Check Point
SOFTWARE TECHNOLOGIES LTD

СЕТЕВАЯ БЕЗОПАСНОСТЬ С РЕШЕНИЯМИ CHECK POINT

10 ФЕВРАЛЯ 2021

Sergey Zabula | Channel SE Team Lead, Check Point

szabula@checkpoint.com

О КОМПАНИИ

- Мировой лидер – 100,000+ заказчиков, 88+ стран, 6,200+ партнеров
- Опыт в индустрии ИБ – более 25 лет
- Лидер в инновациях, с наибольшим количеством разработчиков в штате
- Штаб-квартира – г. Тель-Авив (Израиль)
  НЕ ПОДДЕРЖИВАЕТ САНКЦИИ!
- 5,100+ сотрудников по всему миру
  50+ сотрудников в России

ПОРТФОЛИО РЕШЕНИЙ БЕЗОПАСНОСТИ

CLOUD

- CloudGuard Dome9 — Cloud Posture Management
- CloudGuard LOG.IC — Network Traffic Analysis
- CloudGuard Workload — Runtime Workload Protection
- CloudGuard SaaS — SaaS, Email Security
- CloudGuard IaaS — Cloud Access Control, Prevention
- CloudGuard Edge / CloudGuard Connect — Branch Threat Prevention

Multi & Hybrid Cloud

SD-WAN

NETWORK

SandBlast NETWORK

Headquarters

- Access Control
- Data Protection
- Multi Layered Security
- Advanced Threat Prevention

Branch

- Access Control
- Multi Layered Security
- Advanced Threat Prevention
- Wi-Fi, DSL, PPoE Ready

CHECK POINT INFINITY NEXT

Shared Threat Intelligence

THREATCLOUD

R80

Consolidated Security Management

MOBILE

SandBlast MOBILE

- App Protection
- Network Protection
- Device Protection

Capsule WorkSpace/Docs

- Remote Access
- Secure Business Data
- Protect Docs Everywhere

INTERNET of THINGS

Risk Analysis, Auto Segmentation, Threat Prevention

ENDPOINT

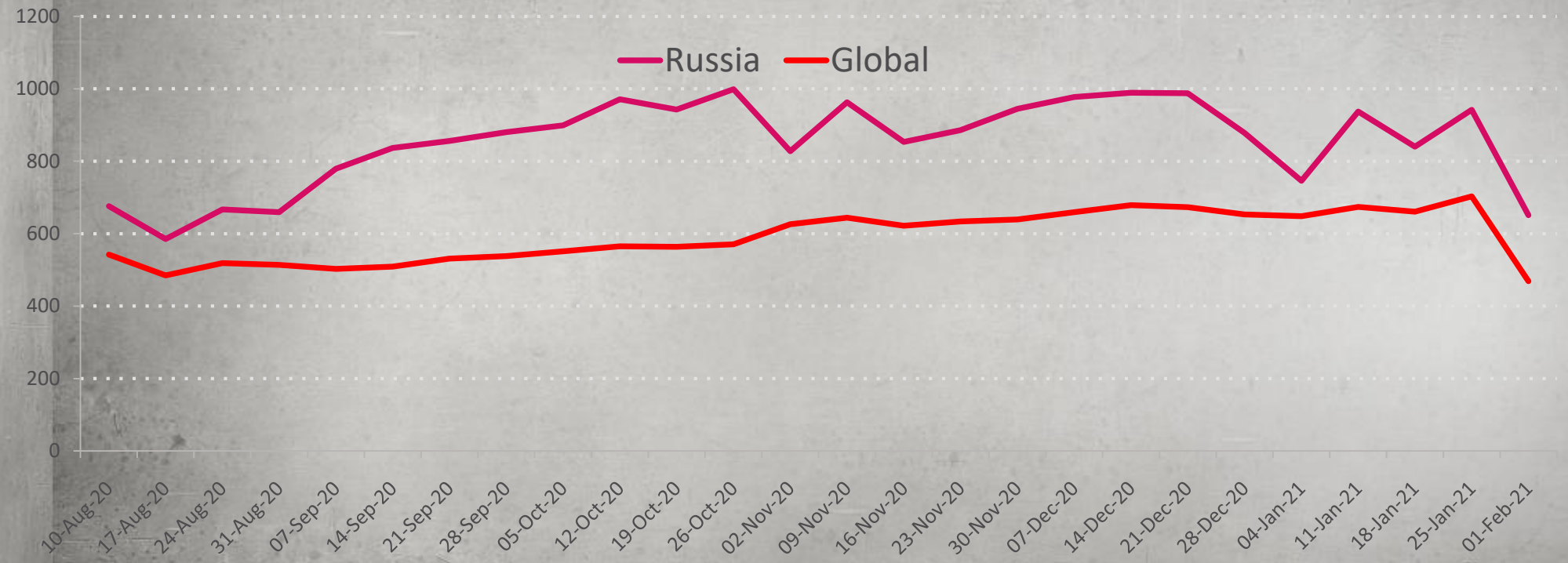
SandBlast AGENT

- Threat Prevention
- Anti-Ransomware
- Forensics

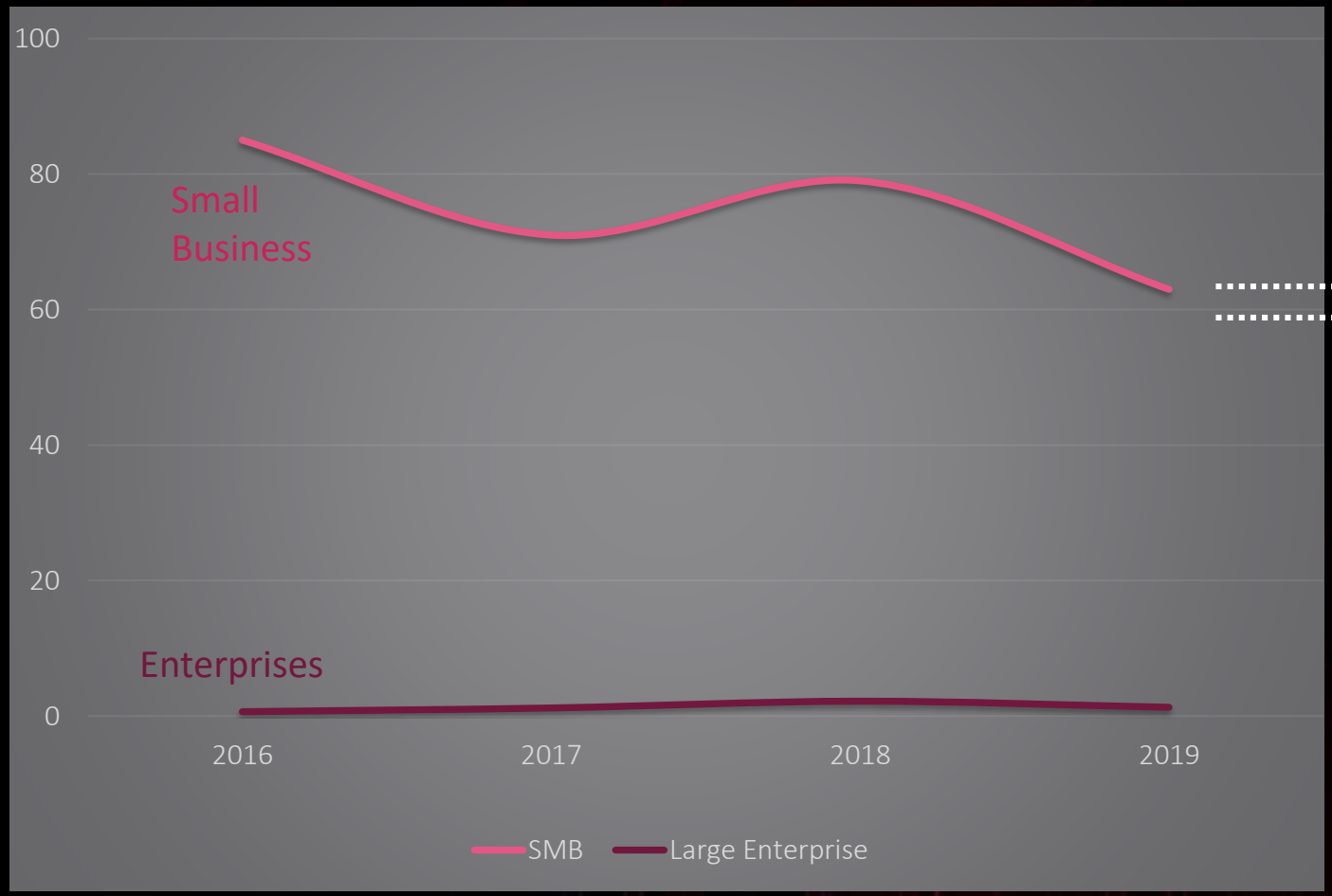
Access/Data Security

- Access Control
- Secure Media
- Secure Documents

Атаки на предприятия – за последние 6 месяцев



Аналитика атак



43%

атак на SMB

63%

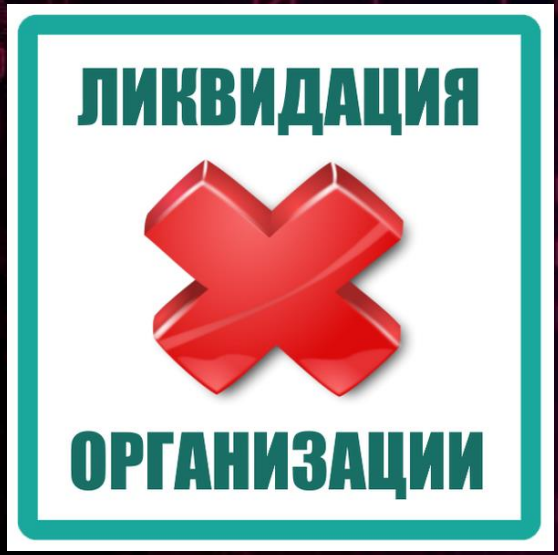
успешных атак на SMB

*Data Breach Investigations Report, years: 2016, 2017, 2018, 2019

Цели злоумышленников

- Списки клиентов
- Информацию о кредитных картах клиентов
- Банковские реквизиты компании
- Ценовую политику компании
- Дизайн продуктов
- Планы расширения
- Производственные процессы

60% - SMB



Последствия атаки

- Финансовые потери от кражи банковской информации
- Финансовые потери от остановки работы компании
- Большие затраты на восстановление сети
- Репутационный ущерб после уведомления клиентов о том, что их информация была скомпрометирована

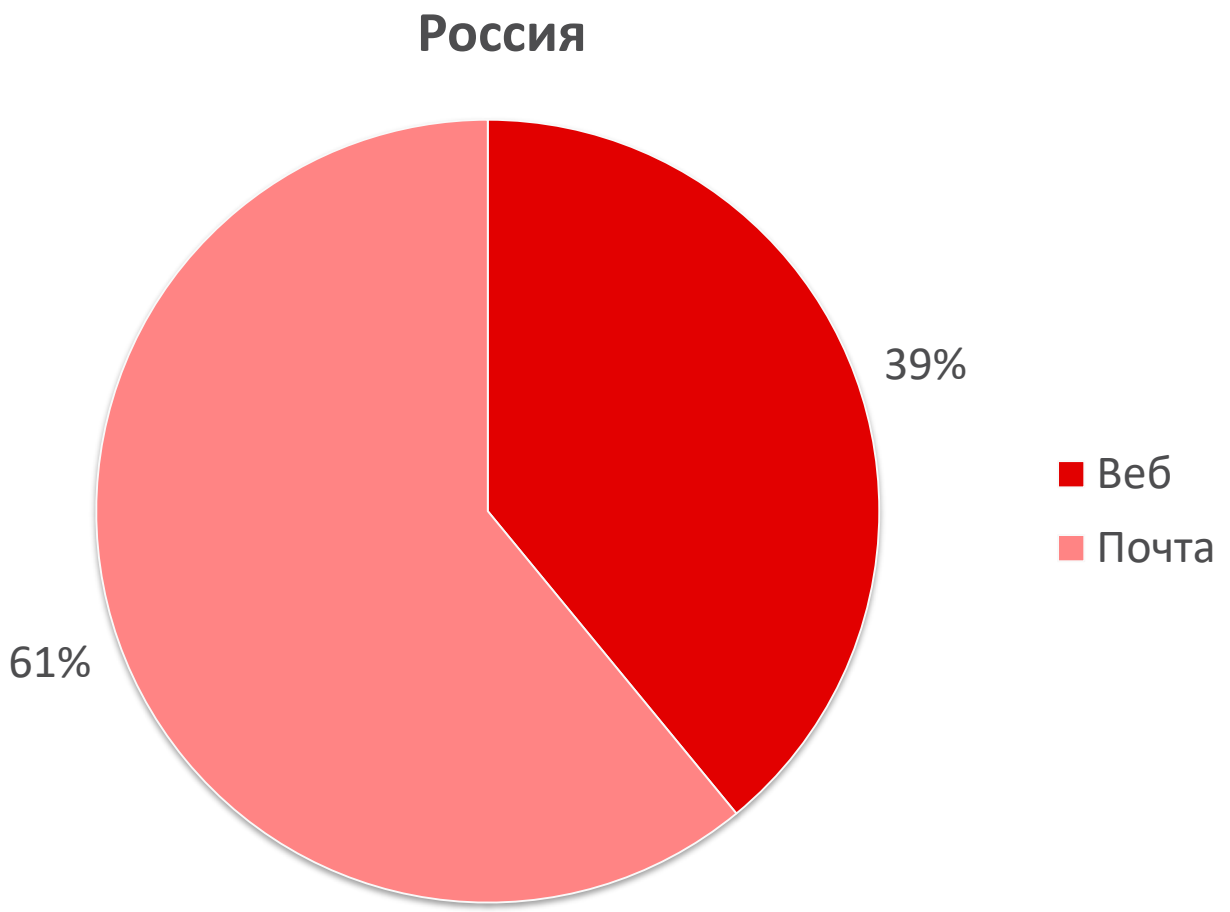
Аналитика угроз

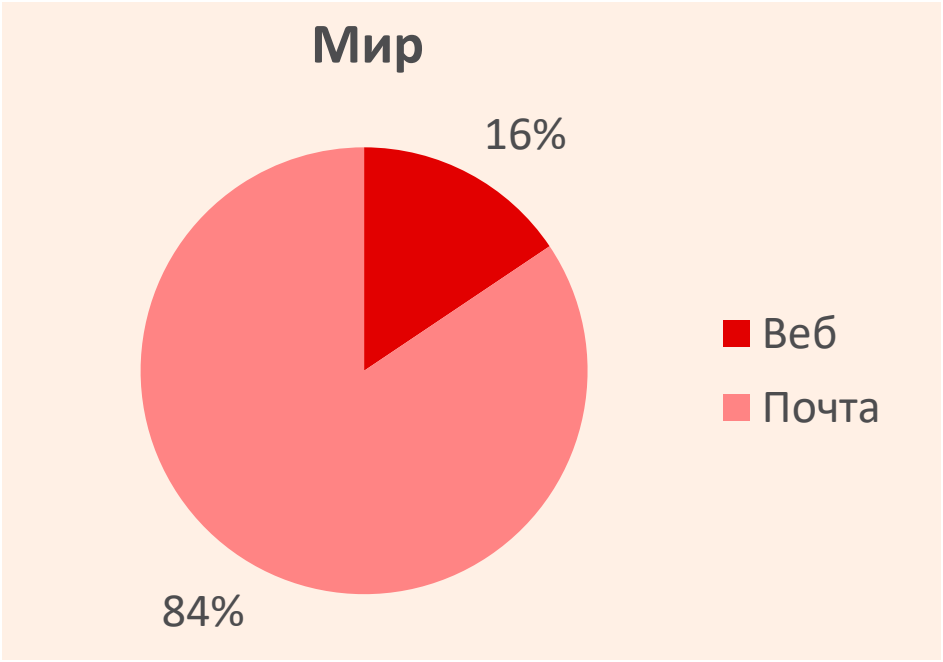
- Компании в России подвергаются атакам в среднем 852 раза в неделю за последние 6 месяцев по сравнению с 591 атакой на компанию во всем мире.
- Главный зловред в России - QBot, инфицировано 22% организаций.
- В рейтинге вредоносных программ в России входят троян Fareit, 1 банковский троян (Trickbot), 1 криптомайнер (XMRig) и 1 ботнет (Phorpiex)
- 60% вредоносных файлов в России были доставлены по электронной почте.
- Наиболее распространенным типом эксплойтов в России является удаленное выполнение кода, которым подвержены 68% организаций.
- Статистика выявленного вредоносного ПО:

	Mobile	Banking	Cryptominer	Botnet	InfoStealer
Russia	1.0%	9.2%	7.4%	14.6%	5.1%
Global	0.9.%	4.1%	3.6%	8.2%	2.3%

View the latest publications by Check Point Research

Формат доставки вредоносных файлов – прошедшие 30 дней





Quantum

Security Gateway

ПРЕДОТВРАЩЕНИЕ УГРОЗ

FW & VPN Software Blades

IPS Software Blade

Application Control Software Blade

Identity Awareness Software Blade

Antivirus Software Blade

URL Filtering Software Blade

Anti-Bot Software Blade

Threat Emulation/Extraction Software Blades

Main office

Endpoint protections

- Desktop Firewall
- Application control
- Full disk encryption
- Media encryption and port protection
- Anti-Malware
- VPN
- Anti-Bot and Forensics
- URL Filtering
- Compliance

Data loss prevention

DDoS Hardware protection

Site to site VPN

Check Point Security Gateway

Private cloud and virtualisation protections

Virtual security gateway

CHECK POINT CloudGuard

ACI

vmware NSX

openstack

Industry leading zero-day sandbox solution

Unified management console

Security incident and event reporting

Policy Management

ШЛЮЗЫ БЕЗОПАСНОСТИ QUANTUM

Линейка для бизнеса любого размера

Новые модели

Старые модели

Branch Office

3600, 3800

До 1.5 Gbps

+180%

3100 - 3200

0.58 Gbps

Small Enterprise

6200, 6400

До 2.5 Gbps

+60%

5100 - 5400

1.46 Gbps

Midsize Enterprise

6600, 6700

До 5.8 Gbps

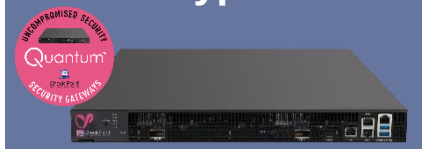
+55%

5600 - 5900

6.1 Gbps

Large Enterprise

16600 Hyperscale



7000, 16200

До 17.6 Gbps

+70%

15000

10 Gbps

Data Center

26000, 28000

До 30 Gbps

+50%

23000

20 Gbps

Telco & High-End

Maestro 140 | 170

До 1,500 Gbps

+680%

64000

44000

Up to 190 Gbps

ПРОИЗВОДИТЕЛЬНОСТЬ THREAT PREVENTION

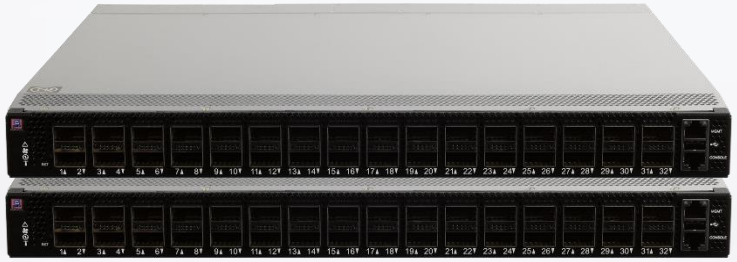
Quantum

Maestro

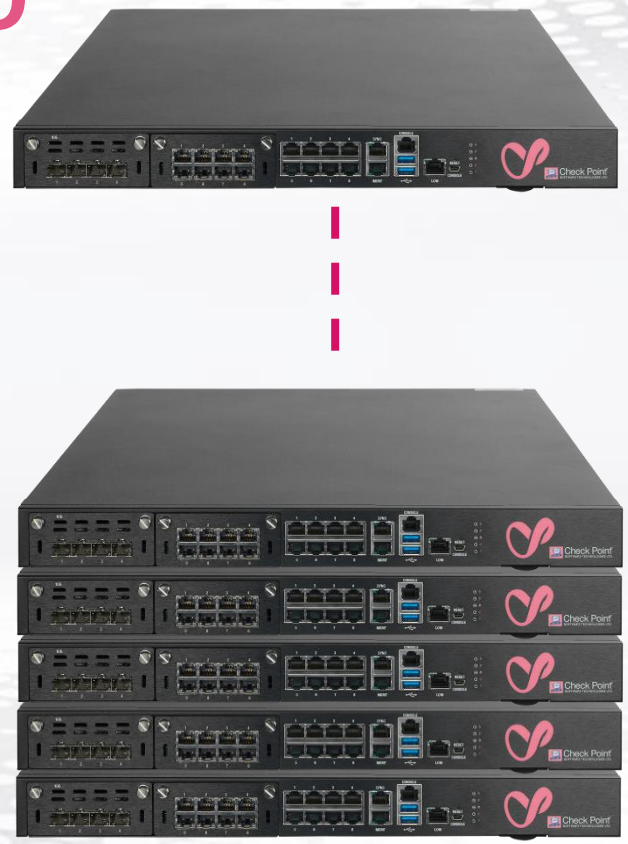
ГИПЕРМАСШТАБИРУЕМОСТЬ

НУЖНО БОЛЬШЕ МОЩНОСТИ ДЛЯ ГЛУБОКОЙ ИНСПЕКЦИИ? ЛИНЕЙНО-МАСШТАБИРУЕМАЯ АРХИТЕКТУРА MAESTRO

Check Point
SOFTWARE TECHNOLOGIES LTD



MAESTRO
HYPERSCALE ORCHESTRATOR



6800 Security Gateway

450 Gbps

До 52 устройств

26.7 Gbps
17.8 Gbps
8.9 Gbps

Threat Prevention

Полная готовность к работе за 6 минут

SANDBLAST NETWORK: РЕШЕНИЕ КЛАССА «ПЕСОЧНИЦА»

Защита от угроз 0-дня и направленных атак

СЕМЕЙСТВО ПРОДУКТОВ SANDBLAST

NETWORK

Защита периметра и внутренней сети

SandBlast Cloud emulation

SandBlast Local emulation

AGENT

Безопасность рабочих станций и браузеров

SandBlast Agent

SandBlast Agent for Browsers

CLOUD

Безопасность приложений в облаках

CloudGuard SaaS

MOBILE

Безопасность мобильных устройств

SandBlast Mobile

Сокращаем площадь атаки

Контролирем двери в крепость (и каждую комнату)

Куда и как можно попасть из нашей сети?

Кто и что может попасть в нашу сеть?

Firewall

VPN, SSL Inspection

URL Filtering

Identity Awareness

Application Control

Content Awareness

Geo Protection

Инфекции по SMB

BLOCKED

Инфекции через соц. сети, анонимайзеры

BLOCKED

Исполняемые файлы, экзотические архивы

BLOCKED

Сокращение площади атаки и предотвращение ущерба

Сегментация сети и строгая политика NGFW, инспекция SSL

No.	Name	Source	Destination	Services & Applications	Content	Action
Access To Internet (5)						
5	Access to Internet according to Web control policy	InternalZone	Internet	Any	Any	Web Control
5.1	DNS server should have access to	DNS Server	ExternalZone	domain-udp-Protoc... domain-tcp-Protoc...	Any	Accept
5.2	Block abuse/ high risk applications	Corporate LANs Branch Office LAN	Internet	Inappropriate Sites Anonymizer	Any	Drop Blocked Messa...
5.3	HR can acc... network ap...					Inform Access Approval

All | dnscat2

DNSCAT2

DNSCAT2

Primary Category: **Anonymizer** Risk: 5 **Critical**

DNSCAT2 is a dns tunneling tool. DNSCAT2 allows users to implement a tunnel over the dns protocol and to remotely connect to a dns server.

Match By

- Application Signature
- Services:
  - udp/53

Сокращение площади атаки и предотвращение ущерба

Сегментация сети и строгая политика NGFW, инспекция SSL

Контроль векторов атаки по форматам файлов

No.	Name	Source	Destination	Services & Applications	Content	Action	Track
5.3	HR can access to social network applications	HR	Internet	Facebook Twitter	Download Traffic Executable File Archive File Source Code - Shell Scrip	Drop	Log
5.4	HR can access to social network applications	HR	Internet	Facebook Twitter	Any		
5.5	All employees can access YouTube for work purposes	Corporate LANs Branch Office LAN	Internet	YouTube Vimeo	Any		

All | Search...

- Archive File
- CAD-CAM Designs
- Certificate Files
- Certificate Signing Request File
- Certificates and Private Keys
- Credit Card Numbers or IBAN
- CSV File

Фильтруем известные атаки

Предотвращаем то, что уже знаем

Блокируем вредоносные файлы и сайты

Anti-Virus

BadRabbit Ransomware

BLOCKED

Блокируем сетевые атаки и эксплойты

IPS

EternalBlue Exploit

BLOCKED

Блокируем каналы управления

Anti-Bot

Data Exfiltration

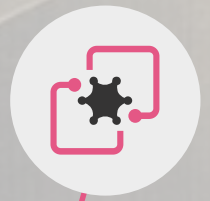
BLOCKED

Эмулируем неизвестные атаки

Раскрываем истинные цели **неизвестных** файлов

Динамический анализ по поведению в песочнице

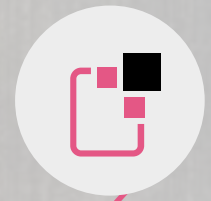
Проактивная очистка и мгновенная доставка



Threat Emulation

BadRabbit Download

BUSTED



Threat Extraction

DDE Macro-Less attack

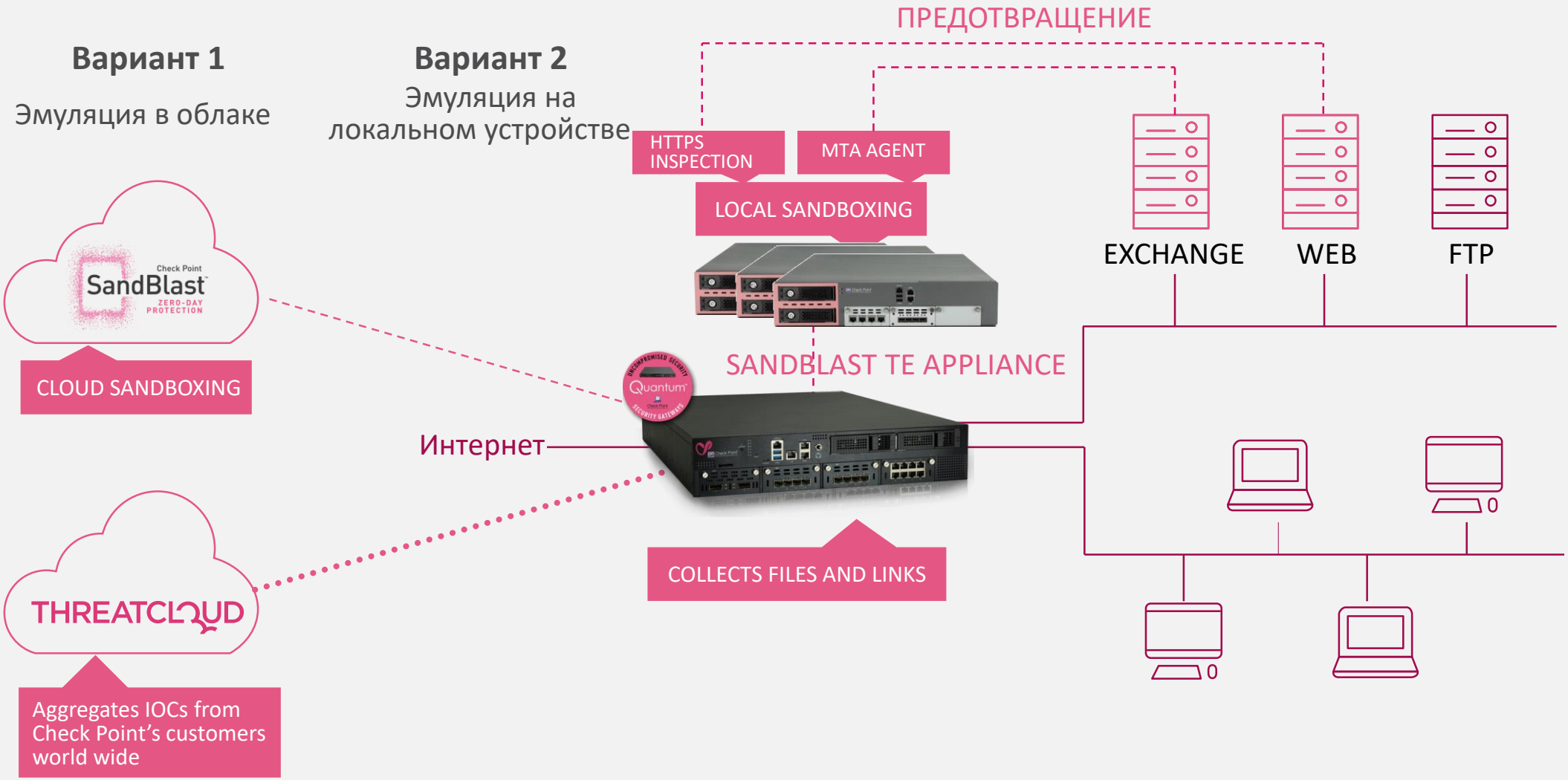
BUSTED

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

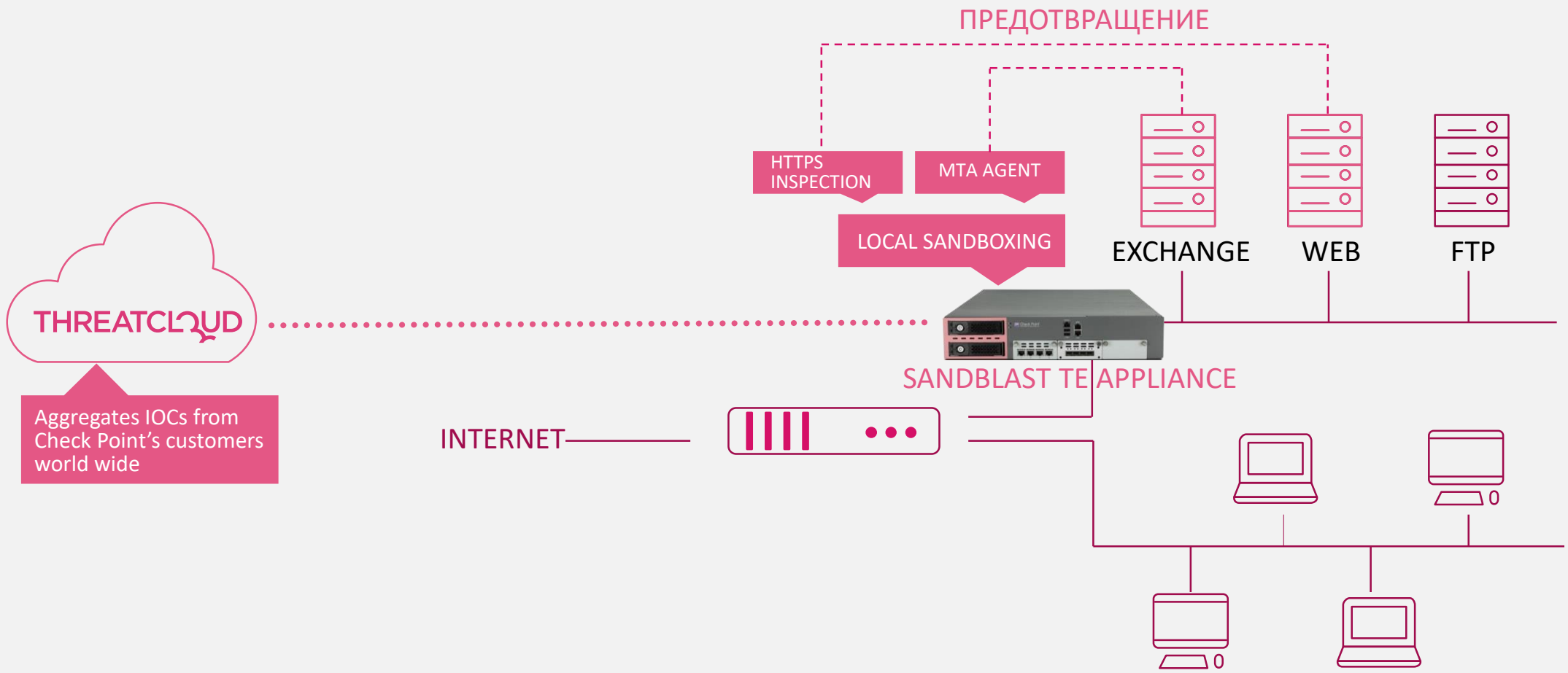
Классическая схема

Просто, гибко и масштабируемо



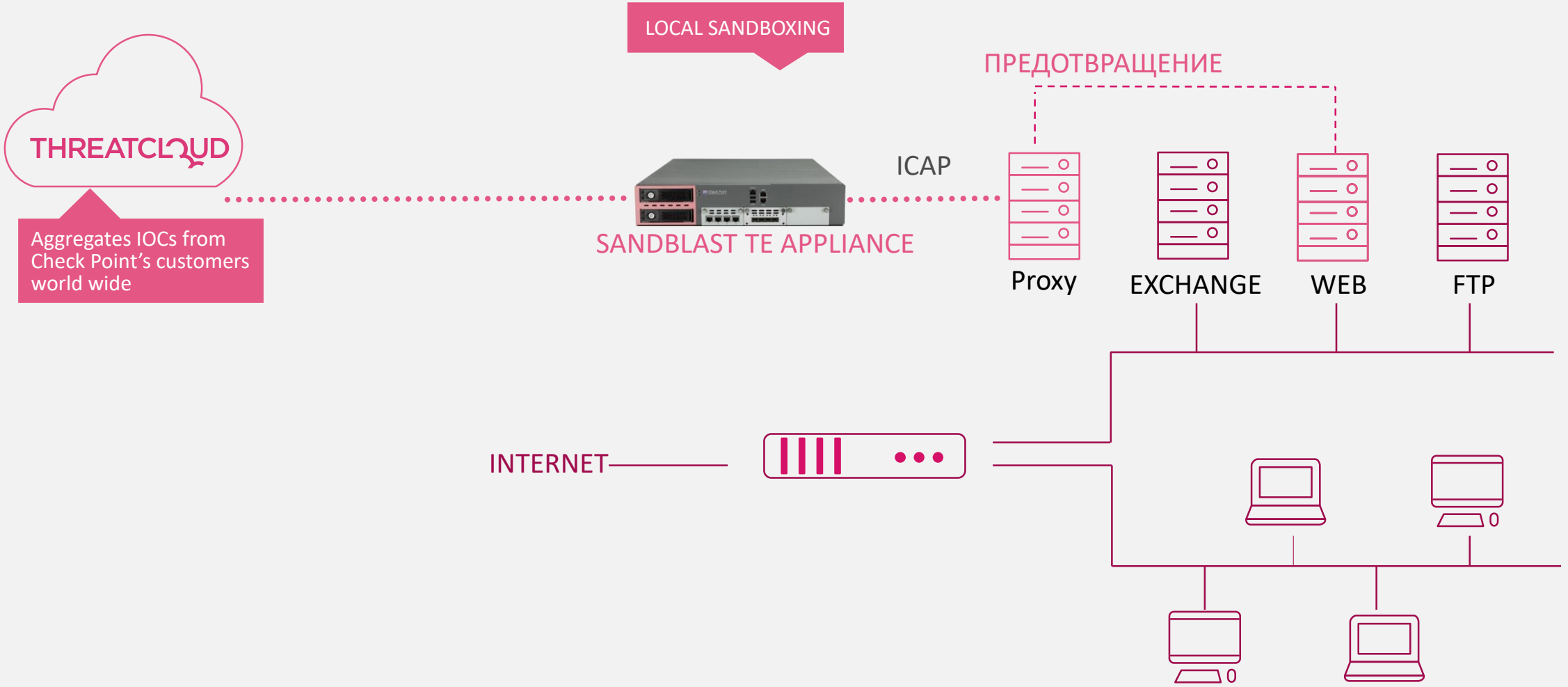
Установка в разрыв

Для клиентов без шлюзов Check Point



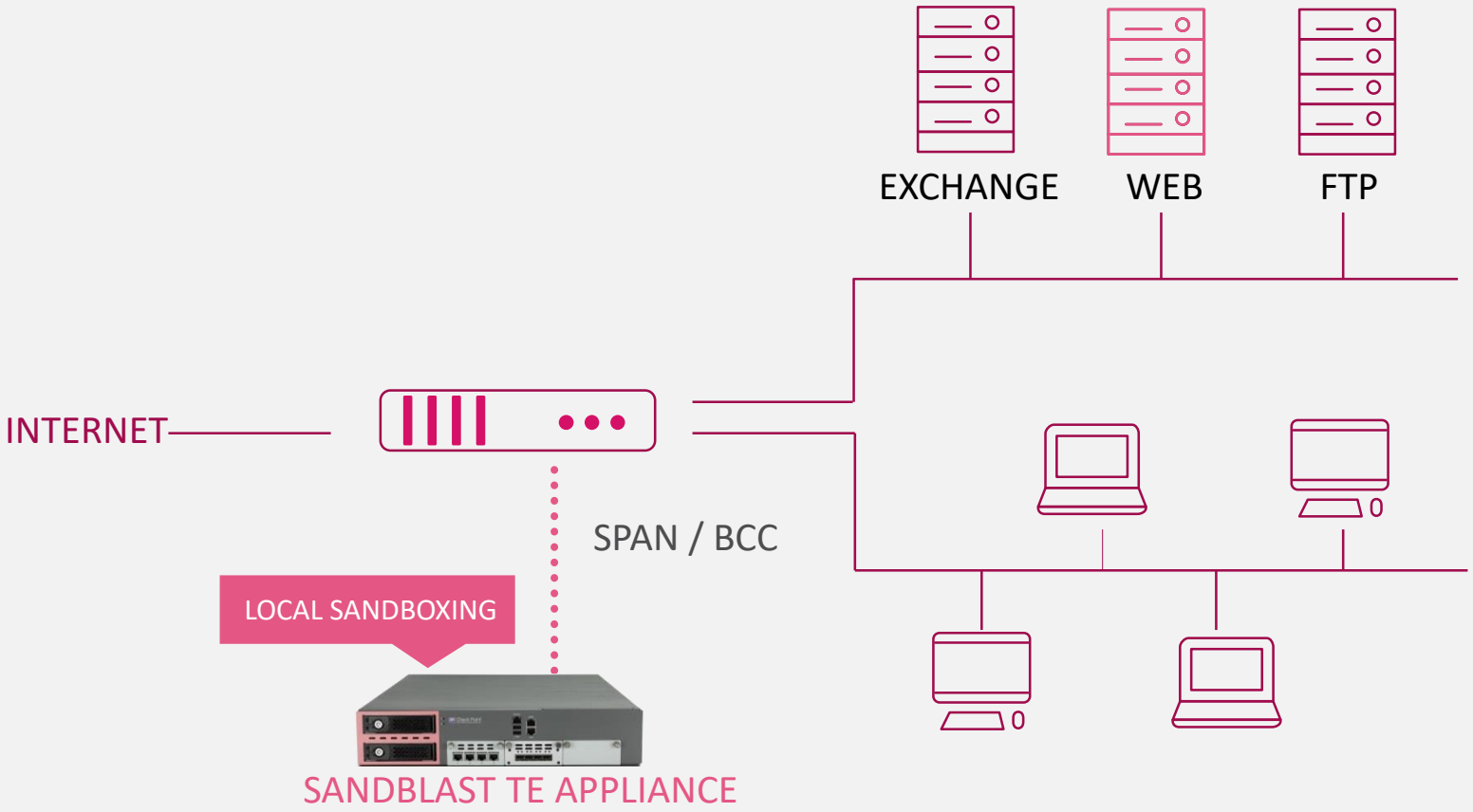
Интеграция по ICAP

Для клиентов без шлюзов Check Point



Режим обнаружения

Используется для пилотных проектов



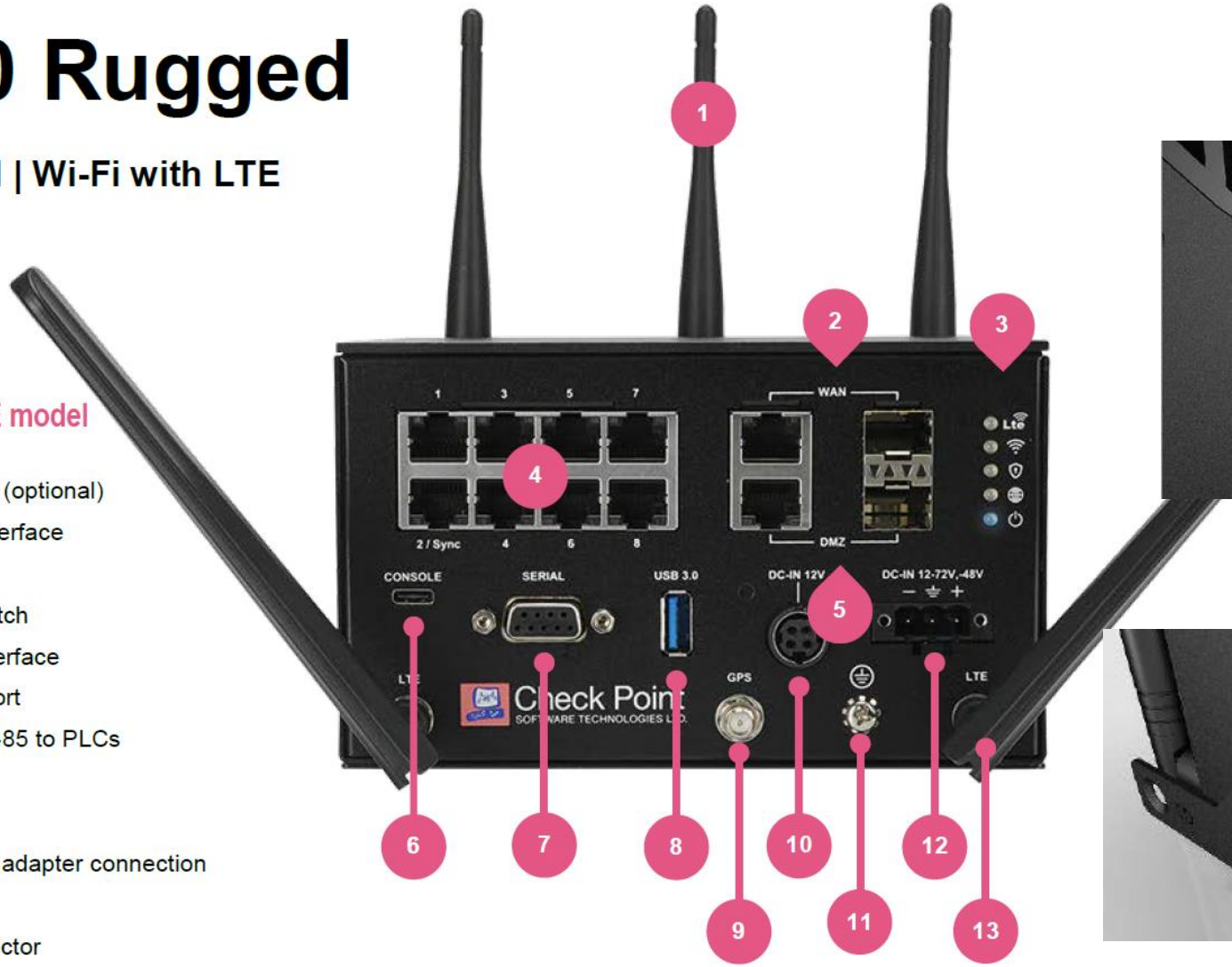
Добро пожаловать

В мир SMB

Новое поколение SMB устройств

1570 Rugged

Wired | Wi-Fi with LTE



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

Firewall IPS App Control URL Filtering Antivirus Anti-Bot

HTTPS inspection Remote access Threat Emulation

Check Point
SOFTWARE TECHNOLOGIES LTD

Безопасность

100% отражение атак и производительность R80

Производительность

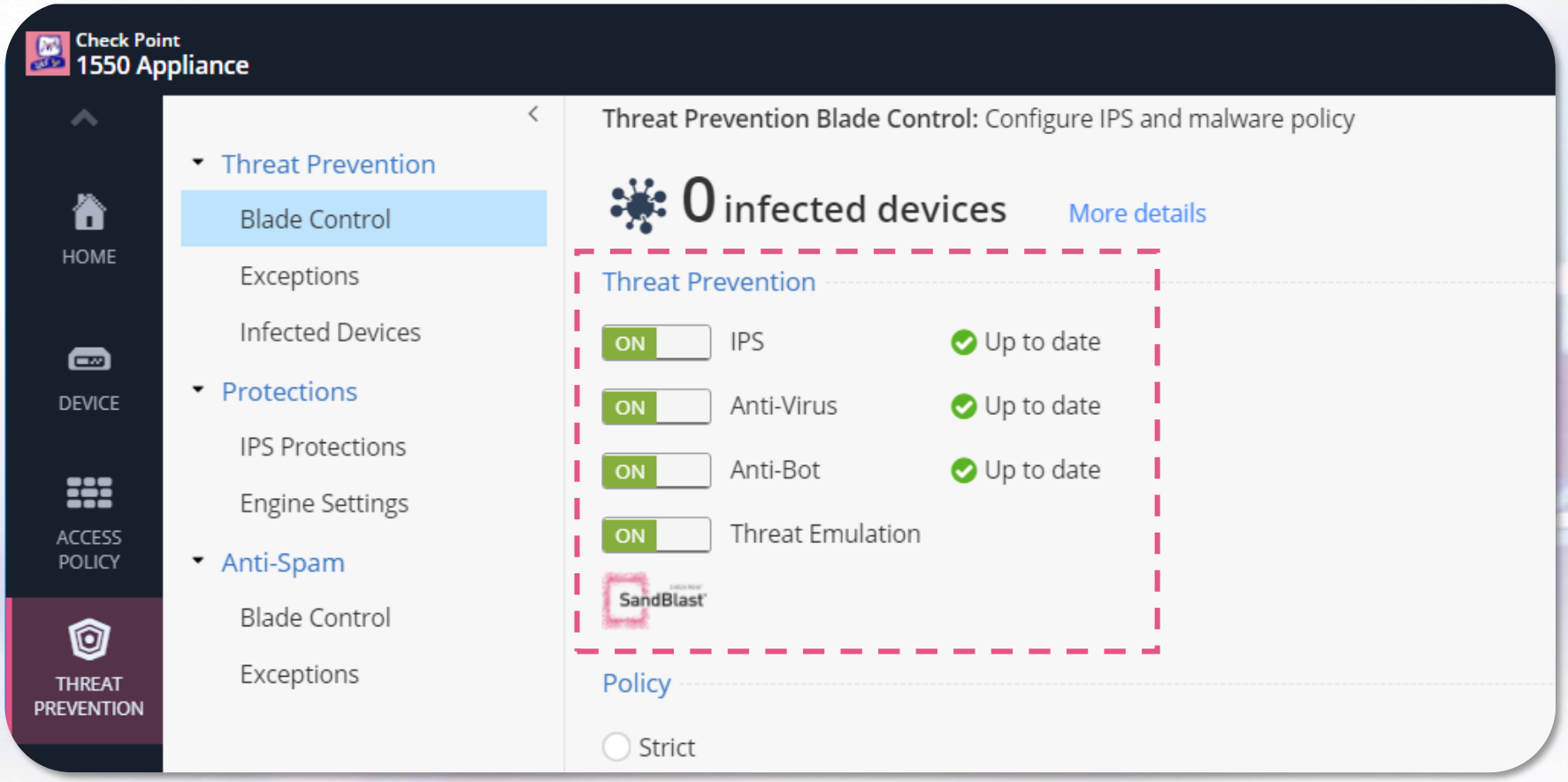
в 2 раза больше производительности

Удобство

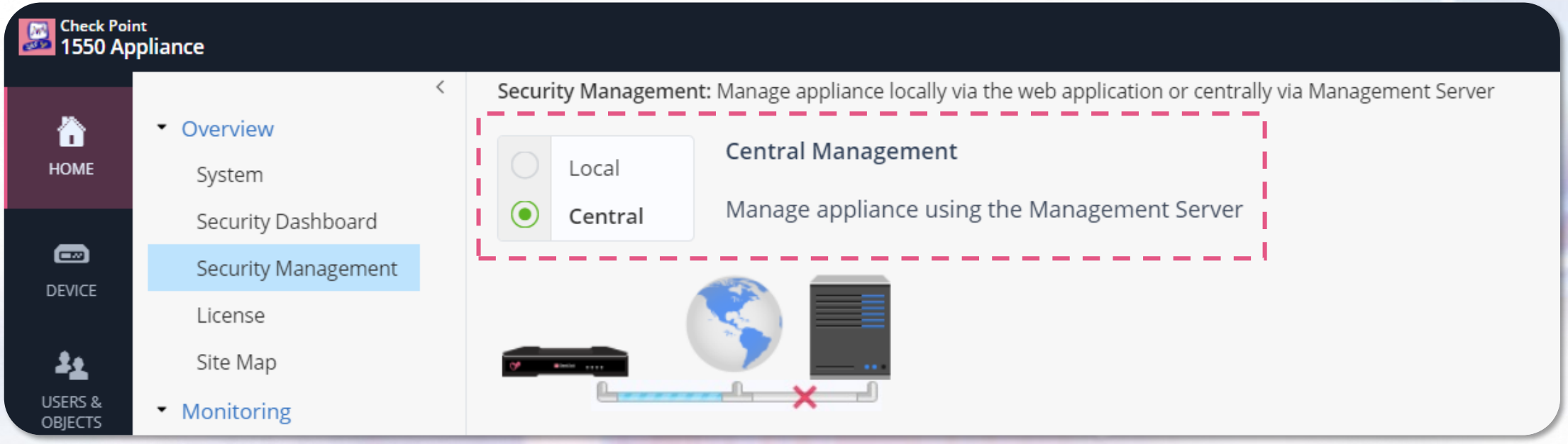
Управление через:

- Облако
- Локально
- Мобильное устройство
- Централизованный менеджмент

Поддержка всех технологий предотвращения угроз



Управление централизованное или локальное

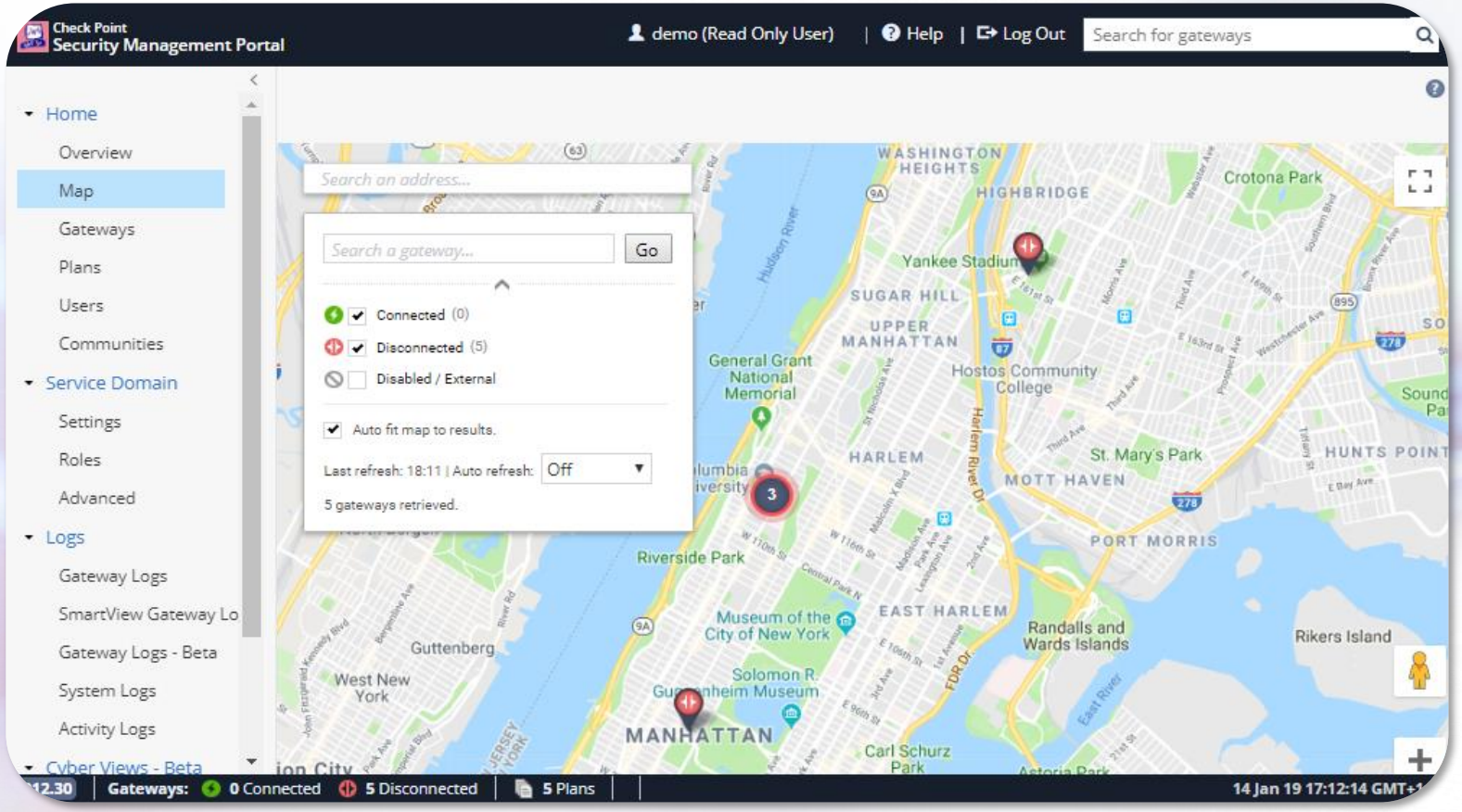


Облачная система управления

Check Point
SOFTWARE TECHNOLOGIES LTD

Система управления безопасностью

Облачная, многопользовательская, легко масштабируемая

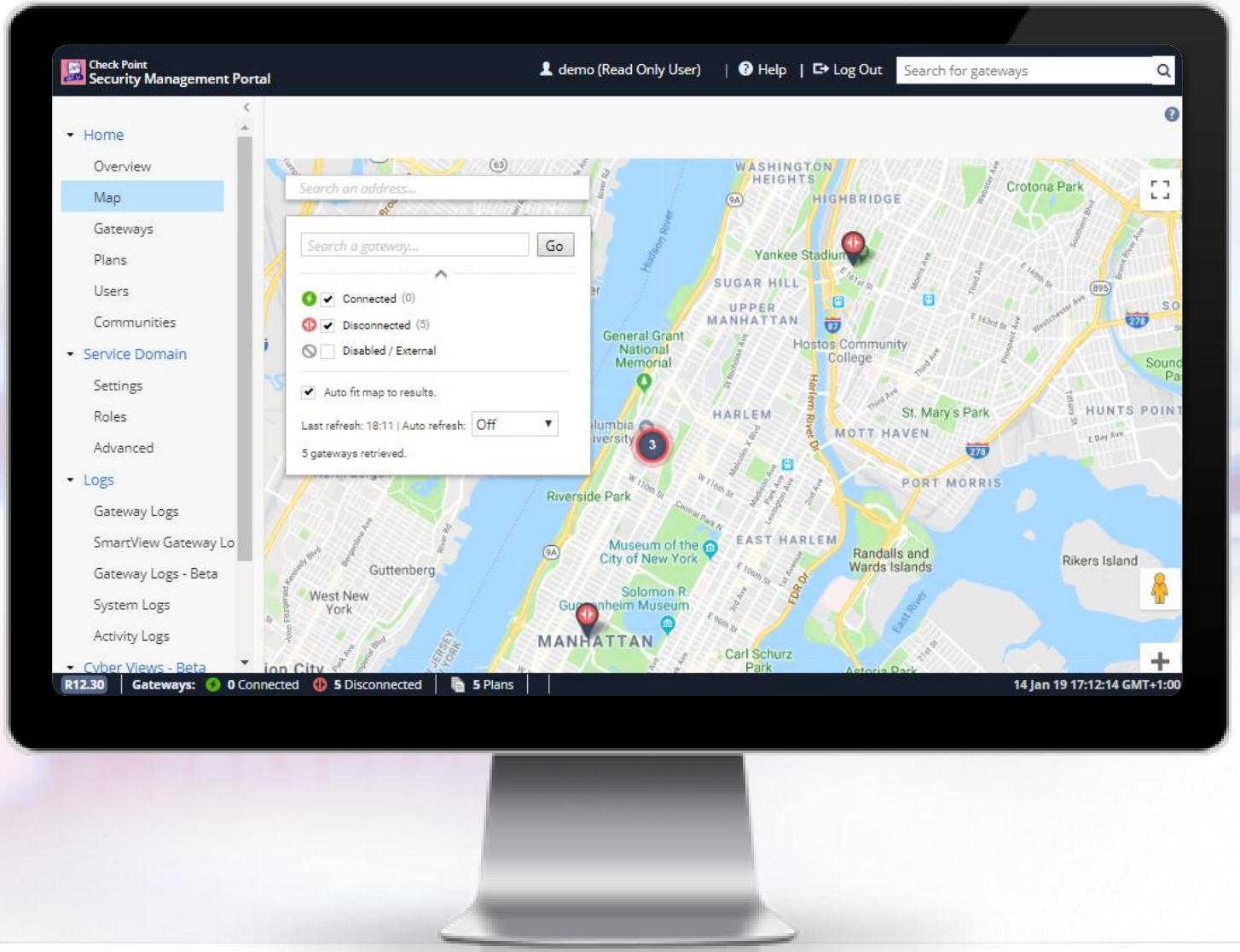


Безопасность без ограничений

Управляйте:

- Шлюзами,
- Облаками,
- Endpoint,
- Мобильными устройствами

в Infinity Portal



Гибкий контроль при помощи многоуровневой политики

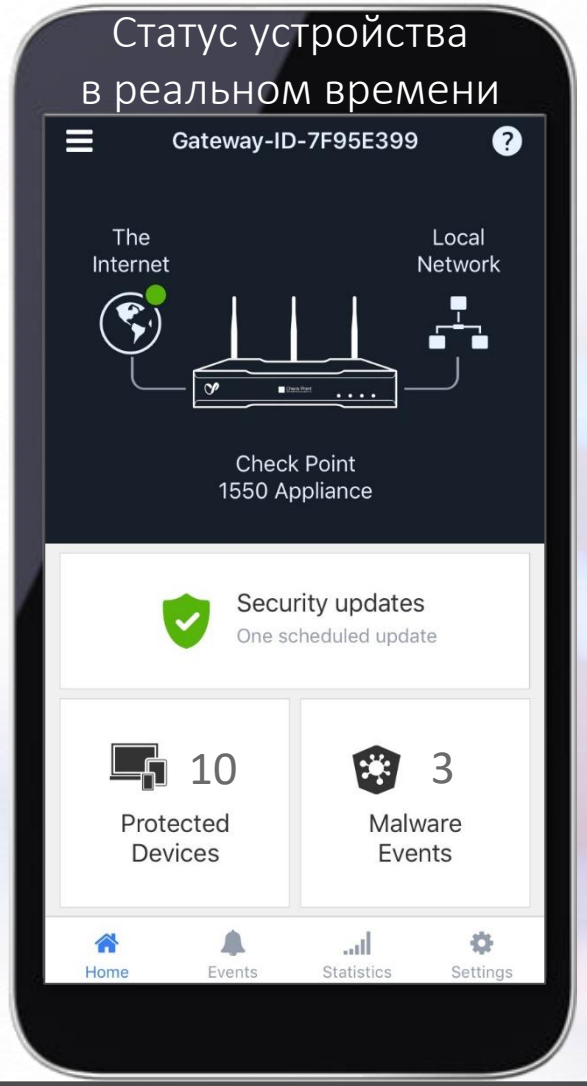
Install Policy | Actions | Search for IP, object, action, ...

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1		InternalNet	Any	Any	Any	Inline1	N/A	My_1550
1.1		Any	DMZNet	Any	Any	Accept	None	My_1550
1.2		Any	Any	Any	Any	Drop	Log	My_1550
1.3		Any	Any	Any	Any	Drop	None	Policy Targets
2		Any	Any	Any	Computers / Internet	Drop Blocked Messa...	Log Accounting	Policy Targets
3	Cleanup rule	Any	Any	Any	Any	Accept	Detailed Log Accounting	Policy Targets

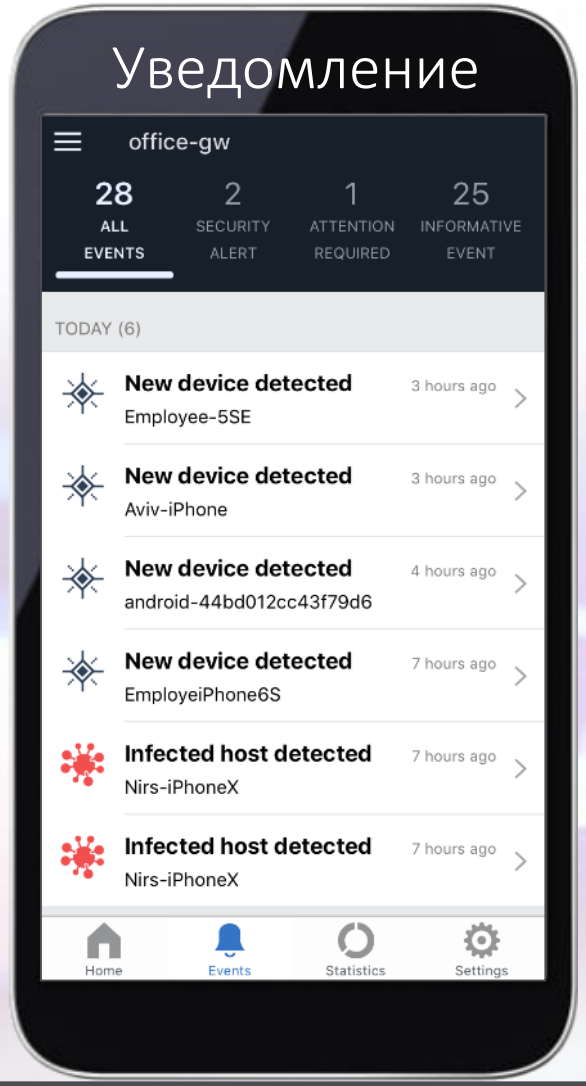
Безопасность на ладони: WATCH TOWER

Check Point
SOFTWARE TECHNOLOGIES LTD

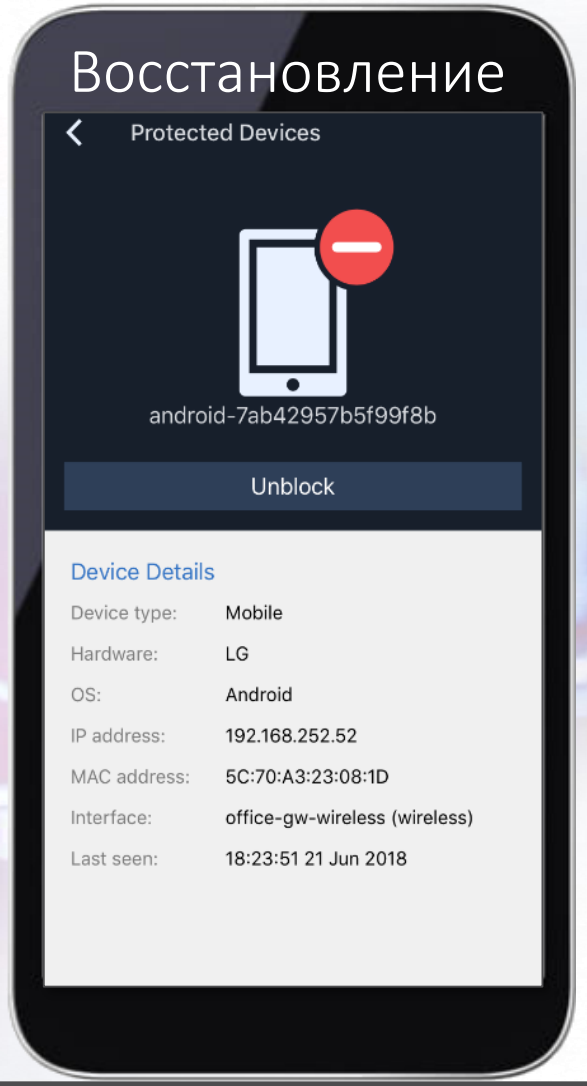
Статус устройства
в реальном времени



Уведомление

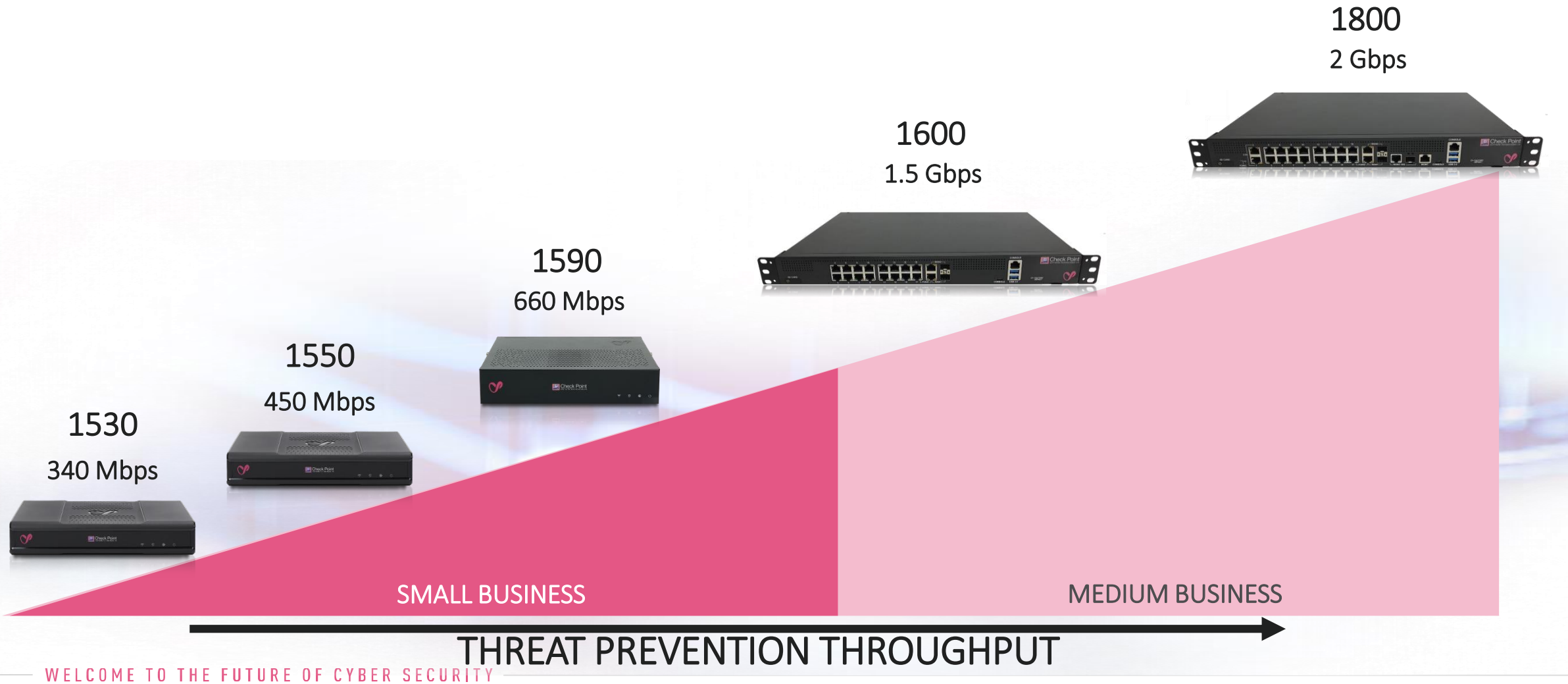


Восстановление



Лёгкость управления безопасностью!

SMB-устройства



Новые устройства 1600/1800

2Gbps
Threat Prevention

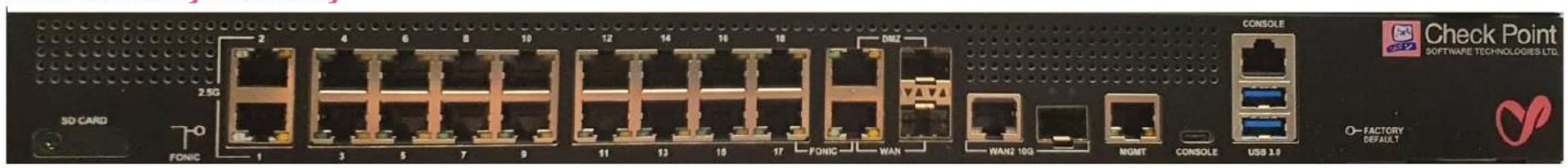
2 блока
питания

2.5G/5G
RJ45 LAN Ports

Link Aggregation
IP aliases
Clustering

10GbE SFP+
WAN Ports

1800 Security Gateway

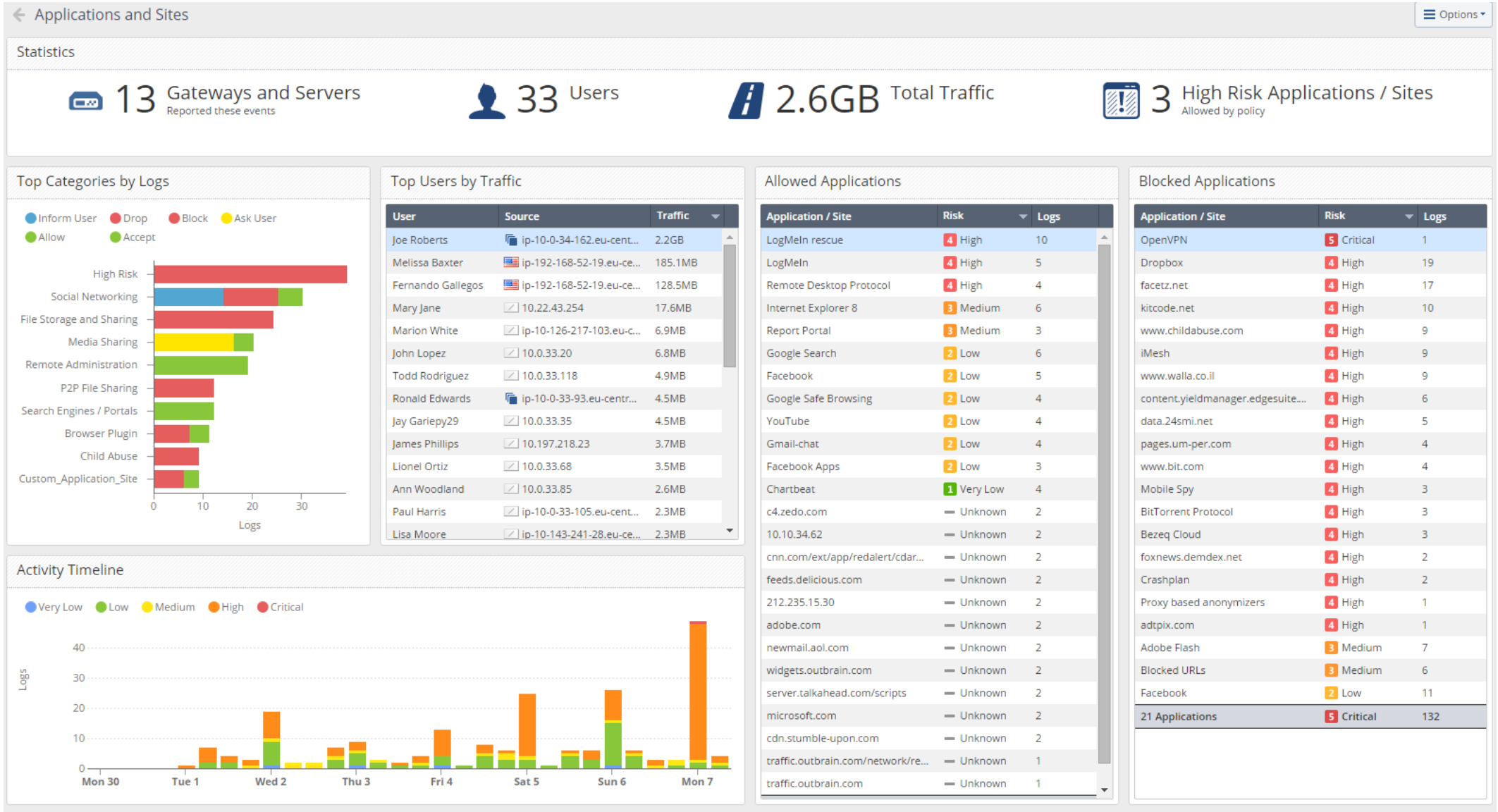


Check Point
SOFTWARE TECHNOLOGIES LTD

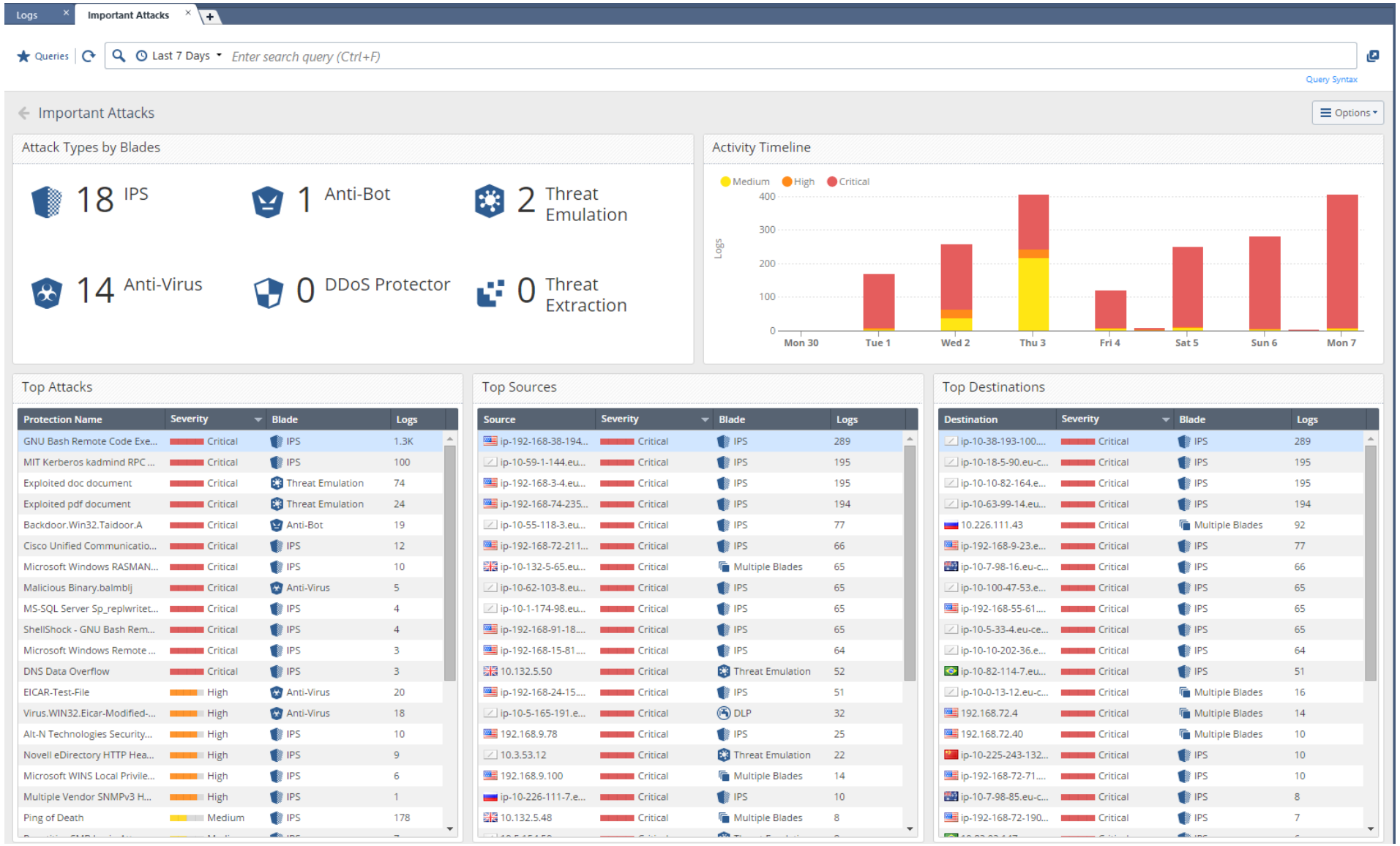
	1600	1800
Gen V Security Performance with Full Threat Prevention including SandBlast	1500 Mbps	2000 Mbps
Gen III Security Next-Gen Firewall	2800 Mbps	3500 Mbps
Gen II Security Firewall Bandwidth	2900 Mbps	3400 Mbps
Concurrent Connections	500,000	1 000,000
WAN Port	2 x 10/100/1000Base-T RJ-45 / 1x 1000BaseF SFP port	2 x 10/100/1000Base-T RJ-45 / 1x 1000BaseF SFP port
WAN Port (10 Gbps)	-	1 x 5Gbps Base-T RJ-45 ports / 1 x 10Gbps SFP+
LAN ports (2.5 Gbps)	-	2 x 10/100/1000/2500 Base-T RJ-45 ports
LAN ports	16 x 10/100/1000 Base-T RJ-45 ports	16 x 10/100/1000 Base-T RJ-45 ports


«Надежный периметр»

ОБЗОР УГРОЗ СО ВСЕЙ ИНФРАСТРУКТУРЫ

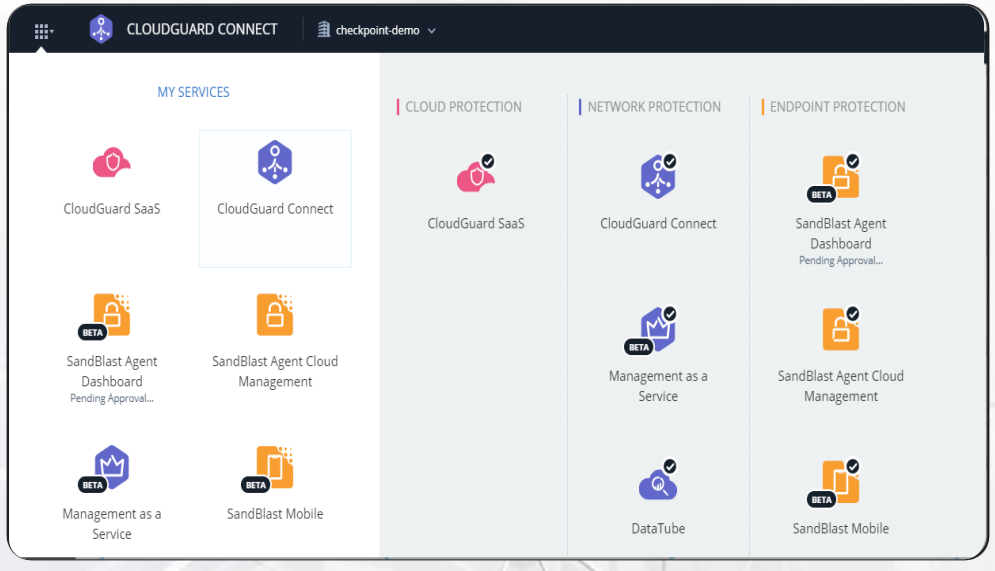


ОБЗОР УГРОЗ СО ВСЕЙ ИНФРАСТРУКТУРЫ



ГИБКИЕ ВАРИАНТЫ УПРАВЛЕНИЯ

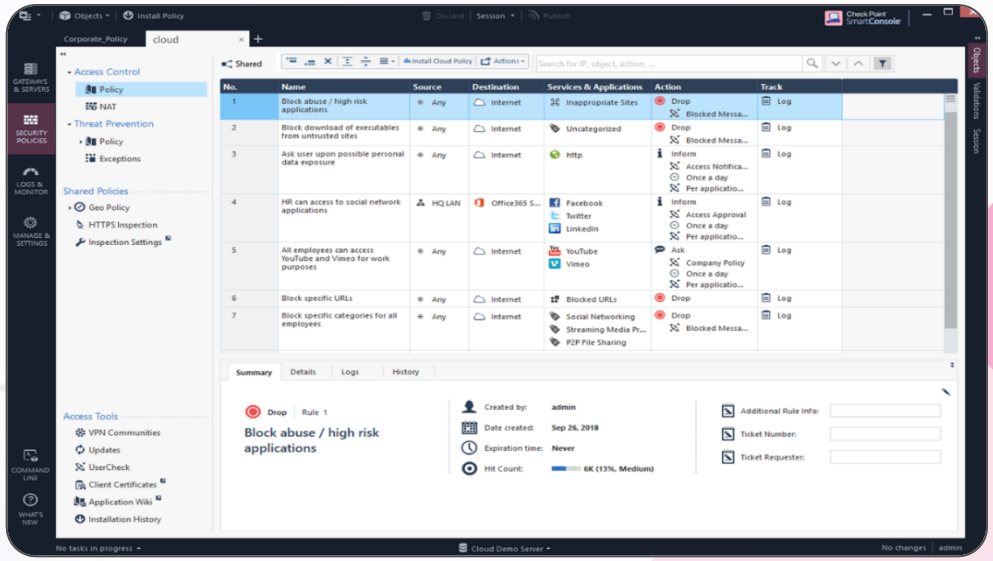
CHECK POINT
INFINITY



Единый облачный Infinity Portal

https://portal.checkpoint.com

R80.30



Классический менеджмент

Check Point®
SOFTWARE TECHNOLOGIES LTD

СПАСИБО!

Sergey Zabula | Channel SE Team Lead, Check Point
szabula@checkpoint.com