



# Quantum Spark

Котельников Александр | Security Engineer

[akotelnikov@checkpoint.com](mailto:akotelnikov@checkpoint.com)



YOU DESERVE THE BEST SECURITY

Добро  
пожаловать

В мир

SMB



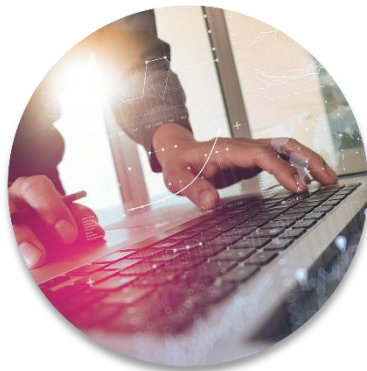
# Рабочее место в SMB может выглядеть так

Гибридная рабочая среда — работа в офисе и удалёнка

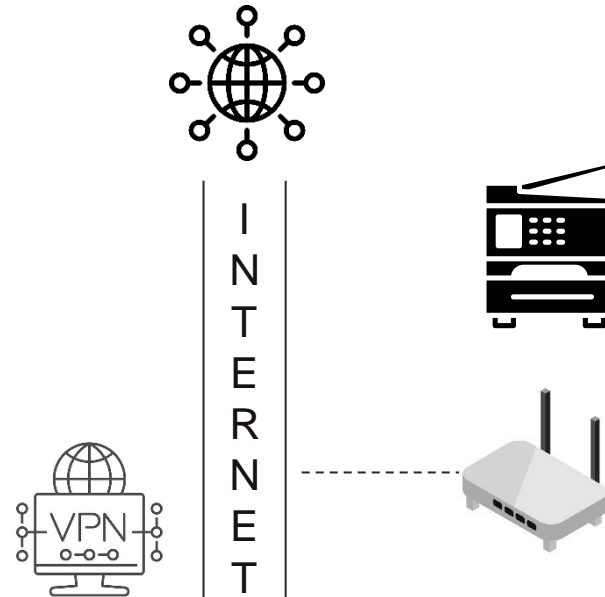


Смартфон/Планшет

SaaS приложения

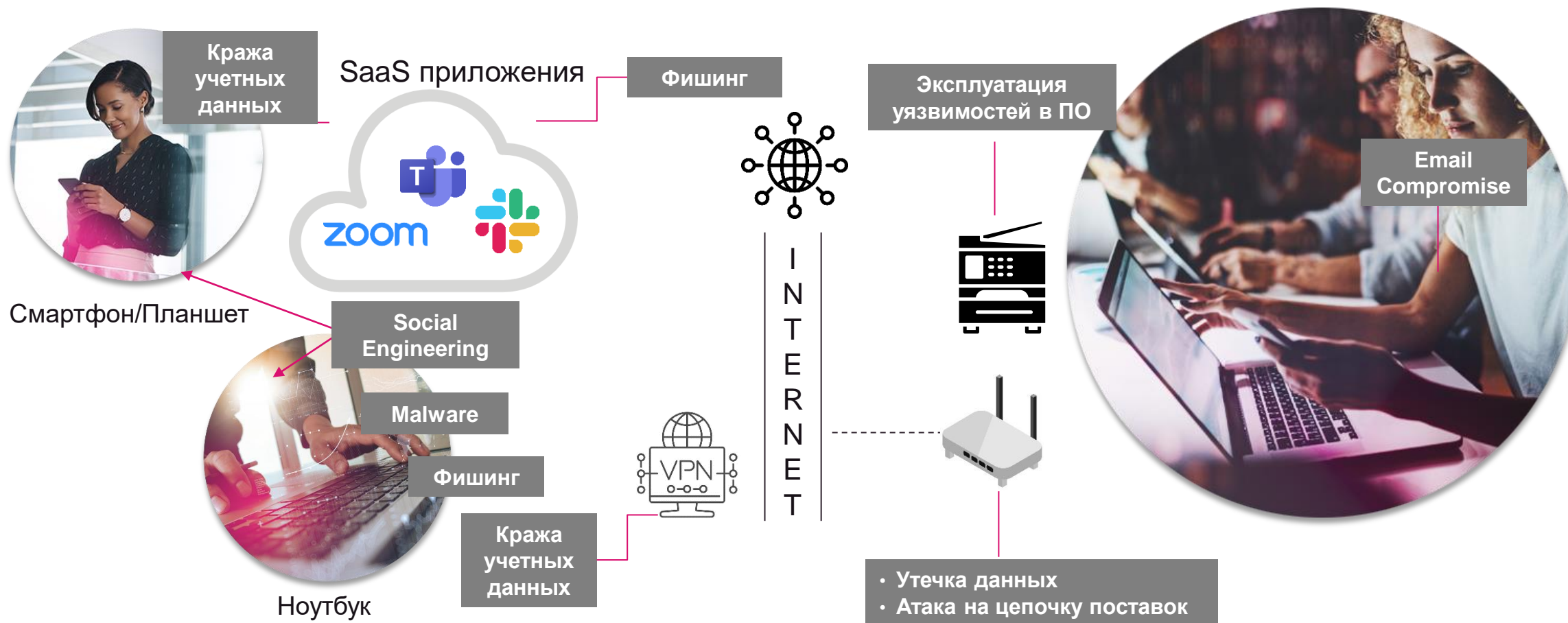


Ноутбук



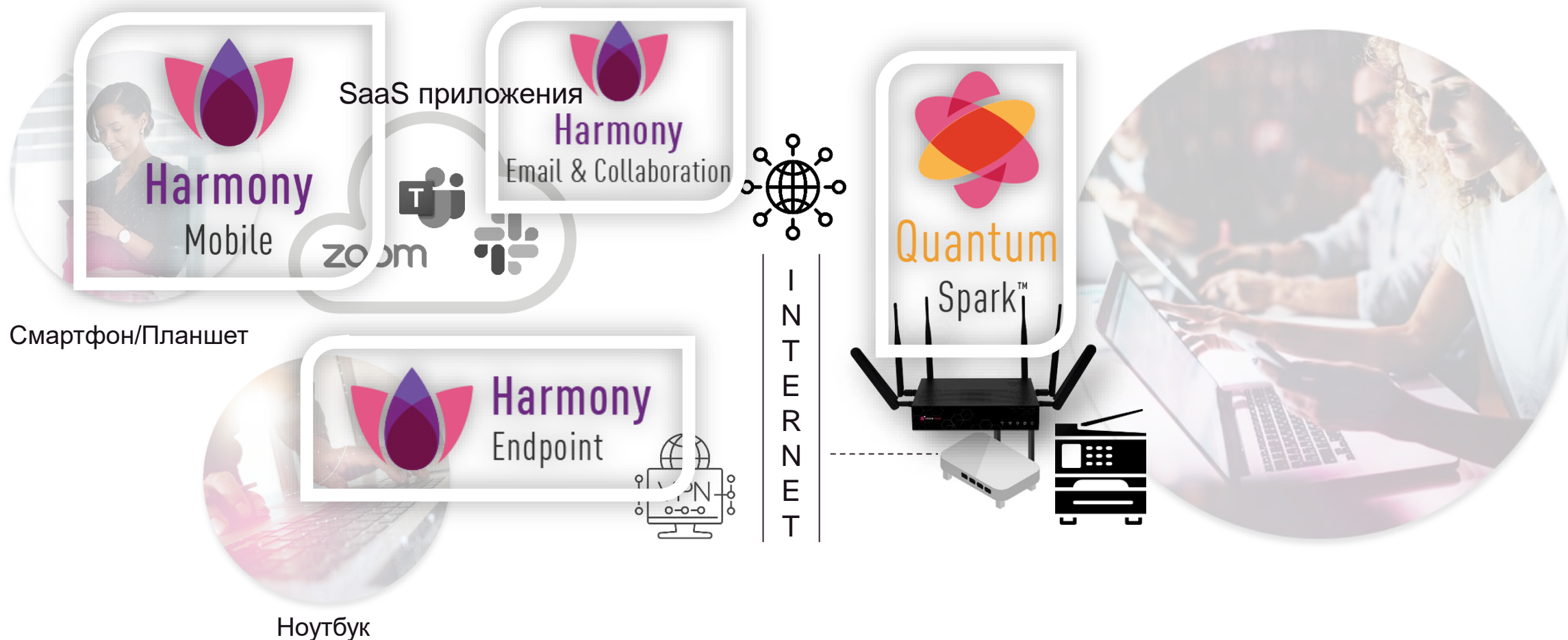
# Но злоумышленник видит это так

Гибридная рабочая среда — работа в офисе и удалёнка



# Check Point защищает от всех видов атак

Гибридная рабочая среда — работа в офисе и удалёнка



# Infinity Spark – безопасность для бизнеса

Полная безопасность, предназначенная для защиты малого и среднего бизнеса



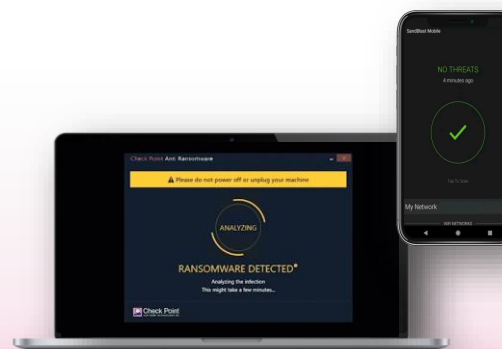
## Защита сети

2.6 Gbps Threat Prevention  
производительность, быстрое  
подключение



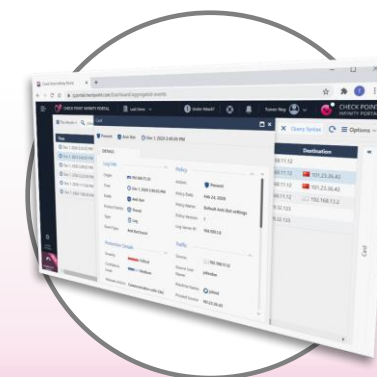
## Защита почты и онлайн-приложений

99.2% снижение количества  
фишинговых атак по  
электронной почте



## Защита устройств

Защитите пользовательские устройства от  
программ-вымогателей, фишинга и  
вредоносных файлов и приложений.



## Унифицированное управление

Decrease MSP operational  
costs by 50%

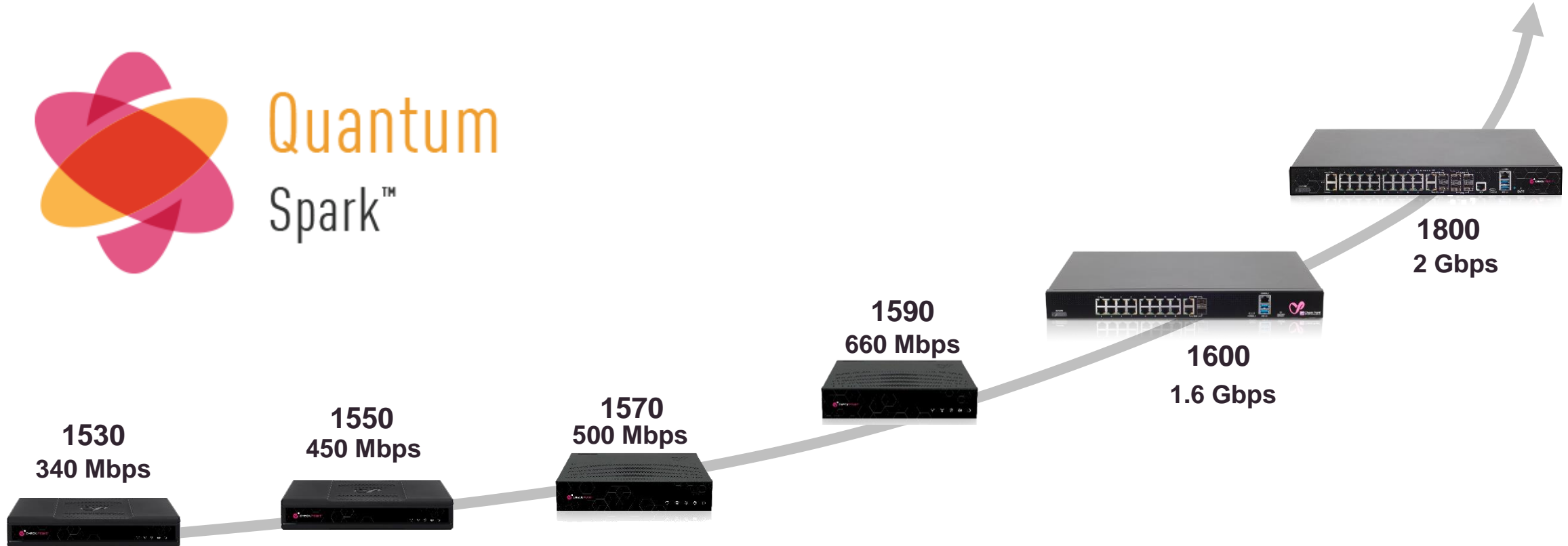
# БЕСКОМПРОМИССНАЯ БЕЗОПАСНОСТЬ ИЗ КОРОБКИ



# Предыдущее поколение Quantum Spark NGFW



Quantum  
Spark™



SMALL BUSINESS

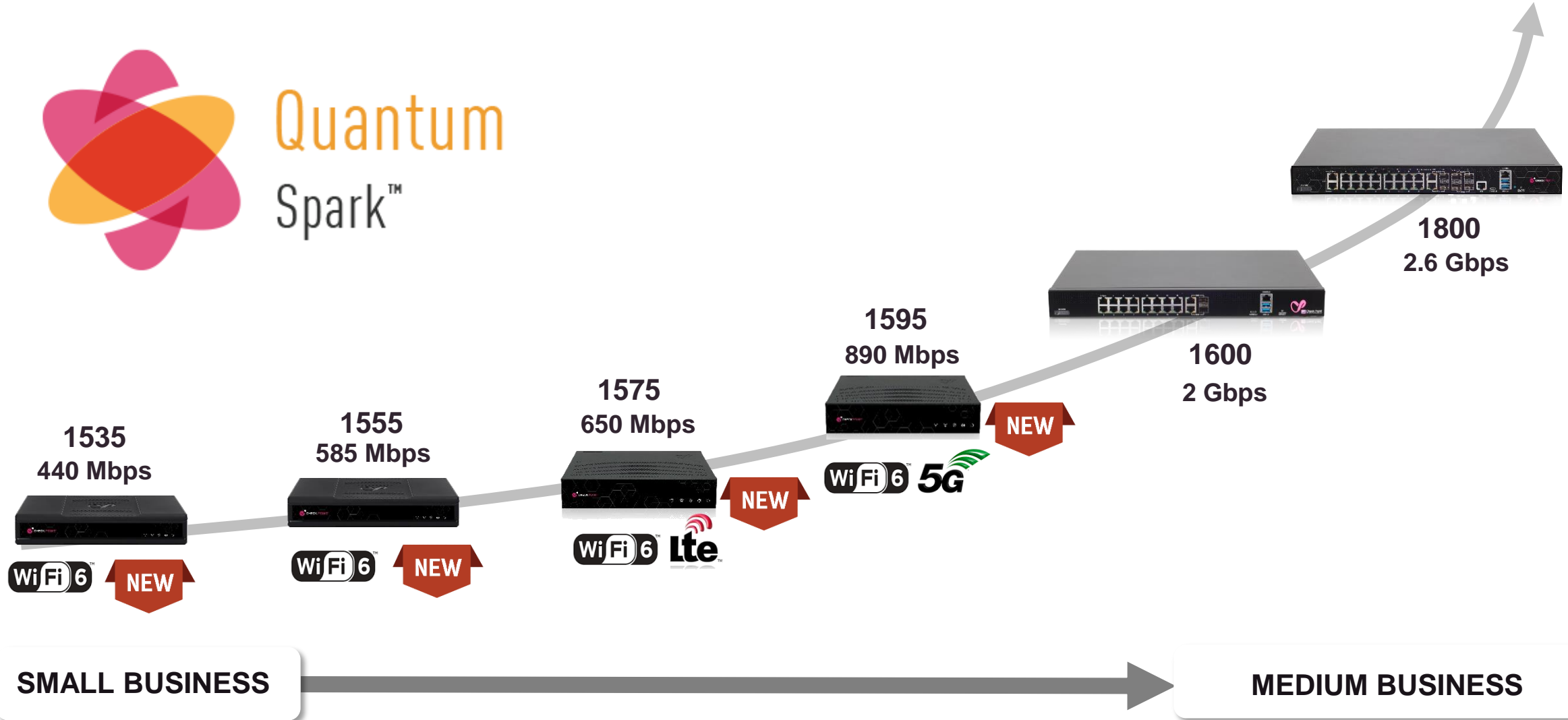
MEDIUM BUSINESS



# Quantum Spark 1500 Pro



Quantum  
Spark™



# Quantum Spark 1500 Pro

Первый в отрасли шлюз с интегрированной системой безопасности с ИИ, 5G и Wi-Fi 6.



The image shows a black Quantum Spark 1500 Pro router with eight external antennas. The front panel features the Check Point logo and several status icons. Surrounding the router are callouts for its key features: Wi-Fi 6, 5G Cellular, AI powered security, Quantum SD-WAN, 2.8Gbps Firewall, 900Mbps Threat Prevention, and 2x Capacity & User Support.

**WiFi 6**  
4x better in dense environments

**5G**  
Cellular  
1Gbps throughput

**AI powered security**

**Quantum SD-WAN**  
Optimal App Performance

**2.8Gbps**  
Firewall

**900Mbps**  
Threat Prevention

**2x**  
Capacity & User Support

# Новый функционал в Quantum Spark R81.10.05

## Для локально управляемых шлюзов :

- Двухфакторная аутентификация через SMS и электронную почту для удаленных пользователей VPN (поддержка по всему миру)
- Простое развертывание и использование SSL inspection,
- Расширенная конфигурация кластера через WebUI
- Повышение производительности с помощью движка Smart Accel
- Утилиты диагностики Dr. Spark и Dr.Load

# Новый функционал в Quantum Spark R81.10.05

## Для филиалов предприятия (централизованно управляемые шлюзы)

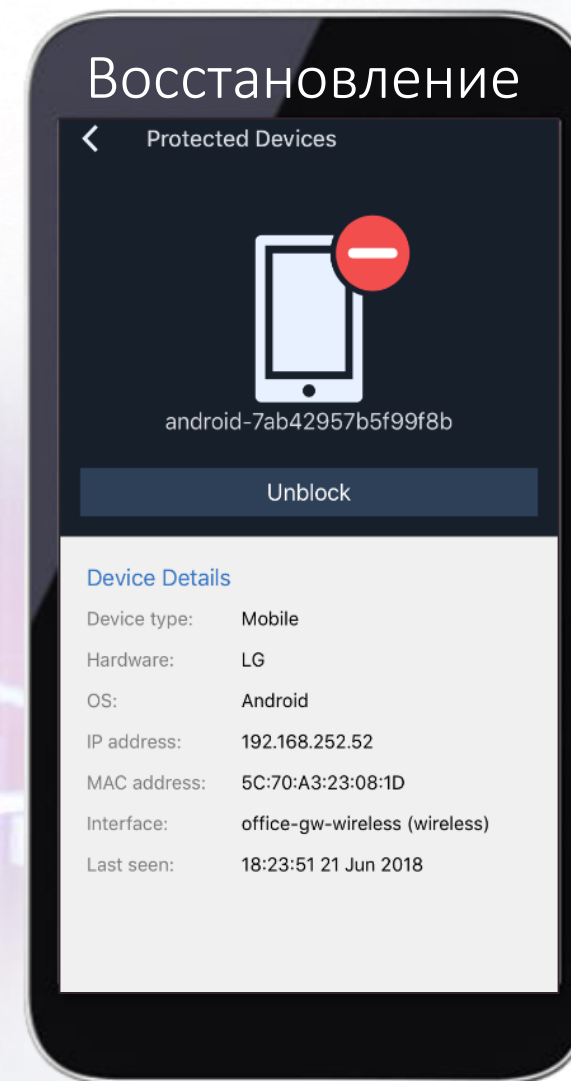
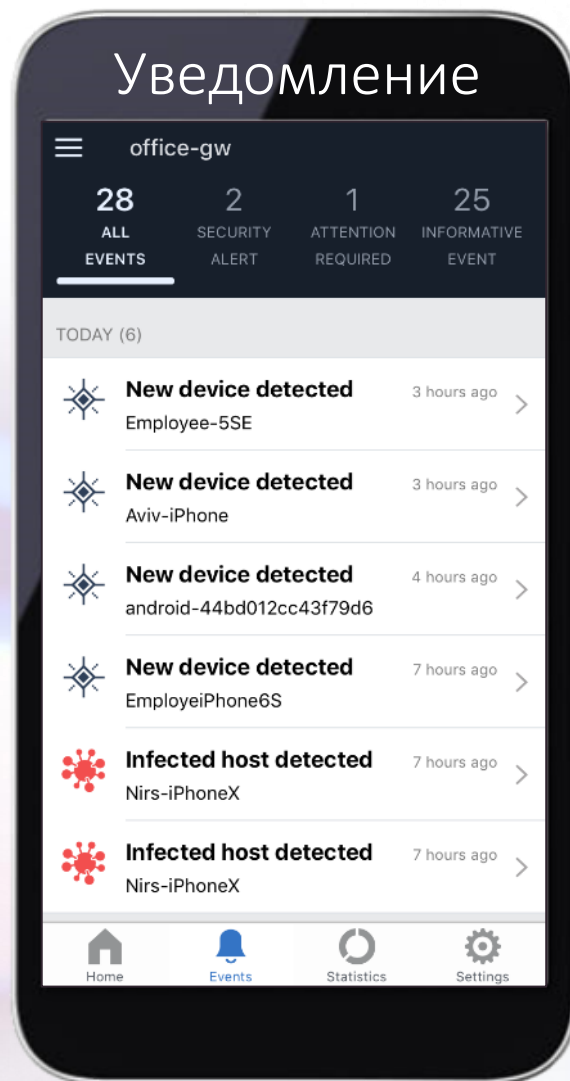
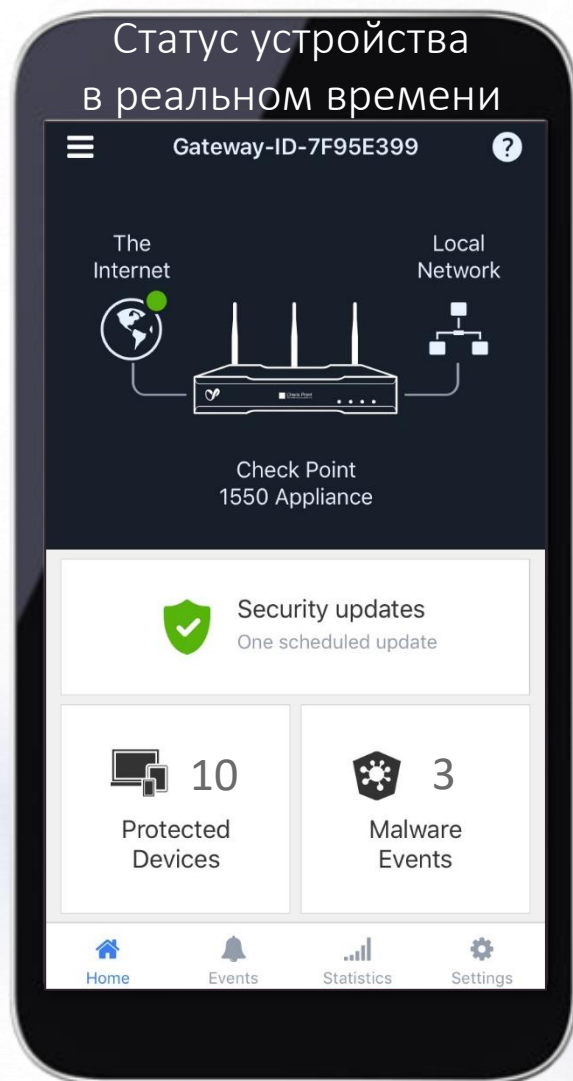
- SD-Wan
- IoT Protect

# ДОРОЖНАЯ КАРТА SPARK НА 2023 ГОД

## Планируемый функционал для R81.10.10

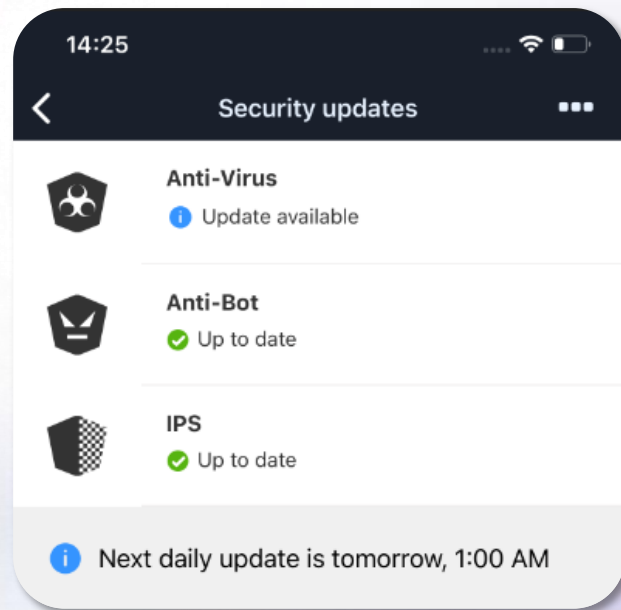
- GRE
- BGP IPv6
- OSPFv3 IPv6
- Поддержка Jumbo frame
- Google Authenticator 2FA
- Сброс пароля in WebUI
- Автоматическая блокировка зараженные хостов
- Работа с системой мониторинга Check Point Skyline
- Настройка 2FA «на пользователя»
- Threat Prevention Bypass при критической нагрузке
- Поддержка Cluster XL в Bridge Mode
- VPN мониторинг в Quantum Spark Management портале
- SD-WAN для локально управляемых шлюзов
- IoT для локально управляемых шлюзов

# Мобильное приложение WatchTower

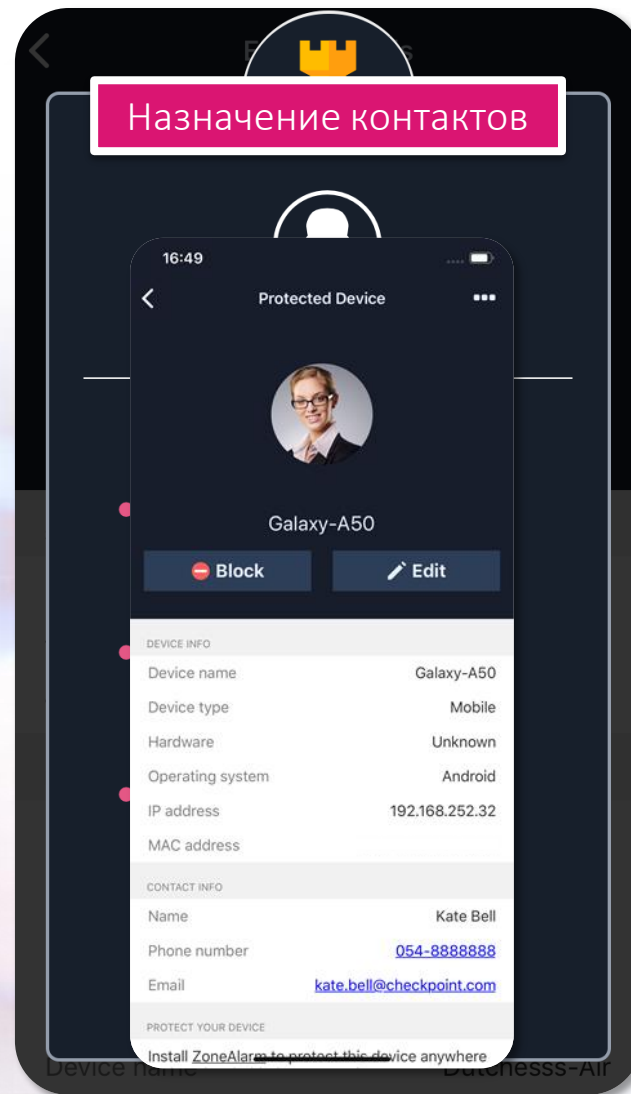


# Мобильное приложение WatchTower

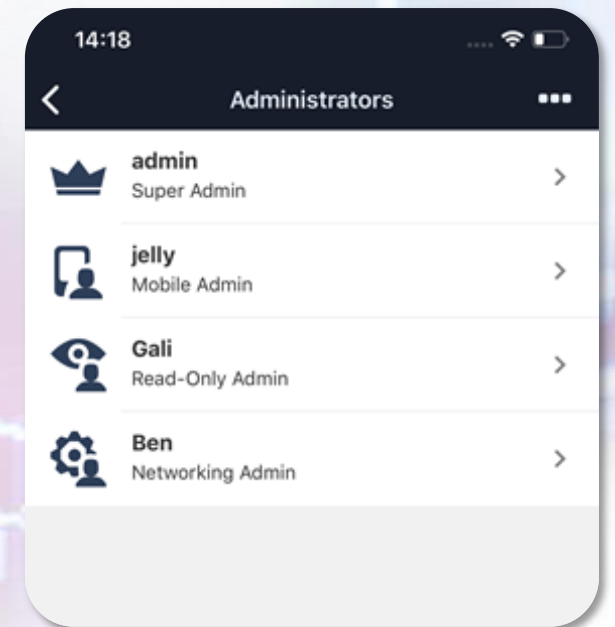
Статус обновлений



Назначение контактов



Расширенные возможности для администраторов



# Отчеты

Consolidated view of identified threats

Security status for entire system

283 Malwares Found by **Anti-Bot**

364 Malwares Found by **Anti-Virus**

3 Attacks Found by **IPS**

---

**Top Bandwidth Consuming**

- High Bandwidth | Top category  
47.2GB(28%) Bandwidth
- youtube.com | Top site  
31.6GB(19%) Bandwidth
- youtube.com | Top user  
31.6GB(19%) Bandwidth

130GB Total Received

40GB Total Sent

---

**Bandwidth Usage by Applications**

Total traffic: **170GB**

Top 5 Apps: **78.4GB**

15% YouTube	4% Facebook
12% Gmail	4% Kerberos Protocol
11% SSL Protocol	54% Other

---

**7 INFECTED HOSTS**

- 5 High\Critical infected Hosts
- 4 Infected Servers
- 7 Recently active infected hosts

**15 HIGH RISK APPLICATIONS**

- Most used high risk applications:** WinMX World, 3proxy.com, eMule, DroidVPN, more...
- Top users of high risk applications:** John A, Tim R, Dan B, Jill F, Beth D, Jeffie M, more...

Bandwidth usage by applications



# Быстрое развертывание

- Готовность к работе за 60 секунд
- Нет необходимости в техническом специалисте. Подключить, включить питание – и все готово



# Stay secure when out of the office

## Harmony Endpoint & Mobile

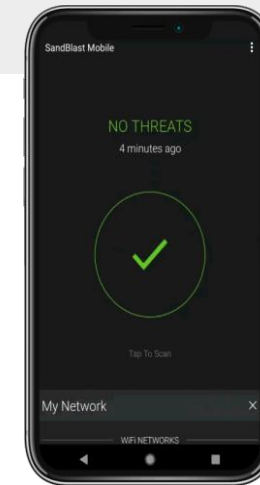


### Endpoint Security

- 1 Reduce the attack surface
- 2 Prevent zero-days
- 3 Block ransomware

### Mobile Threat Defense


- 1 Block Malicious Applications
- 2 Stop Network-based attacks
- 3 Real-time Device & OS risk assessment



# Infinity Spark Complete Security Package

Ove vendor for best SMB cyberattacks protection

1




**Quantum Spark 1550**  
Bundled for 10 Users

- 10 Endpoint Security Licenses
- 10 Mobile Security Licenses
- 10 Email & Office Licenses

**585 Mb/s Max Bandwidth**

2



**Quantum Spark 1570**  
Bundled for 25 Users

- 25 Endpoint Security Licenses
- 25 Mobile Security Licenses
- 25 Email & Office Licenses

**650 Mb/s Max Bandwidth**

3




**Quantum Spark 1590**  
Bundled for 50 Users

- 50 Endpoint Security Licenses
- 50 Mobile Security Licenses
- 50 Email & Office Licenses

**890 Mb/s Max Bandwidth**

4



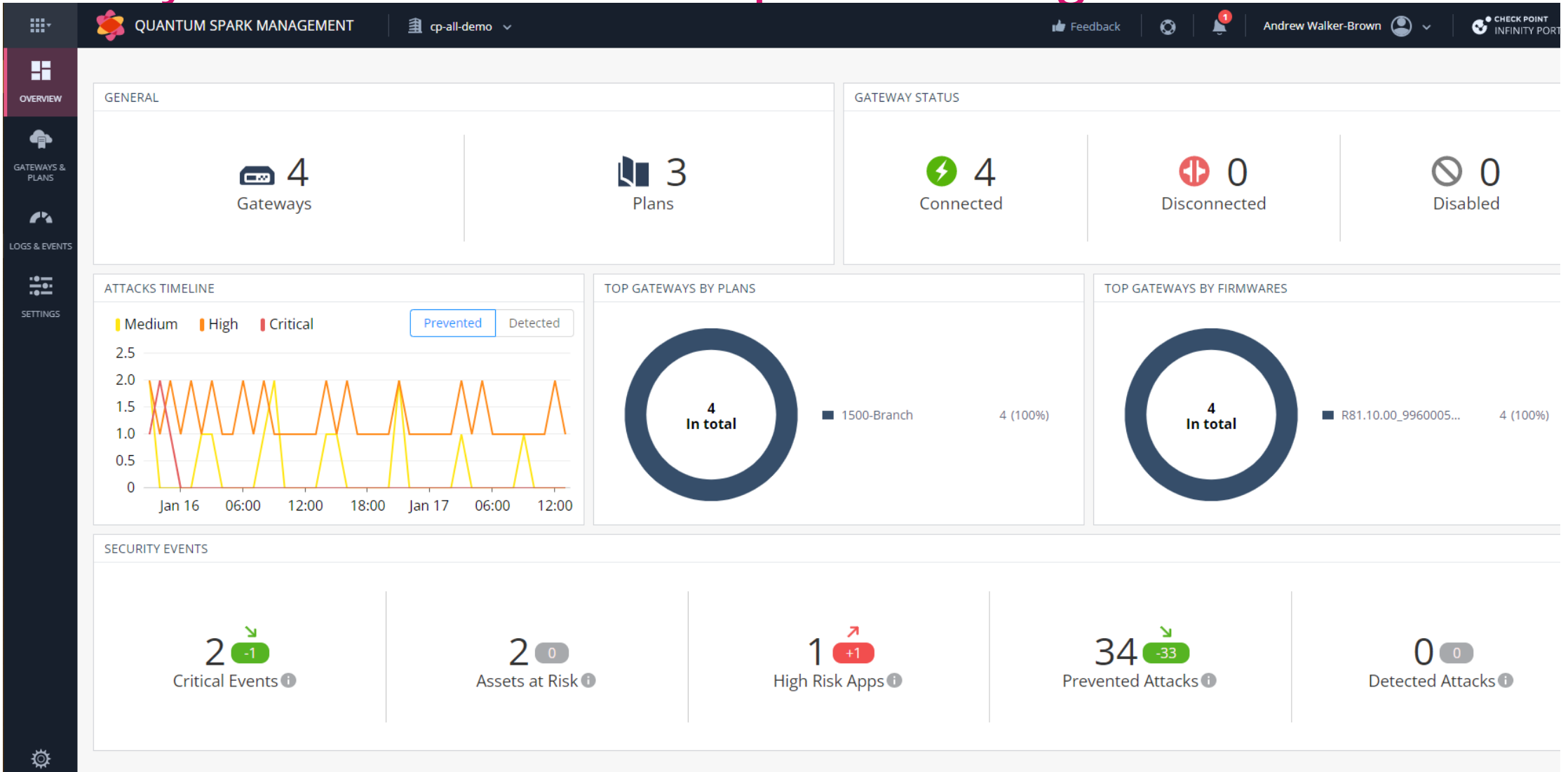
**Quantum Spark 1600**  
Bundled for 100 Users

- 100 Endpoint Security Licenses
- 100 Mobile Security Licenses
- 100 Email & Office Licenses

**2Gb/s Max Bandwidth**

Protect Your  
Network | Laptops & Mobile Devices | Email & Office Apps

# Infinity Portal - Quantum Spark Management



# Infinity Portal - Quantum Spark Management

QUANTUM SPARK MANAGEMENT | Solid-Lab.Space | Feedback | Alexander Kotelnikov

Overview | Gateways | Gateway Owners | **Map** | Plans | Logs & Events | Community | Settings

Search an address...  
Search a gateway... Go

- Connected (1)
- Disconnected (0)
- Disabled / External (0)

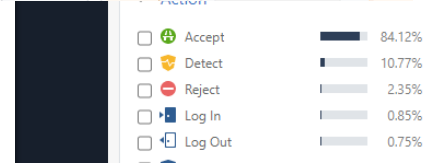
Auto fit map to results.

Last refresh: 20:35 | Auto refresh: Off

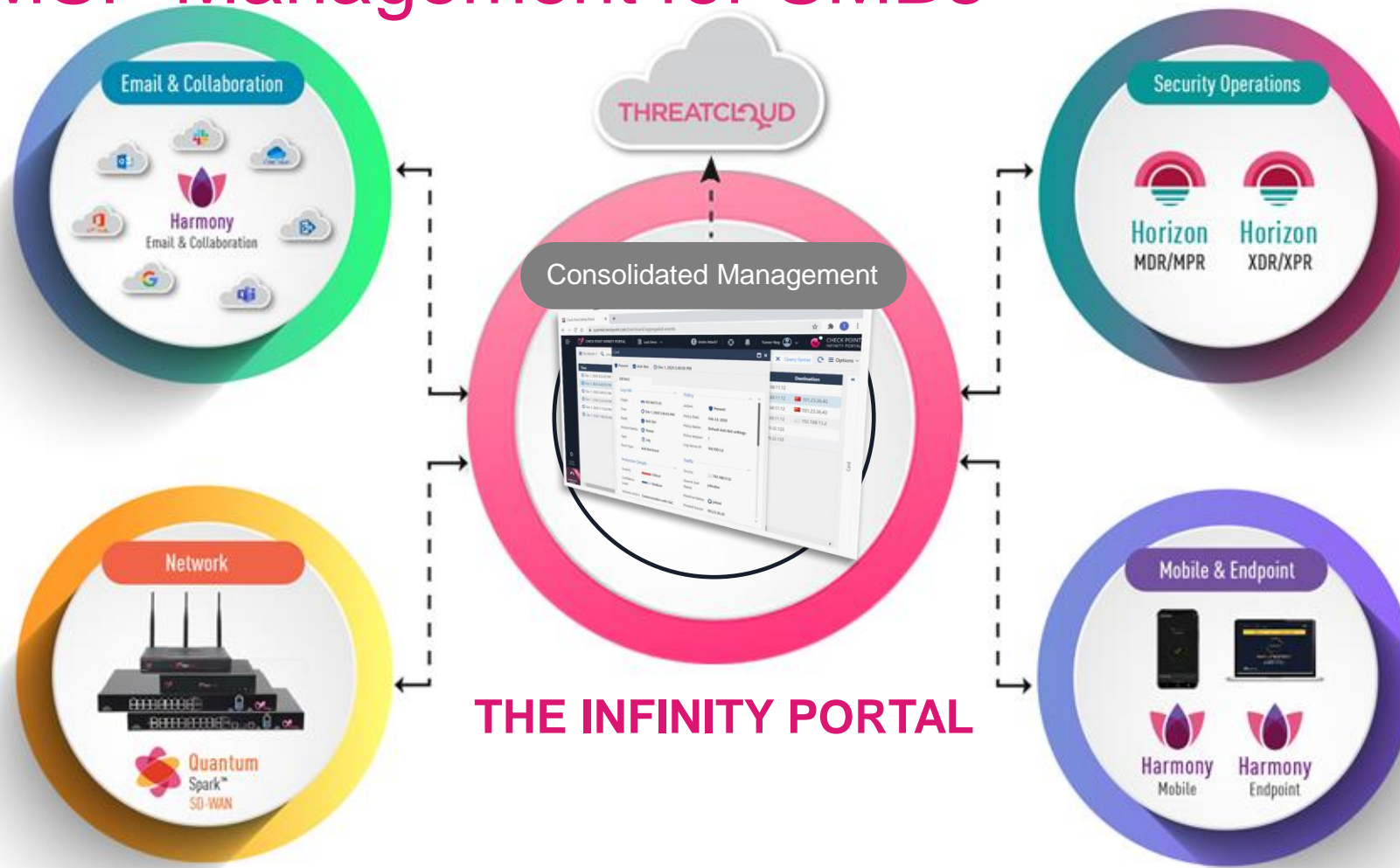
1 gateways retrieved (0 without location).

Prevented Attacks | Detected Attacks | Access (Preview)

Time	Gate...	Blade	Action	Type	Desti...	Interf...	Source	Desti...	Service	Origin	Rule ID	Rule ...	User	Proto...	Card
0	A...	cp-15...	U...	A...	S...		w...			cp-15...				HTTPS	Log Info
0	A...	cp-15...	U...	A...	S...		w...			cp-15...				HTTPS	Origin:
0	A...	cp-15...	U...	A...	S...	443	W...	192.1...	9...	HTTPS	cp-15...			HTTPS	Gateway Name:
0	A...	cp-15...	U...	A...	S...	443	W...	192.1...	9...	HTTPS	cp-15...			HTTPS	Service Domain:
0	A...	cp-15...	U...	A...	S...		w...			cp-15...				Unkn...	Gateway Mac Add
0	A...	cp-15...	U...	A...	S...		w...			cp-15...				HTTP	Time:
0	A...	cp-15...	U...	A...	S...	443	W...	192.1...	2...	HTTPS	cp-15...			HTTPS	Blade:
0	A...	cp-15...	U...	A...	S...		w...			cp-15...				Unkn...	Product Family:
0	A...	cp-15...	U...	A...	S...		w...			cp-15...				HTTP	Type:
0	A...	cp-15...	U...	A...	S...	443	W...	192.1...	3...	HTTPS	cp-15...			HTTPS	Traffic
0	A...	cp-15...	U...	A...	S...	443	W...	192.1...	1...	HTTPS	cp-15...			HTTPS	App Protocol:
0	A...	cp-15...	U...	A...	S...	443	W...	192.1...	2...	HTTPS	cp-15...			HTTPS	Session
0	A...	cp-15...	U...	A...	S...	443	W...	192.1...	5...	HTTPS	cp-15...			HTTPS	Creation Time:
0	A...	cp-15...	U...	A...	S...	443	W...	192.1...	6...	HTTPS	cp-15...			HTTPS	Duration:
0	A...	cp-15...	U...	A...	S...	443	W...	192.1...	1...	HTTPS	cp-15...			HTTPS	Number of conne.
0	A...	cp-15...	U...	A...	S...	443	W...	192.1...	1...	HTTPS	cp-15...			HTTPS	Policy
0	A...	cp-15...	U...	A...	S...	4244	W...	192.1...	5...	tcp-hi...	cp-15...			HTTPS	Action:
0	A...	cp-15...	U...	A...	S...	443	W...	192.1...	9...	HTTPS	cp-15...			HTTPS	Accounting
0	A...	cp-15...	U...	A...	S...	443	W...	192.1...	8...	HTTPS	cp-15...			HTTPS	
0	A...	cp-15...	U...	A...	S...	443	W...	192.1...	8...	HTTPS	cp-15...			HTTPS	
0	A...	cp-15...	U...	A...	S...	443	W...	192.1...	1...	HTTPS	cp-15...			HTTPS	
0	A...	cp-15...	U...	A...	S...	443	W...	192.1...	1...	HTTPS	cp-15...			HTTPS	



# Унифицированное управление Infinity MSP Management for SMBs



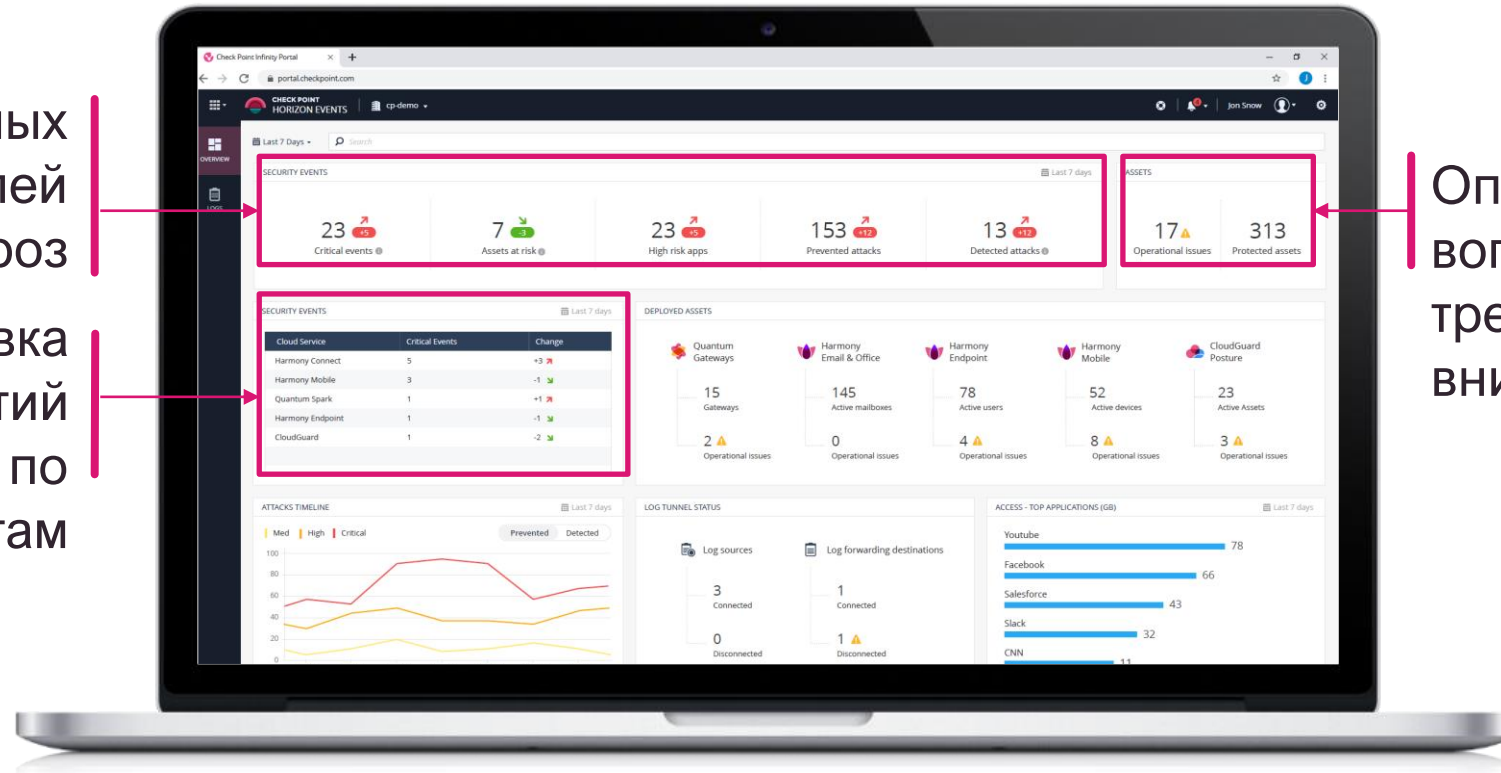
# Infinity Portal for MSP

## Полная видимость тенантов всех клиентов и их продуктов

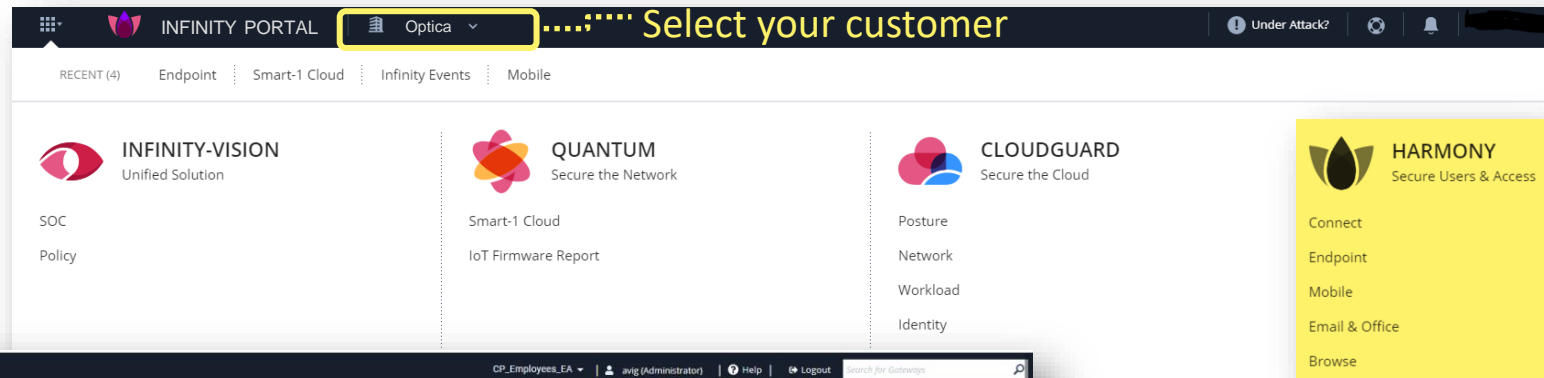
Обзор основных показателей безопасности и угроз

Разбивка критических событий безопасности по продуктам

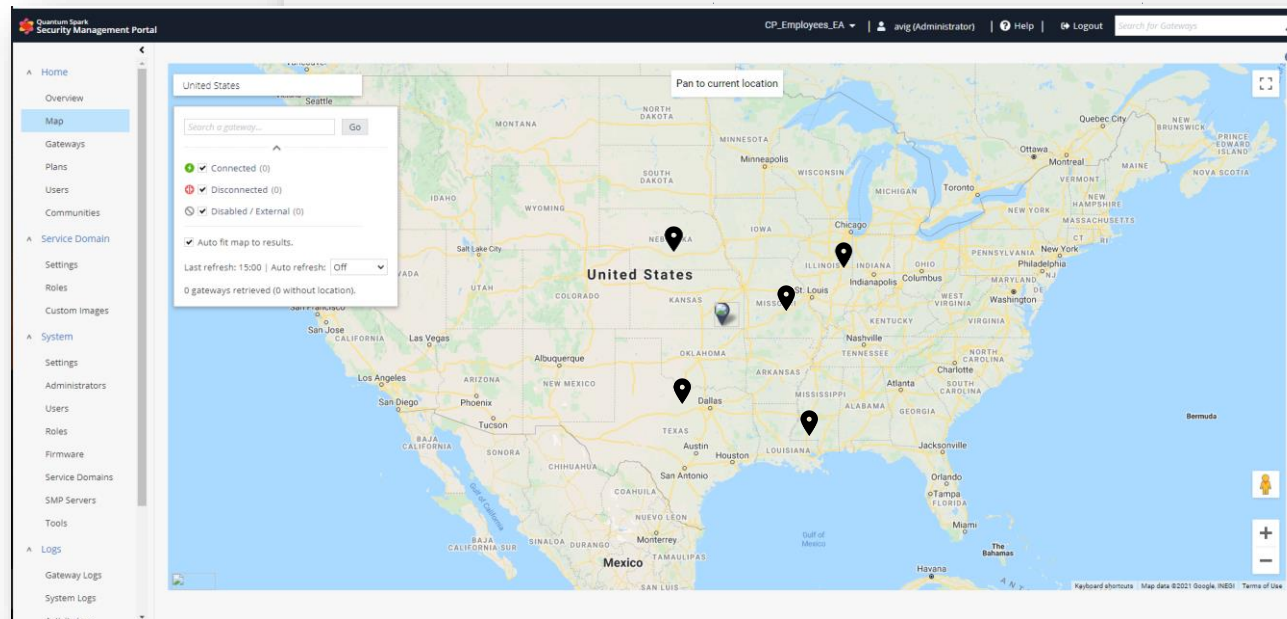
Операционные вопросы, требующие внимания



# Упрощение операций MSP с мульти-тенантным управлением в Infinity Portal



Manage your endpoints





# Pay-As-You-Go для безопасности SMB

Early Availability

1 No minimum order

2 Managed everything from Check Point Infinity Portal

3 Grow or remove users at any time

The screenshot displays the 'USAGE' section of the Check Point Infinity Portal for an account named 'Optica'. The interface includes navigation tabs for 'ACCOUNT SETTINGS', 'ADMINISTRATORS', 'SERVICES & CONTRACTS', and 'USAGE'. A dropdown menu shows 'This month'. There are buttons for 'License Report', 'Export', and a search bar. The main content is a table with the following data:

Service name	Package	Avg. monthly usage	Yearly contracts	Monthly PAYG
Harmony Mobile		100 Devices	200	-
CloudGuard Network		50 devices	-	50
Harmony Endpoint	-	355 users	325	30
Harmony Endpoint	BASIC	300 users	300	-
Harmony Endpoint	ADVANCED	55 users	25	30

# MSP: Быстрый старт

## \$0

Стоимость адаптации с полностью автоматизированной регистрацией, порталом самообслуживания и отчетностью

## Unlimited

Облачное управление предоставляется как SaaS (инвестиции в инфраструктуру не требуются)

## 60 Sec

Запуск у клиента  
Кастомизированная прошивка

**2 операционных сотрудника управляют 30000 клиентами**

# White labeling: шлюз, отчеты, Mobile App

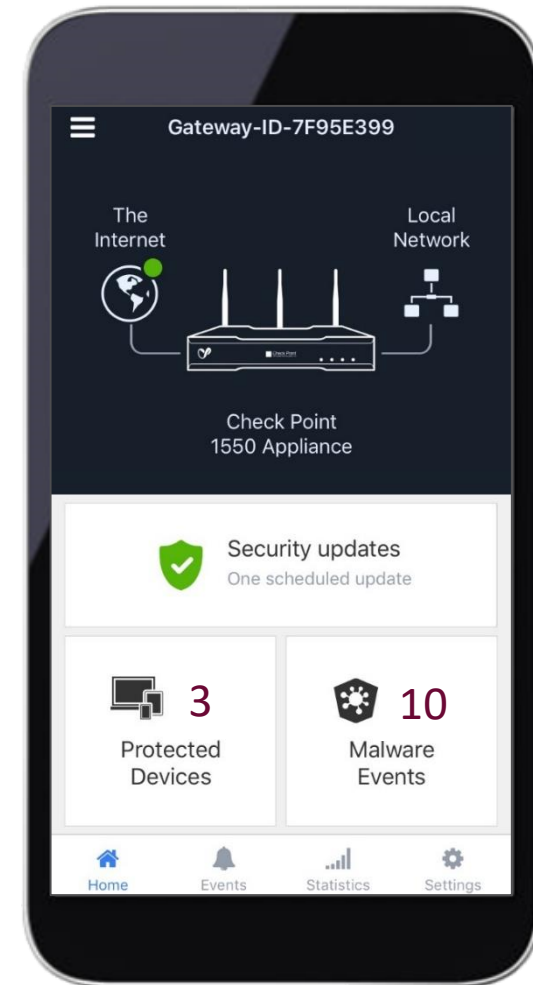


# White labeling: шлюз, отчеты, Mobile App

## Automated Reporting



## Mobile App



# CheckMe



PRODUCTS / SOLUTIONS

SUPPORT / SERVICES

PARTNERS

COMPANY

**Ransomware Attack**

**Identity Theft/Phishing**

**Browser Attack**

**Anonymizer Usage**

## ARE YOU PROTECTED?

CheckMe runs a series of simulations to test if your existing security technologies can block standard and advanced attacks.

CheckMe

GEN V

CHECK POINT INFINITY

Select Simulation Target(s):

- Zero Day Vulnerabilities**  
Network  
Bot Infections  
[More](#)
- Data Leakage**  
Endpoint  
Cloud  
Mobile  
[More](#)

Requires downloading & running an executable

\*Requires available infrastructure with internet connectivity

\*Requires app download

<http://www.cpcheckme.com/checkme/>

[sk115236](#)

# Check Point Security CheckUP – инструмент продаж, способ показать клиенту состояние безопасности сети

## Выявление рисков, угрожающих компании

- Анализ всего спектра рисков и угроз безопасности сети
- Подробный отчет с анализом обнаруженных угроз
- Рекомендации по защите сети от рисков



ОБСЛЕДОВАНИЕ РЕАЛЬНОЙ СЕТИ  
НИКАКОГО РИСКА ДЛЯ СЕТИ:

работа только с копией трафика

Оптимальный срок для прохождения **Security CheckUP** – 1-2 недели

[sk112732](#)

# SECURITY CHECKUP

## THREAT ANALYSIS REPORT

<https://pages.checkpoint.com/security-checkup.html>

Дата  
Подготовлено  
для  
Кем  
подготовлено

Отрасль  
Размер компании  
Страна

Продолжительность анализа  
Анализ сети  
Версия шлюза безопасности  
Устройство безопасности

Трафик пр

### ИТОГОВЫЕ РЕЗУЛЬТАТЫ

SECURITY CHECKUP

Следующий отчет Security Checkup предоставляет результаты оценки безопасности, проведенной в вашей сети. Данный отчет указывает места, где ваша организация может быть подвержена угрозам безопасности, а также предлагает рекомендации по реагированию на данные риски.

Для оценки риска трафик был проверен Check Point для обнаружения ряда угроз безопасности, включая: заражение вредоносным ПО, использование веб-приложений высокой степени риска, попытки вторжения, утечка важных данных и т.п.

#### Интернет доступ высокой степени риска

**5** опасных веб-приложений

**2.2GB**

Потенциальные риски: открытие бэкдоров в вашу сеть, сокрытие пользовательской активности, возможность утечки данных или заражения вредоносным ПО.

**0** опасных веб-сайтов

**0** hits

Потенциальные риски: Подверженность сети к Интернет угрозам и заражению вредоносным ПО. Примеры: СПАМ, зараженные и фишинговые сайты.

**0** Облачные приложения

**0B**

Риск утечки данных и нарушение соответствия требованиям регуляторов и стандартов безопасности. Примеры: Dropbox, Google Drive, OneDrive.

#### Утечка данных

**49** потенциальных утечек данных

**7** категорий данных

Отображает информацию, отправленную за пределы сети компании или неавторизованным сотрудникам внутри компании.

#### Вредоносное ПО и атаки

**7** зараженных ботами компьютеров

**19** communications with C&C\* sites

\* C&C - командный центр управления. Если используется прокси-сервер, то число зараженных компьютеров на деле может быть больше.

**14** известных вирусов, зашруженных

**8** пользователей

**14** новых вирусов загружено

Новая модификация вредоносного ПО - это атака 0 000 000 000000000000 000 неизвестной еще для антивируса сигнатурой.

**18** попыток использовать уникальные программные уязвимости

Отображает потенциальные атаки на компьютеры в вашей сети.

© Check Point Software Technologies Ltd. All rights reserved. Classification: [Restricted] ONLY for designat

# Непревзойдённая безопасность для SMB



	CHECK POINT	FORTINET	SONICWALL	WatchGuard	SOPHOS	CISCO Meraki
Unified Cloud Management	✓	●	●	●	✓	●
Complete SMB Security Suite – Network, Endpoint, Mobile, Cloud SaaS	✓	●	●	●	●	●
Flexible Payment Options for SMBs	✓	●	●	✓	●	●
Integrated Wi-Fi 6	✓	●	●	●	●	●
Integrated 5G	✓	●	●	●	●	●



# NEXT STEPS...



01

Стать партнёром с SMB специализацией:

<https://www.checkpoint.com/partners/channel/>

02

Пройти наш бесплатный SMB-Jump Start and Harmony Endpoint курс:

[Partner Training](#)

03

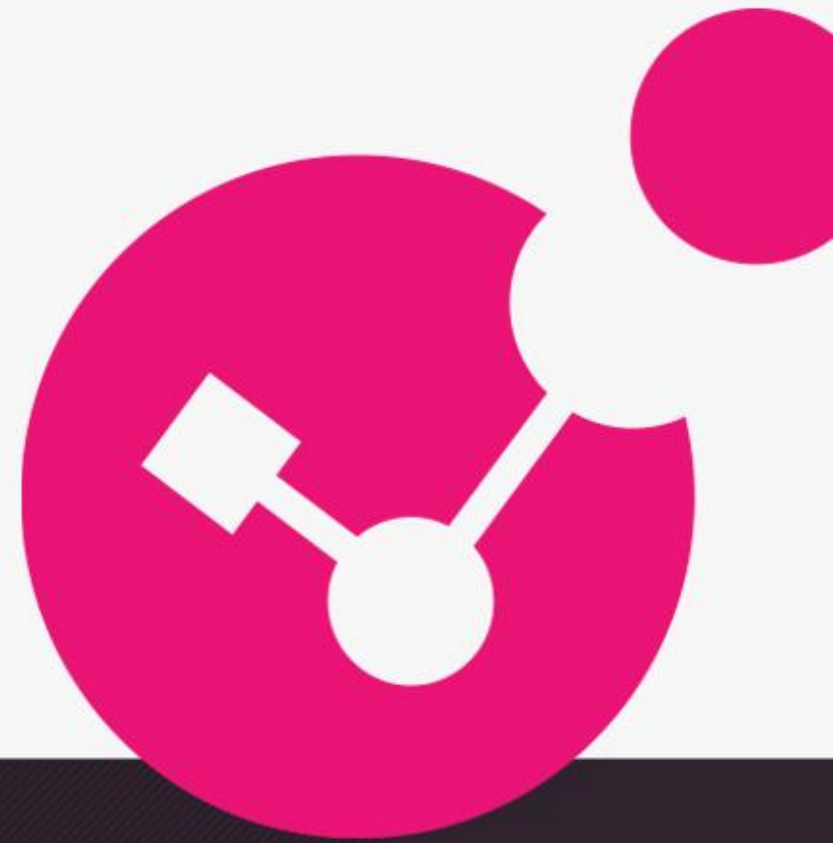
Посетить [страницу продуктов SMB](#)



Спасибо!

Котельников Александр | Security Engineer

[akotelnikov@checkpoint.com](mailto:akotelnikov@checkpoint.com)



YOU DESERVE THE BEST SECURITY