Check Point
SOFTWARE TECHNOLOGIES LTD

SECURITY
BEYOND THE PERIMETER

На бегу и в облаках: как защитить сотрудников, не мешая их эффективности

ЦИФРОВОЙ МИР – ОПАСНОЙ МЕСТО

Check Point SOFTWARE TECHNOLOGIES LTD

January — Monetary Theft

Coincheck

$534M were stolen from Japan's largest digital currency exchange.

February — Business Disruption

The City of Atlanta suffers an attack that locks down city systems for over a week.

March

AdultSwine, a mobile malware infecting children's game apps with adware, is downloaded by up to seven million users.

Monetary Theft

April — Business Disruption

CITY OF COPENHAGEN

Users of Copenhagen's city bikes are denied access due to the system being hacked.

May

The luxury retailers, Saks and Lord & Taylor, has five million customers' credit card details stolen.

Saks Fifth Avenue

Data Theft

June — Data Theft

SingHealth

Singapore suffers its biggest cyber attack with the theft of 1.5 million patient records, including the Prime Minister's.

July

340 million records of Americans and business are leaked from the Florida-based marketing firm.

EXACTIS

Data Theft

August — Data Theft

facebook

30 million Facebook users' phone numbers and personal details are exposed in a major attack.

September

Hackers stole gradually over $13 million via ATM machines in 28 countries in just two days.

COSMOS BANK

THE COSMOS CO-OP. BANK LTD. (Multistate Scheduled Bank)

Monetary Theft

October

Onslow Water and Sewer Authority suffers a ransomware attack impeding efforts to provide services.

ONWASA

Business Disruption

November

Cryptocurrency mining platform NiceHash is compromised and loses 4,700 bitcoin ($70 million) to hackers.

bitcoin

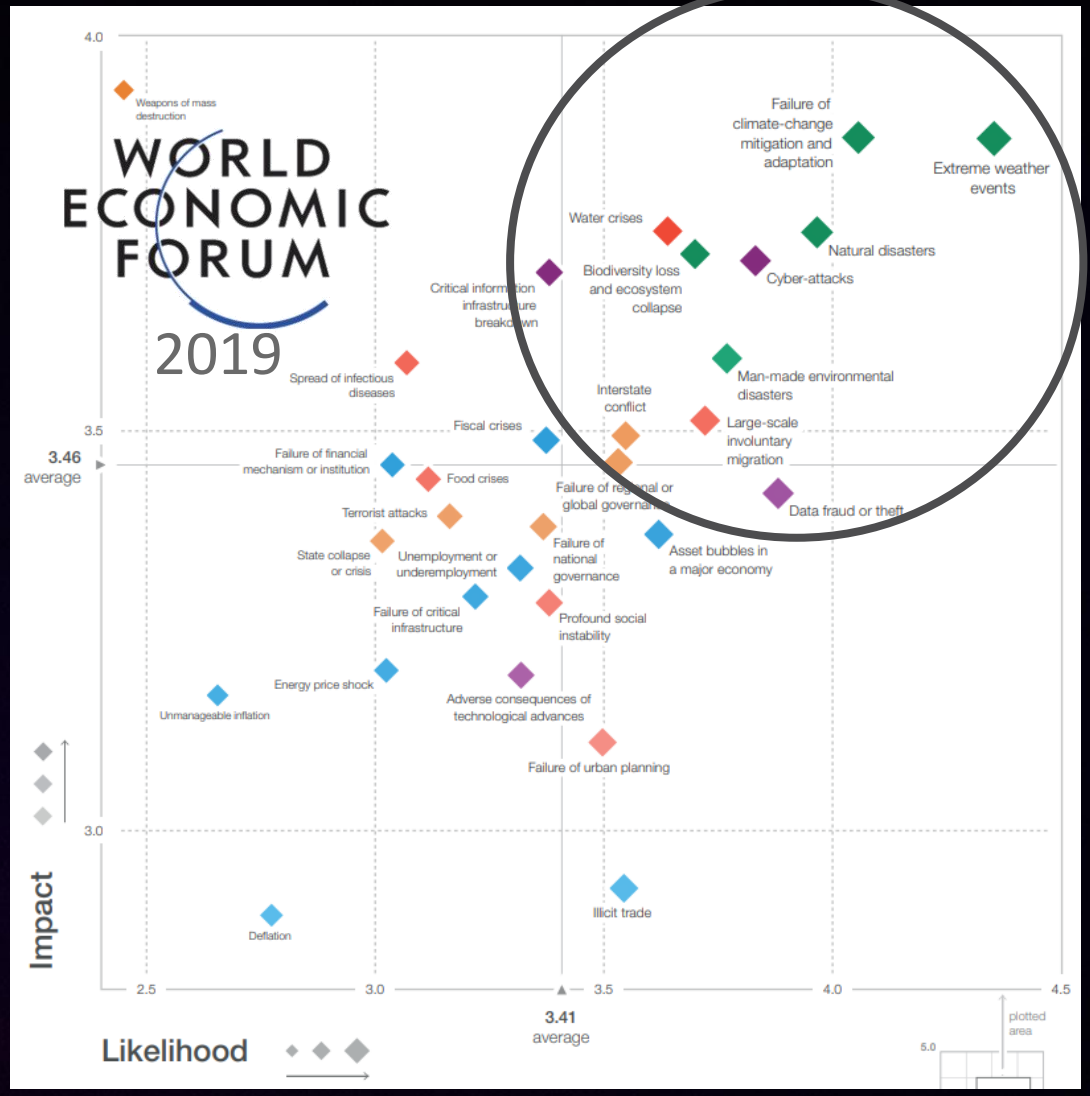
Monetary Theft

December — Data Theft

Marriott HOTELS · RESORTS · SUITES

Hackers steal the personal details of 500 million Marriot Hotel customers.

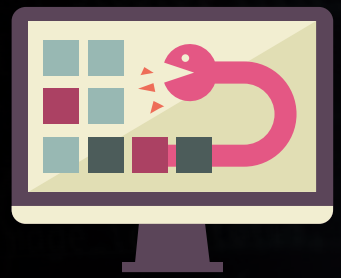
ЦИФРОВОЙ МИР – ОПАСНОЕ МЕСТО



Традиционная защита неэффективна

Сигнатурные и Репутационные решения не защищают от zero-day атак

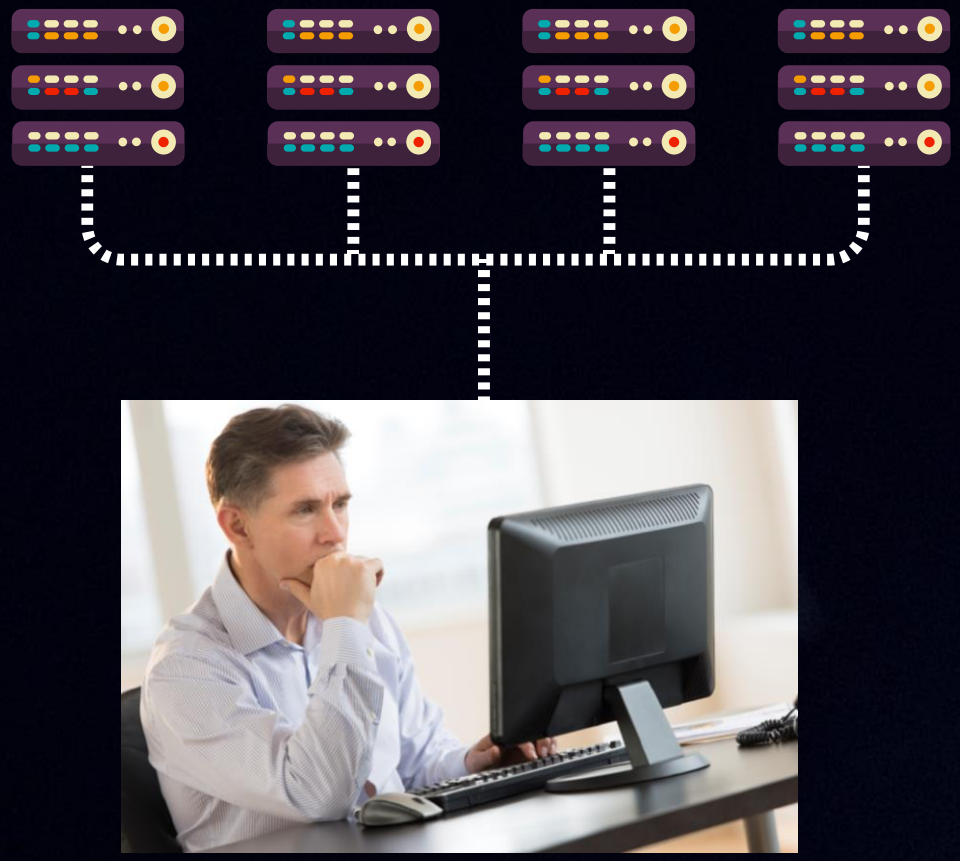
- **Zero-day Вирусы** - Всего **45%** зловредов обнаруживаются AV* (источник: theguardian.com)
- **Zero-day URLS** – Недавно созданные фишинговые страницы не имеют репутации
- **Zero-day мобильные зловреды**



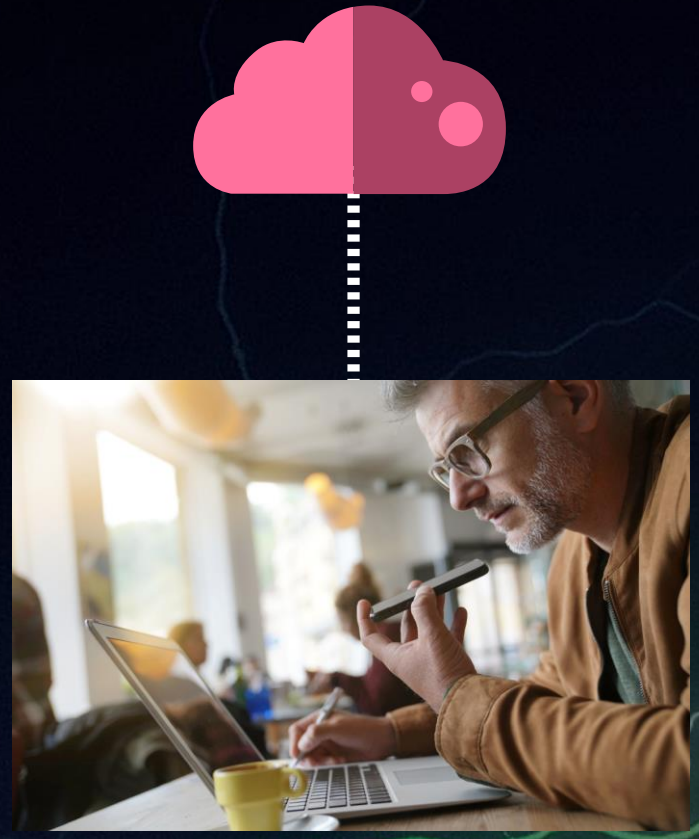
Полиморфные атаки легко преодолевают песочницы 1-го поколения

ПЕРИМЕТР РАЗМЫВАЕТСЯ

Меняется сама IT архитектура – Должна меняться и безопасность



Бизнес Вчера



Бизнес Сегодня

Типичные вектора современных атак

LAPTOPS

E-Mail

File Share

Malicious Network

Man in the Middle

Web

Phishing

Account Take Over

SMARTPHONES & TABLETS

E-Mail

File Share

Malicious Network

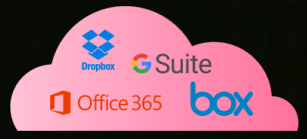
Man in the Middle

Web

Phishing

Malicious Application

Account Take Over



CLOUD APPLICATIONS

E-Mail

File Share

Phishing

Malicious Application

Account Take Over

Требуется новая Парадигма безопасности

- Консолидация информации об угрозах со всех направлений
- Предотвращение атак, а не обнаружение
- Защита от небрежного поведения пользователей и ошибок

Безопасность на бегу и в облаках
Защищаем устройства, защищаем данные

Облачные сервисы

Рабочие станции

Смартфоны и планшеты

Единая база угроз

Check Point
SOFTWARE TECHNOLOGIES LTD

Предотвращение Современных Угроз на рабочих станциях

ПРЕДСТАВЛЯЕМ:

Check Point
SandBlast™
AGENT

> *“For customers looking for a solid combination of new technology and traditional suite capabilities in a single console, Check Point should easily make the shortlist (Forrester – Wave Report, June 2018)”*

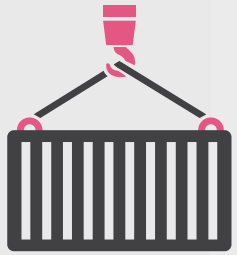
FORRESTER®
WAVE
LEADER 2018
Endpoint Security
Suites

3 УРОВНЯ ОБОРОНЫ

ДОКАЗАННЫЙ ПОДХОД ЗАЩИТЫ **РАБОЧЕЙ СТАНЦИИ**

ПРЕДОТВРАТИТЬ

Лучший способ защиты - полностью остановить атаку до её начала



ОБНАРУЖИТЬ И ОСТАНОВИТЬ

Ущерб после заражения растет стремительно. Атаку необходимо обнаружить и остановить как можно раньше.

УСТРАНИТЬ ПОСЛЕДСТВИЯ

Автоматическое устранение последствий, восстановление данных, расследование инцидентов.

ЗАЩИТА ОТ УГРОЗ НУЛЕВОГО ДНЯ

Browser Extension
Web downloads

Threat Extraction &
Threat Emulation

SANDBLAST SERVICE
Cloud or Appliance

File-System Monitor
Any file copied or created (from USB, Network Shares, etc)

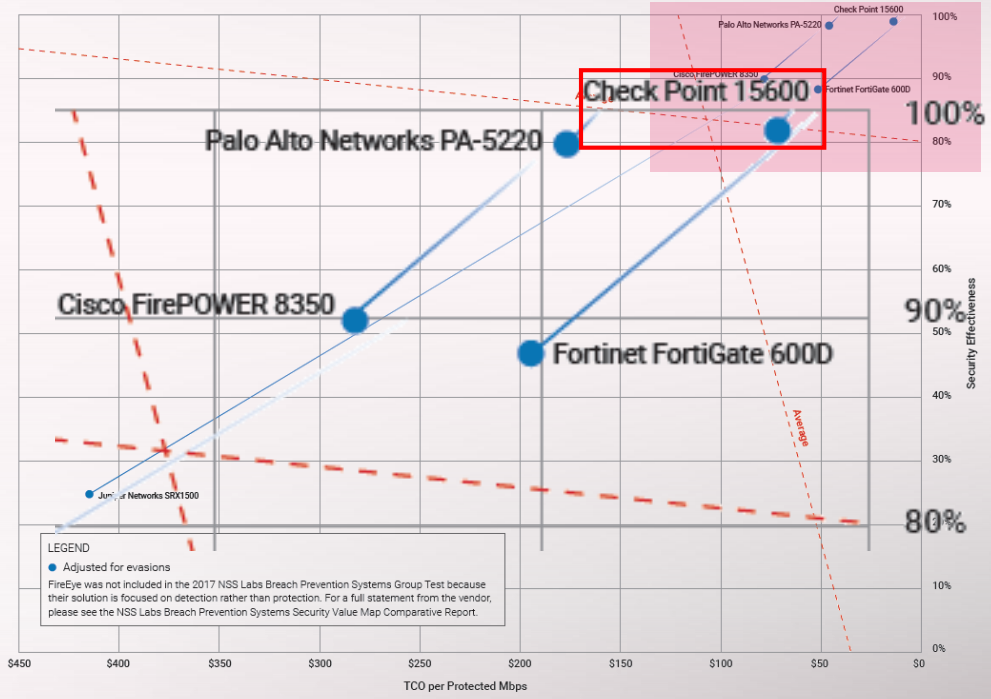
Threat Emulation

When it Comes to Prevention: Think Check Point

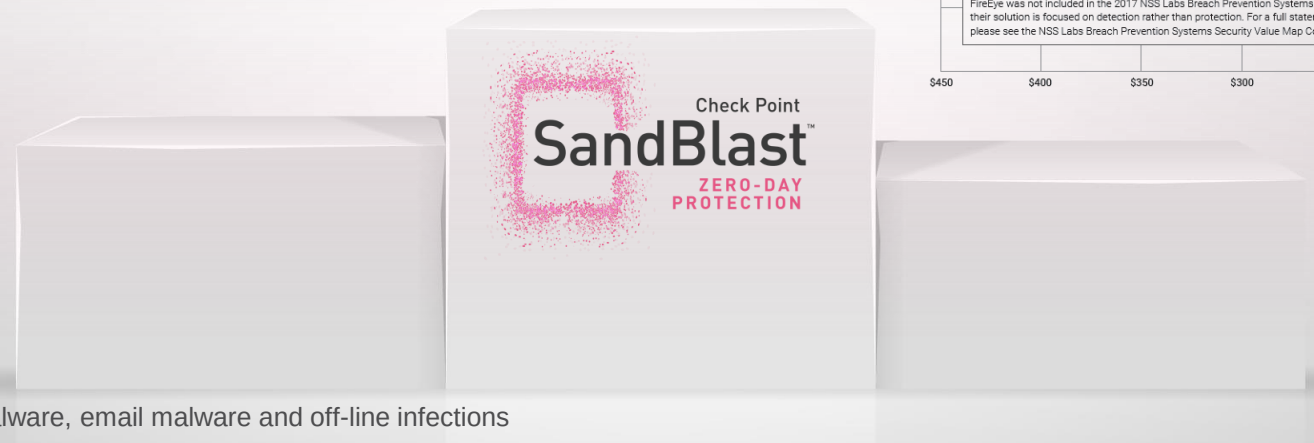
SandBlast earns highest security effectiveness score and lowest TCO

CHECK POINT
Check Point Software Technologies
15600 Next Generation Threat Prevention & SandBlast™ (NGTX) Appliance R77.30
BREACH PREVENTION SYSTEM
NSS LABS
RECOMMENDED
DEC 2017

- **Highest scores** in 1st ever Breach Prevention System test
- Lowest TCO
- Single consolidated gateway, running at 10Gbps
- **100%** Breach Prevention System Combined Score
  - **100%** Block rate
  - **99.2%** Evasion score
- **0.0%** False Positives



DECEMBER 2017



*Against drive-by exploits, social exploits, HTTP malware, email malware and off-line infections

АНАЛИЗ ПОВЕДЕНИЯ И РАССЛЕДОВАНИЕ ИНЦИДЕНТА

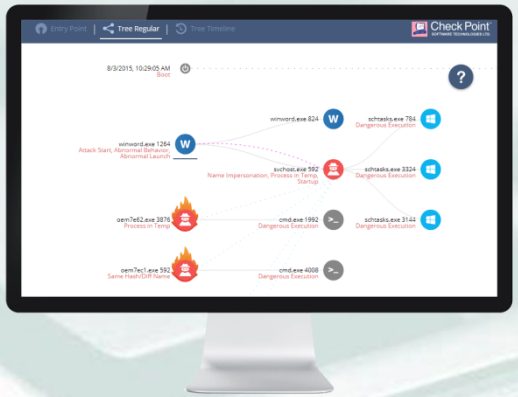
1 Постоянный сбор информации об ОС с множества сенсоров

2 Автоматическое создание отчета при срабатывании триггера. Триггером может быть внутренний сенсор или сторонний AV

Обнаружена угроза

3 Обновляемые алгоритмы анализируют «сырые» данные логов

4 **Последствия устранены** и полный отчет создан на SmartEvent



ENDPOINT ANTI-EXPLOIT

Уязвимость → Эксплойт → Шелкод → Нагрузка

Check Point SandBlast AGENT with Anti-Exploit

Защита на основе анализа файлов и поведения

SANDBLAST AGENT ОБНАРУЖИВАЕТ ВЗЛОМ:

Используется ROP для обхода DEP

Попытка доступа к IAT/EAT Table

VBS/JS God mode

И много других способов…

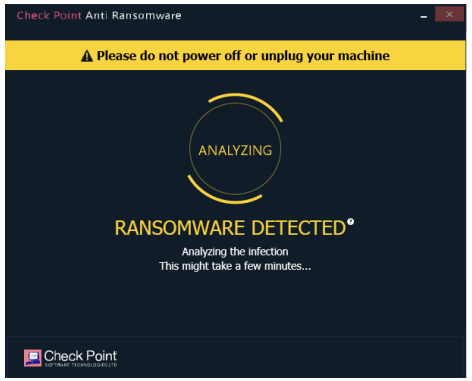
ANTI-RANSOMWARE

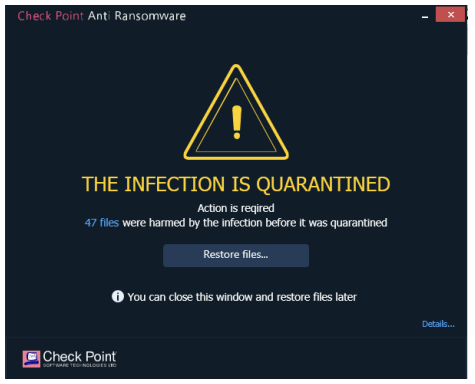
Отражение атаки и восстановление данных

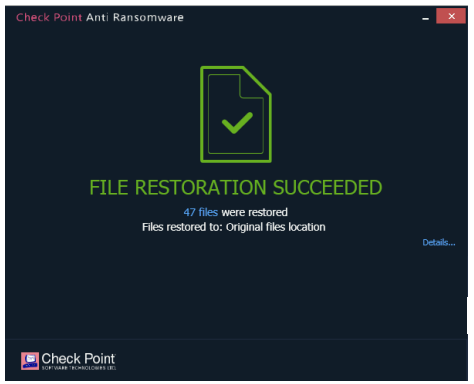
Check Point
SOFTWARE TECHNOLOGIES LTD

ПОСТОЯННО

В СЛУЧАЕ АТАКИ







АНАЛИЗ ПОВЕДЕНИЯ

Постоянное ожидание специфических событий вымогательского ПО

РАЗБОР

Начало разбора инцидента и анализ деталей атаки

КАРАНТИН

Остановка и карантин всех частей атаки

БЕКАП ФАЙЛОВ

Постоянно создаются временные копии файлов

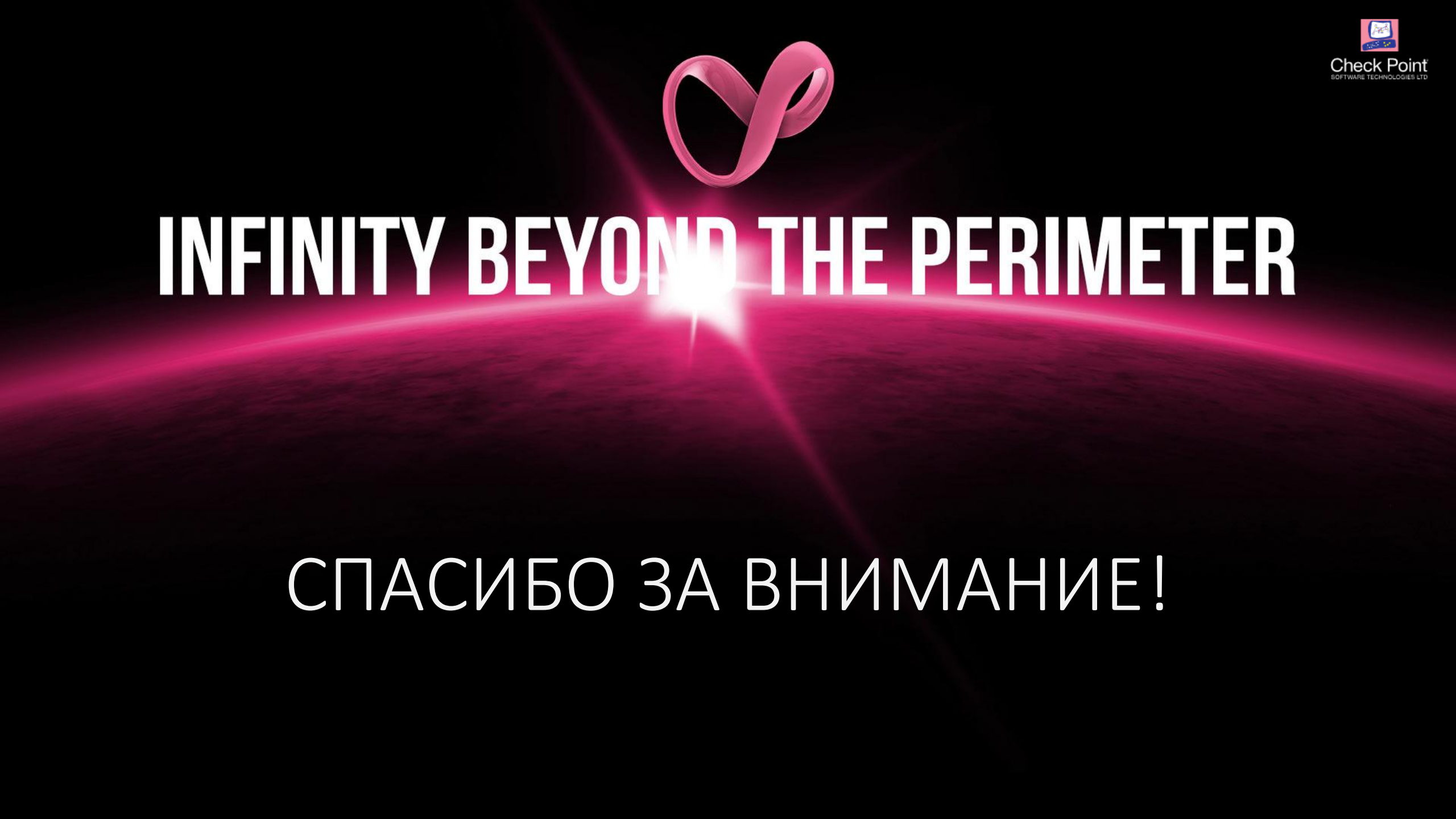
ВОССТАНОВЛЕНИЕ

Используются временные бекапы

Check Point
SOFTWARE TECHNOLOGIES LTD

Check Point
SandBlast™
AGENT

ДЕМО...



СПАСИБО ЗА ВНИМАНИЕ!