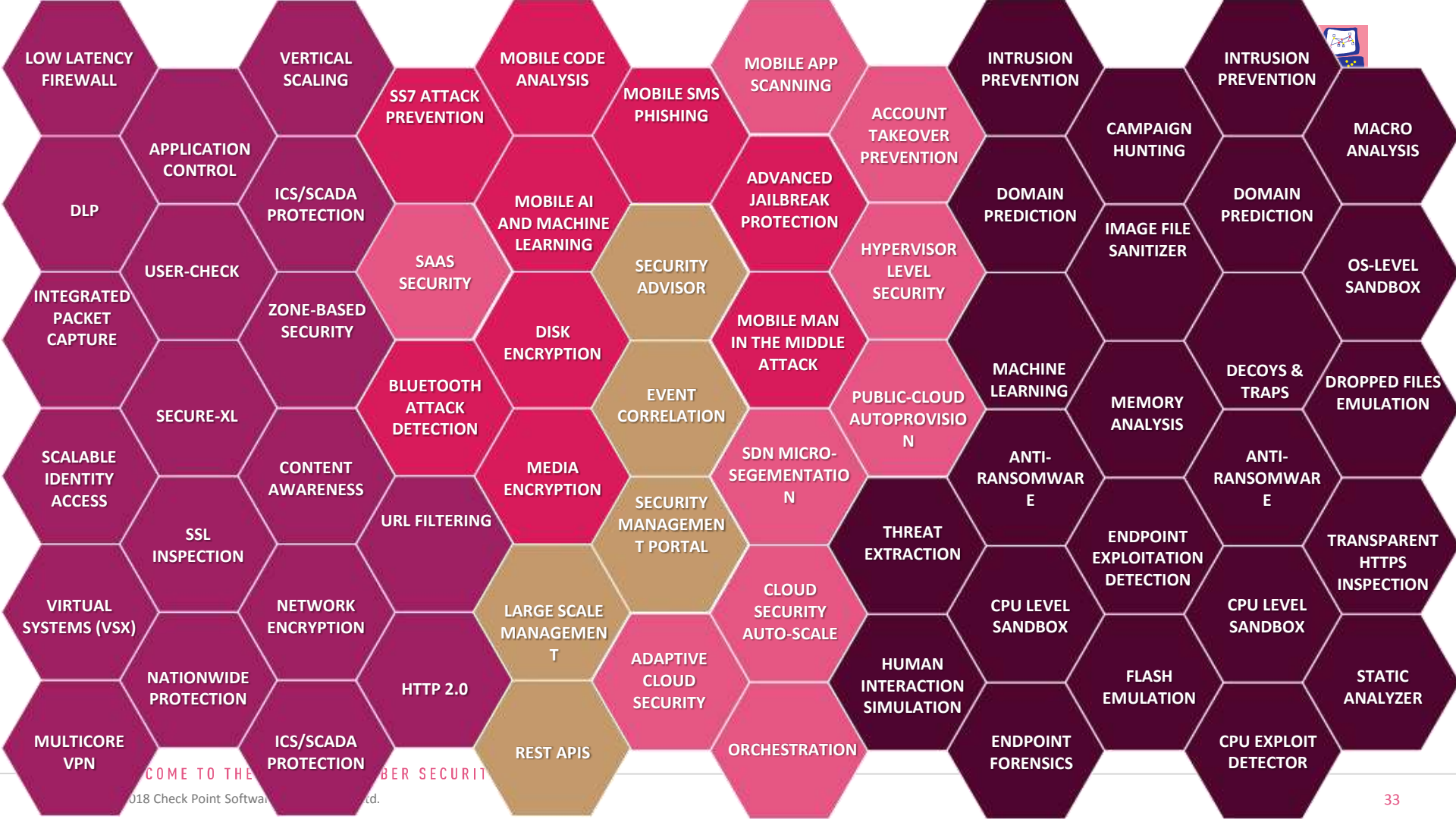
НЕВОЗМОЖНОЕ

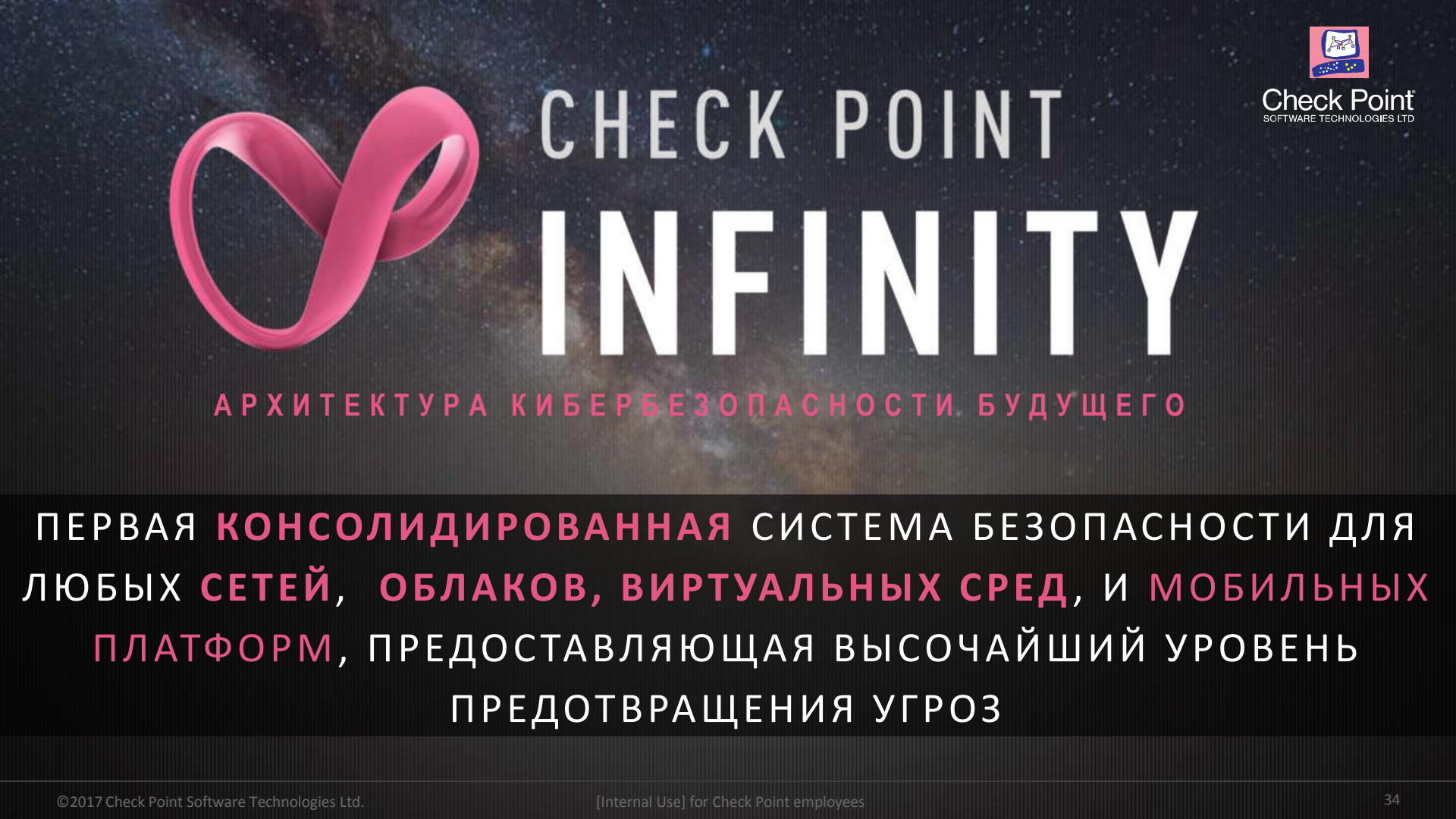
МЫ ДЕЛАЕМ МГНОВЕННО

ЧУДЕСА ЗАНИМАЮТ ЧУТЬ БОЛЬШЕ ВРЕМЕНИ

.

(Charles Alexandre de Calonne, 1794)

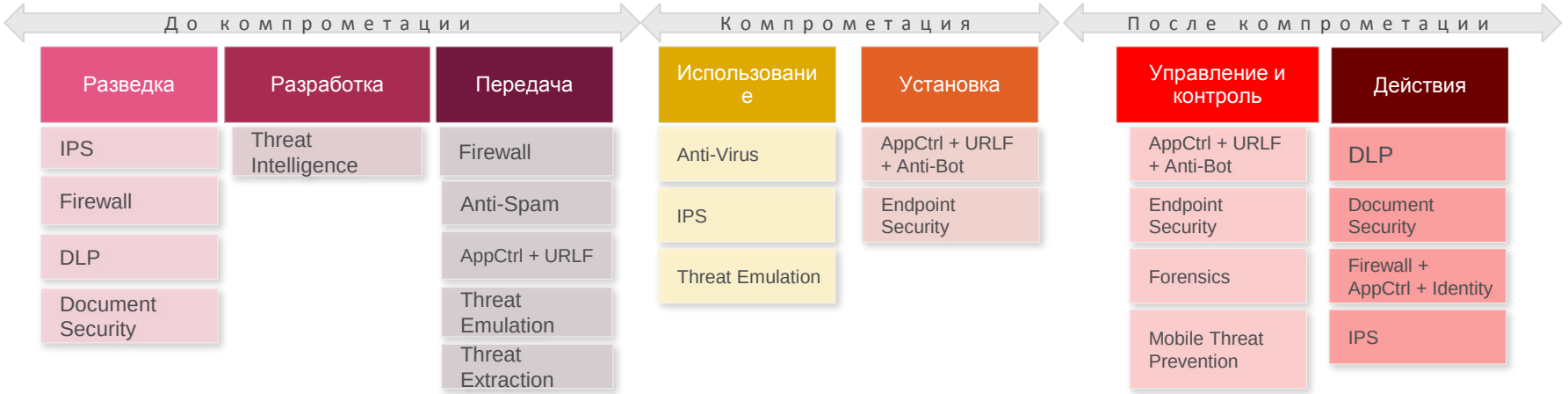

LOW LATENCY FIREWALL
VERTICAL SCALING
SS7 ATTACK PREVENTION
MOBILE CODE ANALYSIS
MOBILE SMS PHISHING
MOBILE APP SCANNING
INTRUSION PREVENTION
INTRUSION PREVENTION
APPLICATION CONTROL
ACCOUNT TAKEOVER PREVENTION
CAMPAIGN HUNTING
MACRO ANALYSIS
DLP
ICS/SCADA PROTECTION
MOBILE AI AND MACHINE LEARNING
ADVANCED JAILBREAK PROTECTION
DOMAIN PREDICTION
DOMAIN PREDICTION
IMAGE FILE SANITIZER
USER-CHECK
SAAS SECURITY
SECURITY ADVISOR
HYPERVISOR LEVEL SECURITY
OS-LEVEL SANDBOX
INTEGRATED PACKET CAPTURE
ZONE-BASED SECURITY
DISK ENCRYPTION
MOBILE MAN IN THE MIDDLE ATTACK
MACHINE LEARNING
DECOYS & TRAPS
MEMORY ANALYSIS
DROPPED FILES EMULATION
SECURE-XL
BLUETOOTH ATTACK DETECTION
EVENT CORRELATION
PUBLIC-CLOUD AUTOPROVISIO N
SCALABLE IDENTITY ACCESS
CONTENT AWARENESS
MEDIA ENCRYPTION
SDN MICRO-SEGEMENTATIO N
ANTI-RANSOMWAR E
ANTI-RANSOMWAR E
SSL INSPECTION
URL FILTERING
SECURITY MANAGEMEN T PORTAL
THREAT EXTRACTION
ENDPOINT EXPLOITATION DETECTION
TRANSPARENT HTTPS INSPECTION
VIRTUAL SYSTEMS (VSX)
NETWORK ENCRYPTION
LARGE SCALE MANAGEMEN T
CLOUD SECURITY AUTO-SCALE
CPU LEVEL SANDBOX
CPU LEVEL SANDBOX
NATIONWIDE PROTECTION
HTTP 2.0
ADAPTIVE CLOUD SECURITY
HUMAN INTERACTION SIMULATION
FLASH EMULATION
STATIC ANALYZER
MULTICORE VPN
ICS/SCADA PROTECTION
REST APIS
ORCHESTRATION
ENDPOINT FORENSICS
CPU EXPLOIT DETECTOR



Решение основных Задач:

Защита сети	▪ Защита периметра и региональных офисов ▪ Защита от DDoS ▪ Сегментация и защита ЦОД ▪ Защита систем виртуализации на уровне гипервизора
Объединение сетей	▪ Организация масштабных VPN-сетей с использованием отечественных алгоритмов шифрования ГОСТ ▪ Организация защищенного удаленного доступа
Рабочие станции и мобильные устройства	▪ Создание защищенной среды для работы с корпоративной информацией на смартфонах ▪ Комплексная защита рабочих станций ▪ Идентификация и контроль приложений ▪ Защищенная работа с документами
Управление	▪ Единая консоль для всей инфраструктуры ИБ ▪ Построение отчетов о событиях в режиме реального времени
Неизвестные атаки	▪ Защита от таргетных атак и угроз «нулевого» дня ▪ Защита от многовекторных атак в обслуживании (DDoS-атак)

УСПЕШНАЯ СТРАТЕГИЯ ЗАЩИТЫ
на всех этапах атаки для каждого вектора



Предотвращение ИЗВЕСТНЫХ атак

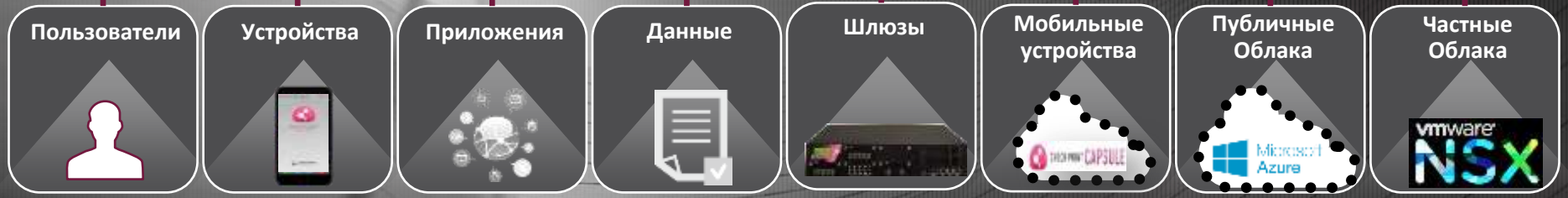
Применение защиты на основе сигнатур на каждом шаге для быстрого блокирования вторжений

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	Azure VMWare



Что мы предлагаем в 2018 ?

CHECK POINT

GEN V

РАЗНЫЕ МОДЕЛИ ПОТРЕБЛЕНИЯ

СОФТ,ЖЕЛЕЛЕЗО, СЕРВИСЫ , ВСЕ ВКЛЮЧЕНО

НОВЫЕ ПЛАТФОРМЫ

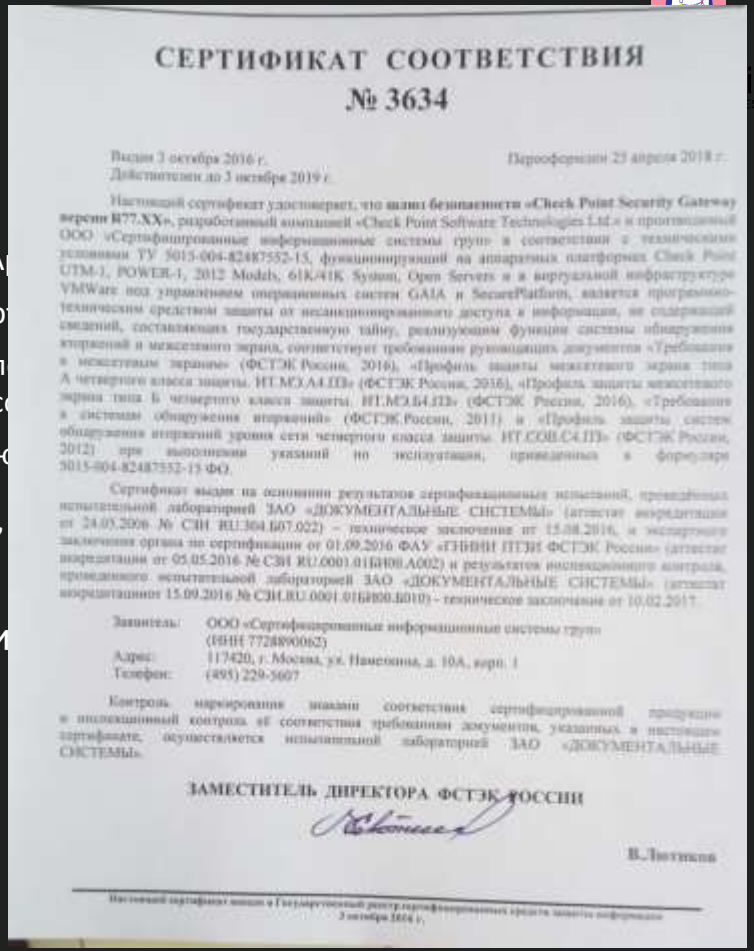
POWERING THE 5TH GENERATION OF CYBER SECURITY

CHECK POINT *CLOUDGUARD*

ПРЕВЕНТИВНАЯ ЗАЩИТА ОБЛАКОВ И SAAS APPS

Кто мы в России и СНГ

- Крупнейший вендор сетевой безопасности в России
- Офис -42 человека +3 в 2018
  - Из них 28 инженеров включая локальный Professional Services, А
  - Полный доступ к ресурсам HQ – как по сервисам так и по саппорт
  - Сертификация ФСТЭК шлюзов и end point (ИТ.МЭ.А4/Б4.ПЗ - 10 л
    (Корректность встраивания Крипто Про 4.0) – в процессе (Согласс
  - Локальное производство железа (Made in Russia) по запросу с ию
- Отсутствие Санкционных (поименных, финансовых,
  ограничений на поставки, поддержку, обучение.
- Локальные программы сотрудничества и интеграци
  - Крипто Про –ГОСТ VPN
  - Лаборатория Касперского (Антивирусный движок)
  - Infowatch – DLP интеграция с шлюзами безопасности
  - Positive Tech. – Интеграция с WAF
  - Attack Killer – Интеграция с WAF в процессе
  - Возможна интеграция по запросу на проектном уровне



СЕРТИФИКАТ СООТВЕТСТВИЯ

№ 3634

Выдан 3 октября 2016 г. Переоформлен 25 апреля 2018 г.
Действителен до 3 октября 2019 г.

Настоящий сертификат удостоверяет, что **шлюз безопасности «Check Point Security Gateway версии R77.XX»**, разработанный компанией «Check Point Software Technologies Ltd.» и производимый ООО «Сертифицированные информационные системы груп» в соответствии с техническими условиями ТУ 5015-004-82487552-15, функционирующий на аппаратных платформах Check Point UTM-1, POWER-1, 2012 Models, 61K/41K System, Open Servers и в виртуальной инфраструктуре VMWare под управлением операционных систем GAIA и SecurePlatform, является программно-техническим средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, реализующим функции системы обнаружения вторжений и межсетевого экрана, соответствует требованиям руководящих документов «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевого экрана типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016), «Профиль защиты межсетевого экрана типа Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011) и «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012) при выполнении указаний по эксплуатации, приведенных в формуляре 5015-004-82487552-15 ФО.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ЗАО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ» (аттестат аккредитации от 24.05.2006 № СЗИ RU.304.Б07.022) – техническое заключение от 15.08.2016, и экспертного заключения органа по сертификации от 01.09.2016 ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002) и результатов инспекционного контроля, проведенного испытательной лабораторией ЗАО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ» (аттестат аккредитации 15.09.2016 № СЗИ.RU.0001.01БИ00.Б010) - техническое заключение от 10.02.2017.

Заявитель: ООО «Сертифицированные информационные системы груп»
(ИНН 7728890062)
Адрес: 117420, г. Москва, ул. Наметкина, д. 10А, корп. 1
Телефон: (495) 229-5607

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям документов, указанных в настоящем сертификате, осуществляется испытательной лабораторией ЗАО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 3 октября 2016 г.

ПОМНИТЕ: СЛЕДУЮЩУЮ АТАКУ МОЖНО ПРЕДОТВРАТИТЬ!

ПОМНИТЕ:
ЕСТЬ ВЕНДОР КОТОРЫЙ ПОМОЖЕТ ЭТО СДЕЛАТЬ!

Check Point
SOFTWARE TECHNOLOGIES LTD

ВОПРОСЫ?

Василий Дягилев
Генеральный директор
Check Point Россия и СНГ
vasilyd@checkpoint.com

WELCOME TO THE FUTURE OF
CYBER SECURITY
POWERED BY CHECK POINT INFINITY
CLOUD • MOBILE • THREAT PREVENTION

JETSECURITY
CONFERENCE 2018

Спасибо за внимание!

БОЛЬШЕ ЧЕМ БЕЗОПАСНОСТЬ