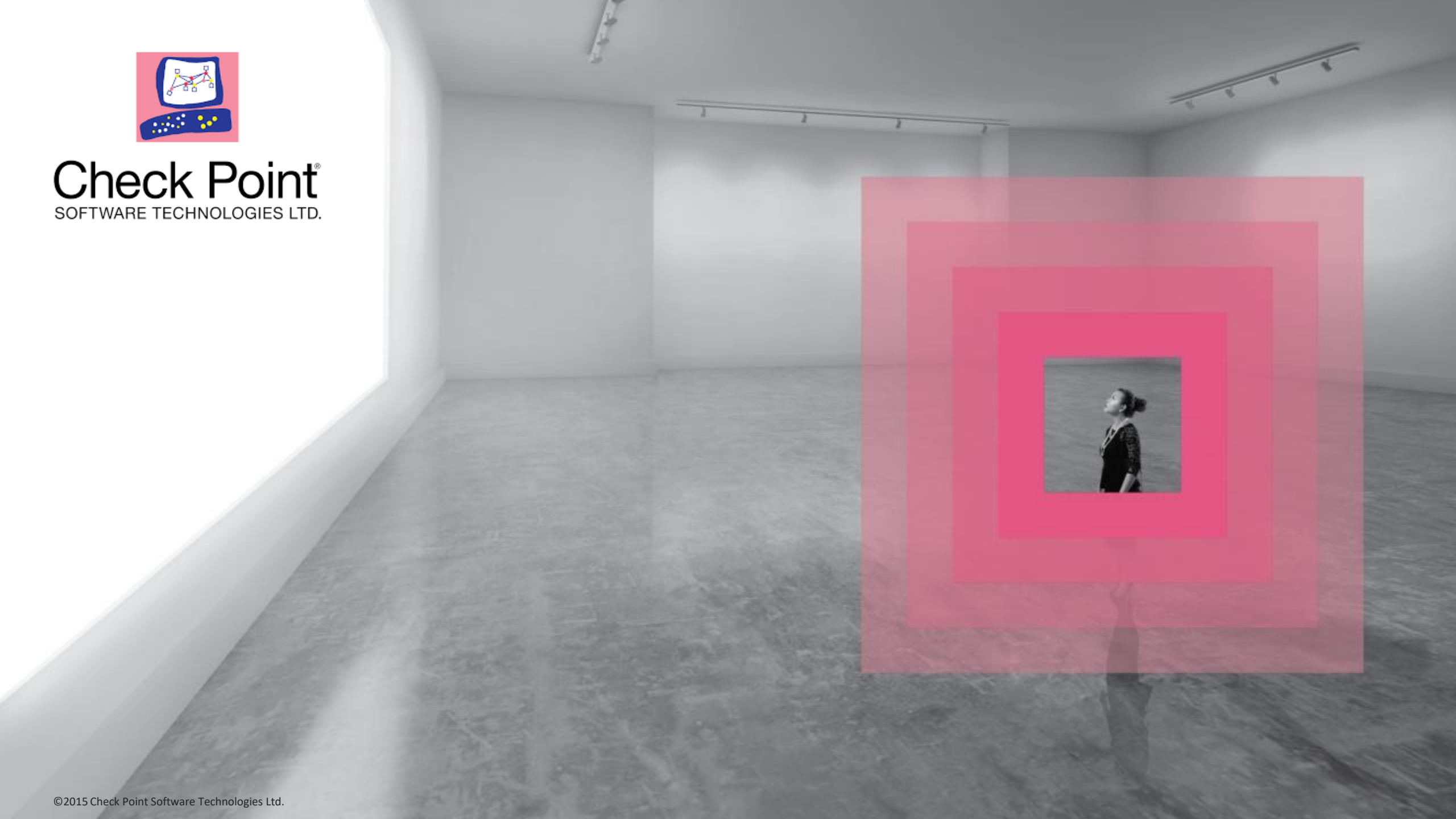
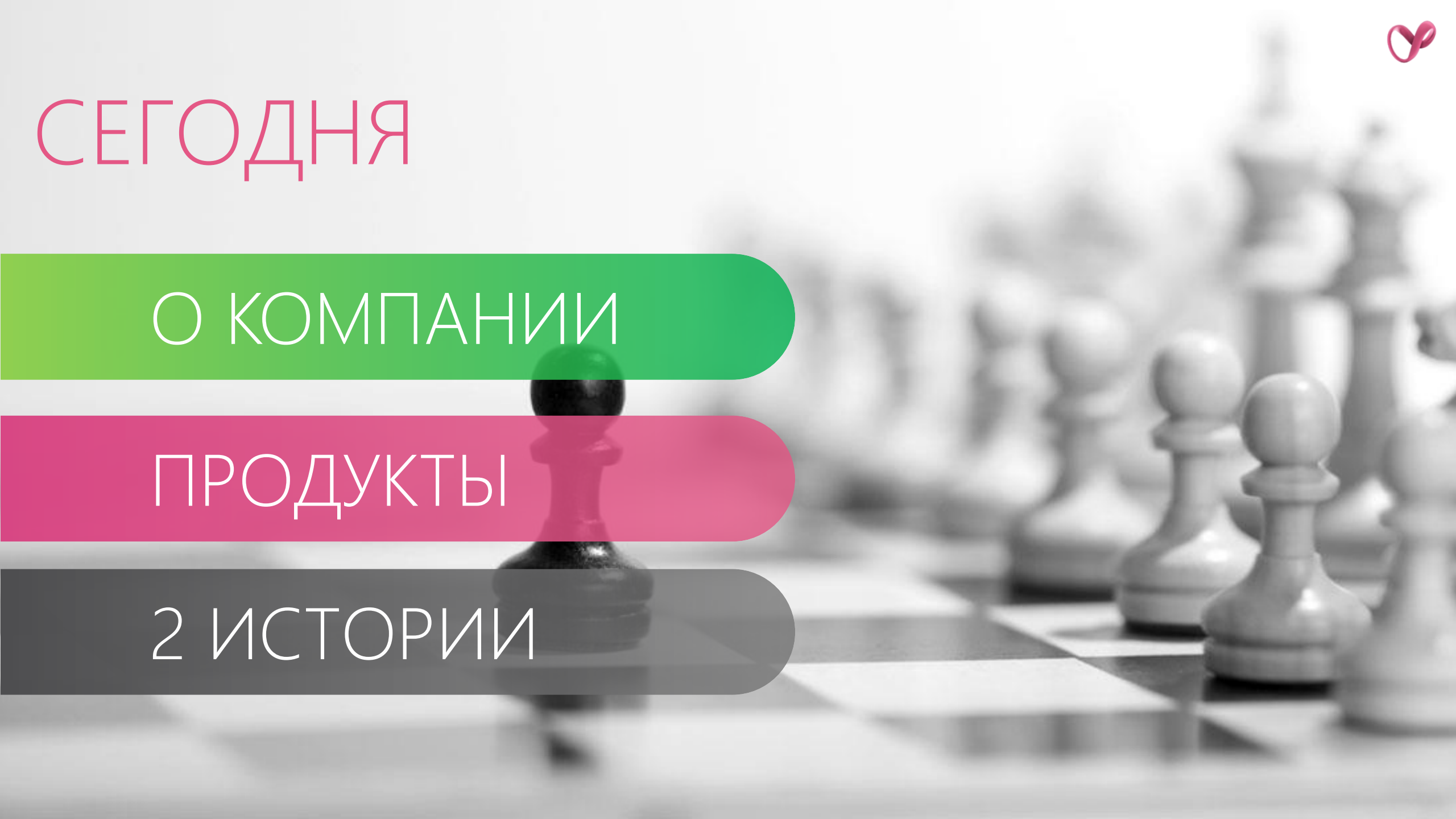


Check Point®
SOFTWARE TECHNOLOGIES LTD.

# СЕГОДНЯ



О КОМПАНИИ

ПРОДУКТЫ

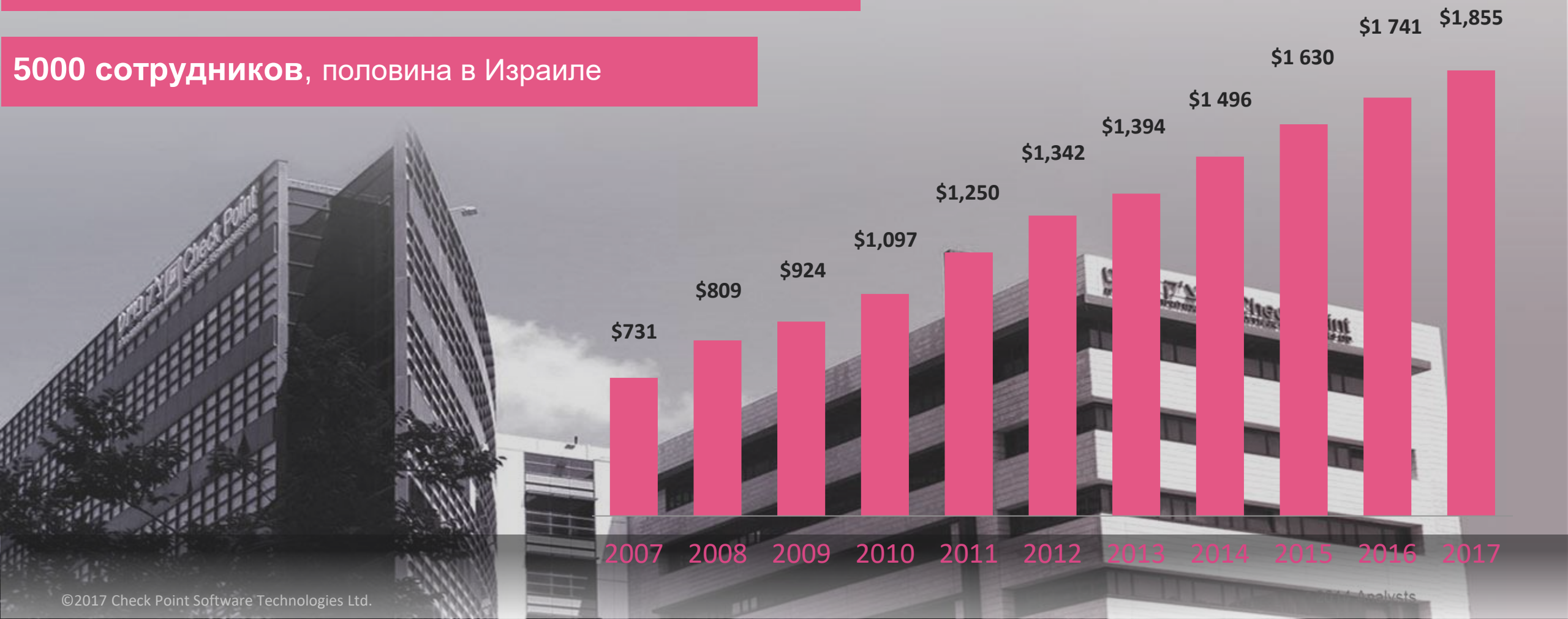
2 ИСТОРИИ

# Check Point: факты

КОНКУРЕНТЫ приходят и уходят

**$1.855B** годовая прибыль; **$18B** рыночная капитализация

**5000 сотрудников**, половина в Израиле



# ИННОВАЦИИ. ВИДЕНИЕ. ЛИДЕРСТВО.

**MOST** NSS RECOMMENDED PRODUCTS, **18 послдених тестов** с **2013**

**ЛИДЕР** отчета Enterprise FW Magic Quadrant с 1997 года

**98% КОМПАНИЙ ИЗ FORTUNE 500** – клиенты Check Point

**ВСЕ КОМПАНИИ ИЗ FORTUNE 100** – клиенты Check Point

ТОЛЬКО **ИНФОРМАЦИОННАЯ БЕЗОПАСНСОТЬ.**

1,855 МЛРД ДОЛЛ – 2017 ГОД

**ПЕРВЫЙ В ОТРАСЛИ МЕЖСЕТЕВОЙ ЭКРАН**

был разработан компанией Check Point

HIGHEST MALWARE CATCH RATE

LEADS CYBERSECURITY VISION AND INNOVATION

BEST SECURITY MANAGEMENT

FASTEST TO STOP ZERO DAY MALWARE

# АВТОРИЗОВАННЫЙ УЧЕБНЫЙ ЦЕНТР

Check Point
SOFTWARE TECHNOLOGIES LTD

CHECK POINT
STARS
PARTNER
AUTHORIZED
TRAINING CENTER

CHECK POINT
STARS
PARTNER
COLLABORATIVE
ENTERPRISE
SUPPORT

Check Point
SOFTWARE TECHNOLOGIES LTD

# ОБЗОР РЕШЕНИЙ CHECK POINT

WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY CHECK POINT INFINITY

CLOUD • MOBILE • THREAT PREVENTION

# CHECK POINT INFINITY

## MOBILE

Check Point SandBlast MOBILE

- App Protection
- Network Protection
- Device Protection
- Blocks SMiSing Attacks

**Capsule Workspace & Docs**

- Remote Access
- Secure Container Business apps
- Protect docs everywhere

## ENDPOINT

Check Point SandBlast AGENT

- Threat Emulation & Extraction
- Anti - Ransomware
- Zero - Phishing
- Forensics & Quarantine

**Complete Protection**

- Firewall, VPN & Compliance Check
- Disk & Media Encryption
- Anti-Malware
- Anti-Bot
- Secure Documents

## Threat Intelligence THREATCLOUD


## CLOUD

**Infrastructure**

CloudGuard IaaS

- Advanced Threat Prevention
- Adaptive Security
- Automation and Orchestration
- Cross Cloud Dynamic Policies
- Multi-Cloud

Microsoft Azure · Azure Stack · vmware NSX · openstack · aws

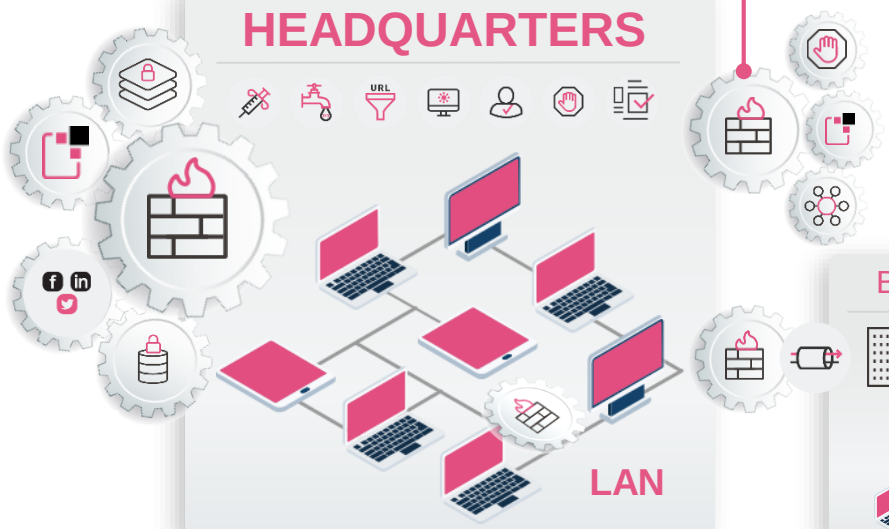
**Applications**

CloudGuard SaaS

- Zero-Day Threat Protection
- Sensitive Data Protection
- End-to-end SaaS Security
- Identity Protection

Office 365 · salesforce · Google Apps · Dropbox · servicenow

## HEADQUARTERS




## BRANCH / ICS


WELCOME TO THE FUTURE OF CYBER SECURITY

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

Check Point
SOFTWARE TECHNOLOGIES LTD

## 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

SandBlast

Data loss prevention

DDoS Hardware protection

Site to site VPN

Check Point Security Gateway

Private cloud and virtualisation protections

CHECK POINT CloudGuard

Virtual security gateway

ACI

vmware NSX

openstack

Industry leading zero-day sandbox solution

Unified management console

Security incident and event reporting

Policy Management

# КОНТРОЛЬ

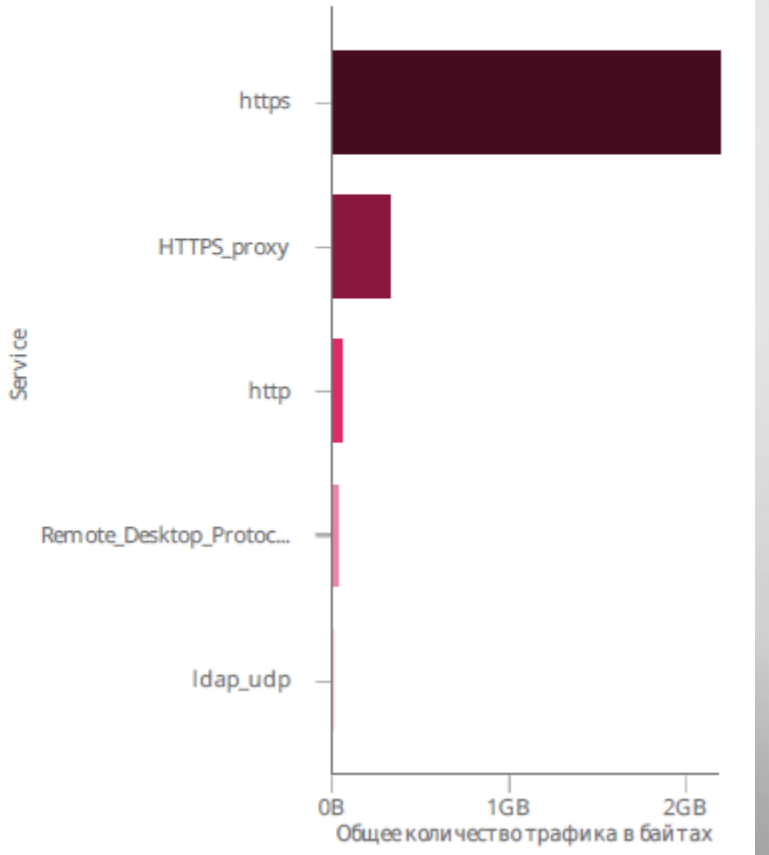
## Самые популярные приложения/сайты (топ 30)

| Приложение / Сайт | Категории | Уровень риска | Источники | Трафик |
|---|---|---|---|---|
| LogMeIn rescue | Remote Administration | 4 High | 10 Источники | 2.2GB |
| YouTube | Media Sharing | 2 Low | 1 Источник | 313.5MB |
| Remote Desktop Protocol | Remote Administration | 4 High | 3 Источники | 23.2MB |
| cnn.com/ext/app/redalert/cdaredalert_iframe/0,12639,84-234-208-20,00.html | Search Engines / Portals | — Unknown | 1 Источник | 22.9MB |
| Google Search | Search Engines / Portals | 2 Low | 2 Источники | 9.2MB |
| newmail.aol.com | Search Engines / Portals | — Unknown | 1 Источник | 3.7MB |
| LDAP Protocol | Network Protocols | 1 Very Low | 1 Источник | 3.0MB |
| LogMeIn | Remote Administration | 4 High | 5 Источники | 2.5MB |
| adobe.com | Computers / Internet | — Unknown | 1 Источник | 2.2MB |
| 212.235.15.30 | Inactive Sites | — Unknown | 1 Источник | 1.1MB |
| cdn.stumble-upon.com | Newsgroups / Forums | — Unknown | 1 Источник | 952.3KB |

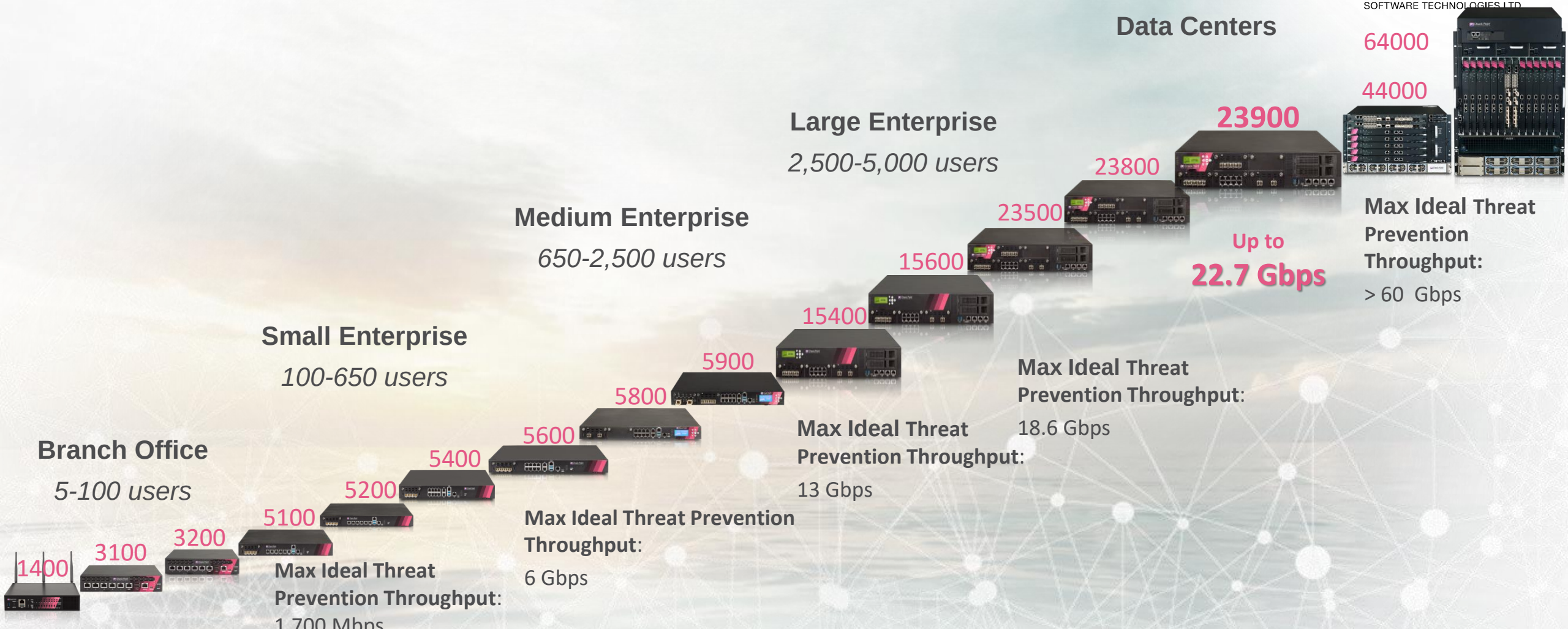
**2.6GB**

Общий объем проверенного трафика

### Трафик по протоколу



# Threat Prevention Security Gateways



# Платы расширения (анонс)

**Network Security Acceleration Card**

- Выделенный процессор для обработки трафика
- Интерфейсы 1G, 10G, 40G
- Поддержка серий 5000, 15000, 23000

# ПЕЧАЛЬНАЯ ИСТОРИЯ

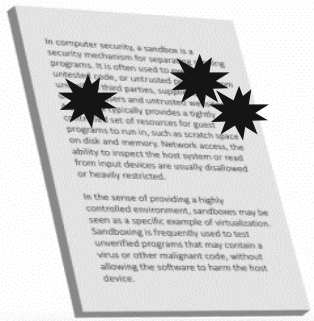

Tweet
Share

patterns associated with senior executives' accounts, and changed related passwords. The security team also began watching for

*(click image for larger view and for slideshow)*

# Эмуляция

## Откроем файл в безопасной среде




Наблюдаем:

- Реестр
- Сетевые соединения
- Действия с файлами
- Действия с процессами

**Поведение – вот что выдает зловредное ПО**

# Традиционная песочница – традиционные задержки

## ПРОВЕРКА ЗАНИМАЕТ ВРЕМЯ

- Как результат, во многих инсталляциях песочницы не используются в режиме блокировки
- Вредоносный файл может попасть к пользователю, пока находится в очереди для проверки


[Prote

# DELIVER CLEAN ATTACHMENTS

## *Threat Extraction* for Documents

### CLEAN MODE

Retain file format, remove active content

### CONVERT MODE

Convert documents to PDF


We recommend
- CONVERT MODE - for Word documents
- CLEAN MODE - for everything else

## GET THE DATA NOT THE RISK

- Fast delivery
- Preserve all text and visual content
- Self-catered access to original files

# Извлечение контента (Threat Extraction)

Check Point
SOFTWARE TECHNOLOGIES LTD

Reply Reply All Forward

Tue 5/4/16 6:03 PM

Yonni Shelmerdine

SECURITY ALERT! Skipped Invoice

To Yonni Shelmerdine

Message invoice.cleaned.pdf

*Check Point SandBlast Threat Extraction has **cleaned** an attachment named **Invoice.doc** as it was determined to contain potentially malicious elements.*

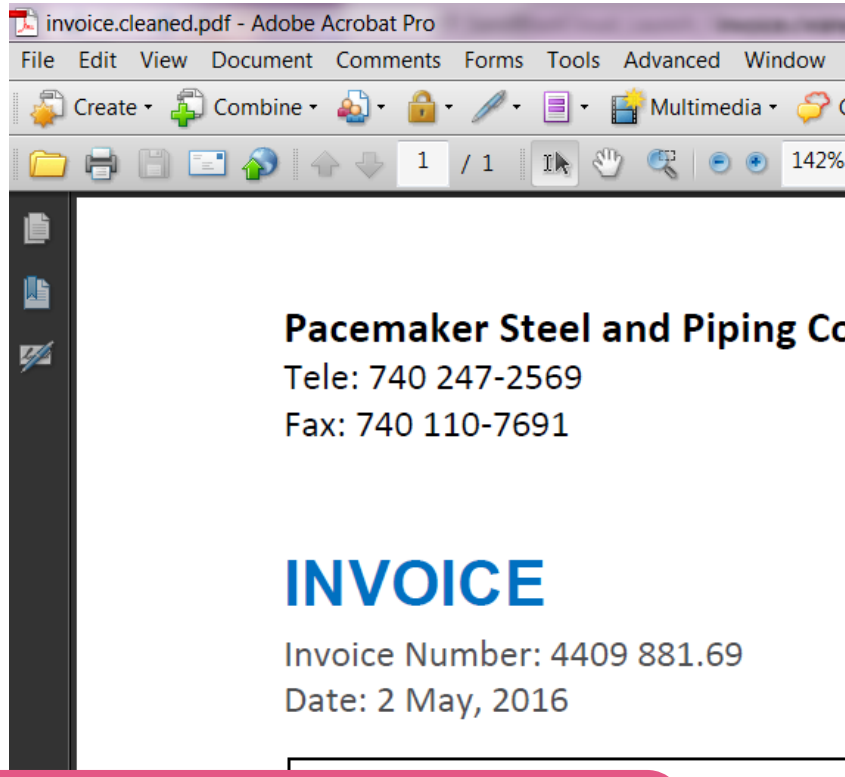
*To access the original file, please click here*

Hi Yonni,
Attached is invoice #4409 881.69 from May which was missing from the original summary.

I am out of the office tomorrow and Monday, so I'm emailing you now to request that you go over the invoice, submit the detail
[Blocked Malicious URL] and complete they payment as soon as possible.

Julia Reyes / Credit Manager
Pacemaker Steel and Piping Co. Inc.
Tele: 740 247-2569
Fax: 740 110-7691

*This Email was secured by Check Point SandBlast Connector for Office 365*




**Конвертация в PDF или извлечение всего активного содержимого**

# Извлечение контента (Threat Extraction)

Check Point
SOFTWARE TECHNOLOGIES LTD

Reply Reply All Forward

Tue 5/4/16 6:03 PM

Yonni Shelmerdine

SECURITY ALERT! Skipped Invoice

To Yonni Shelmerdine

Message invoice.cleaned.pdf

*Check Point SandBlast Threat Extraction has **cleaned** an attachment named **Invoice.doc** as it was determined to contain potentially malicious elements.*

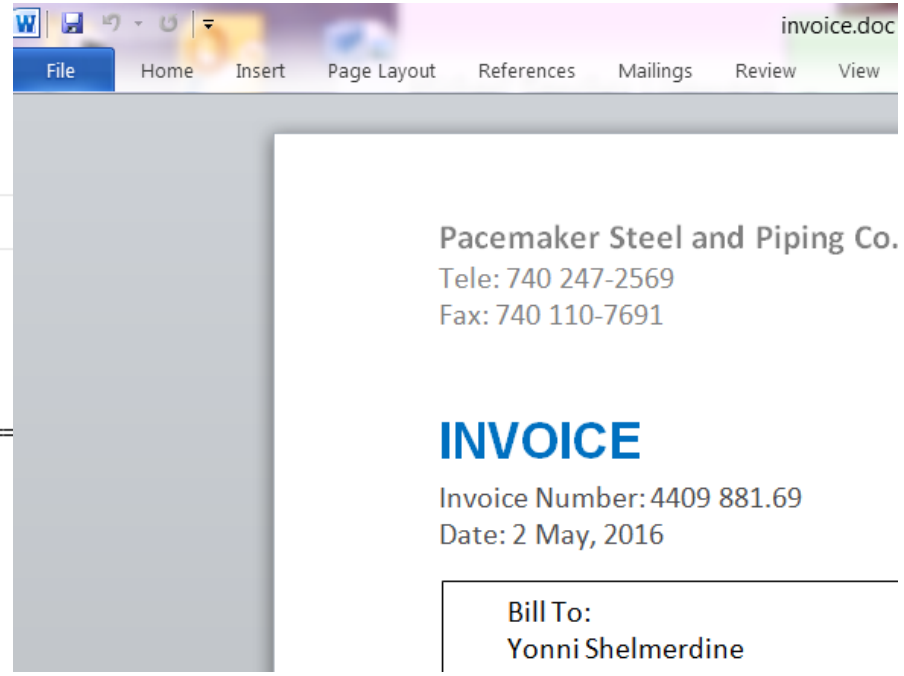
*To access the original file, please click here*

Hi Yonni,
Attached is invoice #4409 881.69 from May which was missing from the original summary.

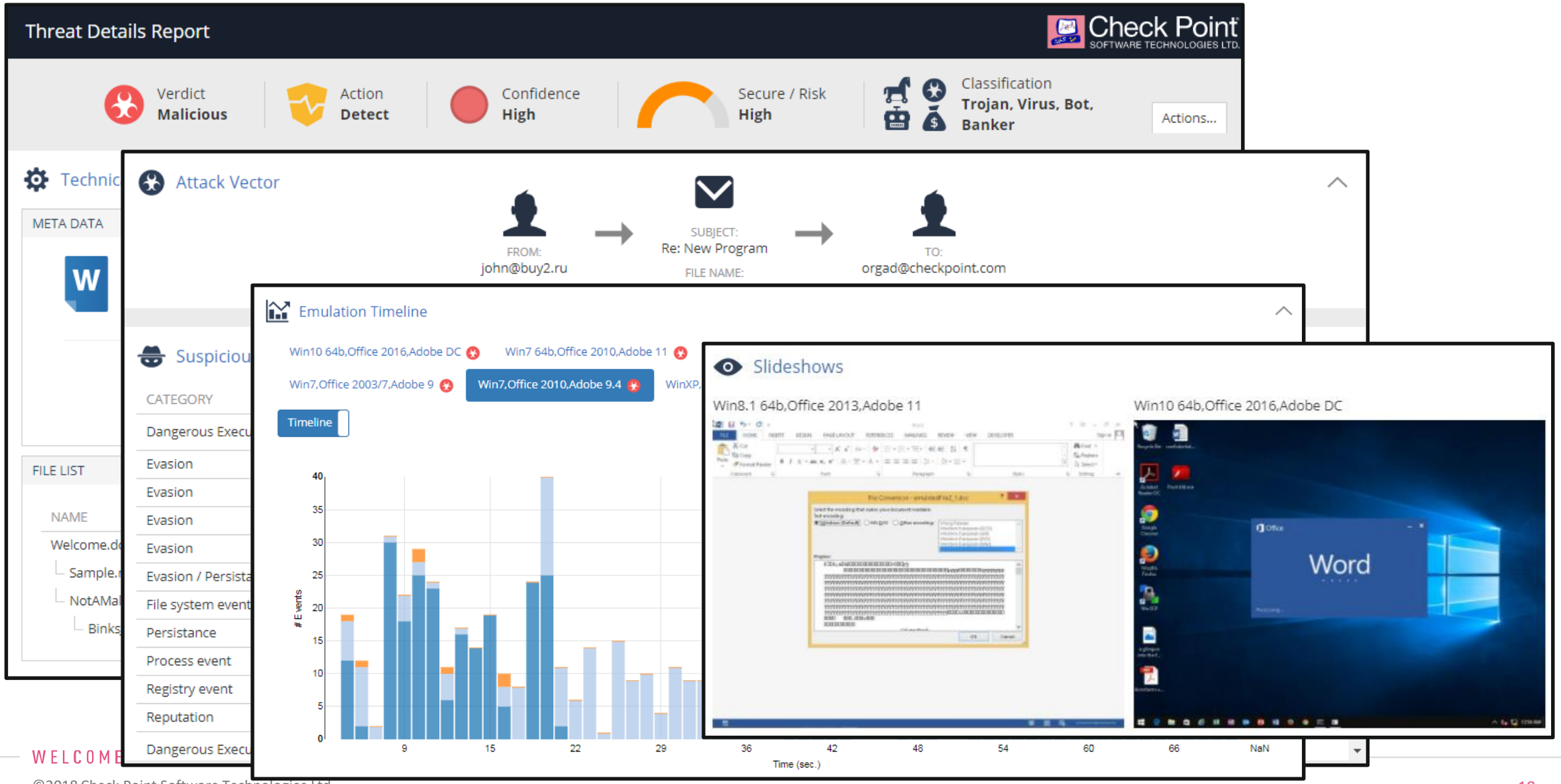
I am out of the office tomorrow and Monday, so I'm emailing you now to request that you go over the invoice, submit the details here [Blocked Malicious URL] and complete they payment as soon as possible.

Julia Reyes / Credit Manager
Pacemaker Steel and Piping Co. Inc.
Tele: 740 247-2569
Fax: 740 110-7691

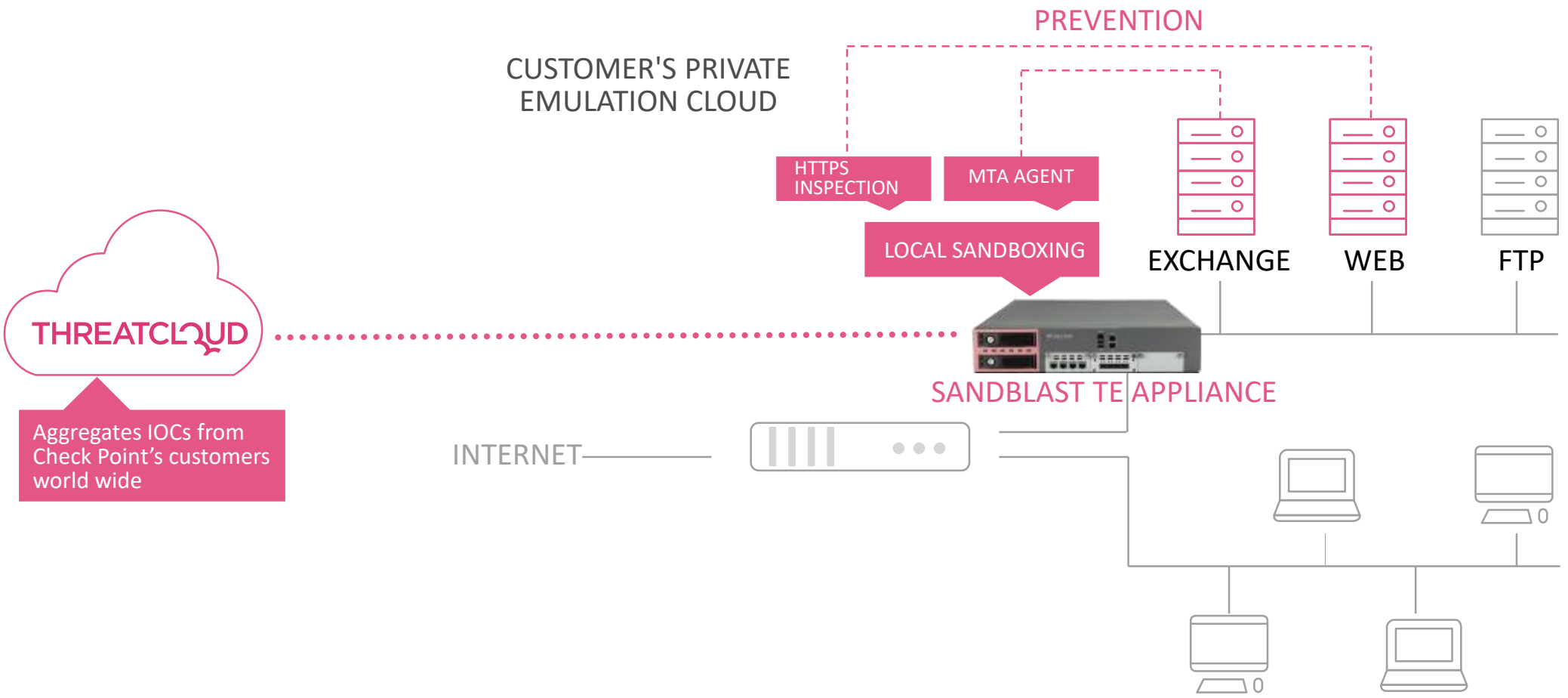
*This Email was secured by Check Point SandBlast Connector for Office 365*



# Отчеты об эмуляции файлов



# Аппаратная песочница

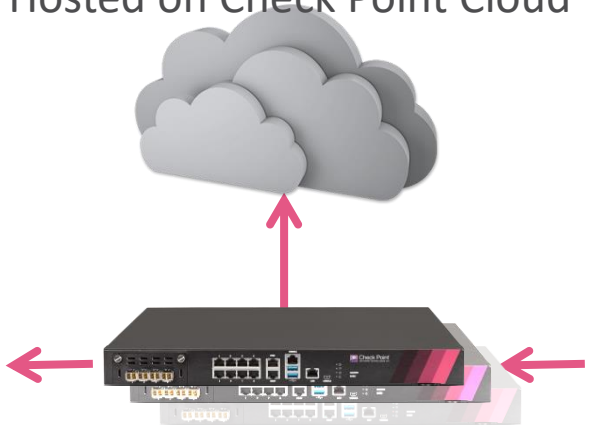


# РАЗЛИЧНЫЕ ВАРИАНТЫ ИНСТАЛЛЯЦИИ

Check Point
SOFTWARE TECHNOLOGIES LTD

## CLOUD SERVICE
Gateways + SandBlast Service

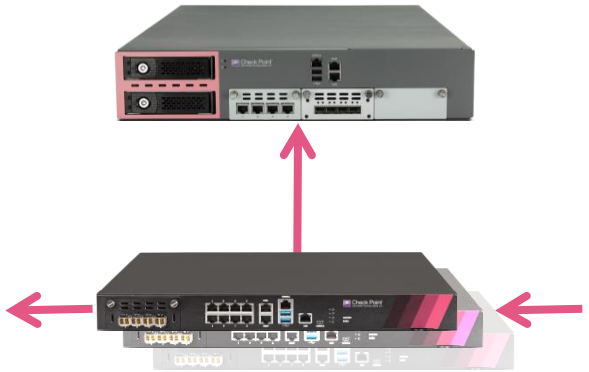
SandBlast Service
Hosted on Check Point Cloud



NGTX Security Gateways

## ON-PREM SERVICE
Gateways + SandBlast TE Appliance

SandBlast TE Appliance



NGTX Security Gateways

## DEDICATED APPLIANCE
Inline SandBlast TE Appliance

SandBlast TE Appliance

- **LEVERAGE SECURITY GATEWAYS** - scale across networks
- Combined with all **NGTP** software blades

**GATEWAYS** и **TE APPLIANCES**:

- Inline / SPAN / TAP
- MTA – mail protection
- ICAP sever – proxy integration

# CHECK POINT ENDPOINT SECURITY

Check Point
SOFTWARE TECHNOLOGIES LTD

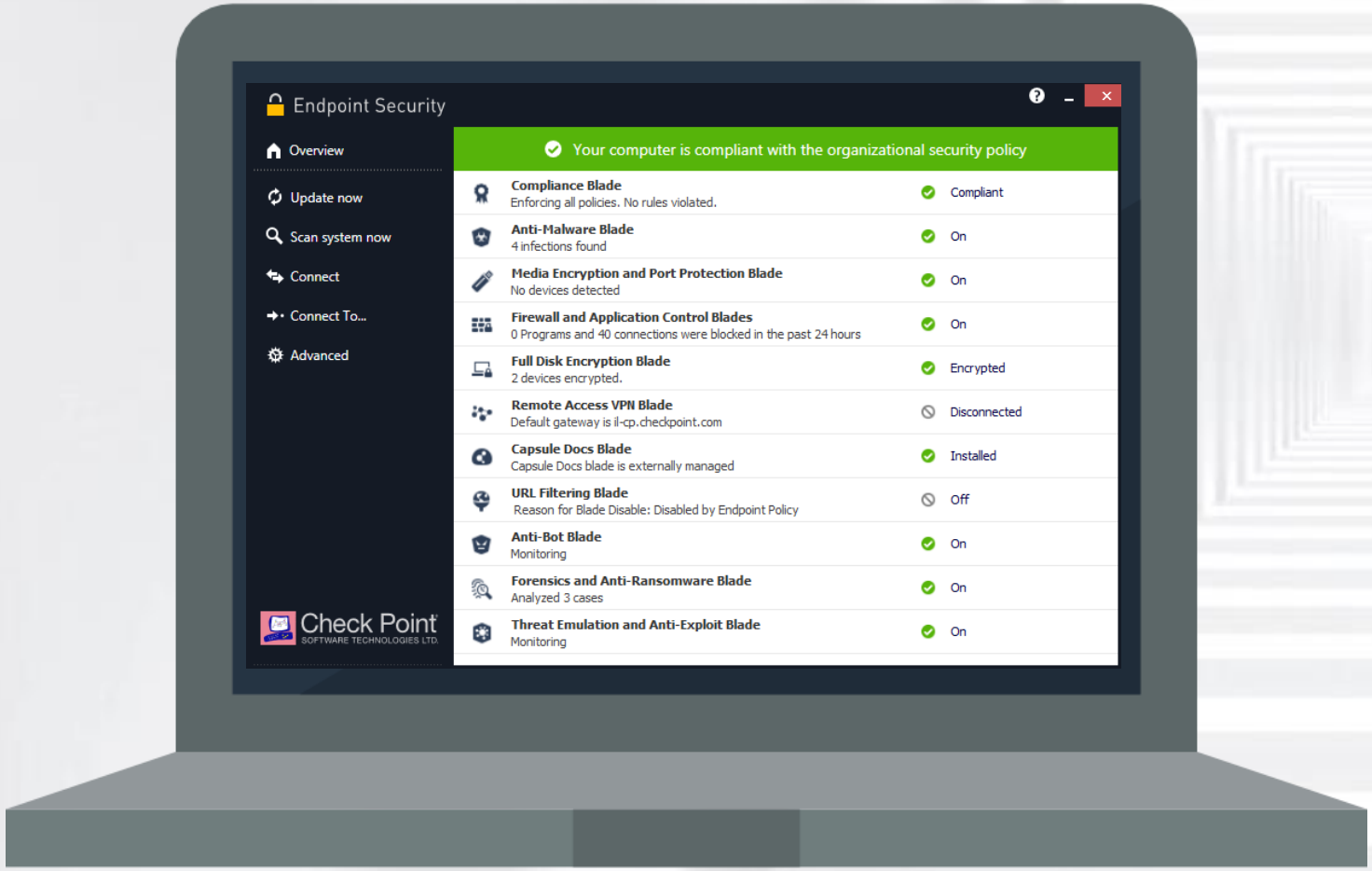
## ENDPOINT

Check Point SandBlast AGENT

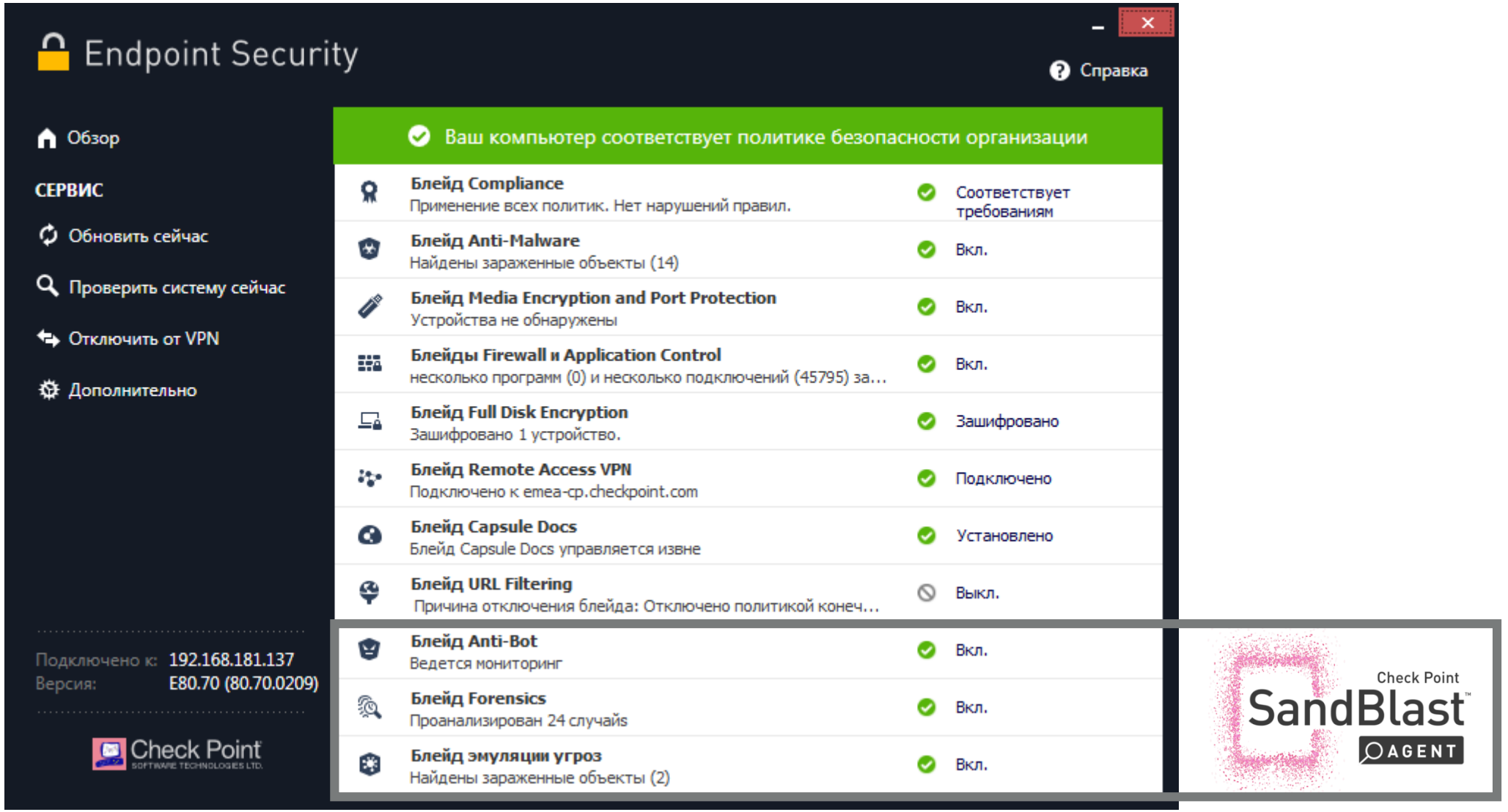
- Threat Prevention
- Anti-Ransomware
- Forensics

**Access/Data Security**

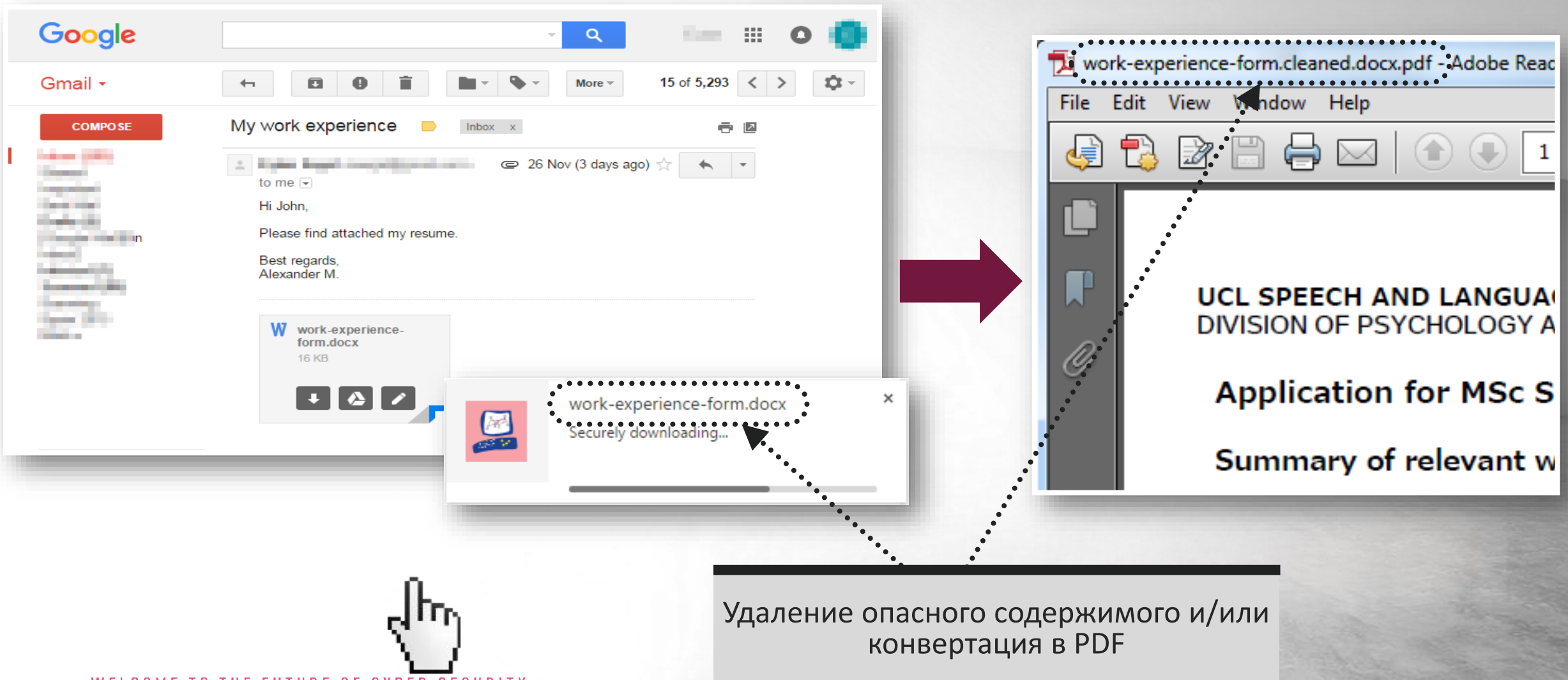
- Access Control
- Secure Media
- Secure Documents



# CHECK POINT ENDPOINT SECURITY



# Защита скачиваемых файлов




Удаление опасного содержимого и/или конвертация в PDF

# Защита от Атак нулевого дня – в два уровня

**Расширение в Браузере**
Для Веб-загрузок

Threat Extraction &

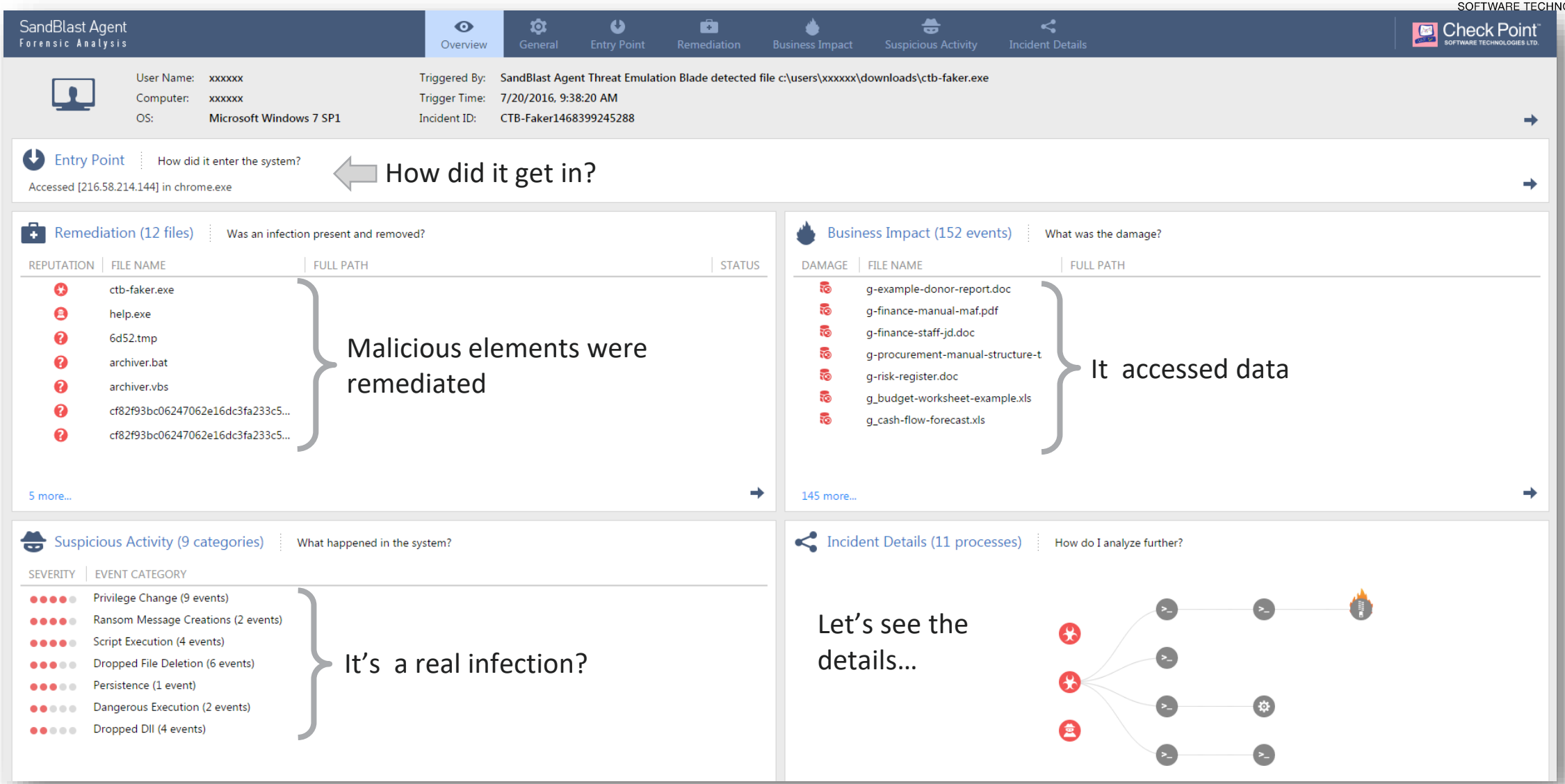
Эмуляция


**Мониторинг Файловой Системы**
Любого скопированного и созданного файла

Эмуляция

**SANDBLAST CLOUD**

# РАССЛЕДОВАНИЕ



**Начало атаки**

Использование браузера Chrome

**Эксплойт**

Процесс-носитель вируса

**Выполнение**

Вредонос записывается на запуск после перезагрузки системы

chrome.exe
Entry Point
aatakiigar.com\...

handle.tmp
Process in Temp, Startup

schtasks.exe
Dangerous Execution

**Триггеры атаки**

Автоматическое обратное отслеживание атаки

Boot

**Загруженный вредонос**

Suspicious Events (1) | Damage (1)

Show 100 entries Search:

| Resource | Impact |
|---|---|
| c:\users\pashap\documents\companysecret.doc | Data Loss: Document |

**Кража данных**

Вредонос читает конфиденциаль-ные данные

**Активация**

Постоянные задачи запускаются после старта системы

oem7ec2.exe
Trigger: akdenizp.com\...

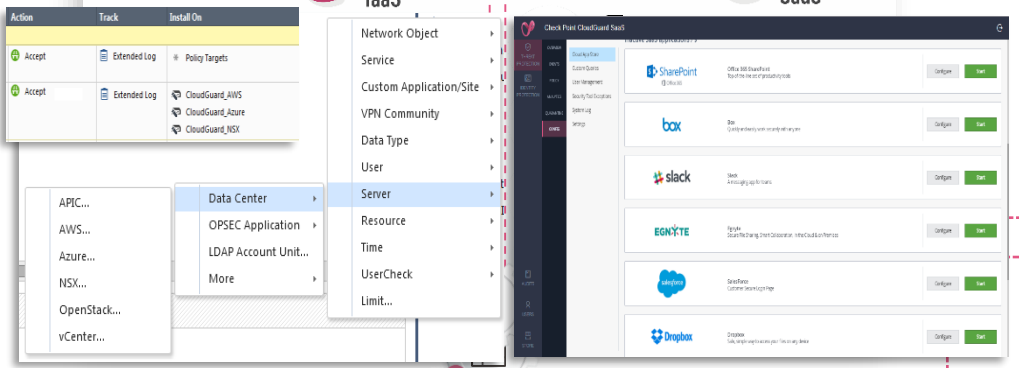
cmd.exe
Dangerous Execution

# CHECK POINT INFINITY

## CLOUD

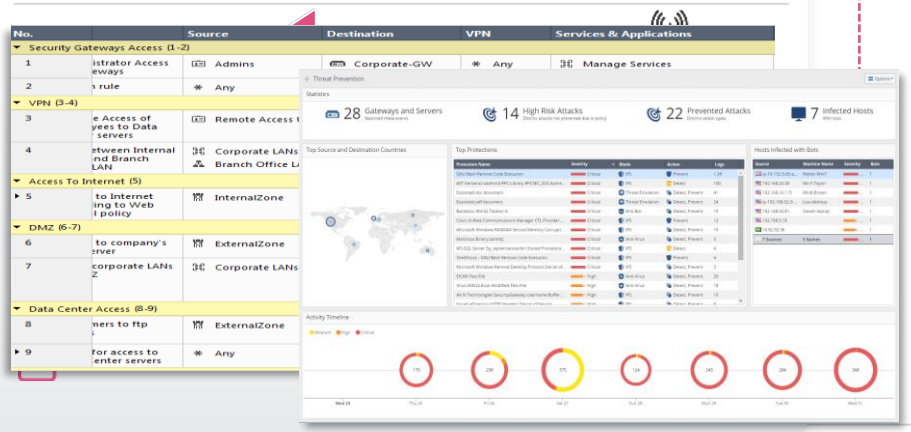
Infrastructure — CloudGuard IaaS

Applications — CloudGuard SaaS




Hybrid Cloud

## NETWORK



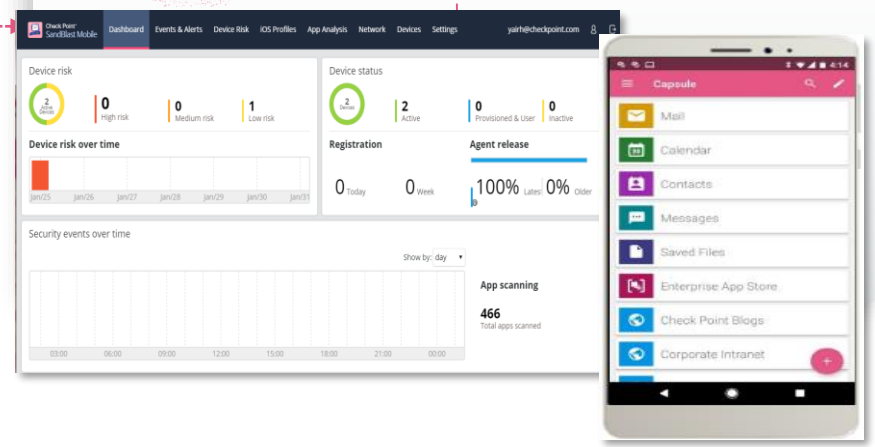

Shared Threat Intelligence

## THREATCLOUD

## MOBILE

Check Point SandBlast MOBILE

Capsule WorkSpace/Docs



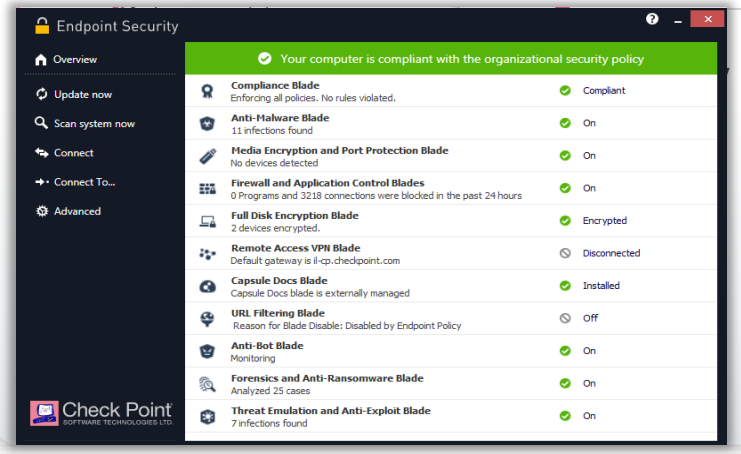

SmartEvent

Compliance

Unified Policy

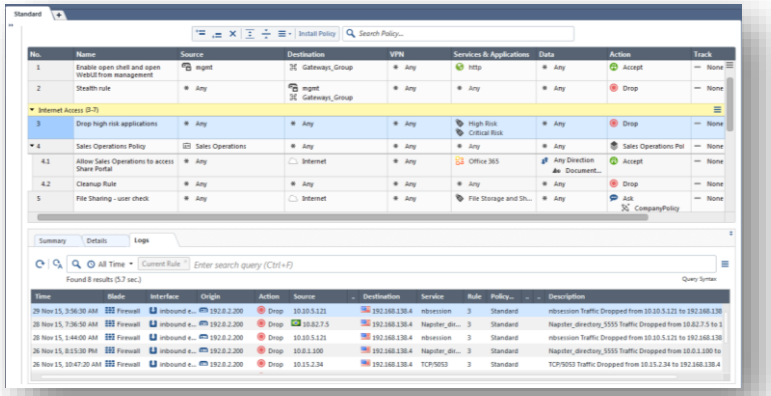
R80 Consolidated Security Management

## ENDPOINT

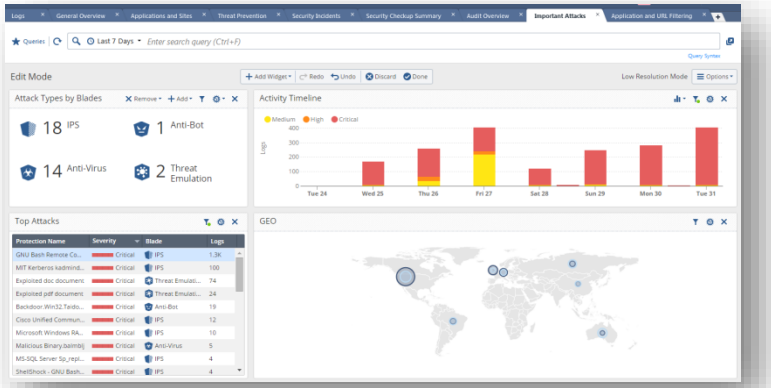


# ЕДИНАЯ СИСТЕМА УПРАВЛЕНИЯ

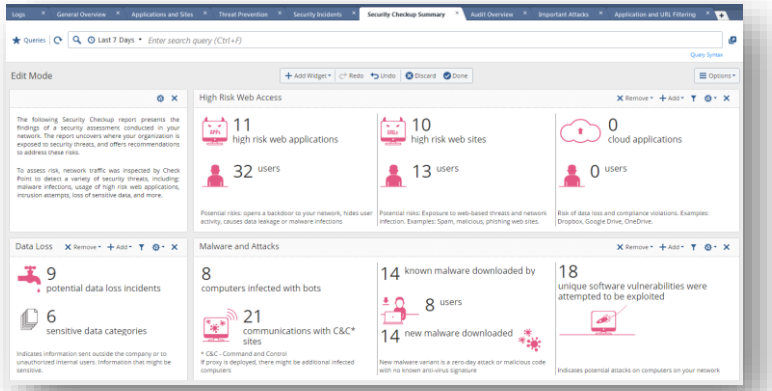
Check Point
SOFTWARE TECHNOLOGIES LTD



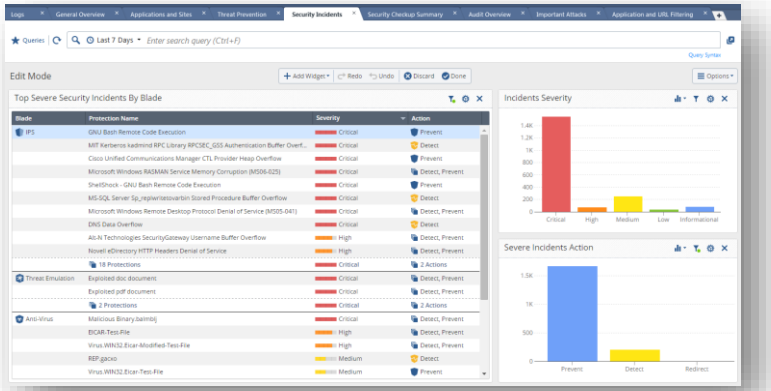
UNIFIED POLICY MANAGEMENT



THREAT MANAGEMENT



REPORTING & COMPLIANCE



FORENSIC ANALYSIS

WELCOME TO THE FUTURE OF CYBER SECURITY


| | |
|---|---|
| Android Antivirus | Network Threats (MiTM,...) |
| OS Vulnerability Research | Apps Analysis / Emulation |

SANDBLAST MOBILE

| | |
|---|---|
| Secure Container | SSL VPN |
| Dual Persona | Native Containment |

CAPSULE WORKSPACE

| | |
|---|---|
| Full-Device VPN / Profile | VDI / VMI |
| Per-App VPN | (Secure) Email Proxy |

CAPSULE VPN

| |
|---|
| Document Repositories |
| Documents Lifecycle |

CAPSULE DOCS

| | |
|---|---|
| Enterprise Apps / Store | Apps White/Black - Listing |
| Apps White/Black - Listing | App Profile Management |

CAPSULE WORKSPACE

| | |
|---|---|
| Device "Fleet" Management | GEO-Location Tracking |
| Device Profiles (Settings) | App Distribution |

MobileIron · MaaS360 · airwatch · XenMobile · Microsoft Intune · BlackBerry UEM

Check Point
SOFTWARE TECHNOLOGIES LTD

# КАК МЫ ЭТО ДЕЛАЕМ?

WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY CHECK POINT INFINITY

CLOUD • MOBILE • THREAT PREVENTION

# Check Point Security CheckUP

## 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**

**БЕСПЛАТНО и конфиденциально**

**Оптимальный срок для прохождения Security CheckUP – 2-4 недели**

# SECURITY CHECKUP

## THREAT ANALYSIS REPORT

Check Point
SOFTWARE TECHNOLOGIES LTD

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



## 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 бекдоров в вашу сеть, сокрытие пользовательской активности, возможность утечки данных или заражения вредоносным ПО.

**0** опасные вэб-сайты

**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 соответствий требованиям регуляторов и стандартов безопасности. Примеры: Dropbox, Google Drive, OneDrive.

### Утечка данных

**49** потенциальных утечек данных

**7** категорий данных

### Вредоносное ПО и атаки

**7** зараженных ботами компьютеров

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

**14** известных вирусов, зашруженных

**8** пользователями

**14** новых вирусов загружено

**18** попыток использовать уникальные программные уязвимости

# CHECK POINT PROVIDES ITS CUSTOMERS THE BEST SECURITY EVERYWHERE WITH THE INDUSTRY'S LARGEST SECURITY ECOSYSTEM

Check Point
SOFTWARE TECHNOLOGIES LTD

## THREAT INTELLIGENCE

Blueliv. NetClean. FLASHPOINT Cyberint Protection Beyond the Perimeter malwarepatrol SIXGILL MINERVA sentrybay IID mnemonic - securing your business SenseCy Sensing Cyber PHISHLABS Prevent. Defend. Fight back. geoedge Add Integrity Malware Patrol Intsights Detect. Analyze. Remediate. ZEROFOX

## MOBILE

MATRIX42 SMARTER WORKSPACE - BETTER LIFE MobileIron COMMUNITAKE SAP Acronis ERICOM Access Done Right airwatch MaaS360 by Fiberlink, an IBM company SOPHOS FancyFon

## CLOUD & INFRASTRUCTURE

OVERTURE vmware technology alliance PARTNER GARLAND TECHNOLOGY See every bit, byte, and packet. PLUMgrid openstack CLOUD SOFTWARE WIND nuagenetworks silver peak IMVISION TECHNOLOGIES ARISTA CISCO ADVA Optical Networking Google Cloud Premier Partner Gigamon Flowmon radware velocloud Premier Partner ECI THE ELASTIC NETWORK intel Telco Systems A BATM Company riverbed Think fast. A10 amazon web services Partner Network ECESSA Microsoft

## APPLIANCES

resilience BLUE COAT hp ADLINK TECHNOLOGY INC. FUJITSU altair A SONY Company

## CASB

CloudLock AVANAN FIRELAYERS ManagedMethods palerra skyhigh

## MANAGEMENT

karmasis SKYBOX SECURITY LogRhythm The Security Intelligence Company Lancope servicenow PICUS WAVECREST RSA READY REDSEAL IBM savvius Trustwave ALIEN VAULT ArcSight Symantec ManageEngine Powering IT ahead PASSLOGY NATION-E tufin NETFORMX netfli Work Smarter. FIREMON algosec BACKBOX eiQ networks splunk> ORACLE Enabling the Information Age cyber OBSERVER indeni the network knowledge co. LogRhythm The Security Intelligence Company SENSAGE Enterprise Security Analytics BLACKSTRATUS solarwinds

## ICS

CyberX NOZOMI NETWORKS RAD Your Network's Edge SCADAfence NATIONE where power gets smart ics2 SECURITY MATTERS

## COMMUNICATIONS

SIEMENS AVAYA ALCATEL Telco Systems A BATM Company AudioCodes

## ENFORCEMENT

VASCO THE AUTHENTICATION COMPANY GuardiCore Carbon Black. Menlo Security McAfee Together is power. ZEROFOX ERPScan zscaler The Leader in Cloud Security BRTOKEN Attivo NETWORKS gemalto security to be free CYBERARK POSITIVE TECHNOLOGIES tripwire fireglass SenseCy Sensing skyhigh RSA READY BRADFORD NETWORKS rapid threat response ForeScout CyberX OpenDNS InfoBay Email Security Just Got Smarter AVANAN GlobalSign GMO INTERNET GROUP CloudLock ics ADALLOM FEITIAN WE BUILD SECURITY SECURITY MATTERS HEXADITE Automated Cyber Incident Response iPass FIRELAYERS portnox boundlessly smart Twistlock SCADAfence IRONSCALES Automated Phishing Response SAFE-T Accelerating Safe Business SECUREPUSH aruba a Hewlett Packard Enterprise company OPSWAT NetFlowAuditor Network Super Visor DAMBALLA SafeNet.

Check Point
SOFTWARE TECHNOLOGIES LTD

**160+**

**TECHNOLOGY PARTNERS**

Source: https://www.checkpoint.com/partners/opsec

Check Point
SOFTWARE TECHNOLOGIES LTD

# СПАСИБО!

WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY CHECK POINT INFINITY

CLOUD • MOBILE • THREAT PREVENTION