



Check Point[®]
SOFTWARE TECHNOLOGIES LTD

НОВАЯ МОДЕЛЬ ПОТРЕБЛЕНИЯ РЕШЕНИЙ ИБ – ПОДХОД CHECK POINT

Sergey Zabula | Channel SE Team Lead, Check Point Russia

szabula@checkpoint.com



Возникающие сложности у предприятий

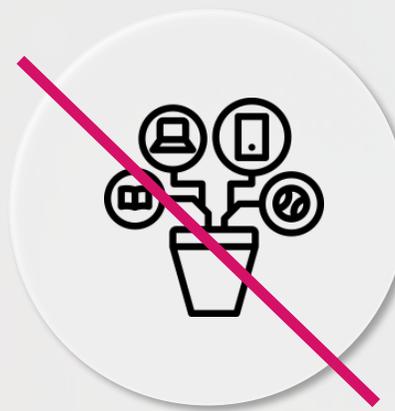
Устаревшие
решения



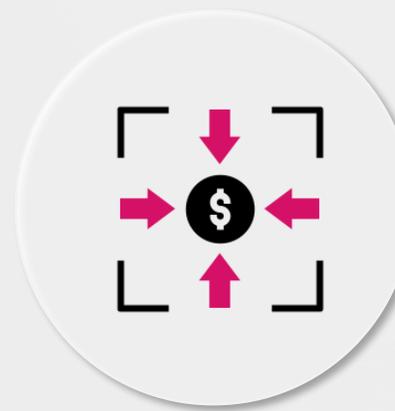
Нужна защита
новых технологий



Не хватает
ресурсов



Бюджет
ограничен



Пандемия всё меняет

01

УДАЛЕННАЯ
РАБОТА

02

ФОКУС
НА КЛИЕНТЕ

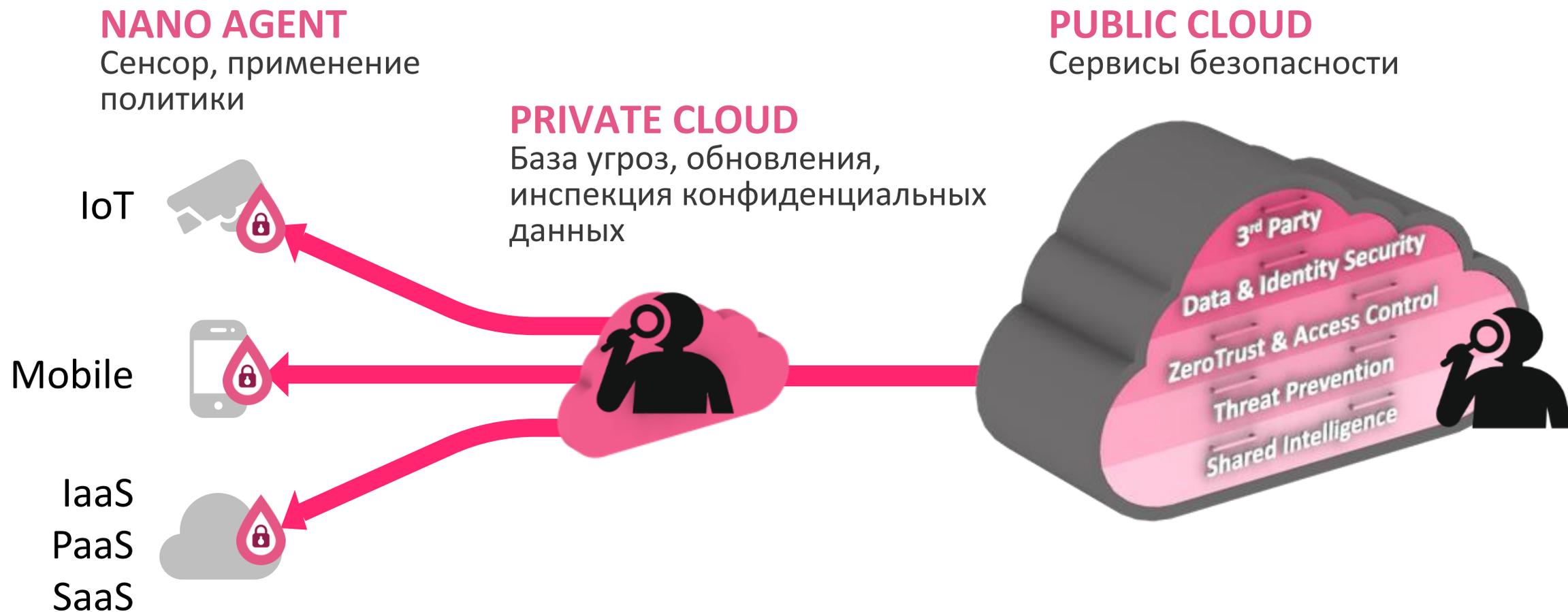
03

ЦИФРОВАЯ
ТРАНСФОРМАЦИЯ

Как пандемия повлияла на IT



Новые сервисы – новые векторы и «периметры»



Количество векторов атак растет



Почта	 	  Exchange	  Exchange	  Exchange
Веб		 		 
Шаринг	 box 	 box 	 box 	 box 
Фишинг				
Man in the Middle		 Malicious Networks		 Malicious Networks
Приложения				 

Новая модель потребления решений ИБ

Традиционные



«Следующего поколения»



Продвинутые сервисы
по подписке



ИБ как сервис

Сервис-провайдер **находится в наилучшей позиции** чтобы помочь заказчикам защитить инфраструктуру

Доступна **платформа безопасности** для защиты от всех угроз

Можно использовать **лучшие практики**, осуществлять внедрение и эксплуатацию

Посчитать **предсказуемую** стоимость владения

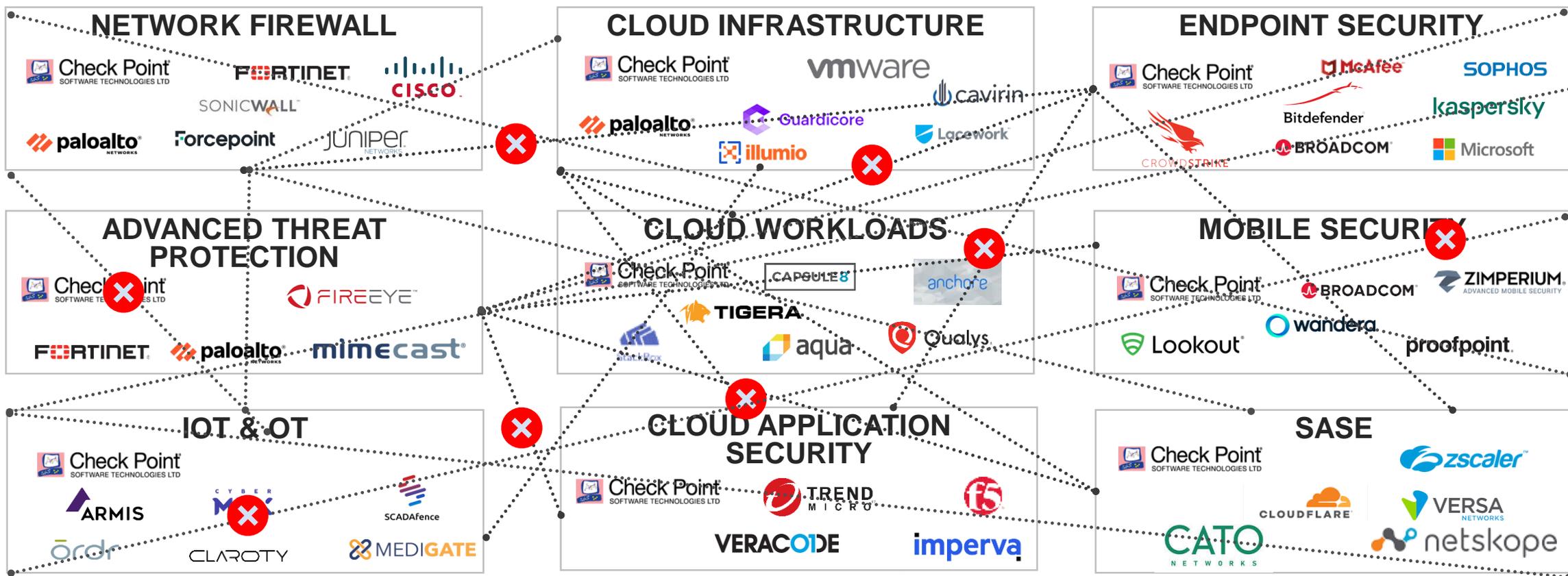
Аутсорсинг это выгодно

Можно попробовать «свой путь»

Сетевая безопасность

Облачная безопасность

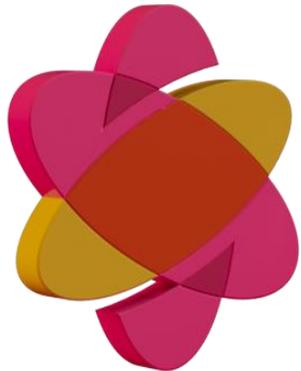
Пользователи и устройства



Максимальная безопасность с консолидированной архитектурой

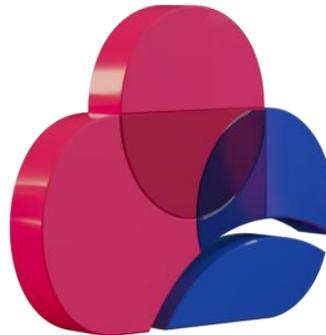
QUANTUM

SECURE THE NETWORK



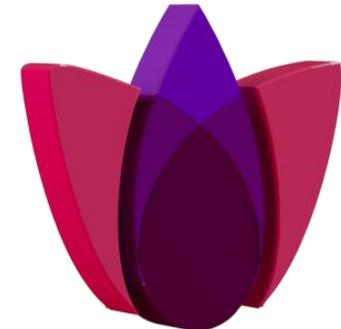
CLOUDGUARD

SECURE THE CLOUD



HARMONY

SECURE USERS & ACCESS



Infinity-Vision

THREATCLUD
Real-time Threat Prevention

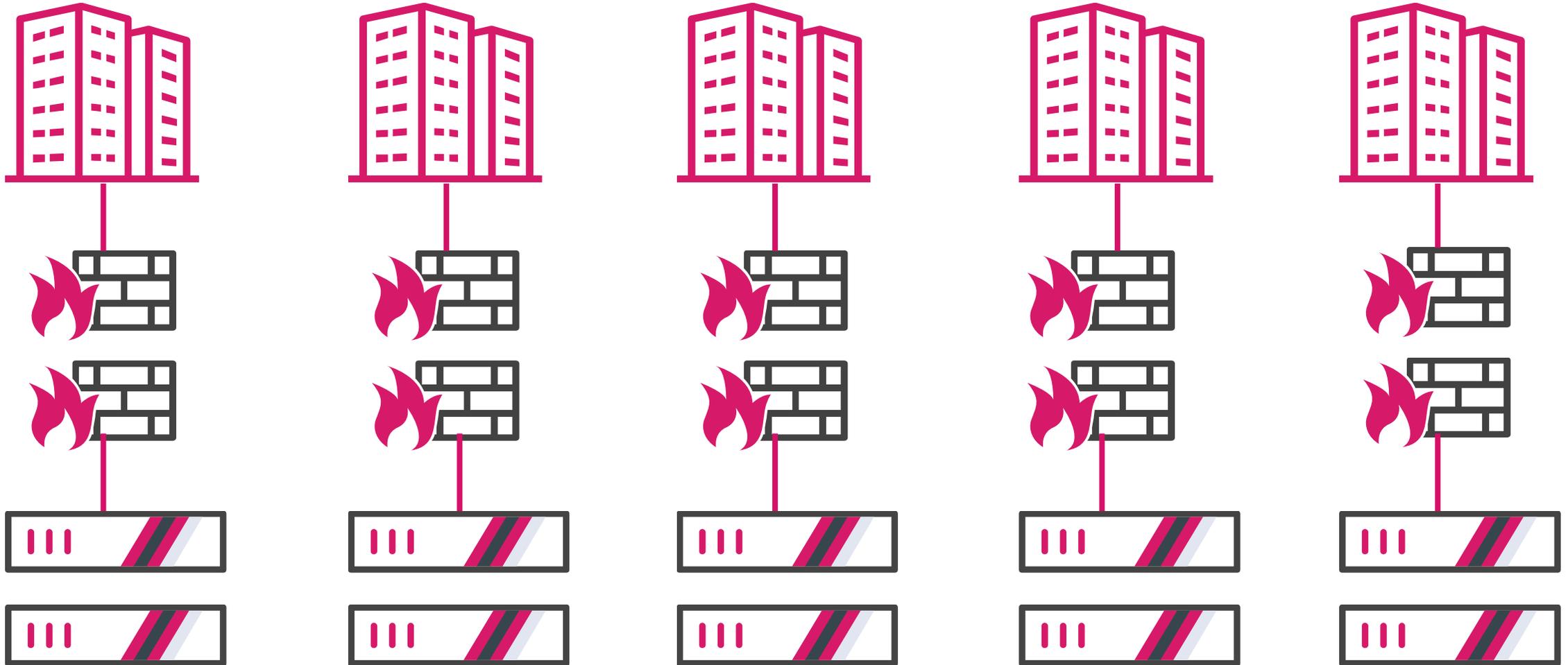
Разные модели

Задача	Продукты	Решение
Персональные данные, КИИ, тайна	Все продукты	<ul style="list-style-type: none">• Онпремис инфраструктура• Сертифицированный по требованиям регулятора ЦОД/MSSP в России
Прочее	Все продукты	<ul style="list-style-type: none">• Онпремис инфраструктура• ЦОД/MSSP в России /вендор
Infinity Total Protection	Все продукты по подписке	<ul style="list-style-type: none">• Цена за пользователя• Предсказуемые траты• Доступ ко всем продуктам

От CAPEX локально до OPEX в облаке



Сколько оборудования нужно онпремис? 5 заказчиков, по 500 пользователей, шлюз+песочница



Сколько оборудования нужно сервис-провайдеру?

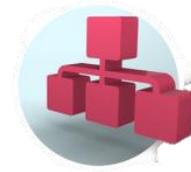
5 заказчиков, по 500 пользователей, шлюз+песочница



ВСЕ по подписке



CHECK POINT
INFINITY



Стоимость за
каждого
пользователя в год



Часть бюджета на
оборудование



Часть бюджета на
обучение и сервисы



24x7

Premium Support

ВСЕ ПРОСТО, ВСЕ ВКЛЮЧЕНО

Унификация решений и корреляция событий



СЕМЕЙСТВО HARMONY

БЕЗОПАСНОСТЬ УДАЛЕННЫХ СОТРУДНИКОВ



ЕДИНЫЙ ПОРТАЛ СО ВСЕМИ СЕРВИСАМИ



The screenshot displays the INFINITY PORTAL interface with the following components:

- Navigation Bar:** INFINITY PORTAL > Devices > Endpoint. User: John Snow. Environment: cp-demo.
- Service Tiles:**
 - INFINITY Unified Solution:** Watchtower, SOC, Policy.
 - QUANTUM Secure the Network:** Smart-1 Cloud, IoT Protect.
 - CLOUDGUARD Secure the Cloud:** Network, Posture, Workload, AppSec, Analytics.
 - HARMONY Secure Users & Access:** Connect, End Point, Mobile, Email & Office, Browser.
 - CHECK POINT LABS Early Availability:** Product Name 1, Product Name 2, Product Name 3.
- Monitoring Dashboard:**
 - Endpoint Settings:** 106 Devices In Progress, 131 Devices Success.
 - Devices report of problems:** 948 total. Bar chart showing problem frequency over time (10:00 to 04:00).
 - ANTI MALWARE UPDATES:** Windows7: 287 (73%), Retrieving: 287 (27%).
 - CLIENT VERSION:** 80.82.4059: 37%, 80.82.4059: 32%, 80.82.4059: 24%, 80.82.4059: 12%, Retrieving: 16%.
 - OPERATION SYSTEM:** Windows7: 287 (73%), Retrieving: 287 (27%).
 - Alerts:** Three alerts regarding "Default clients uninstall password was not changed in general settings" at 12:43.
 - Footer:** AD last sync: 03:00, Cloud Server.

УПРАВЛЕНИЕ ВСЕМИ СЕРВИСАМИ CHECK POINT



New

Унифицированные лог-файлы на Infinity portal

“единый интерфейс” для поиска и анализа

The screenshot displays the Check Point Infinity Portal interface. At the top, the search bar contains the query "johndoe AND severity:Critical". Below the search bar is a table of aggregated events. The table has columns for Time, Destination, and User. The events listed are:

Time	Destination	User
Feb 15, 2021 1:41:02 PM	192.168.11.12	
Feb 15, 2021 1:40:52 PM	192.168.11.12	101.23.36.43
Feb 15, 2021 1:40:51 PM	192.168.11.12	101.23.36.43
Feb 15, 2021 1:39:55 PM	192.168.11.12	192.168.13.2 johndoe
Feb 9, 2021 12:13:46 PM	192.168.11.12	
Feb 9, 2021 12:13:35 PM	101.23.36.43	
Feb 9, 2021 12:13:34 PM	192.168.11.12	101.23.36.43
Feb 9, 2021 12:12:51 PM	192.168.11.12	192.168.13.2 johndoe
Jan 26, 2021 5:13:22 PM	192.168.11.12	
Jan 26, 2021 5:12:10 PM	101.23.36.43	
Jan 26, 2021 5:12:09 PM	101.23.36.43	
Jan 26, 2021 5:08:29 PM	192.168.11.12	192.168.13.2 johndoe
Jan 26, 2021 4:44:48 PM	194.29.32.133	
Jan 26, 2021 4:44:10 PM	194.29.32.133	
Jan 26, 2021 4:44:10 PM	194.29.32.133	
Jan 20, 2021 7:14:31 PM	192.168.11.12	192.168.13.2 johndoe

On the right side of the interface, there is a "Card" section showing details for a selected event. The "Log Info" section includes:

- Origin: 192.168.73.35
- Time: Feb 15, 2021 1:41:02 PM
- Blade: Forensics
- Triggered By: Endpoint Behavioral Guard
- Product Family: Endpoint
- Type: Log
- Attack Status: Active
- Event Type: Forensics Case Analysis

The "Policy" section includes:

- Action: Prevent
- Policy Date: Feb 26, 2020
- Policy Name: Default Forensics settings
- Policy Version: 6

Поиск по пользователю

Детали события

Protection Details

- Severity: Critical
- Confidence Level: Medium
- Malware Action: Communication with C&C

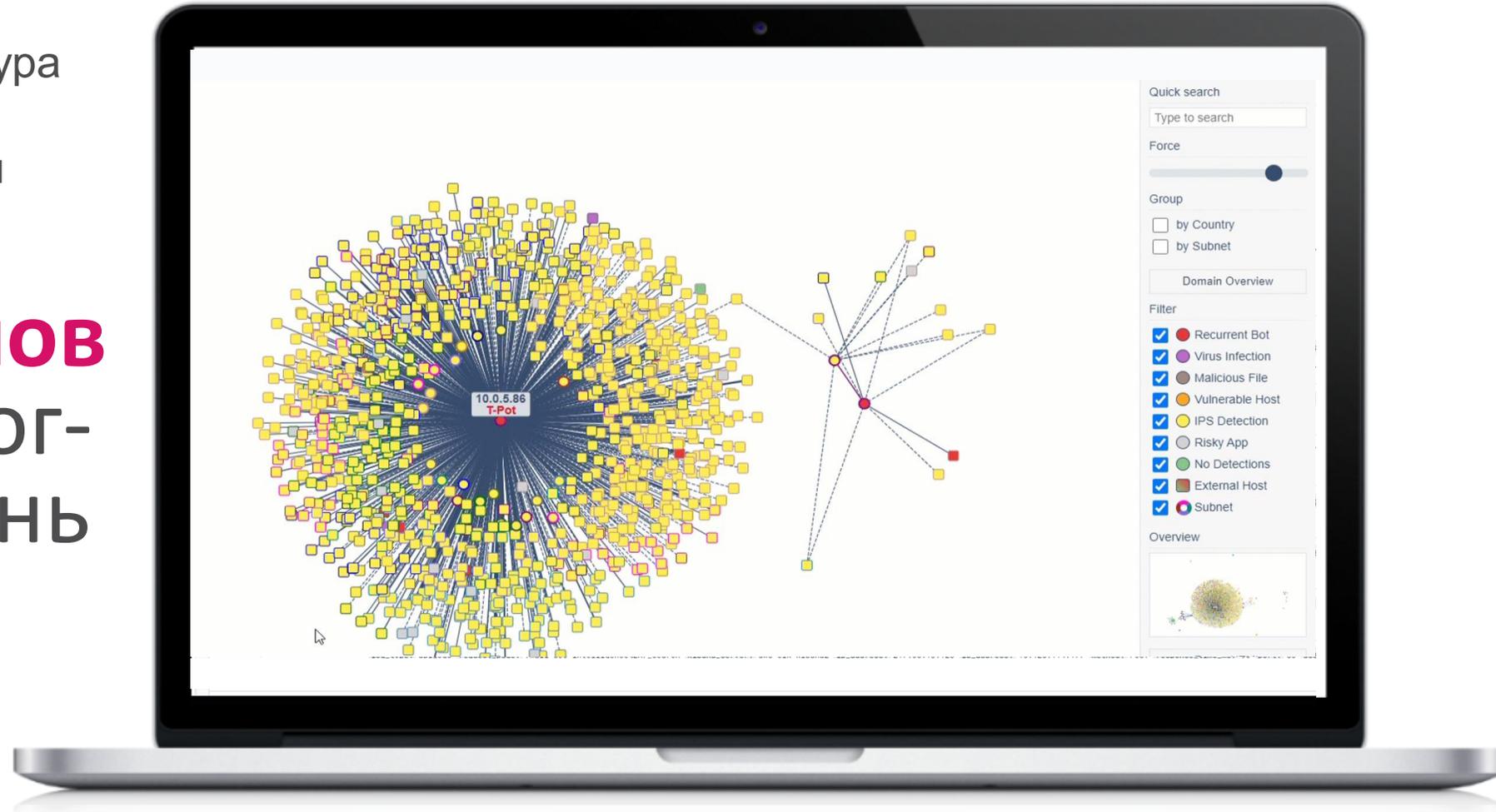


Работа SOC службы каждый день: Ищем иголку в стог сена

Типичная инфраструктура
среднего размера
2,000 пользователей



10 Миллионов
Записей в лог-
файлах в день



ТОЧНОСТЬ

От миллионов записей – к реальным инцидентам

В среднем за неделю:

59,000,000

Записей в лог-файлах – рабочие станции,
сеть, облака, мобильные устройства,
Интернет вещей

3,000

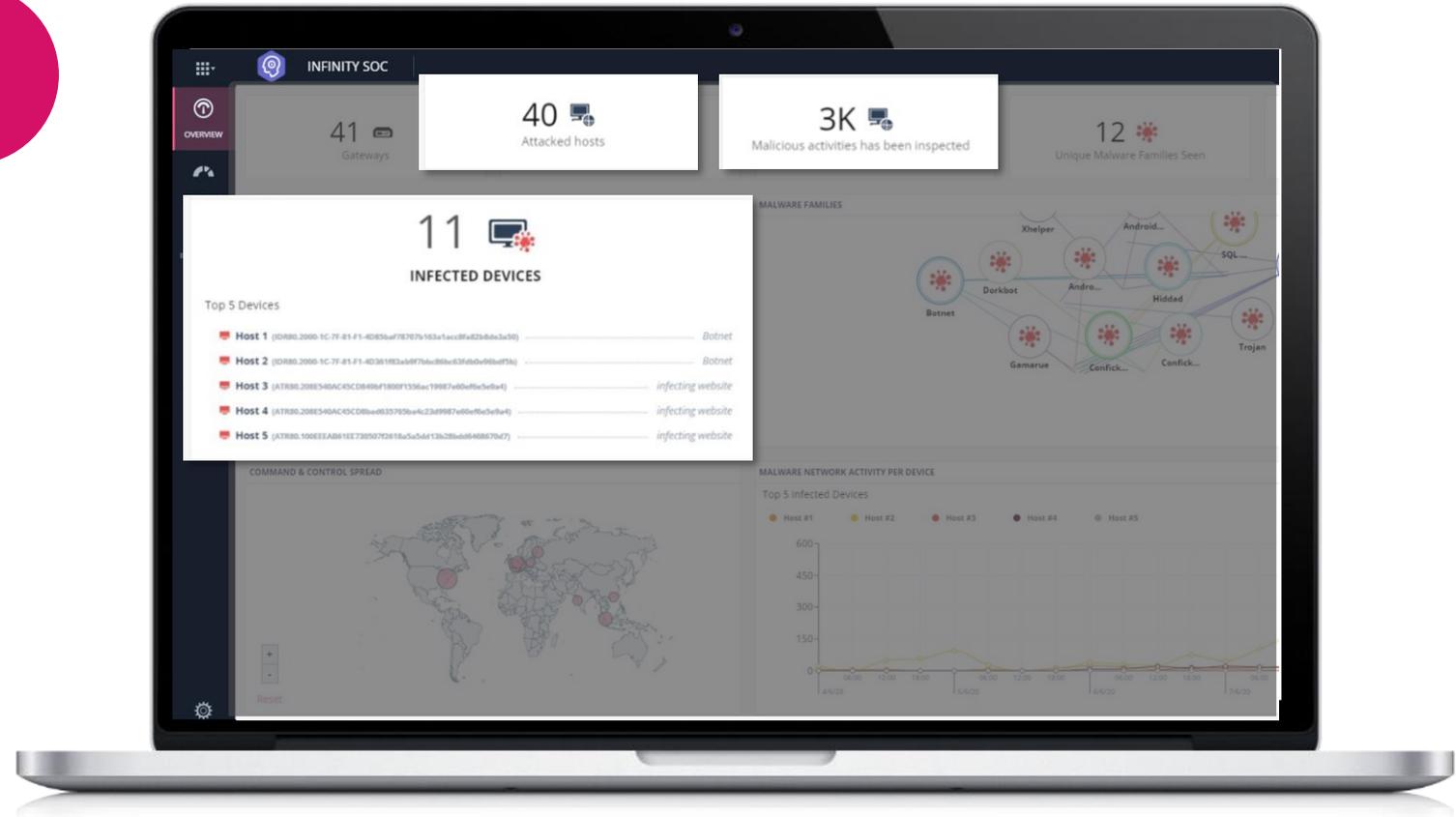
Вредоносных активностей

40

Затронутых
ХОСТОВ

11

Зараженных
ХОСТОВ



Упрощение и уменьшение стоимости владения с единой централизованной SOC платформой

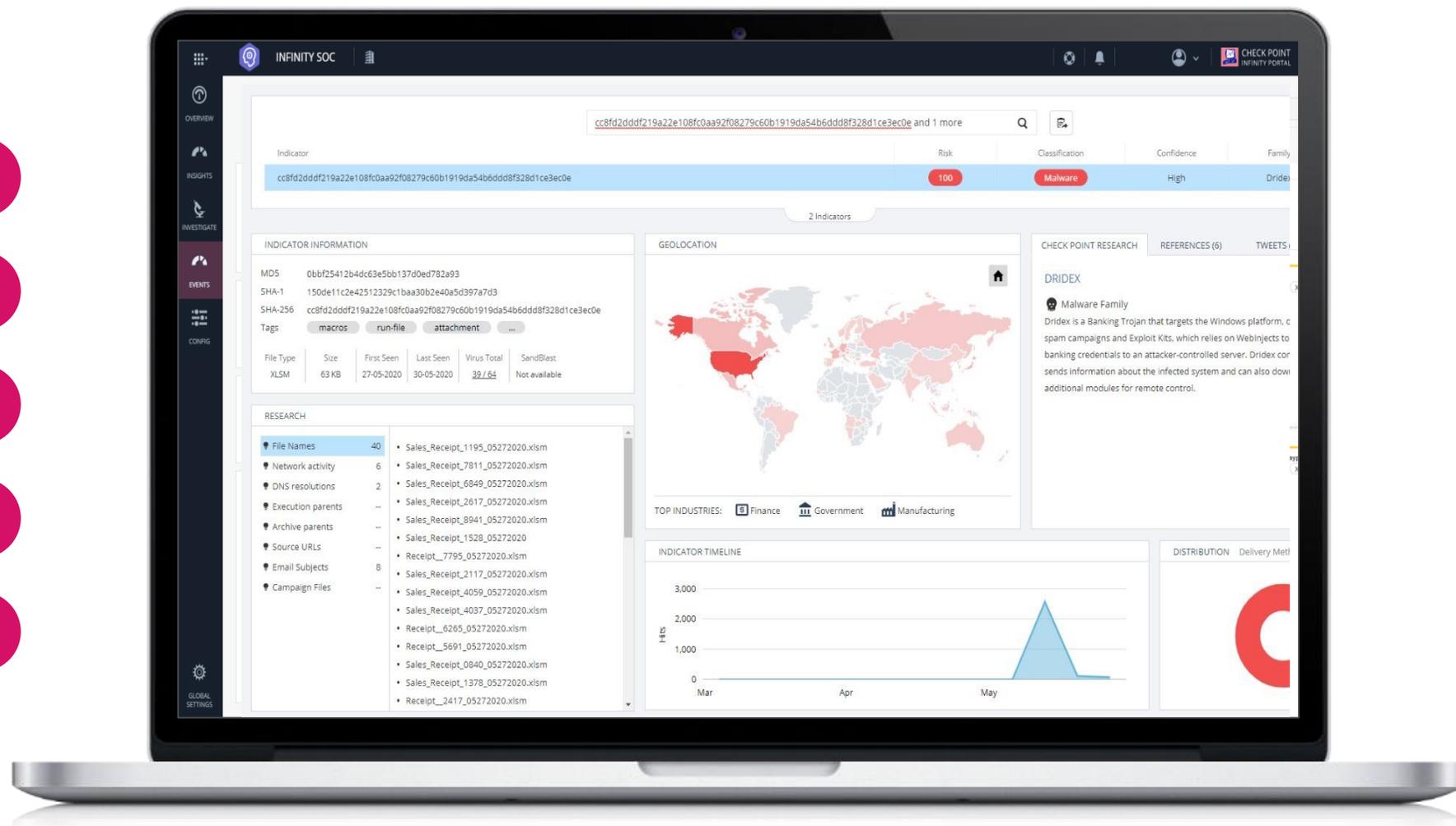
Внутренние угрозы

Внешние угрозы

Восстановление

Расследование

Управление





Check Point[®]
SOFTWARE TECHNOLOGIES LTD

СПАСИБО!

Sergey Zabula | Channel SE Team Lead, Check Point Russia

szabula@checkpoint.com