



QUANTUM SECURITY GATEWAY

Обновления 2023

Дмитрий Махоткин | Channel SE

dmitryma@checkpoint.com

YOU DESERVE THE BEST SECURITY

ОБНОВЛЕНИЕ ПО



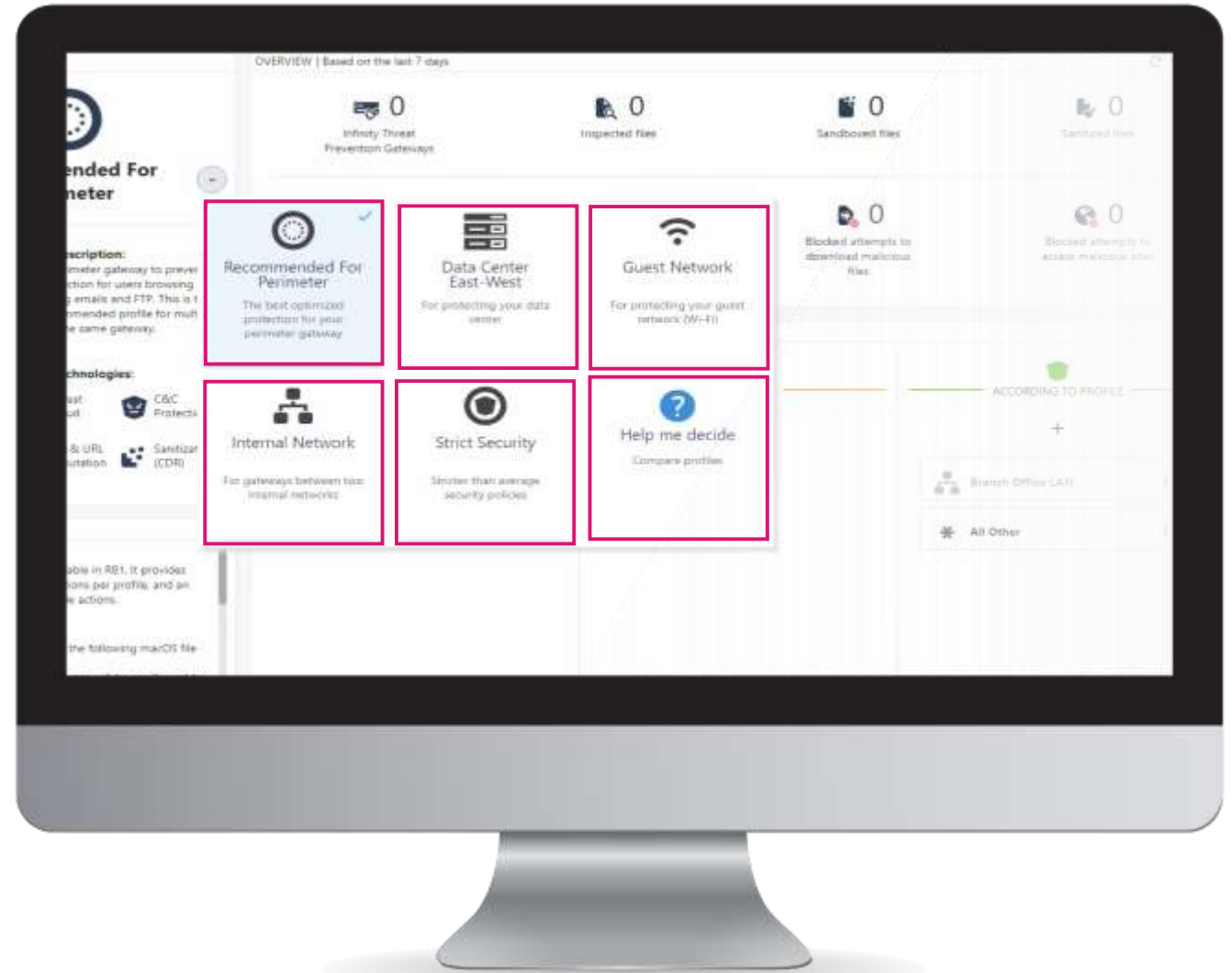


Best Security with Industry's First Autonomous Threat Prevention

ПОЛИТИКИ БЕЗОПАСНОСТИ
НА ОСНОВЕ AI

НАСТРОЙКА В ОДИН КЛИК

ПОЛИТИКИ АВТОМАТИЧЕСКИ
ОБНОВЛЯЮТСЯ В РЕАЛЬНОМ
ВРЕМЕНИ



“We **cut the time** we spend on **managing security** by **80%**, thanks to the **simplicity** of the Check Point solution!”



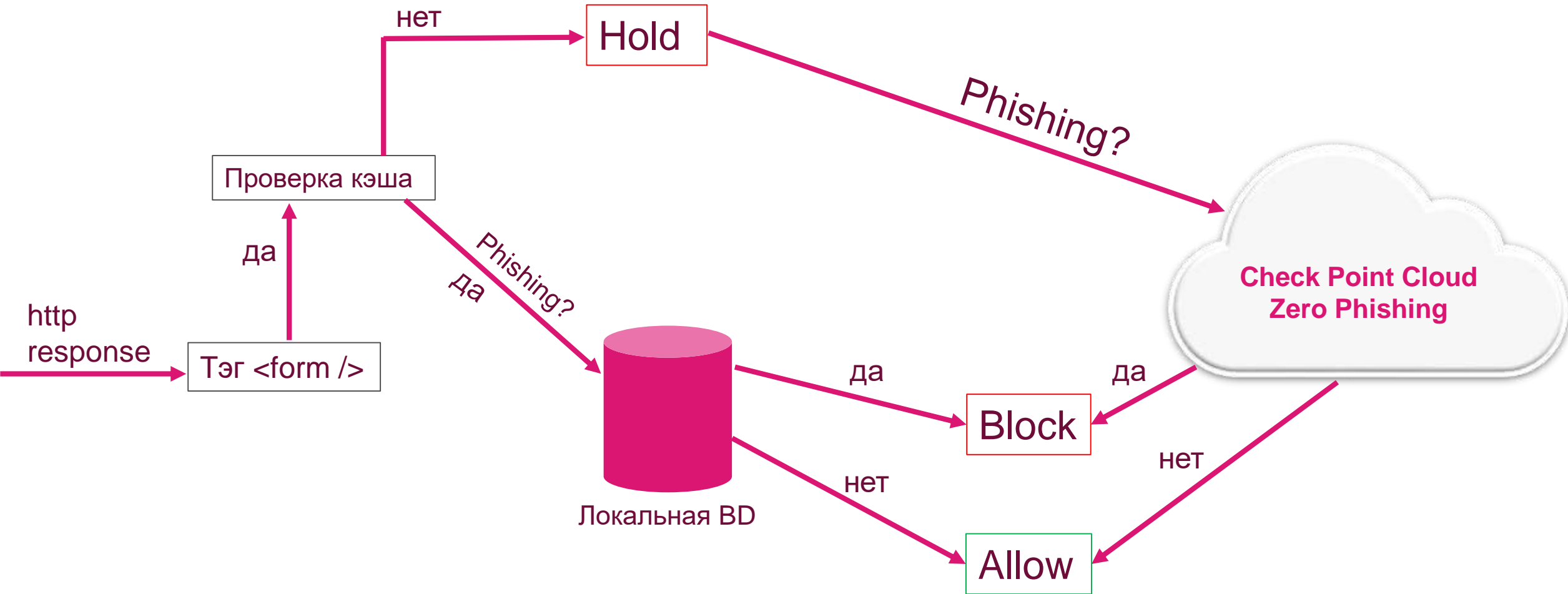
НОВЫЙ БЛЕЙД

ZERO-PHISHIG R81.20

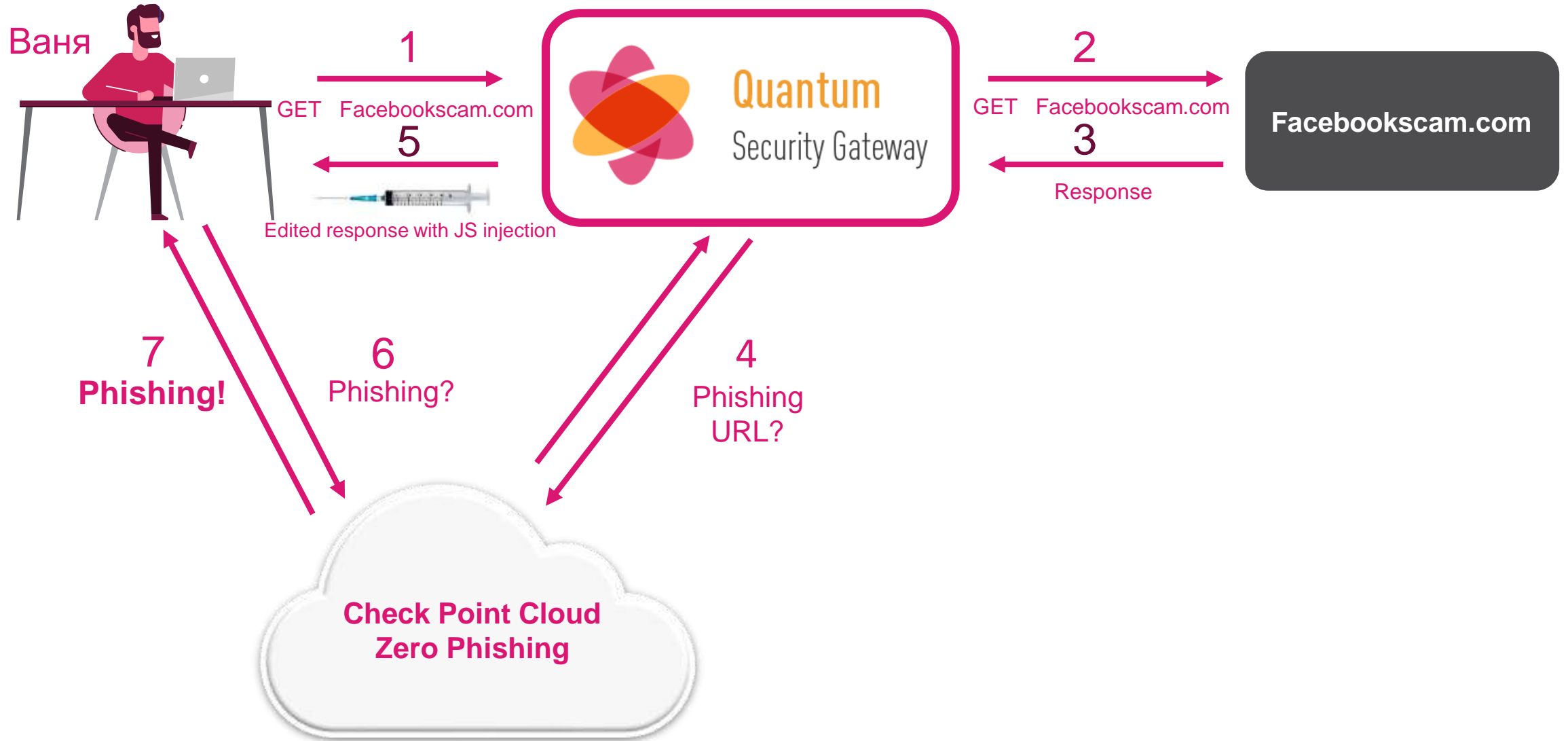
Zero-phishing New Software blade on R81.20

- Защита на основе URL
 - Анализирует URLs, проходящие через шлюз;
 - Анализирует HTML страницы, содержащие тэг <form />;
 - URL проверяются облачными сервисами Check Point.
- Zero-phishing на уровне браузера
 - Javascript инъекция в каждую HTML страницу;
 - Скрипт активируется, когда пользователь кликает на активные элементы;
 - Скрипт отправляет метаданные HTML страницы на анализ в облачные сервисы Check Point.

URL based protection



Inline Zero Phishing (запатентовано)



Zero-phishing blade

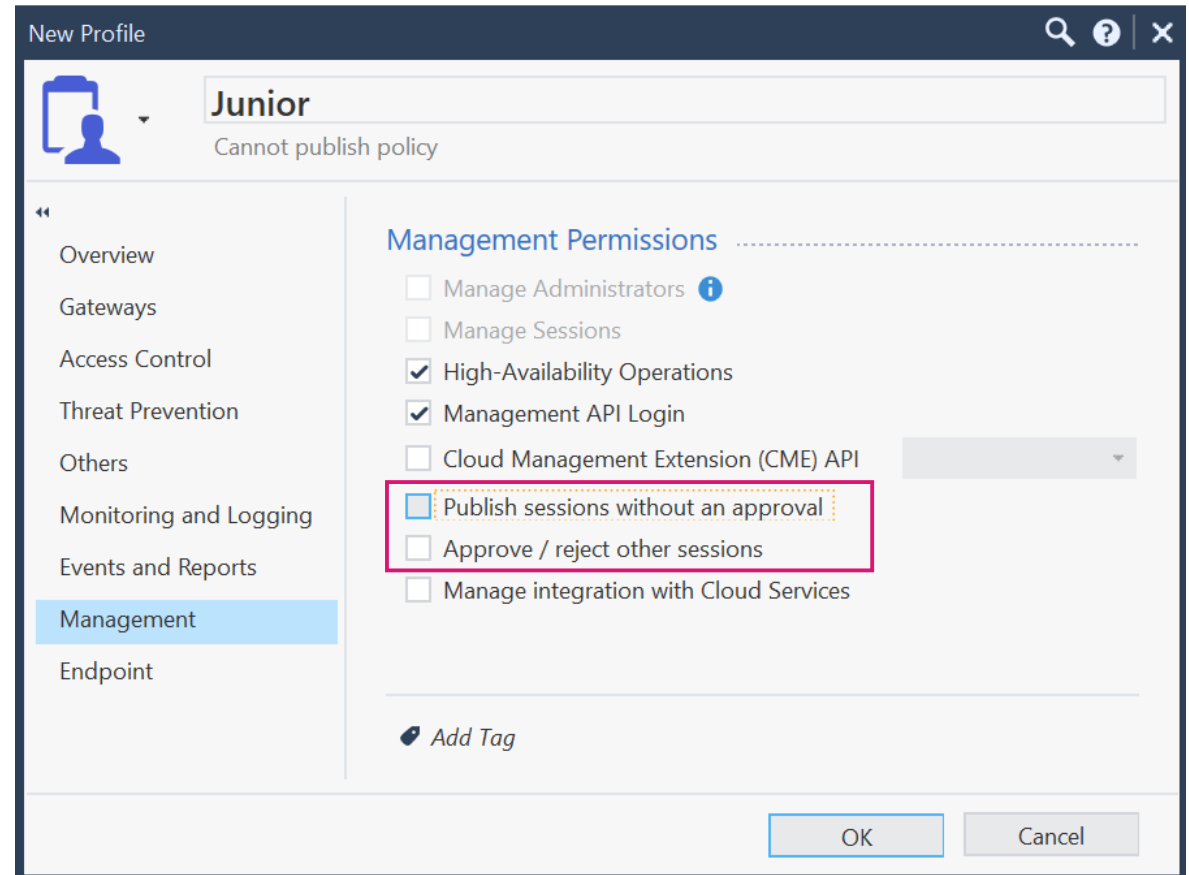
- URL based protection
 - Активен в автономных профилях Perimeter и Strict;
 - Активен всегда, когда активен сам блейд (нельзя выключить).
- In-Browser Zero-phishing
 - Отключен в автономных профилях по умолчанию;
 - Можно выключить в настройках профиля;
- Для активации нужна NGTX лицензия
- Влияние на производительность менее 1%

Smart Workflow

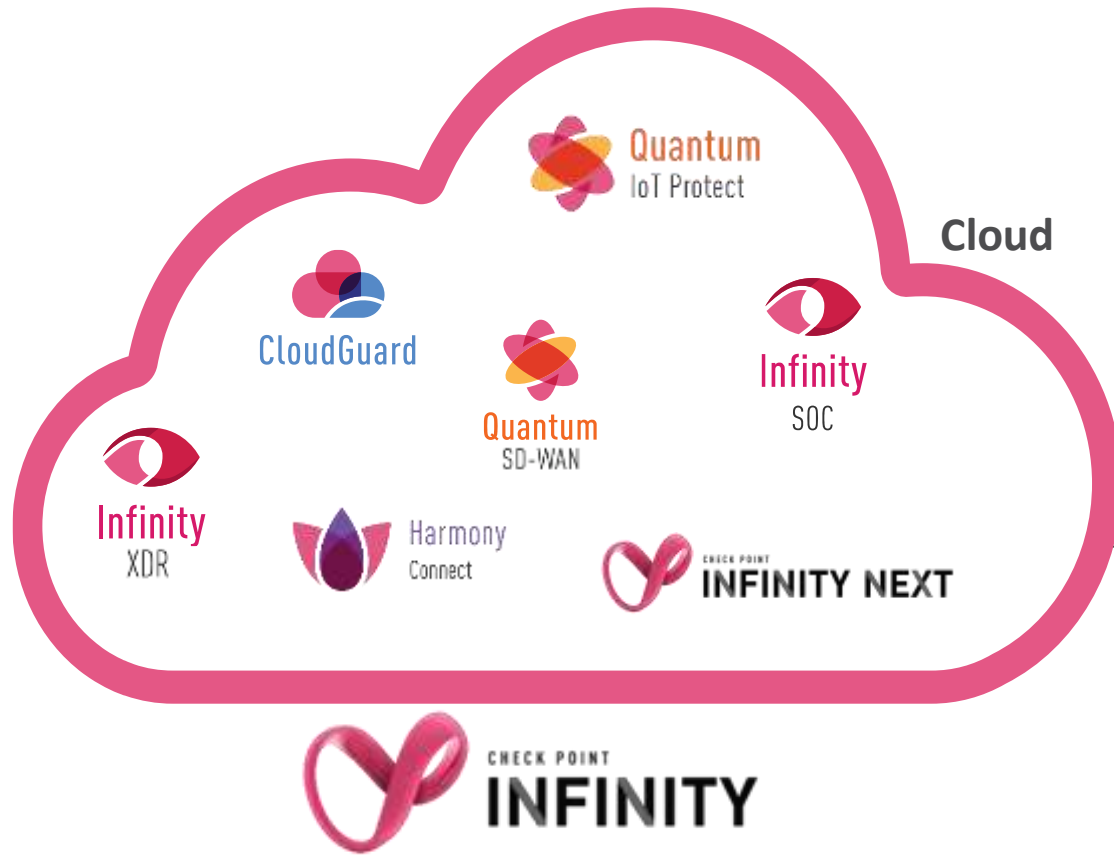
НОВЫЕ РОЛИ БЕЗ ПРАВ
ПУБЛИКАЦИИ ПОЛИТИКИ

ПУБЛИКАЦИЯ ПОЛИТИКИ
ТОЛЬКО ПОСЛЕ РЕВИЗИИ
АДМИНИСТРАТОРА

АДМИНИСТРАТОР ПОЛУЧАЕТ
УВЕДОМЛЕНИЕ ПО ПОЧТЕ
SMARTTASK



Интеграция с INFINITY SERVICES



Обеспечивает интеграцию on-prem инсталляций и облачных сервисов Check Point

On-premises





Quantum
IoT Protect



БЕЗОПАСНОСТЬ ИНТЕРНЕТА ВЕЩЕЙ

IoT Protect в шлюзах безопасности Quantum

IoT устройства – это риск



«Невидимые»



Используют
устаревшие ОС



Нет встроенной
безопасности



Сложно патчить

Слабые пароли



QUANTUM IoT PROTECT

АВТОНОМНЫЙ THREAT PREVENTION ДЛЯ ВСЕХ IOT УСТРОЙСТВ



АВТОМАТИЧЕСКОЕ
ОБНАРУЖЕНИЕ ВО
ВСЕХ ШЛЮЗАХ
QUANTUM



АВТОНОМНЫЕ
ZERO-TRUST
ПОЛИТИКИ & THREAT
PREVENTION



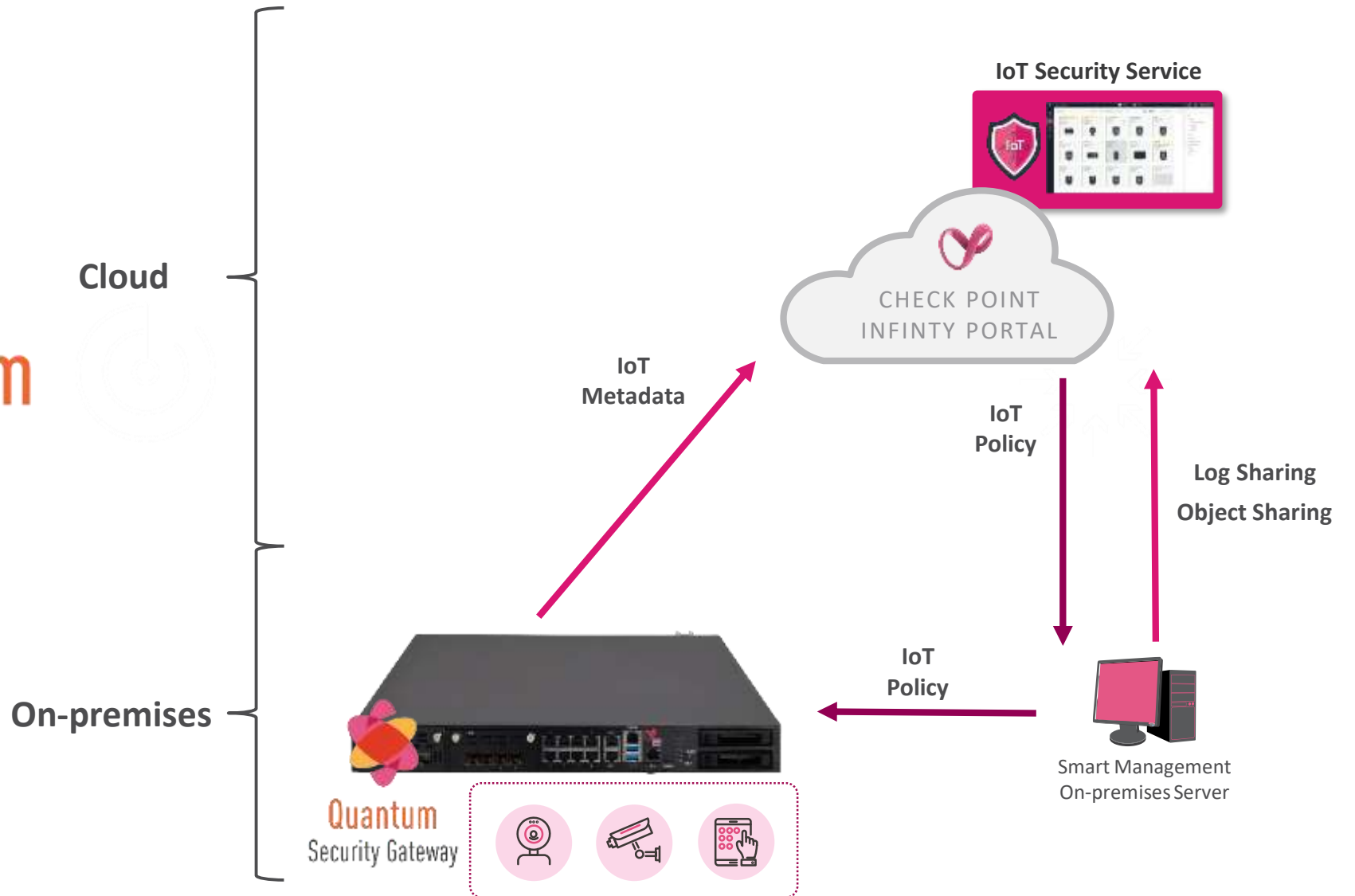
УПРАВЛЕНИЕ
И МОНИТОРИНГ ИЗ
ЕДИНОЙ КОНСОЛИ

QUANTUM IoT PROTECT

АРХИТЕКТУРА



100% технологии
Check Point



Политики контроля доступа и Zero Trust

- Автономные политики применяются автоматически, их видно в SmartConsole
- Разрешаются только легитимные соединения. Решение принимается на основе AI и поведенческого анализа
- Контроль доступа на основе: destinations, applications and services

The screenshot displays the 'Printers' configuration page in SmartConsole. The 'ACCESS CONTROL' tab is active, showing a policy named 'IoT Best Practice' with a mode of 'Prevent'. Below this, the 'Access to internet' section is expanded, showing a policy that restricts discovered printers to only approved destinations. A table lists these approved destinations:

Name	Destination	Service	Description
Brother			
Canon			
HP			
Notification	*hpeprint.com	HTTP HTTPS HP ePrint Service Jabber	Registration and getting notifications about pending printing tasks
Registration and pulling tasks	*hp.com	HTTP HTTPS Jabber	Registration, device configuration, pulling printing tasks and analytics
Telemetry and analytics	download.hpdaas.com	HTTP	Registration, device configuration, pulling printing tasks and analytics

Additional text in the interface includes: 'Discovered printers will be able to access only approved destinations (traffic to other destinations will be blocked)' and 'Traffic to other destinations will be blocked'.

Защита IoT в реальном времени

10,000+ сигнатур для IT и IoT

300+ сигнатур для промышленных систем

Обновления политик в реальном времени



Protection	Severity
OMRON CX-One CX-FLnet Type Heap-based Buffer Overflow	High
OMRON CX-One CX-FLnet Version and Node Name Heap-based Buffer Overfl...	High
OMRON CX-One CX-Position module Buffer Overflow (CVE-2018-18993)	High
OMRON CX-One CX-Programmer Program Use after Free (CVE-2019-6556)	High
OMRON CX-One CX-Protocol CMessage Type Confusion	High
OMRON CX-One CX-Protocol Trace Type Confusion	High
OMRON CX-One CX-Protocol Type Confusion (CVE-2018-19027)	Critical



Quantum
SD-WAN

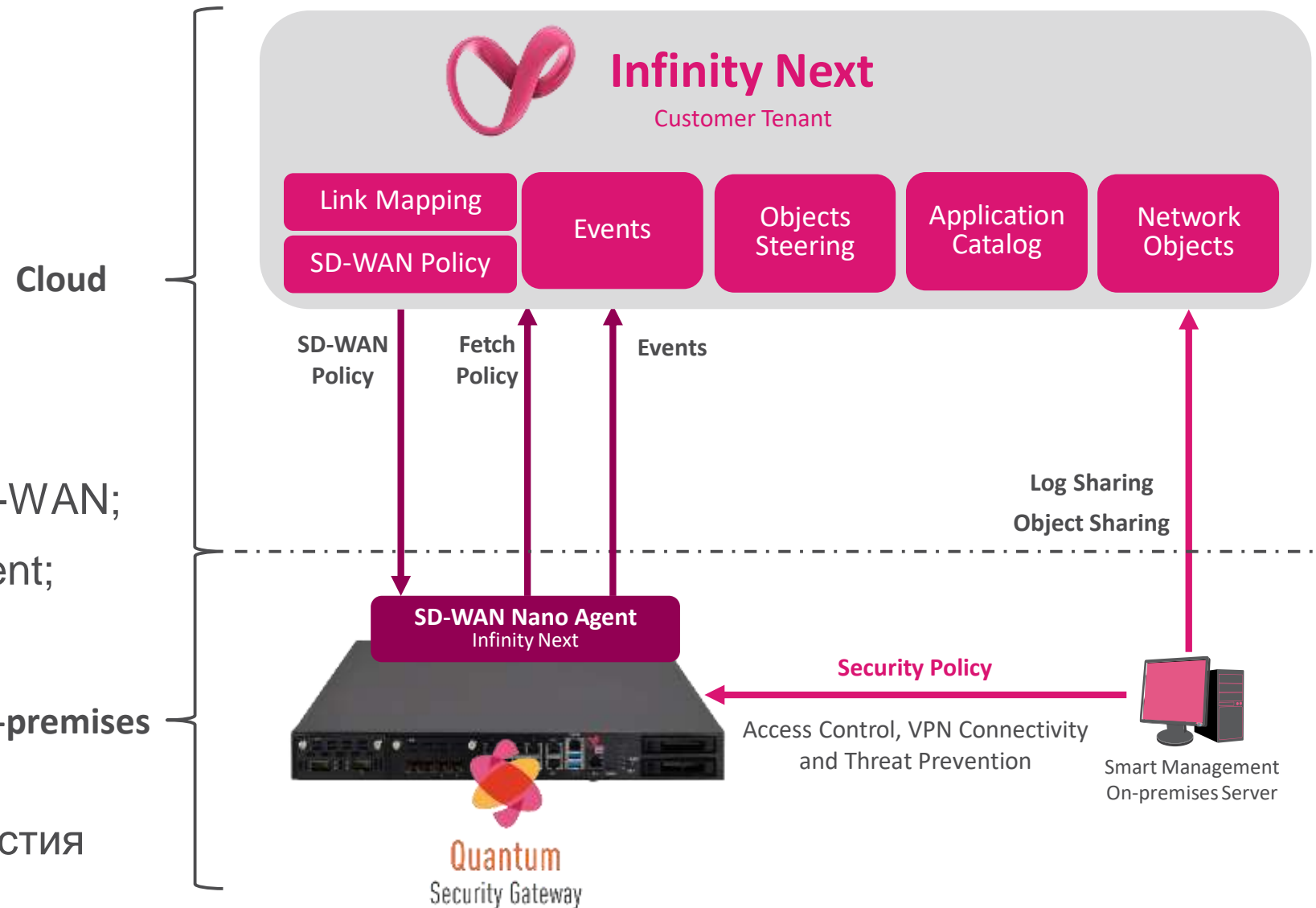


БЕЗОПАСНОСТЬ + SD-WAN

SD-WAN встроен в шлюзы безопасности Quantum

Check Point Quantum SD-WAN Архитектура

- Smart Management
 - Управляет политиками безопасности;
 - Синхронизируется с Infinity Next;
- Infinity Next
 - Управляет политикой SD-WAN;
 - Работает через Nano Agent;
- Nano Agent
 - Применяет политику SD-WAN на шлюзе;
 - Устанавливается без участия администратора.



ПОЛИТИКА SD-WAN

#	Name	Source	Destination	Services & Applications	Behavior
1	Business Application - Loc...	All_Sites	Internet	Microsoft Dynamics CRM, Salesforce	Business Applications Local Br...
2	Video Conference - Local ...	All_Sites	Internet	Zoom, Cisco Webex Teams, Microsoft Teams, Zoom_data_880	Video Conference
	File Sharing - Local Break...	All_Sites	Internet	Box, Dropbox, Google Drive-enterprise, Microsoft OneDrive	File Sharing Local Breakout
	Speedtest	All_Sites	Internet	Fast, FCC Speed Test	Max. Bandwidth
	Remote Desktop	All_Sites	All_Sites	GoToMyPC (Remote Desktop), Microsoft Remote Desktop Con..., Microsoft SMS Remote Control...	Low Latency
6	Default Local Breakout	All_Sites	Internet	Any	Default Local Breakout
7	Default Overlay	All_Sites	All_Sites	Any	Default overlay

Пользователи,
хосты, сети

8К+ приложений
и сервисов

Управление
трафиком:

- Сеть: Overlay или Интернет
- Как измерять качество канала
- Допустимый SLA
- Каналы связи

СЕТЬ OVERLAY

01

Соединяет ЦОД и филиалы

Топология Hub-and-Spoke
(в следующих релизах Meshed)

02

Улучшает UX

Эффективно использует полосы пропускания каналов, выбирает оптимальный маршрут, переключается между каналами за доли секунды

03

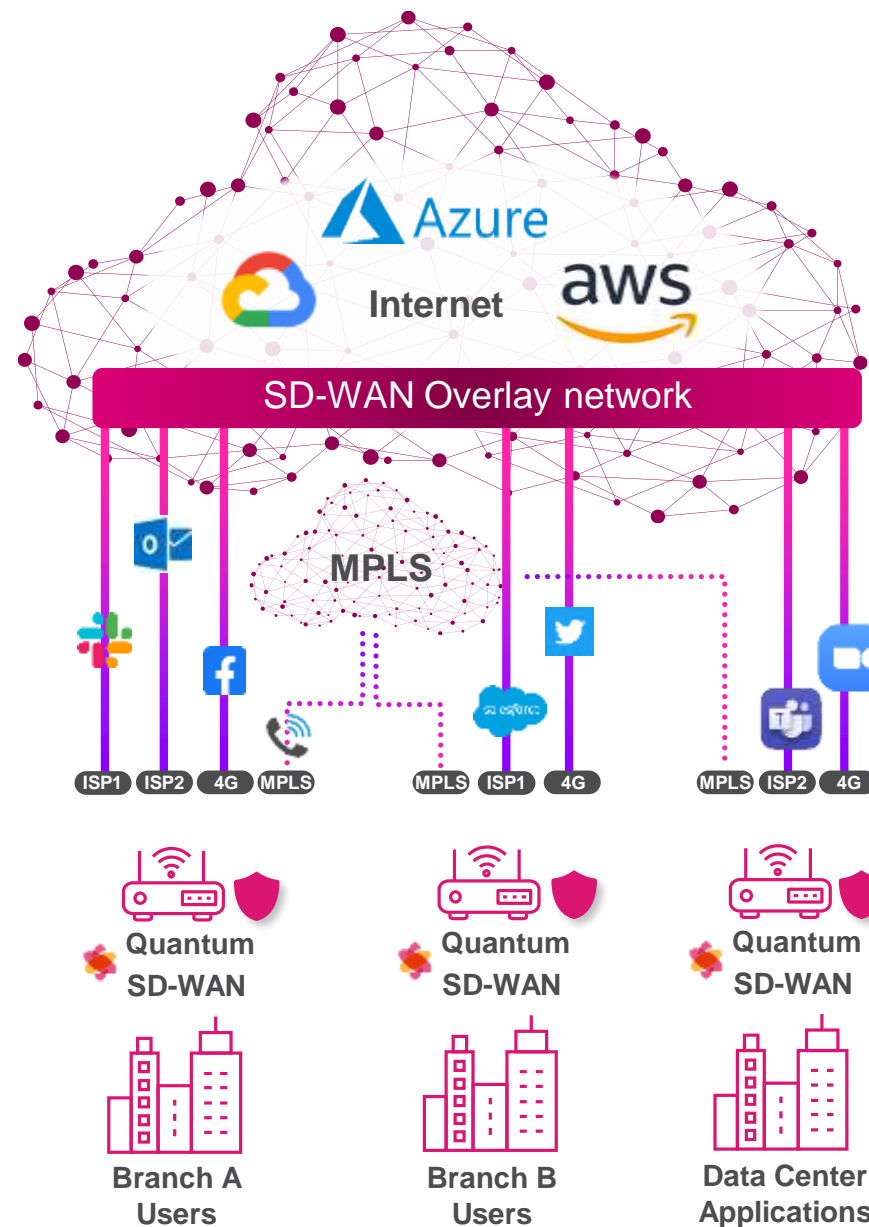
Application-based

Правила для каждого приложения

04

Обеспечивает безопасность

Все соединения защищены
IPsec VPN



ВОЗМОЖНОСТИ SD-WAN


УПРАВЛЕНИЕ ТРАФИКОМ

Простая настройка политик управления трафиком

Лучший маршрут выбирается на основе:
Latency, Jitter, Packet-Loss

Бесшовное переключение между каналами
связи для Overlay сети

Steering

 Name * Video Conference

Comment Optimized connectivity for Zoom, Teams

STEERING CANDIDATES CRITERIA

Connection Type

- Local breakout
- Overlay - VPN & MPLS

Steering Candidates

- All Relevant WAN Links
- Specific WAN Links

ИСПОЛЬЗУЙТЕ СУЩЕСТВУЮЩИЕ ШЛЮЗЫ



Не требует
НОВОГО
оборудования



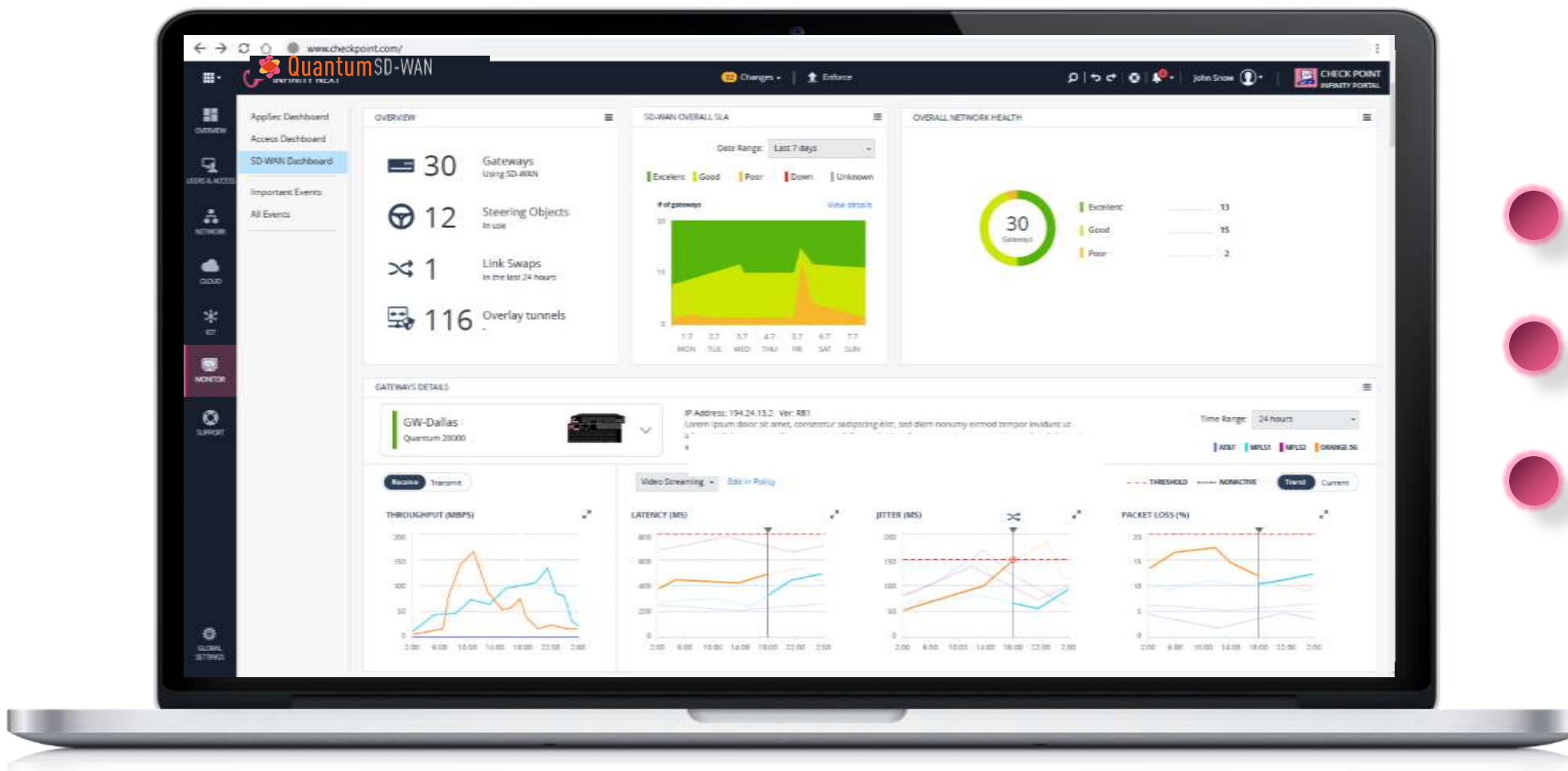
Quantum
SD-WAN



Разворачивается
за минуты

SD-WAN MONITORING DASHBOARD

Доступен в облаке Infinity Next



- SLA мониторинг в реальном времени
- Аналитика переключения каналов связи
- Общая статистика



СПАСИБО ЗА ВНИМАНИЕ

Дмитрий Махоткин | Channel SE

dmitryma@checkpoint.com

YOU DESERVE THE BEST SECURITY