Check Point
SOFTWARE TECHNOLOGIES LTD

РЕАЛЬНАЯ ЗАЩИТА
ОБЪЕКТОВ КИИ
В РЕАЛЬНЫХ УСЛОВИЯХ
ВТОРОЙ ПОЛОВИНЫ

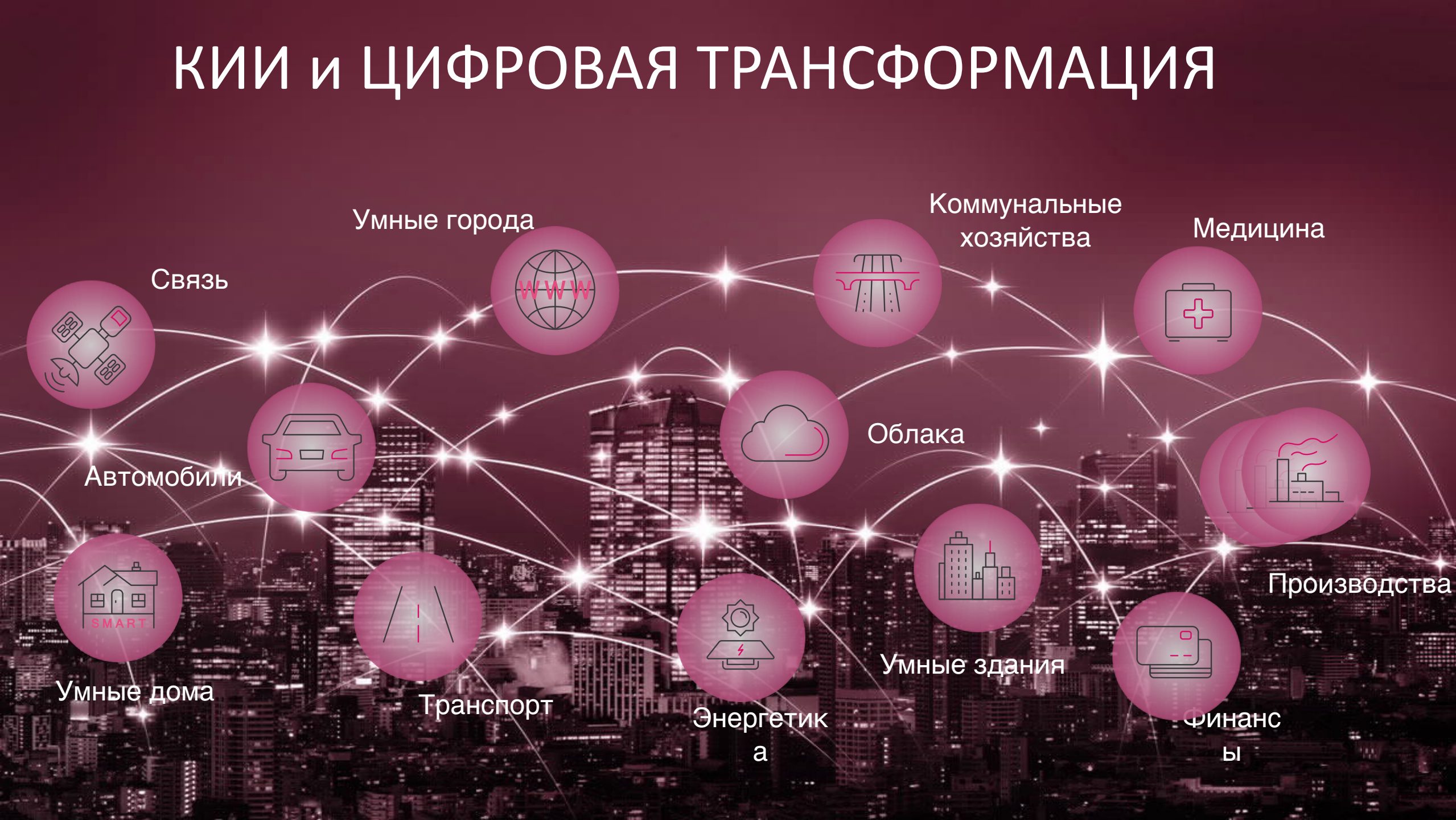
Взгляд Check Point

Василий Широков | заместитель генерального директора Check Point (Russia), к.т.н.

Check Point
SOFTWARE TECHNOLOGIES LTD

КИИ И ЦИФРОВАЯ ТРАНСФОРМАЦИЯ. АКТУАЛЬНЫЕ ЗАДАЧИ

КИИ и ЦИФРОВАЯ ТРАНСФОРМАЦИЯ



ВЫХОД ЗА ПЕРИМЕТР - УСКОРЕНИЕ ЦИФРОВИЗАЦИИ

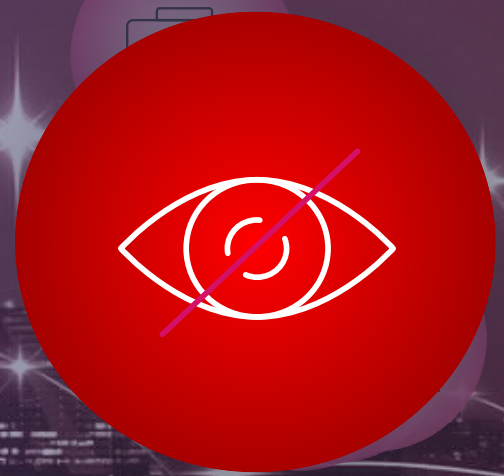
Имея за спиной два «виртуальных квартала», мы теперь можем видеть, что кибербезопасность на самом деле является одним из наиболее важных факторов, благодаря которым мир работает в эти трудные времена.

Невозможно представить, как мир справился бы с пандемией без Интернета, и очень легко представить, что могло бы случиться, если бы Интернет был небезопасен.

КИИ и ЦИФРОВАЯ ТРАНСФОРМАЦИЯ

НЕТ ПЕРИМЕТРА

НОВЫЕ ВЕКТОРЫ АТАК



NO VISIBILITY

БЕСКОНТРОЛЬНОСТЬ

Связь

Умные города

Коммунальные хозяйства

Медицина

Авто

Облака

Производства

Умные дома

Транспорт

Энергетика

Умные здания

Финансы

Реальность такова, что ...

Значимыми объектами КИИ являются практически все системообразующие предприятия и организации страны (и их отнюдь не простые информационные системы, уже вставшие на путь цифровизации)

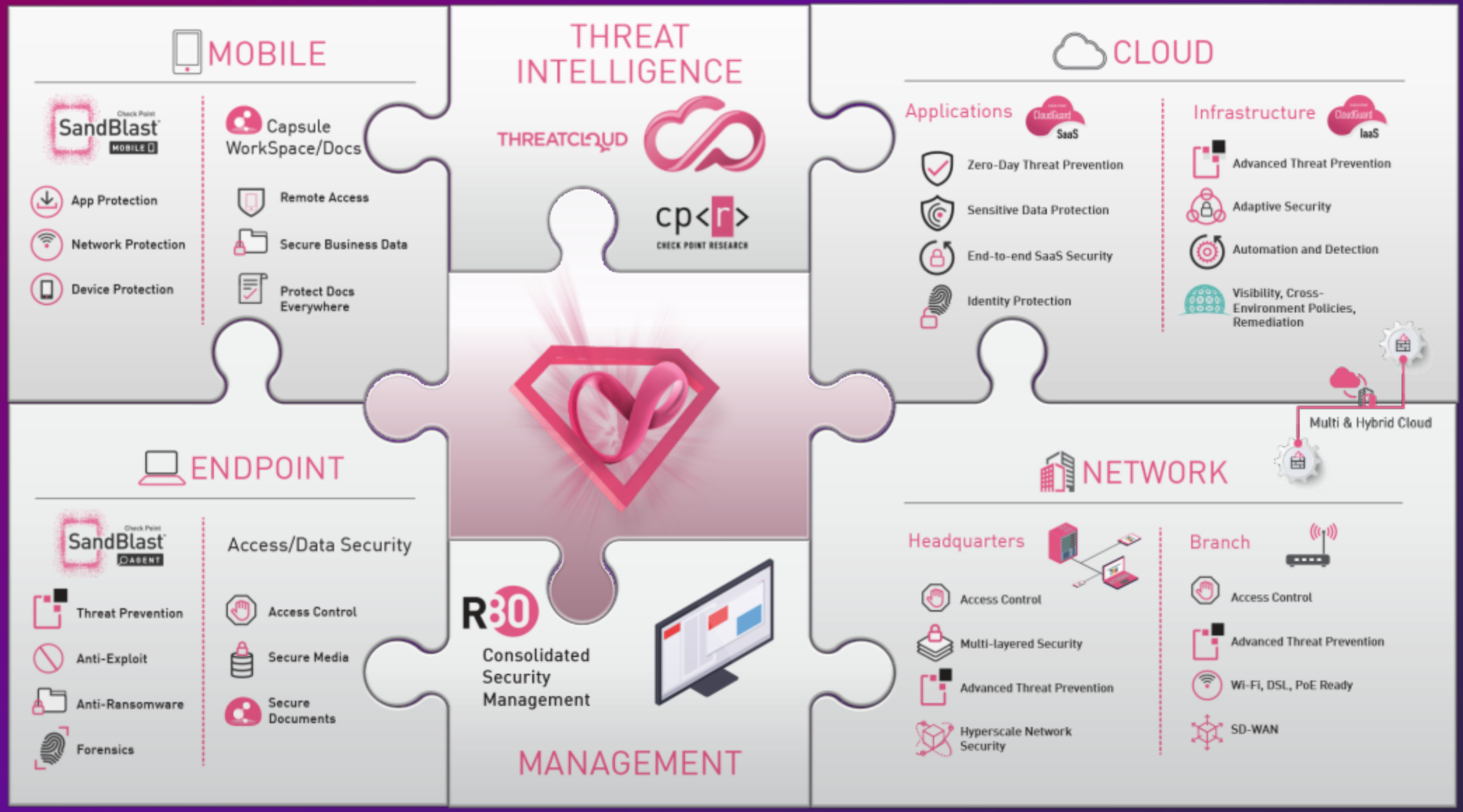
Появились новые векторы атак, связанных с угрозами "нулевого дня", возрос уровень "хактивизма", активизировались кибервойны, ведущиеся крупными компаниями и правительствами

Сложившаяся в мире непростая ситуация потребовала еще более активного перехода к облачным платформам, мобильности и выходу за пределы традиционного периметра безопасности

Реальность такова, что ...

Это со всей очевидностью требует радикального изменения подходов к обеспечению информационной безопасности, совершенствования ее технологий, механизмов и процессов.

АРХИТЕКТУРА БЕЗОПАСНОСТИ



Использование технологий Threat Emulation («песочница») и Threat Extraction (мгновенная «чистая» копия файлов).

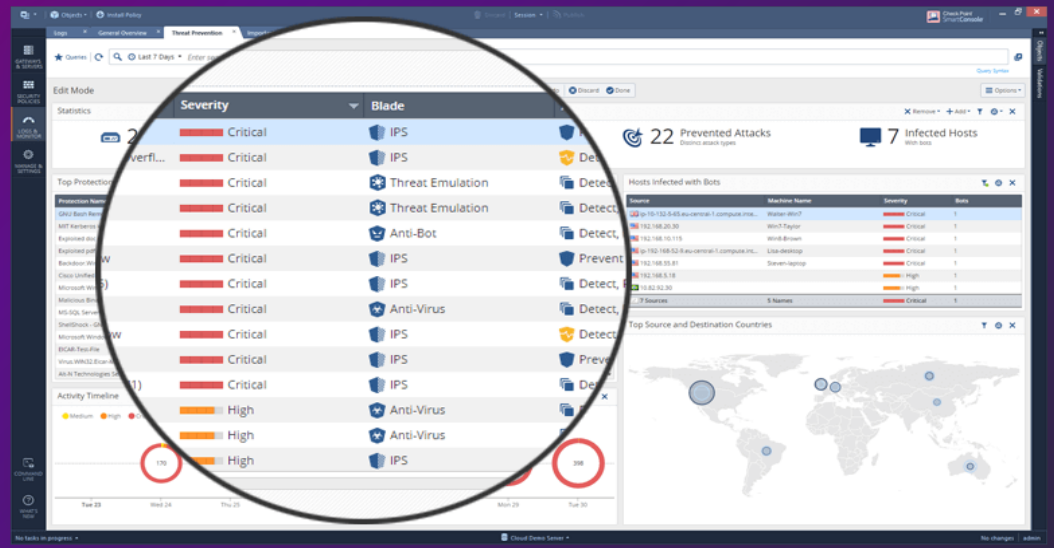
Threat Emulation - набор технологий для обнаружения угроз. Многостадийный анализ, исследование поведения, машинное обучение, работа на уровне ЦПУ = высокая надежность и производительность, постоянная защита от новых видов угроз

Threat Extraction - позволяет мгновенно предоставить пользователю безопасную копию подозрительного документа, пока производится его анализ. При этом SandBlast не «тормозит» бизнес-процессы

- Унифицированная политика безопасности с использованием процедур анализа угроз (threat intelligence) в реальном времени, для сетей, филиалов, мобильных устройств, облаков, сетей IoT

- Интеллектуальная маршрутизация трафика для любого типа устройства, включая [бес] клиентское, [не] управляемое ПО и мобильные устройства

- Принцип Zero Touch для мгновенного развертывания [политики] безопасности филиалов, интегрированный с сервисами SD-WAN



Единая политика безопасности включая IoT

Check Point IoT Protect

Prevent · Adapt · Everywhere

Smart Office IoT

Source	Destination	Service & Application
CAM	IS	VIF protocol

Medical Devices

Source	Destination	Service & Application
RI	CS	OM protocol

OT

Source	Destination	Service & Application
MI	C	odbus protocol - read input register odbus protocol - read holding registers odbus protocol - write multiple coils Modbus protocol - write multiple registers

Камеры

ONVIF Protocol → VMS

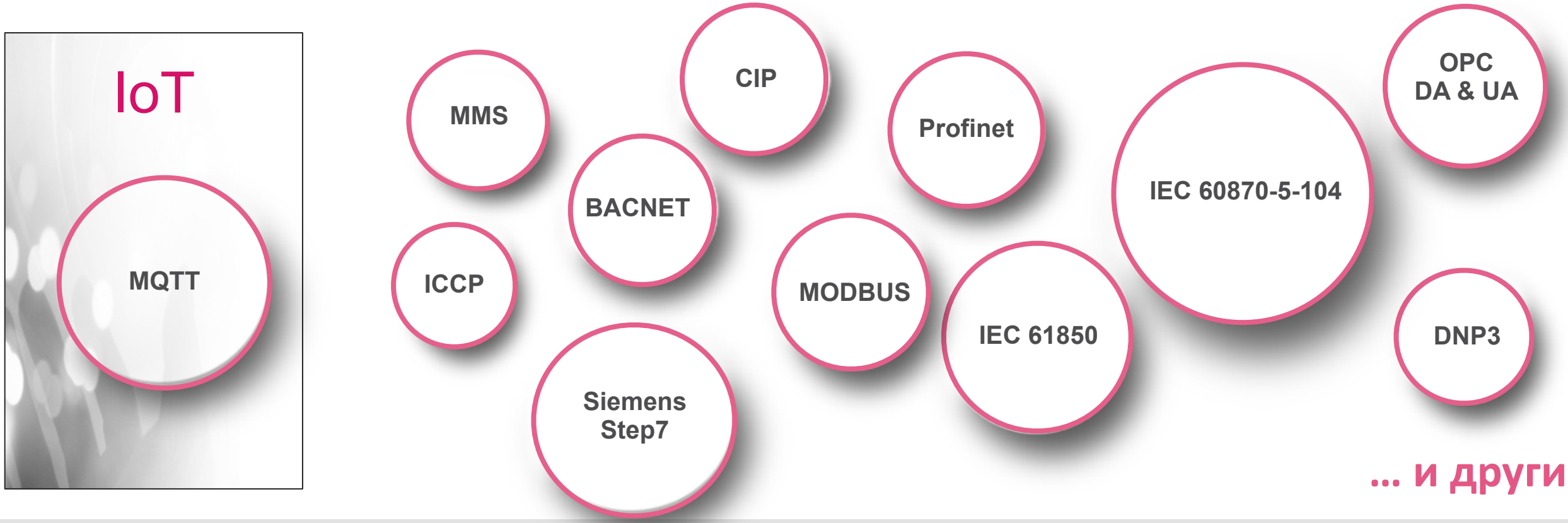
MPT

DICOM Protocol → PACS

SCADA Server/HMI

Modbus Protocol → PLC

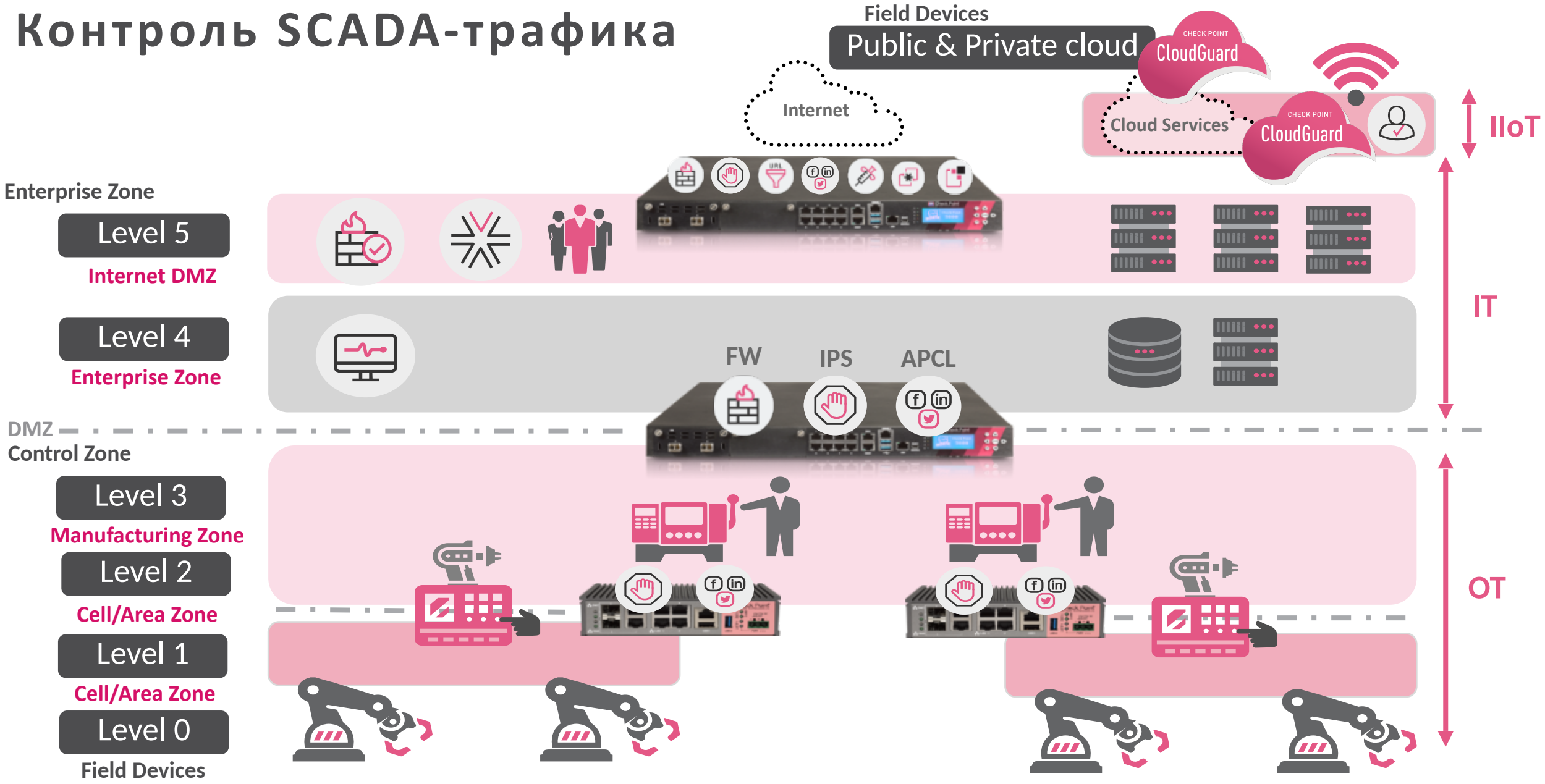
Поддержка протоколов IoT



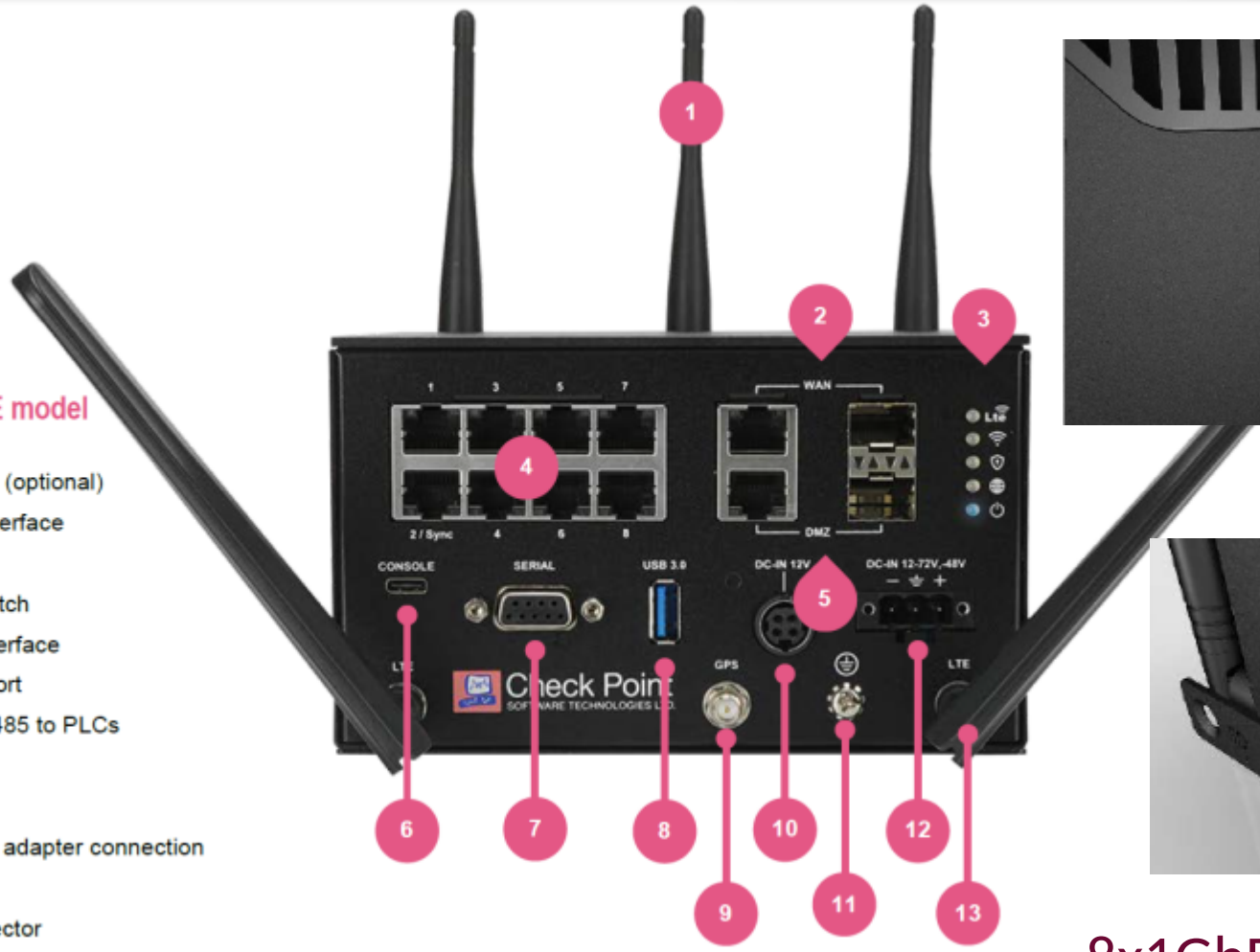
Более 1500 SCADA и IoT команд в Check Point Application Control

Полный перечень: https://appwiki.checkpoint.com

Контроль SCADA-трафика



Check Point 1570R



1570R Wi-Fi, LTE model

1. 802.11 n/ac Wi-Fi (optional)
2. 1x 1GbE WAN interface
3. LED tower
4. 8x 1GbE LAN switch
5. 1x 1GbE DMZ interface
6. USB-C console port
7. DB9 RS232/422/485 to PLCs
8. USB 3.0 port
9. GPS connector
10. AC to DC power adapter connection
11. Ground screw
12. DC power connector
13. Embedded LTE modem (optional)

400 Mbps Threat Prevention

8x1GbE ports

Dual band 802.11ac 3X3 MIMO

Check Point
SOFTWARE TECHNOLOGIES LTD

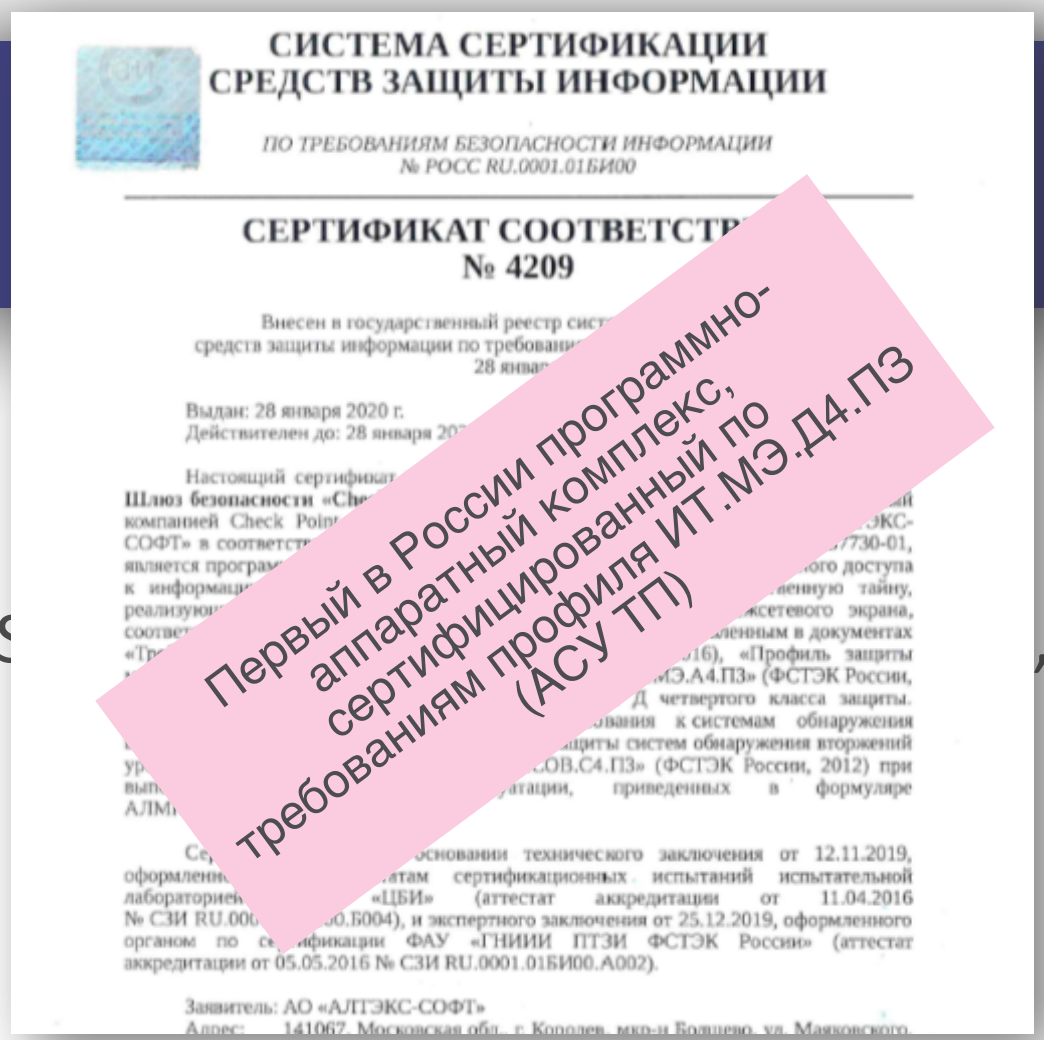
ЗАЩИТА КИИ. РЕГУЛИРОВАНИЕ В РОССИИ

Форма оценки соответствия СЗИ для ЗО КИИ

Сертификация	В случаях, установленных законодательством Российской Федерации, а также в случае принятия решения субъектом критической информационной инфраструктуры
Испытания или приемка (**)	В иных случаях. Проводятся субъектами КИИ самостоятельно или с привлечением организаций, имеющих лицензии на деятельность в области защиты информации в соответствии с 184-ФЗ "О техническом регулировании"

**) Не встроенные в общесистемное и прикладное программное обеспечение СЗИ, оценка соответствия которых проводится в форме испытаний или приемки, дополнительно к указанным требованиям должны соответствовать 6 или более высокому УД.

Государственный реестр сертифицированных средств защиты информации



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВ
№ 4209

Внесен в государственный реестр сист
средств защиты информации по требован
28 янва

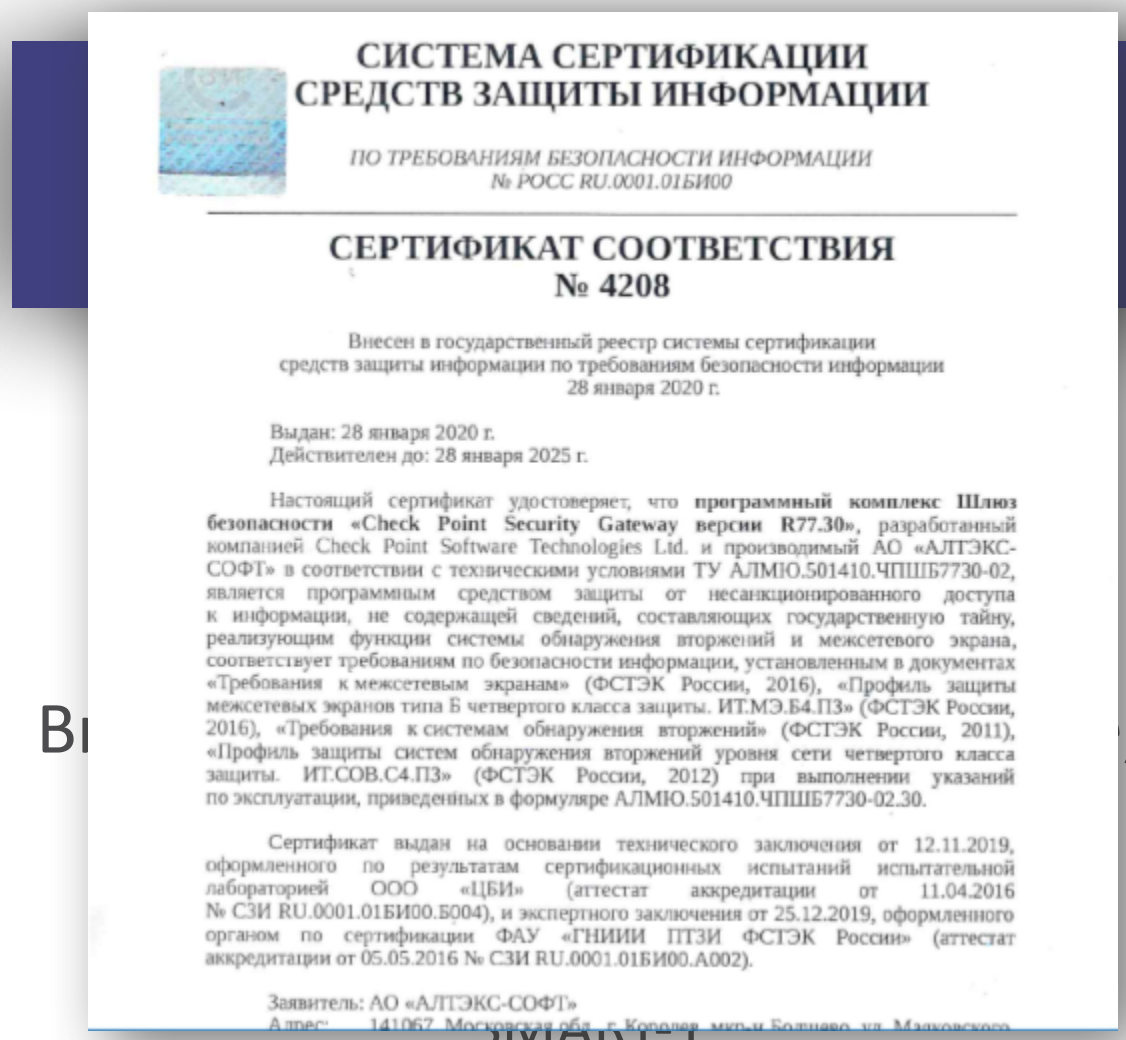
Выдан: 28 января 2020 г.
Действителен до: 28 января 20

Настоящий сертификат
Шлюз безопасности «Ch
компанией Check Poin
СОФТ» в соответств
является програм
к информаци
реализующ
соответ
«Тр
«Профиль защиты
МЭ.А4.ПЗ» (ФСТЭК России,
Д четвертого класса защиты.
вания к системам обнаружения
щиты систем обнаружения вторжений
СОВ.С4.ПЗ» (ФСТЭК России, 2012) при
атации, приведенных в формуляре
АЛМ

Се основании технического заключения от 12.11.2019,
оформлен татам сертификационных испытаний испытательной
лаборатори «ЦБИ» (аттестат аккредитации от 11.04.2016
№ СЗИ RU.00 .Б004), и экспертного заключения от 25.12.2019, оформленного
органом по се ификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат
аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: АО «АЛТЭКС-СОФТ»
Адрес: 141067, Московская обл., г. Королев, мкр-н Болшево, ул. Маяковского,

Первый в России программно-аппаратный комплекс, сертифицированный по требованиям профиля ИТ.МЭ.Д4.ПЗ (АСУ ТП)



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4208

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
28 января 2020 г.

Выдан: 28 января 2020 г.
Действителен до: 28 января 2025 г.

Настоящий сертификат удостоверяет, что **программный комплекс Шлюз безопасности «Check Point Security Gateway версии R77.30»**, разработанный компанией Check Point Software Technologies Ltd. и производимый АО «АЛТЭКС-СОФТ» в соответствии с техническими условиями ТУ АЛМЮ.501410.ЧПШБ7730-02, является программным средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, реализующим функции системы обнаружения вторжений и межсетевого экрана, соответствует требованиям по безопасности информации, установленным в документах «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «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 АЛМЮ.501410.ЧПШБ7730-02.30.

Сертификат выдан на основании технического заключения от 12.11.2019, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.Б004), и экспертного заключения от 25.12.2019, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: АО «АЛТЭКС-СОФТ»
Адрес: 141067, Московская обл., г. Королев, мкр-н Болшево, ул. Маяковского,

Техническая поддержка СЗИ

Поддержка производителя

Применяемые СЗИ должны быть обеспечены гарантийной, технической поддержкой со стороны разработчиков (производителей).

Учет санкций

При выборе СЗИ должно учитываться возможное наличие ограничений со стороны разработчиков (производителей) или иных лиц на применение этих средств на любом из принадлежащих субъекту ЗнО КИИ.

Не допускается:

Наличие удаленного доступа и наличие локального бесконтрольного доступа в том числе к СЗИ для обновления или управления со стороны третьих лиц (включая дочерние предприятия). А также бесконтрольная передача в том числе технологической информации.

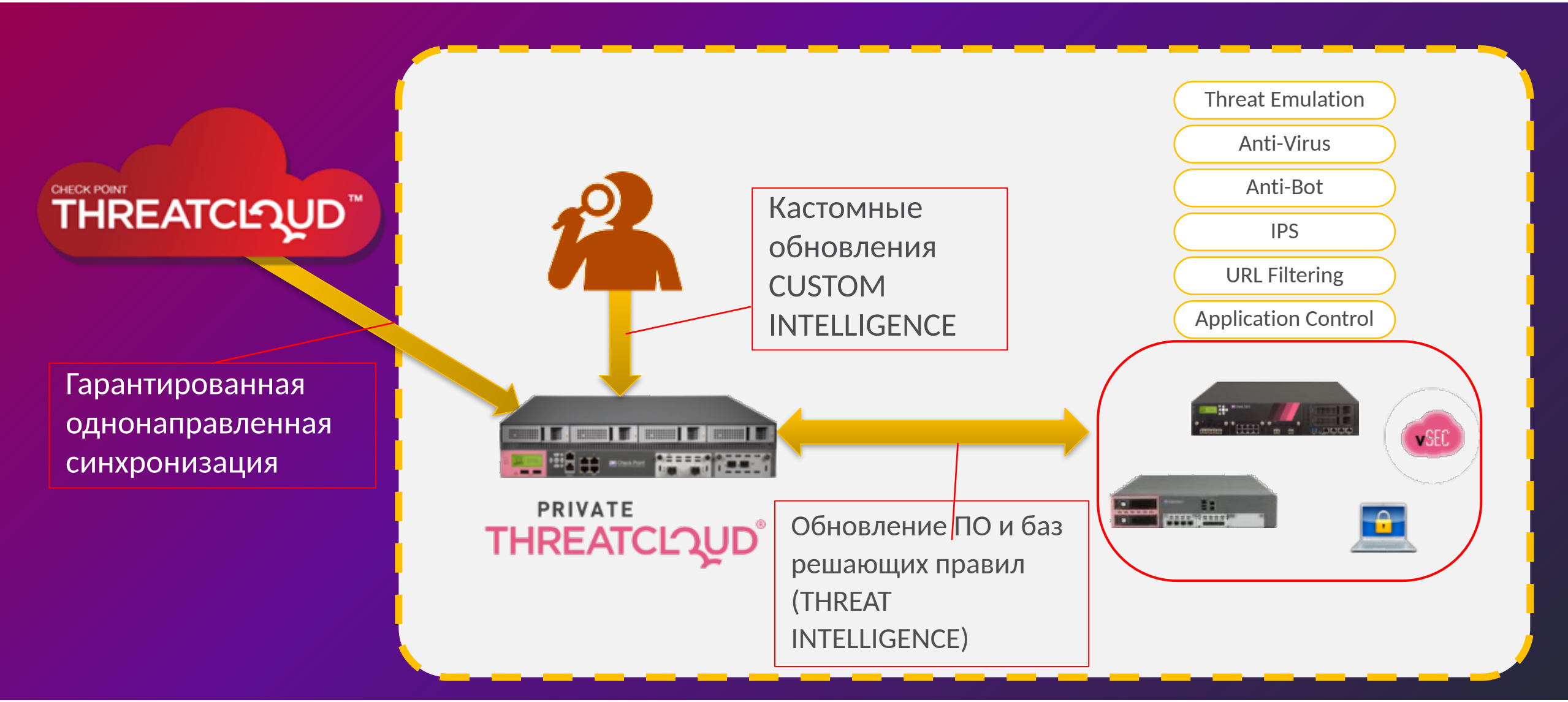
Но ..... В случае технической невозможности .....

ISOLATED NETWORKS ARE QUITE COMMON

Disconnected networks help protect critical assets from intrusion

- Government
- Finance
- ICS
- Defense
- Critical Infrastructure
- Highly regulated industries

Локальный хостинг ThreatCloud



Что насчет новых технологий безопасности?

Доп угрозы безопаснности

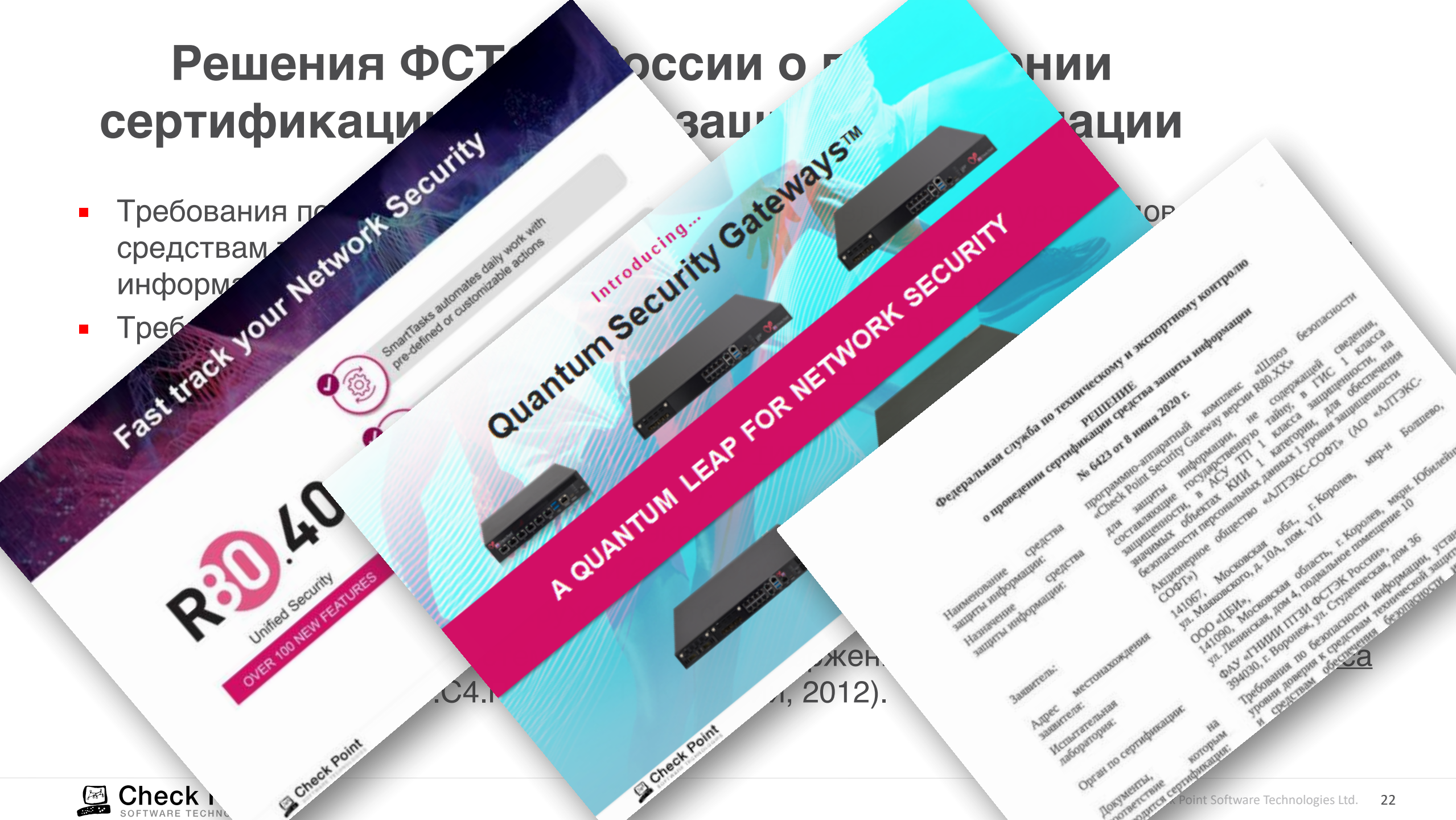
При использовании в ЗО КИИ новых информационных технологий и выявлении дополнительных угроз безопасности информации, для которых не определены меры по обеспечению безопасности, должны разрабатываться компенсирующие меры в соответствии с п. 26 Требований.

Пункт 26 Приказа 239

... должно быть обосновано применение компенсирующих мер, а при приемочных испытаниях (аттестации) оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации

Решения ФСТ[illegible]оссии о [illegible]нии сертификаци[illegible] заш[illegible]ации

- Требования по[illegible]
  средствам [illegible]
  информа[illegible]
- Треб[illegible]



Василий Широков, к.т.н.
Check Point Software Technologies (Russia)