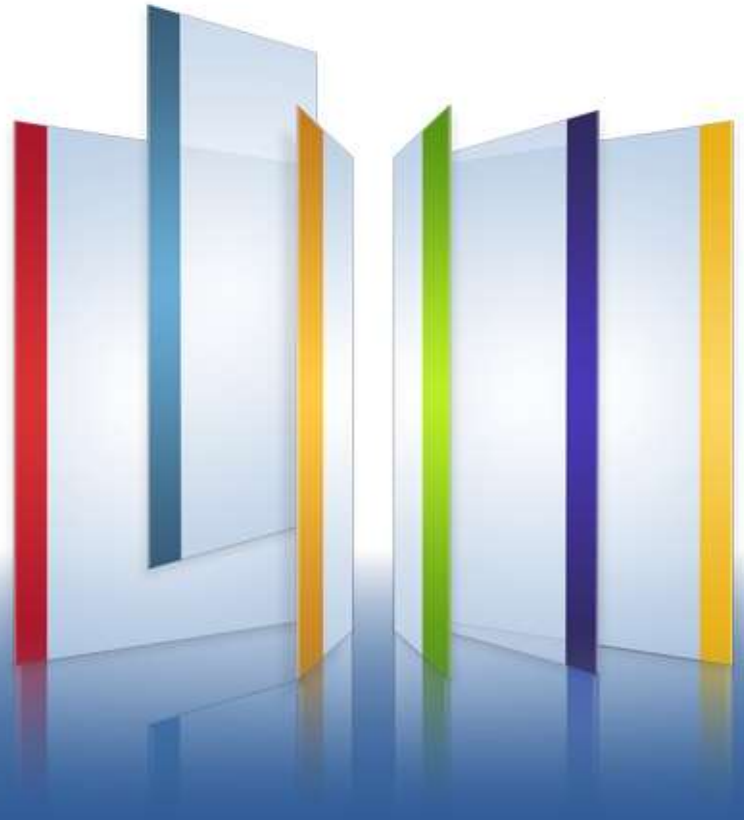
Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Основные угрозы 2012 года, или как не пострадать в 2013 году



Дмитрий Коровин
korovin@checkpoint.com
Консультант по безопасности
Check Point Software Technologies

Шлюзы безопасности

Check Point SOFTWARE TECHNOLOGIES LTD.

Линейка аппаратных, программных и виртуальных решений!

3D SECURITY softwareblades™

61000 **серия**

21000 **серия**

1100 **Серия**

NEW

12000 **серия**

4000 **серия**

2200 **серия**

***Ultra* High-End**

Datacenter Grade

Enterprise Grade

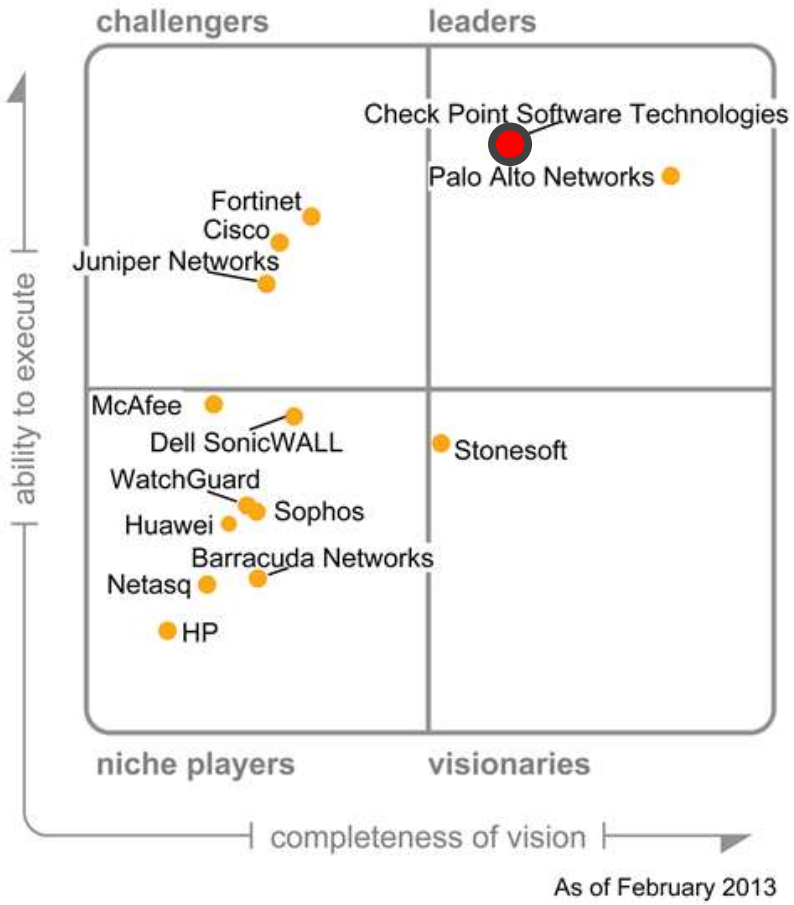
Small Office – Desktop

360° Check Point - лидер рынка

ГОСТ

Check Point SOFTWARE TECHNOLOGIES LTD.

Magic Quadrant
Enterprise Network Firewalls



Единственный лидер рынка с решениями, соответствующими российским реалиям!

Top Scores with Triple Recommend

Check Point SOFTWARE TECHNOLOGIES LTD.

NGFW

98.5%

Management and Security Effectiveness

2013 NGFW Group Test

IPS

99.0%

Overall Protection

Product Analysis Report

Firewall

100%

Management and Security Effectiveness

2013 Firewall Group Test

Требования ФЗ 152

«Положение о методах и способах защиты информации в информационных системах персональных данных» Приказ ФСТЭК России N 58 от 05.02.2010

МЭ 3 класса	IPS	НДВ 4 уровня
Раздел 4.4. Безопасное межсетевое взаимодействие для информационных систем 1 класса при их подключении к сетям международного информационного обмена достигает путем приме средств экра [пер	Раздел 6. Обнаружение вторжений проводится … путем использования в составе информационной системы … средств (систем) **обнаружения вторжений**	Раздел 7. Для информационных систем 1 класса применяется программное обеспечение средств защиты информации, соответствующее 4 уровню контро отсутстви

Начиная с Check Point R65, R71, …

В Check Point R71 , сертификат 2604, 2811

В Check Point R71 , сертификат 2604

Основано на реальных данных

Check Point Appliance

Check Point
SOFTWARE TECHNOLOGIES LTD.

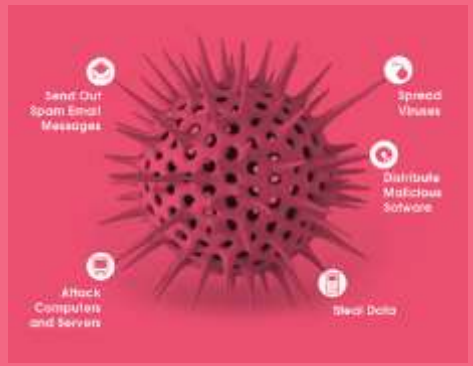
Итого:

888	компаний
1,494	шлюзов
120,000	часов мониторинга
112,000,000	событий безопасности

Три класса проблем

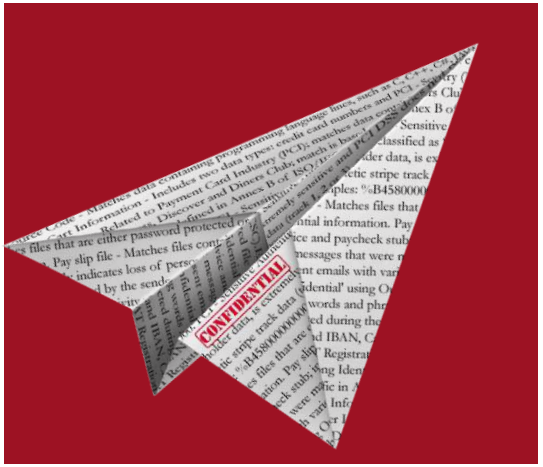
Check Point SOFTWARE TECHNOLOGIES LTD.

Вредоносное ПО

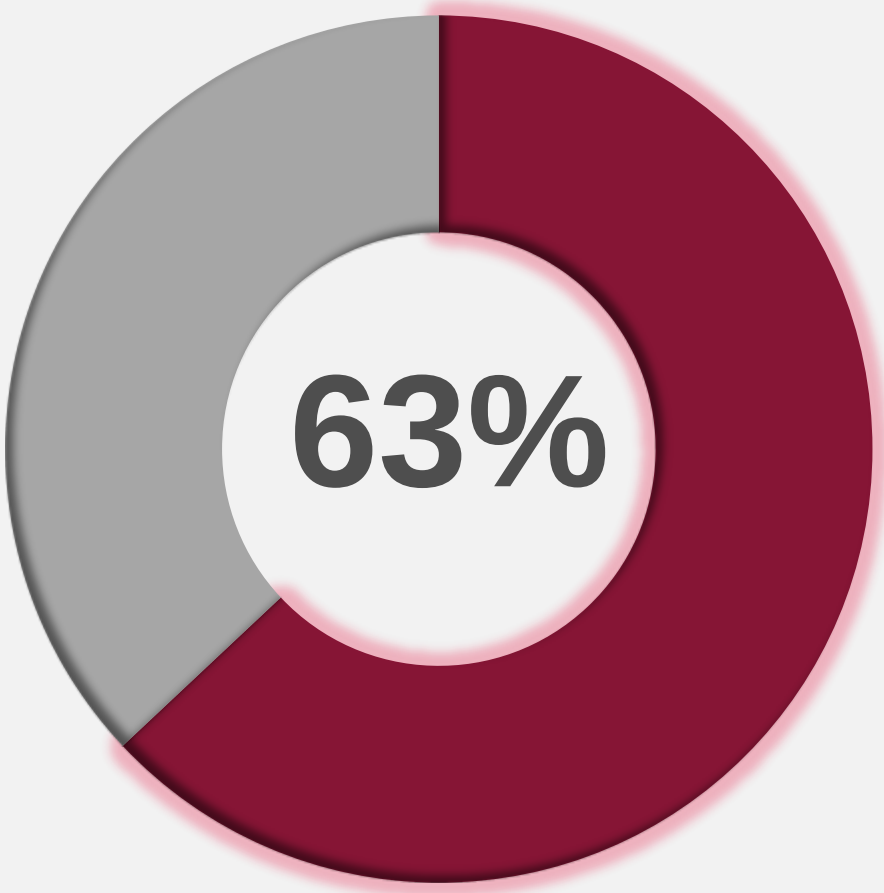


Использование небезопасных сервисов

Утечка данных



Большинство компаний инфицированы!



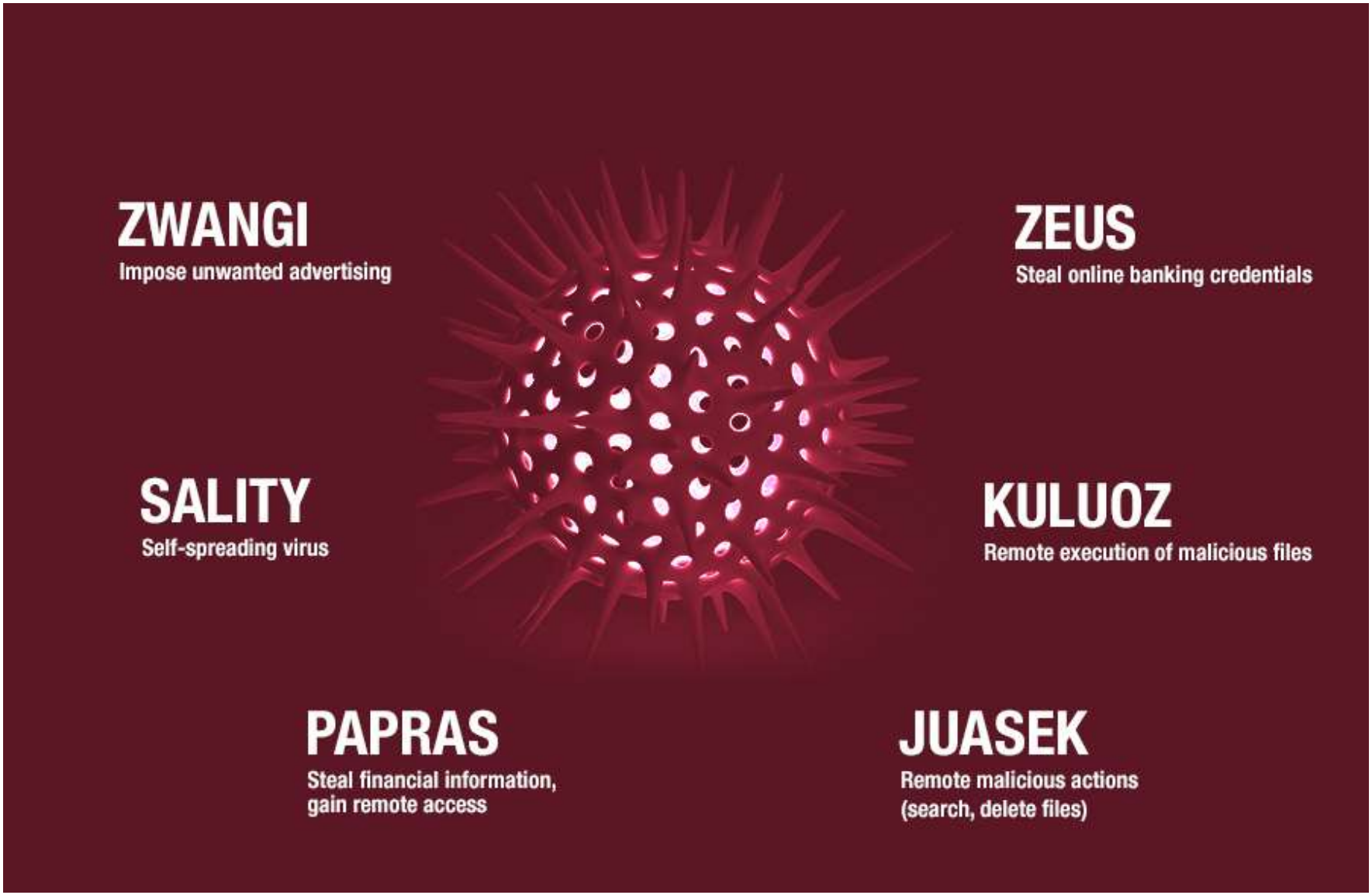
Организаций инфицировано вредоносным ПО (ботнеты…)

Каждый день новая жертва

Это же меня не коснется, так ведь?

Ботнеты…

Основные ботнеты в 2012 году



Не только ботнеты…

Инфицирование в реальном времени

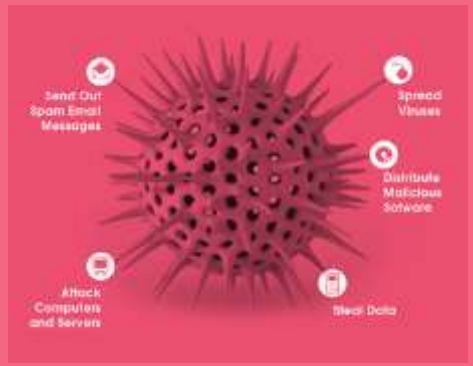
53%

организаций наблюдали скачивание вредоносного ПО

Три класса проблем

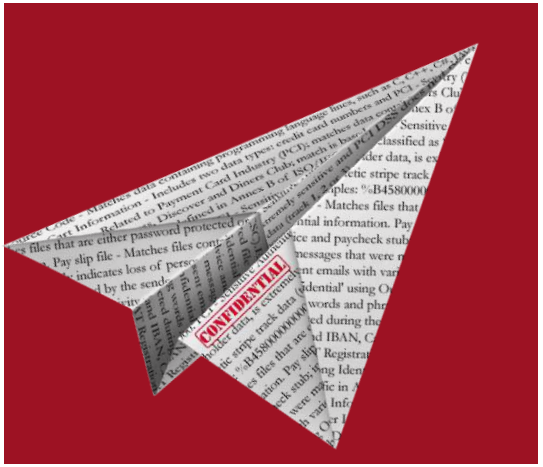
Check Point SOFTWARE TECHNOLOGIES LTD.

Вредоносное ПО



Использование небезопасных сервисов

Утечка данных



Не просто развлечения…

Какие приложений опасны?

Check Point SOFTWARE TECHNOLOGIES LTD.

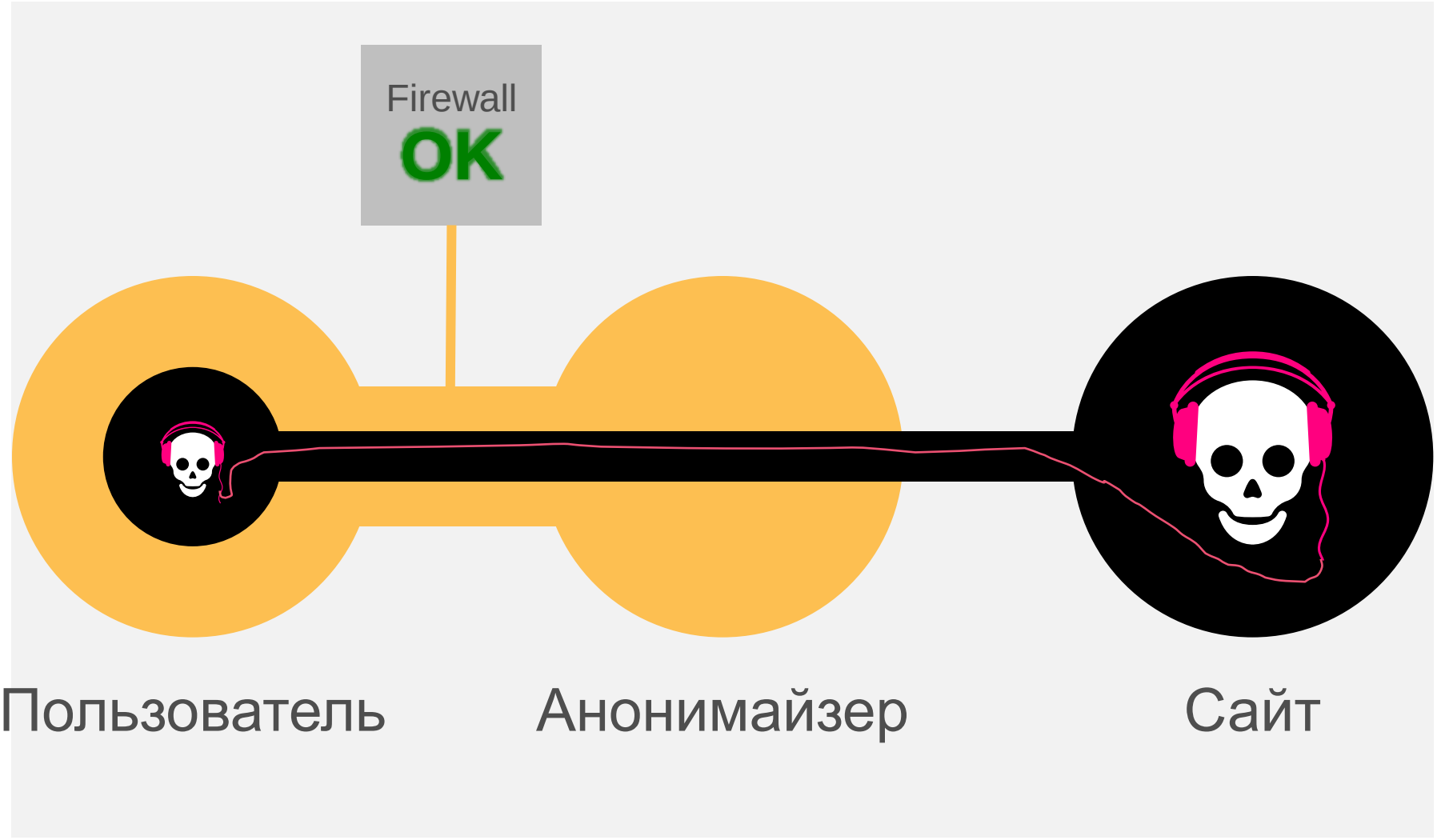
Обходят стандартный периметр безопасности

- P2P file sharing
- Anonymizers

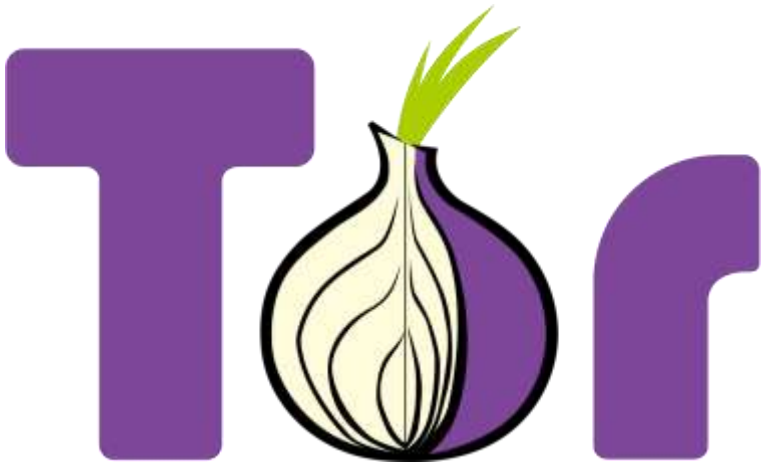
Вред наносится без участия пользователя

- File sharing / storage
- Social networks

Что такое анонимайзеры?



TOR



“The Onion Router”

Создана по заказу ВМС США

80% бюджета 2012 года получено от правительства США

Широко применялся в «Арабской весне»

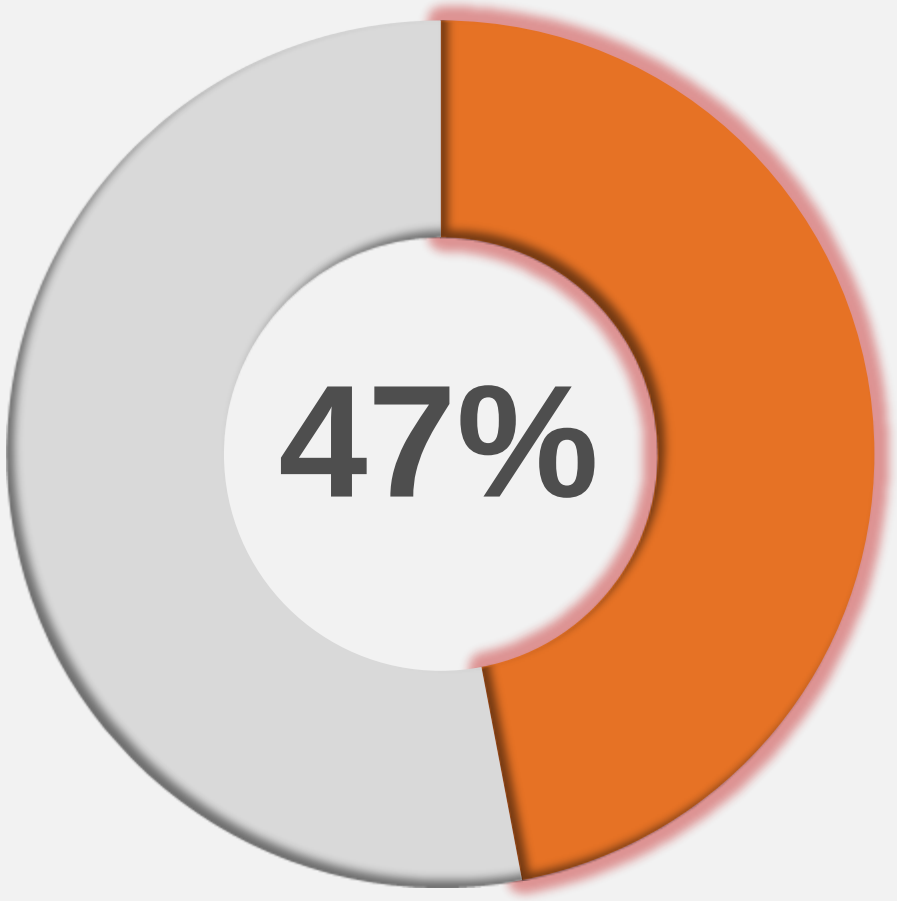
Основные риски

Обход периметр безопасности

Используются ботнетами для связи с командными центрами

Используются пользователями для скрытия нелегитимной активности

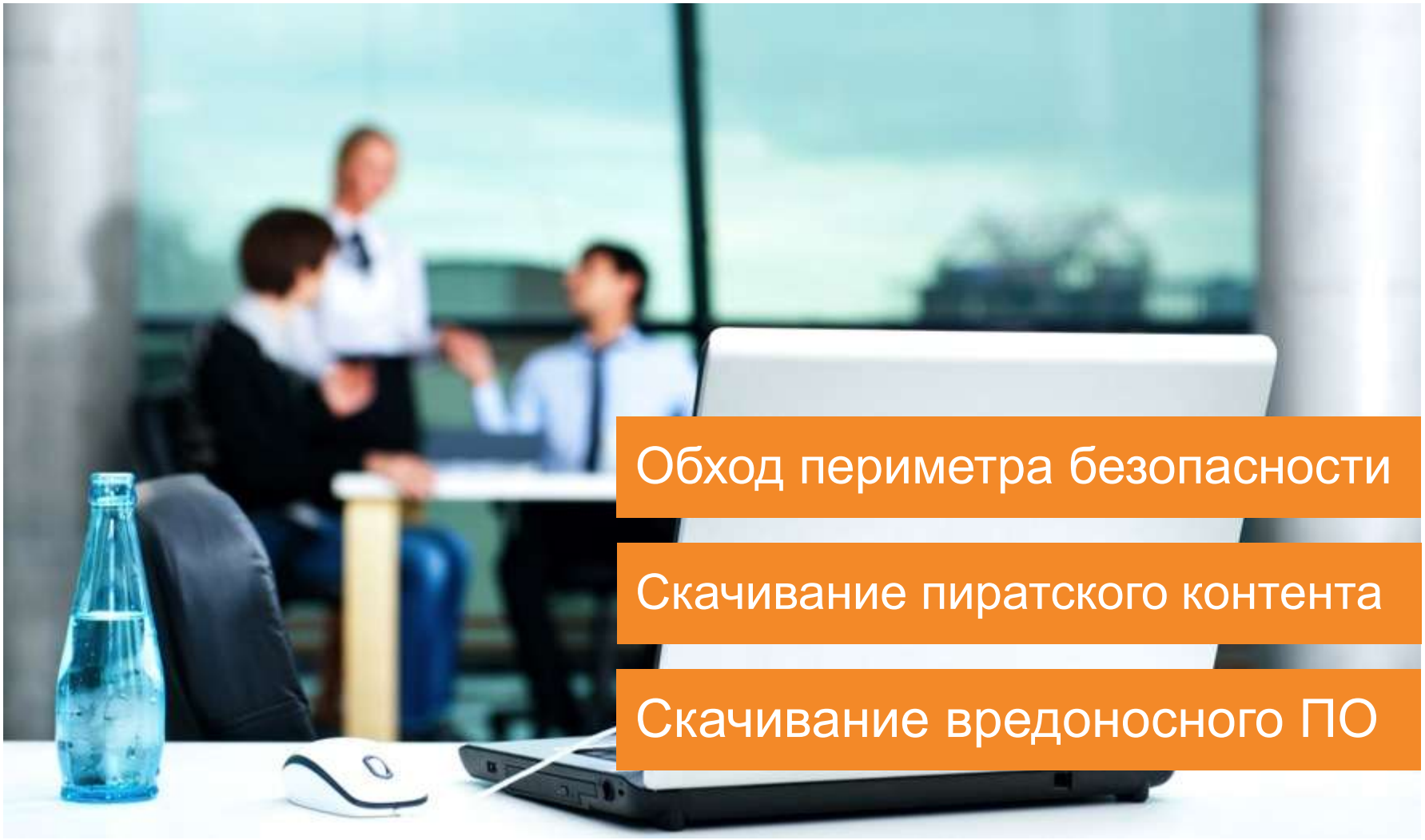
Использование анонимайзеров



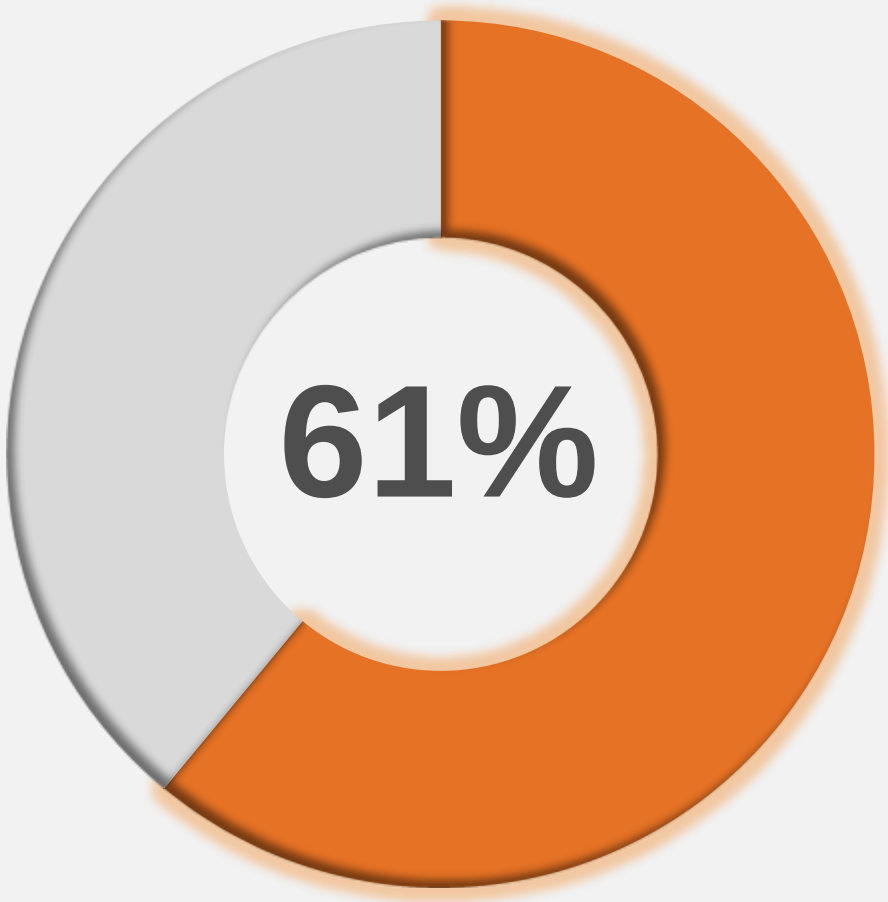
использовали анонимайзеры

(И в 80% случаях об этом не было известно администраторам безопасности)

Риски P2P приложений



Peer-to-peer

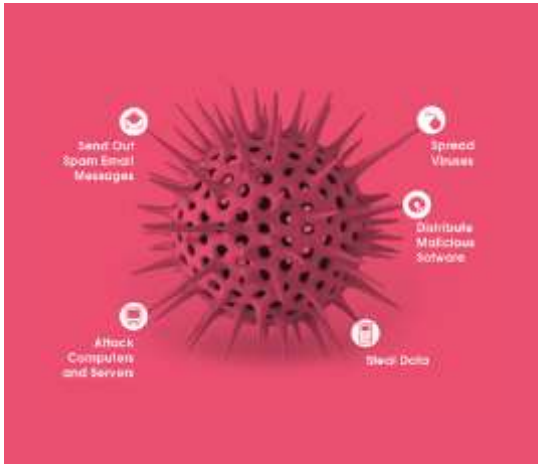


организаций подверглись рискам P2P сетей

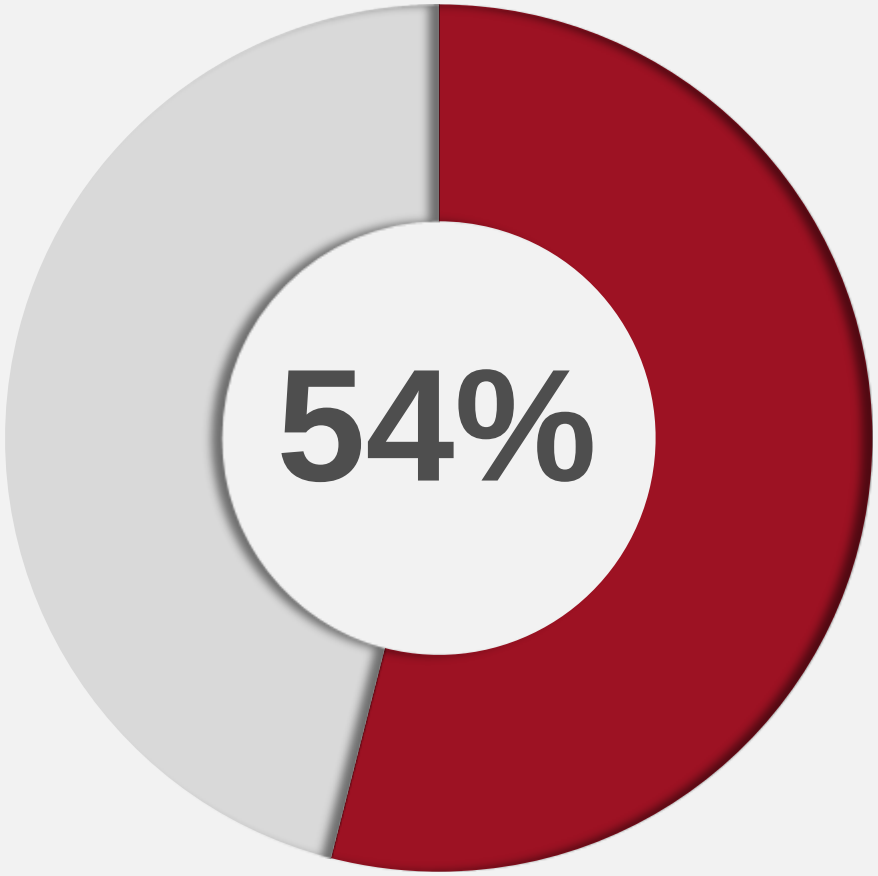
Три класса проблем

Check Point SOFTWARE TECHNOLOGIES LTD.

Вредоносное ПО	Использование небезопасных сервисов	Утечка данных



Как часто это происходи?



организаций пострадали от утечки данных

Что же мы нашли?

24% Source Code

14% Password protected file

7% Email marked as confidential

29% Credit card information

13% Salary compensation information

7% Bank accounts numbers

6% Business data record

21% Other

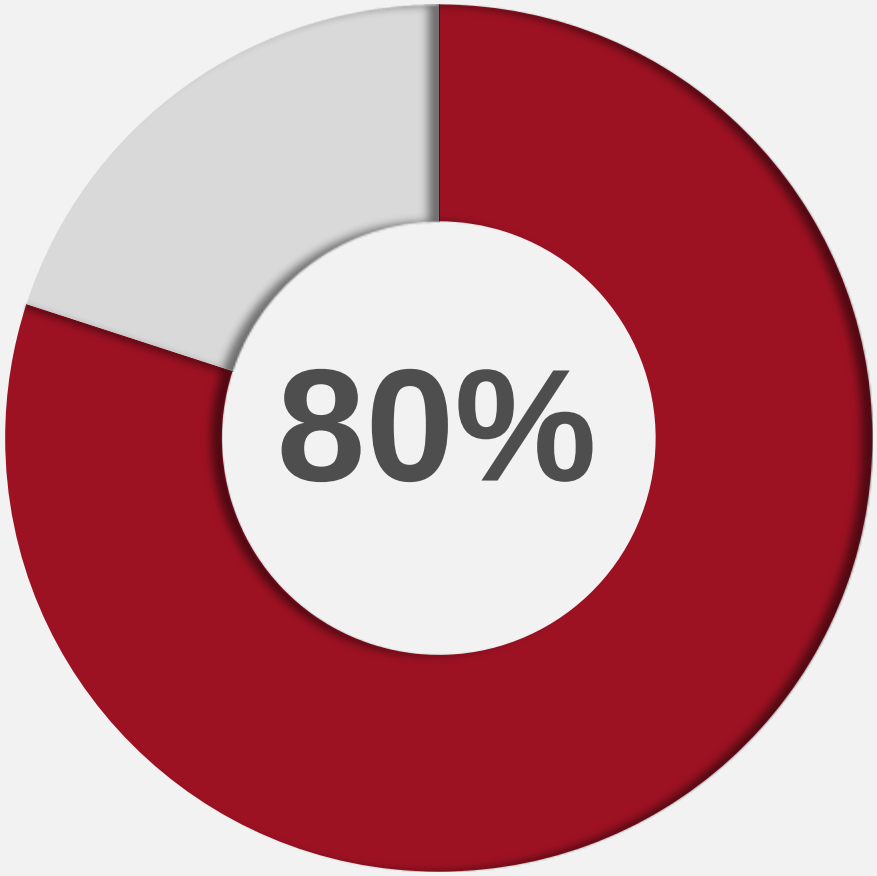
Все встречаются с этой проблемой!

Check Point SOFTWARE TECHNOLOGIES LTD.

Error 552: sorry, that message exceeds my maximum message size limit

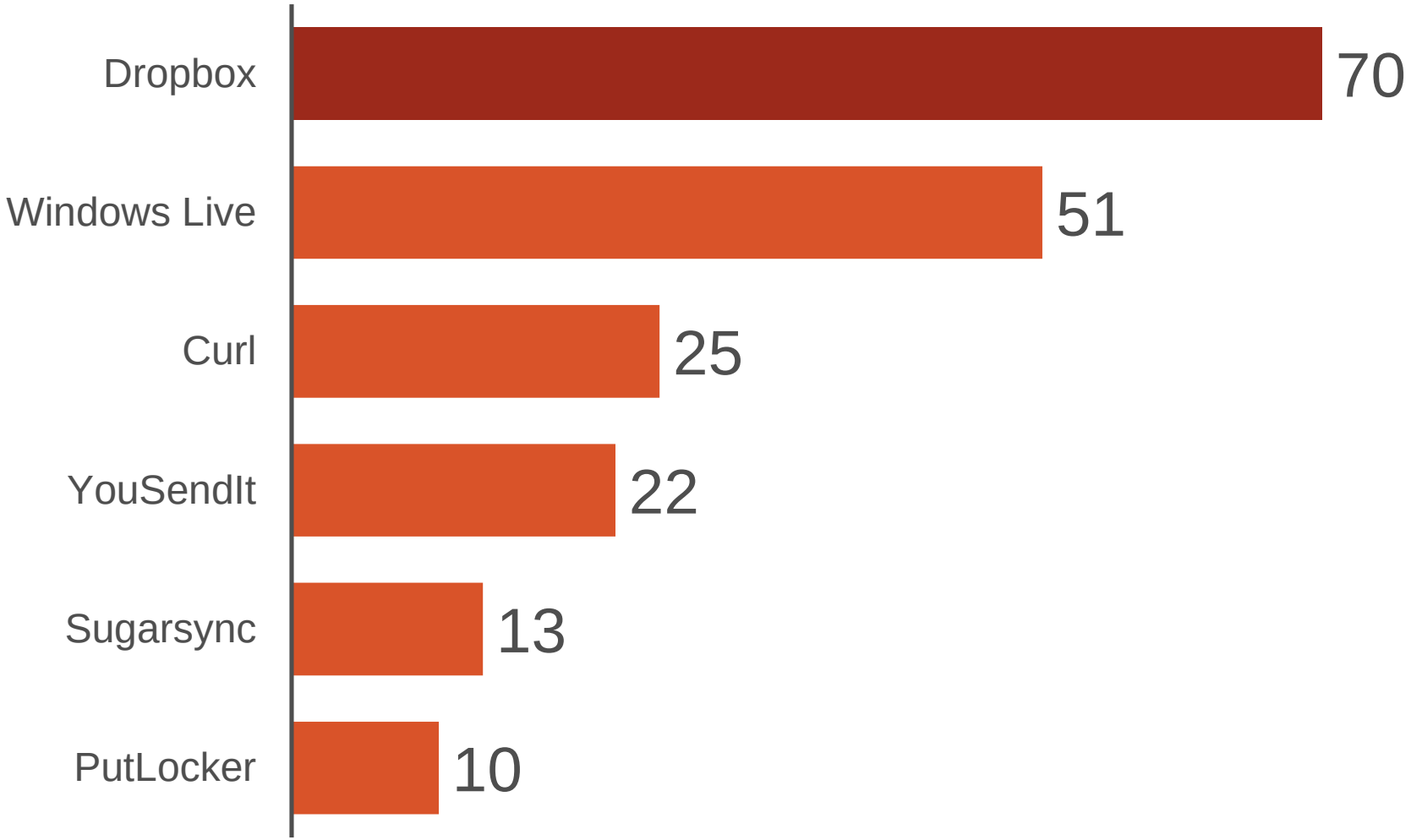
Dropbox? YouSendIt? Windows Live?

File sharing сервисы



Организаций использовали сервисы внешнего хранения файлов

Мы нашли:



Что нужно помнить?

Check Point SOFTWARE TECHNOLOGIES LTD.

Угрозы организации	Риски приложений	Утечка данных
63%	**47%**	**54%**
Инфицированы ботнетами	Использовали анонимайзеры	Столкнулись с утечкой данных

Как заблокировать атаку?

Защита от внешних угроз и вторжений (bots, malwares...)

Firewall

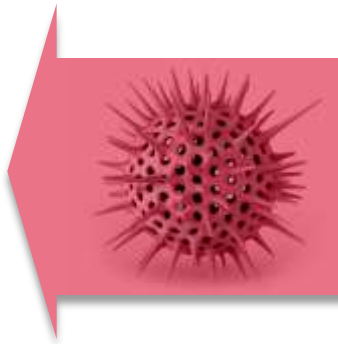
IPS

AntiBot

Antivirus

URL Filtering

Emulation



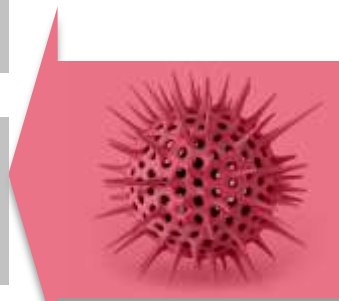
Постоянный мониторинг

R76
Multi Domain Management

SmartDashboard

SmartLog

SmartEvent



ThreatCloud™ Dynamically updated intelligence

Check Point SOFTWARE TECHNOLOGIES LTD.

Глобальное взаимодействие для моментальной реакции

Real-time Security Intelligence

Шлюзы постоянно обновлены

Threat Cloud™ растет

Свыше **250 миллионов** адресов

Свыше **12 миллионов** malware signature

Свыше **1 миллиона** malware-infested sites

1,000 URL обновлений в **день!**

50,000 сигнатур обновляется за **день!**

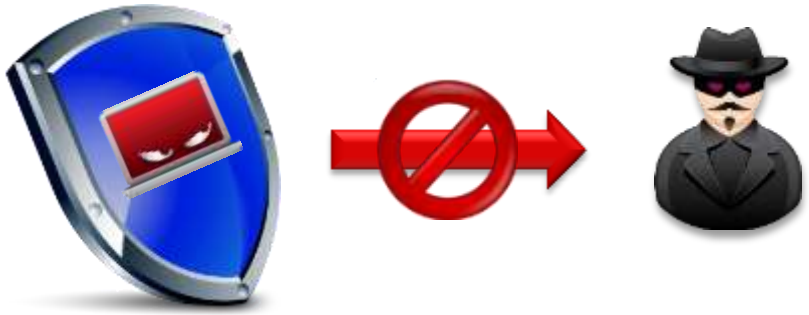
Многоуровневое решение

Check Point SOFTWARE TECHNOLOGIES LTD.

IPS — Prevent exploit of known vulnerabilities

Antivirus — Block download of known malware

Anti-Bot — Block Bot Communication



Emulation — Unknown Threats

Комплексная защита от Check Point

Check Point SOFTWARE TECHNOLOGIES LTD.

IPS

Mobile Access

DLP

Application Control & URL Filtering

Identity Awareness

Network Threat Prevention

Remote VPN – Mobile Access

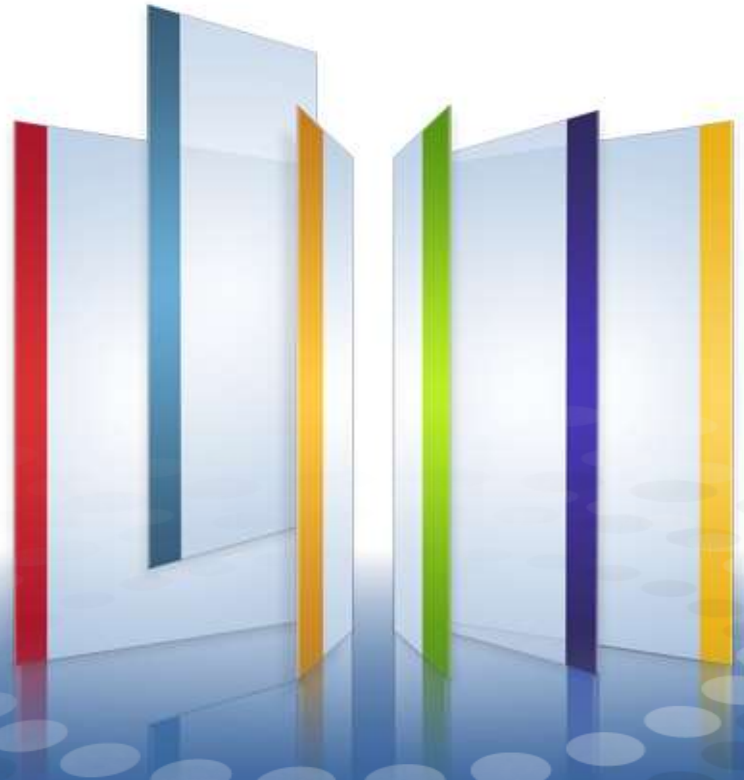
Prevent leakage of corporate Data

Control access to Application and URLs

New User based Policies

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Спасибо!



Дмитрий Коровин
korovin@checkpoint.com
Консультант по безопасности
Check Point Software Technologies