



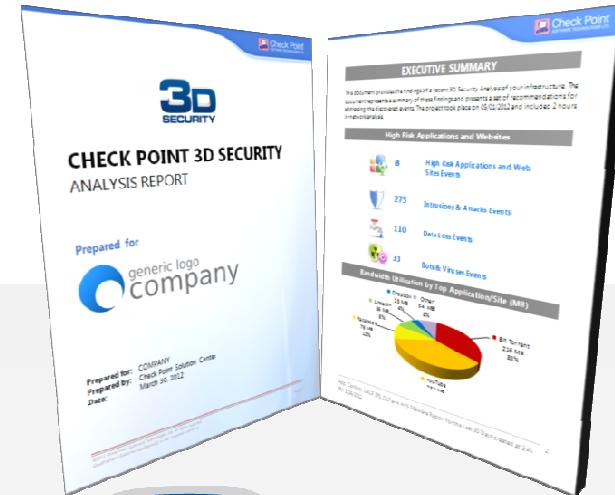
Check Point Appliance



No.	Date	Time	User	Source
1	7Apr2011	16:24:17	setup1	jack jack-8000.ad...
2	8Nov2010	13:22:02	Califo...	Joe Astor... danny.myBiz...
3	1Mar2011	18:18:30	172.1...	john 192.168.2.187
4	1Mar2011	18:18:31	172.1...	john 192.168.2.189
5	1Mar2011	18:18:30	172.1...	john 192.168.2.177
6	8Nov2010	13:22:	All Events	Last 12 Hours show up to 5000 Events
7	8Nov2010	13:22:		Search:
8	8Nov2010	13:22:		Count Product Name Event Name
9	8Nov2010	13:22:	9 Check Point DLP	DLP Incident
10	8Nov2010	13:22:	73 Check Point IPS Software Blade	6 Event Names
11	8Nov2010	13:22:	6 Check Point Security Gateway	Port scan from external network
12	8Nov2010	13:22:	7 Check Point IPS Software Blade	2 Event Names
13	8Nov2010	13:22:	10 Check Point Endpoint Security	2 Event Names
14	8Nov2010	13:22:	16 Check Point DLP	DLP Incident
15	8Nov2010	13:22:	11 Check Point IPS Software Blade	JavaScript Percent Encoding ...
16	8Nov2010	13:22:	7 Check Point DLP	DLP Incident
17	8Nov2010	13:22:	12 Check Point Endpoint Security	4 Event Names
18	8Nov2010	13:22:		2 Event Names
19	8Nov2010	13:22:		
20	8Nov2010	13:22:		
21				
22			4 8 7 37 75	
23			55.228 55.228 55.228	
24				
25				

Security Logs & Events

3D
Security
Analysis
Tool



Connected Inline or Via Mirror Port



softwareblades™

Итого:



888

компаний

1,494

шлюзов

120,000

часов мониторинга

112,000,000

событий безопасности

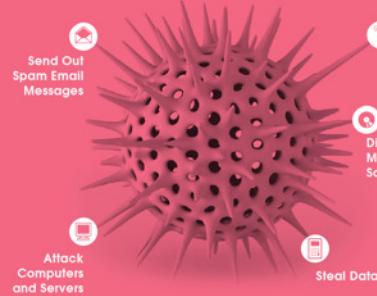


softwareblades™

Три класса проблем



Вредоносное ПО



Использование небезопасных сервисов

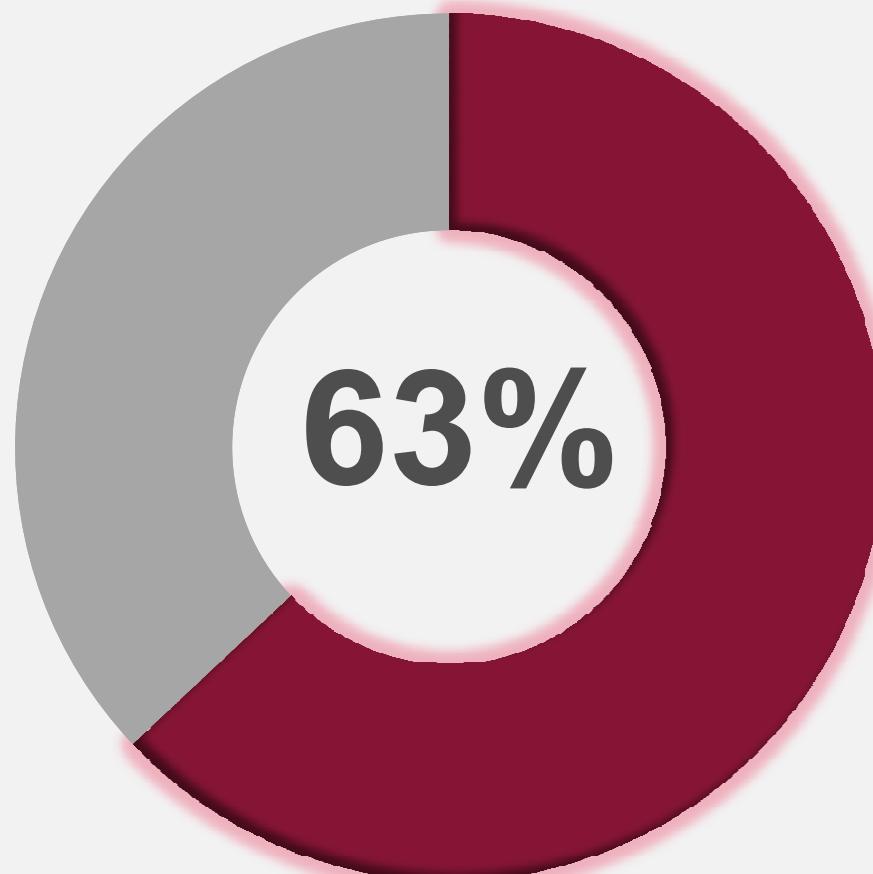


Утечка данных



softwareblades™

Большинство компаний инфицированы!



Организаций
инфицировано
вредоносным
ПО (ботнеты...)



softwareblades™

Каждый день новая жертва



softwareblades™

Это же меня не коснется, так ведь?



softwareblades™

©2012 Check Point Software Technologies Ltd. [PROTECTED] — All rights reserved. | 7



Связь с
командным
центром один
раз в
21
минуту



Основные ботнеты в 2012 году



ZWANGI

Impose unwanted advertising

ZEUS

Steal online banking credentials

SALITY

Self-spreading virus

KULUOZ

Remote execution of malicious files

PAPRAS

Steal financial information,
gain remote access

JUASEK

Remote malicious actions
(search, delete files)



softwareblades™



В среднем
вредоносное ПО скачивается
раз в 23 минуты



Инфицирование в реальном времени



53%

организаций
наблюдали
скачивание
вредоносного ПО

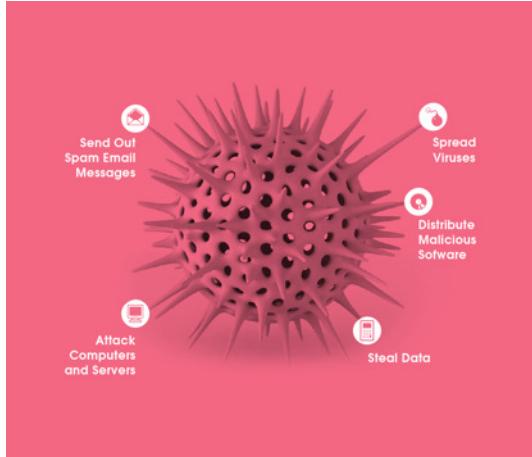


softwareblades™

Три класса проблем



Вредоносное ПО



Использование небезопасных сервисов



Утечка данных



softwareblades™

Не просто развлечения...



softwareblades™

Какие приложений опасны?



Обходят стандартный
периметр
безопасности

Вред наносится без
участия пользователя

P2P file sharing

Anonymizers

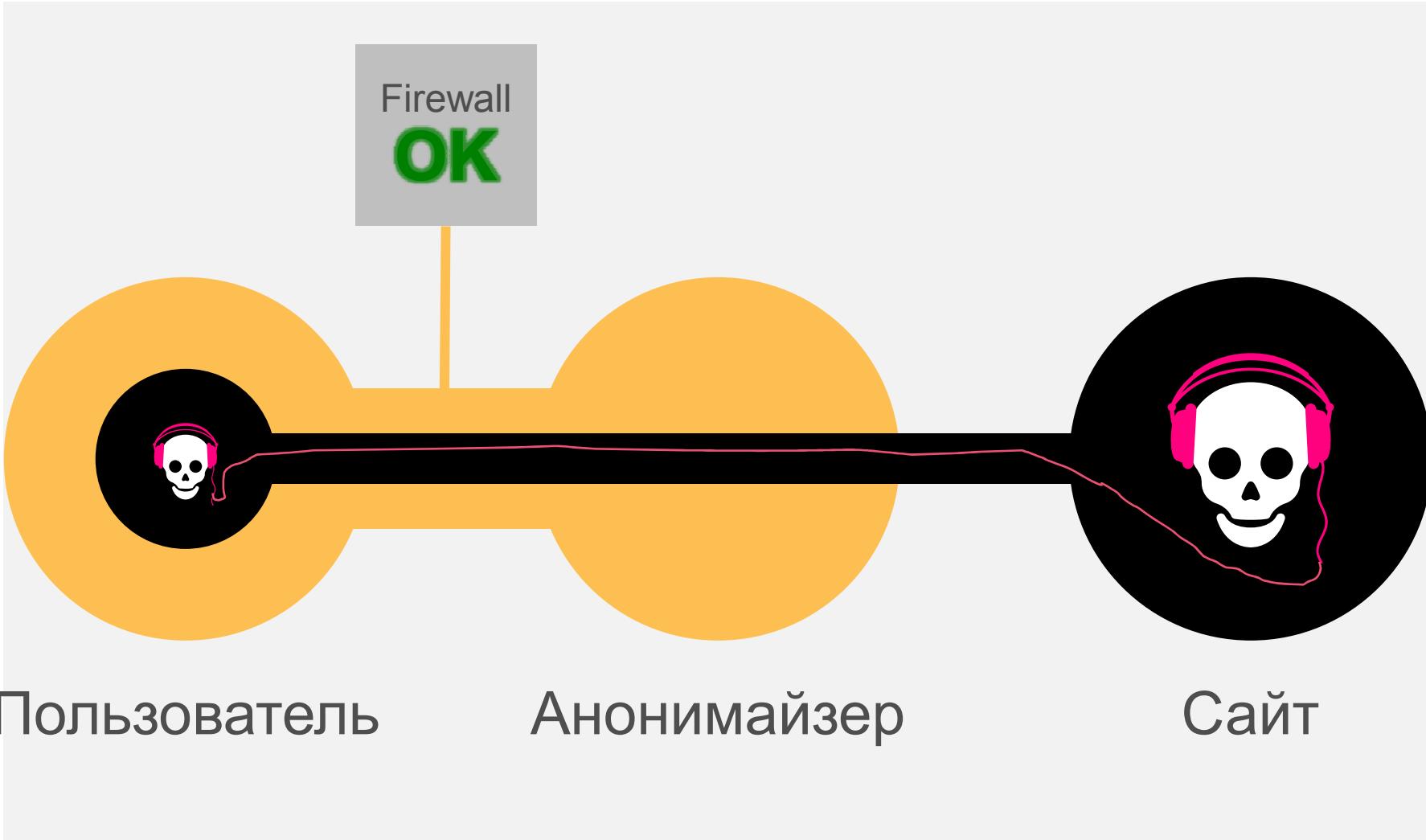
File sharing / storage

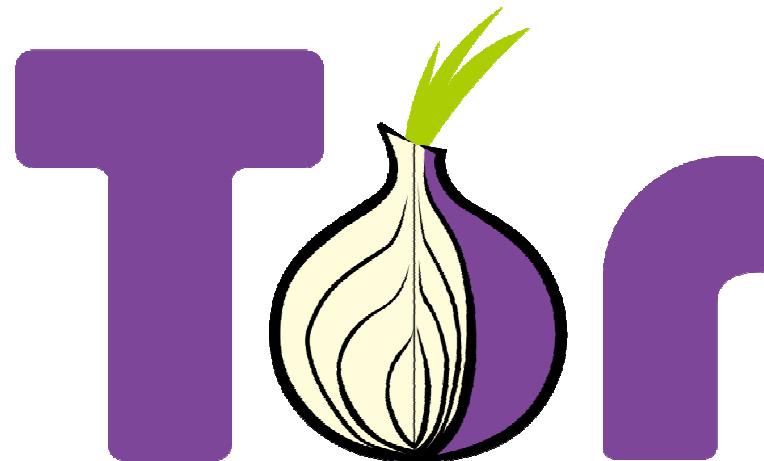
Social networks



softwareblades™

Что такое анонимайзеры?





“The Onion Router”

Создана по заказу
ВМС США

80% бюджета 2012 года
получено от
правительства США

Широко применялся
в «Арабской весне»



Основные риски



Обход периметра безопасности

Используются ботнетами для связи с командными центрами

Используются пользователями для скрытия нелегитимной активности



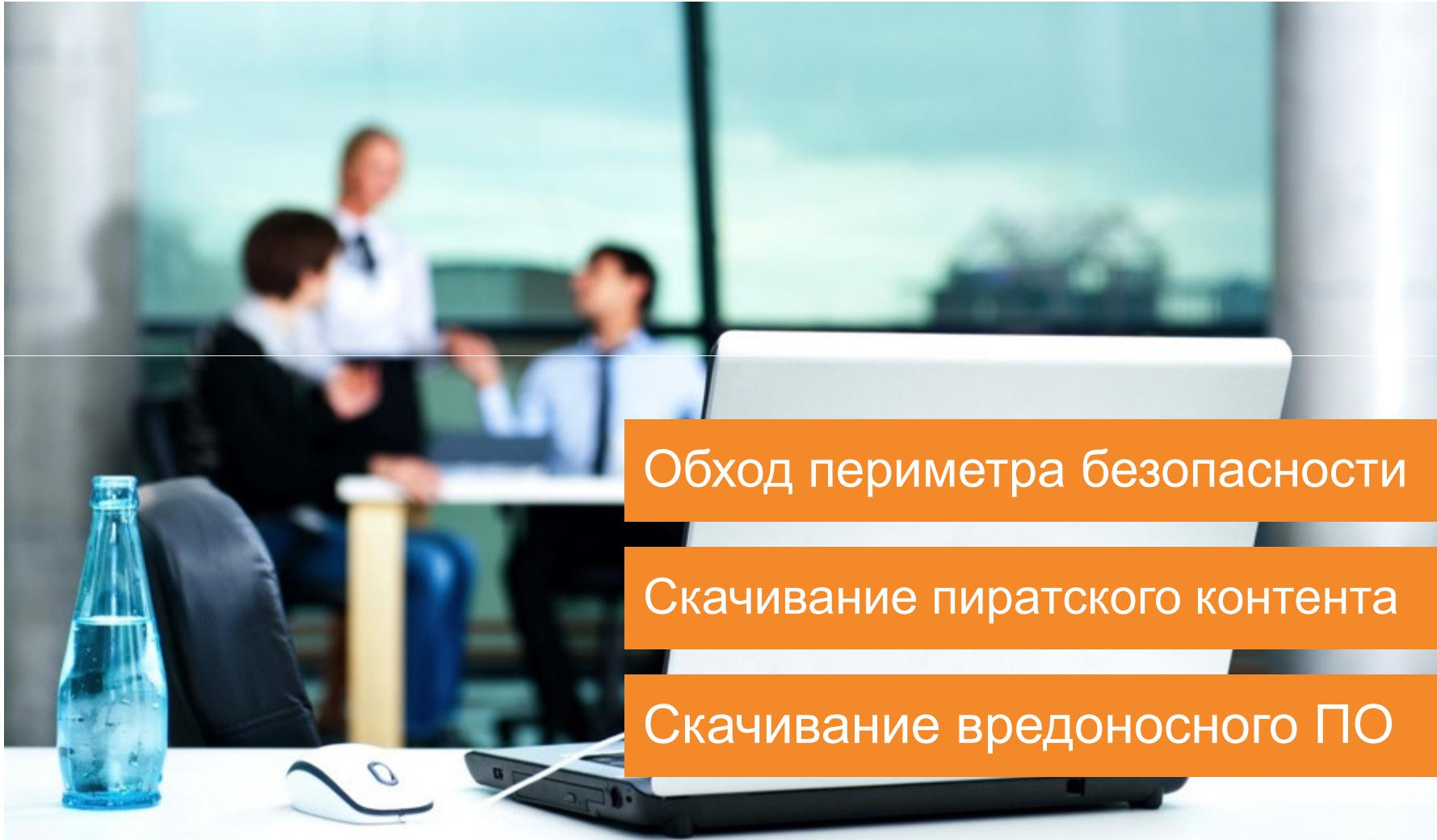
softwareblades™

Использование анонимайзеров



softwareblades™

Риски P2P приложений



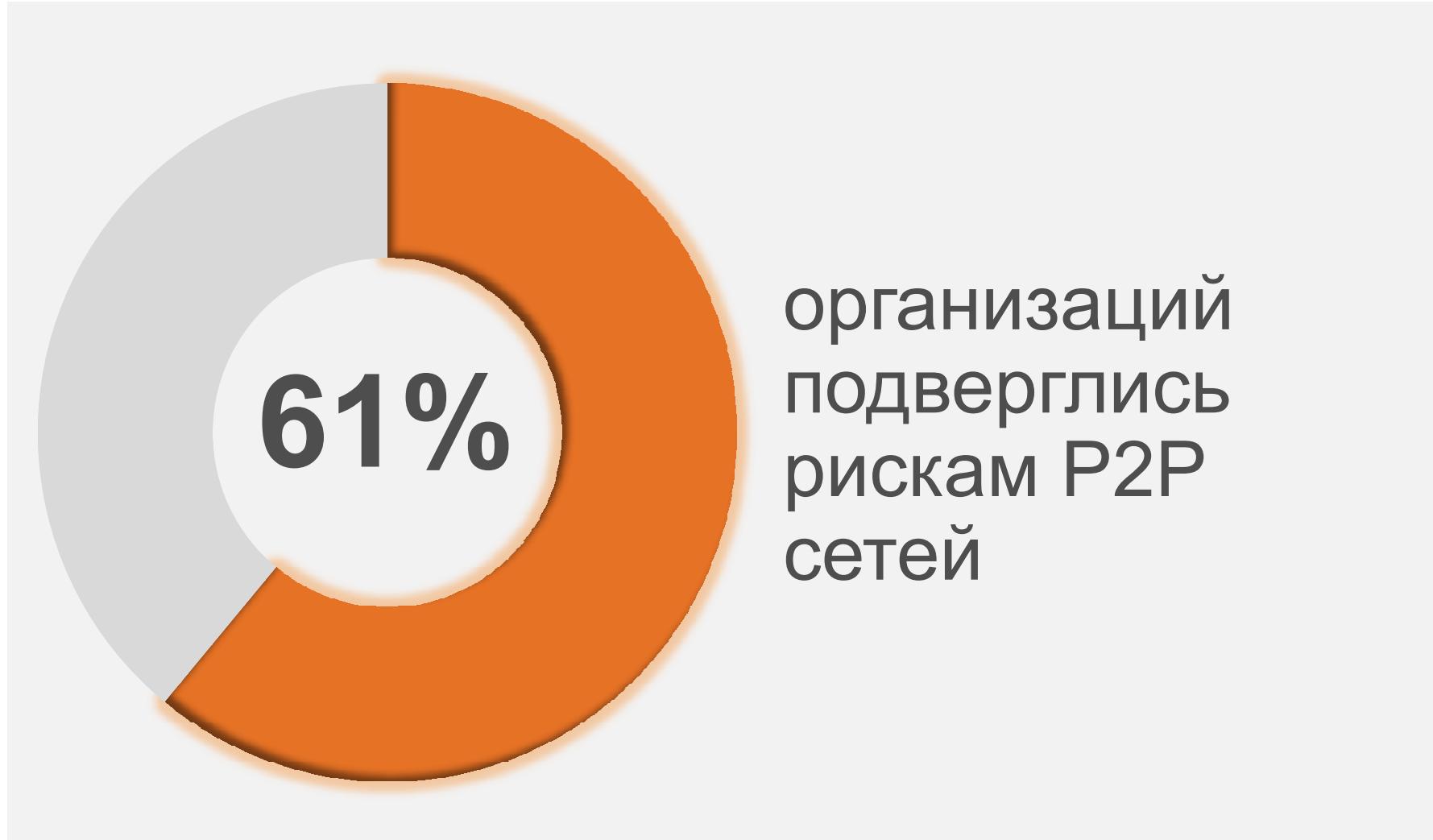
Обход периметра безопасности

Скачивание пиратского контента

Скачивание вредоносного ПО



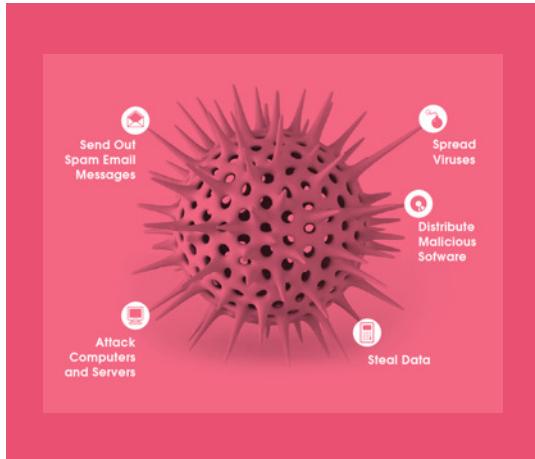
softwareblades™



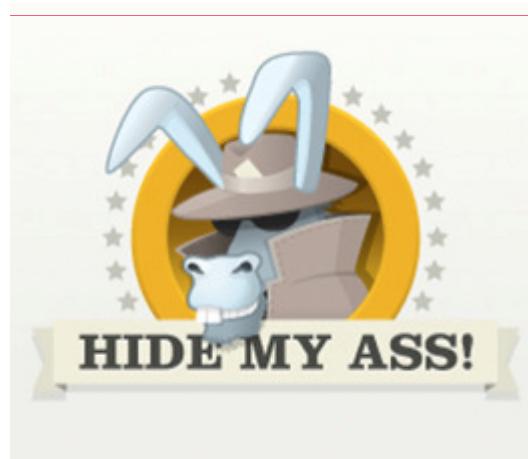
Три класса проблем



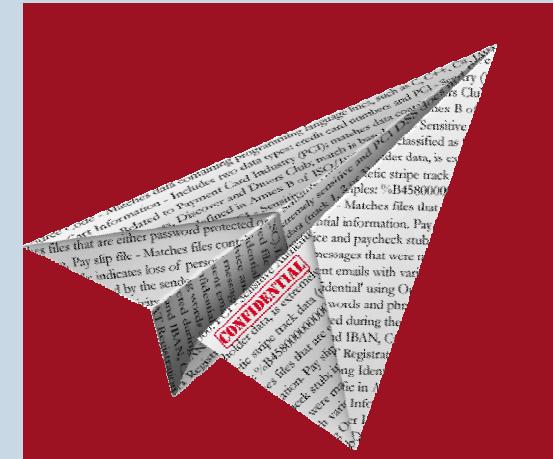
Вредоносное ПО



Использование небезопасных сервисов

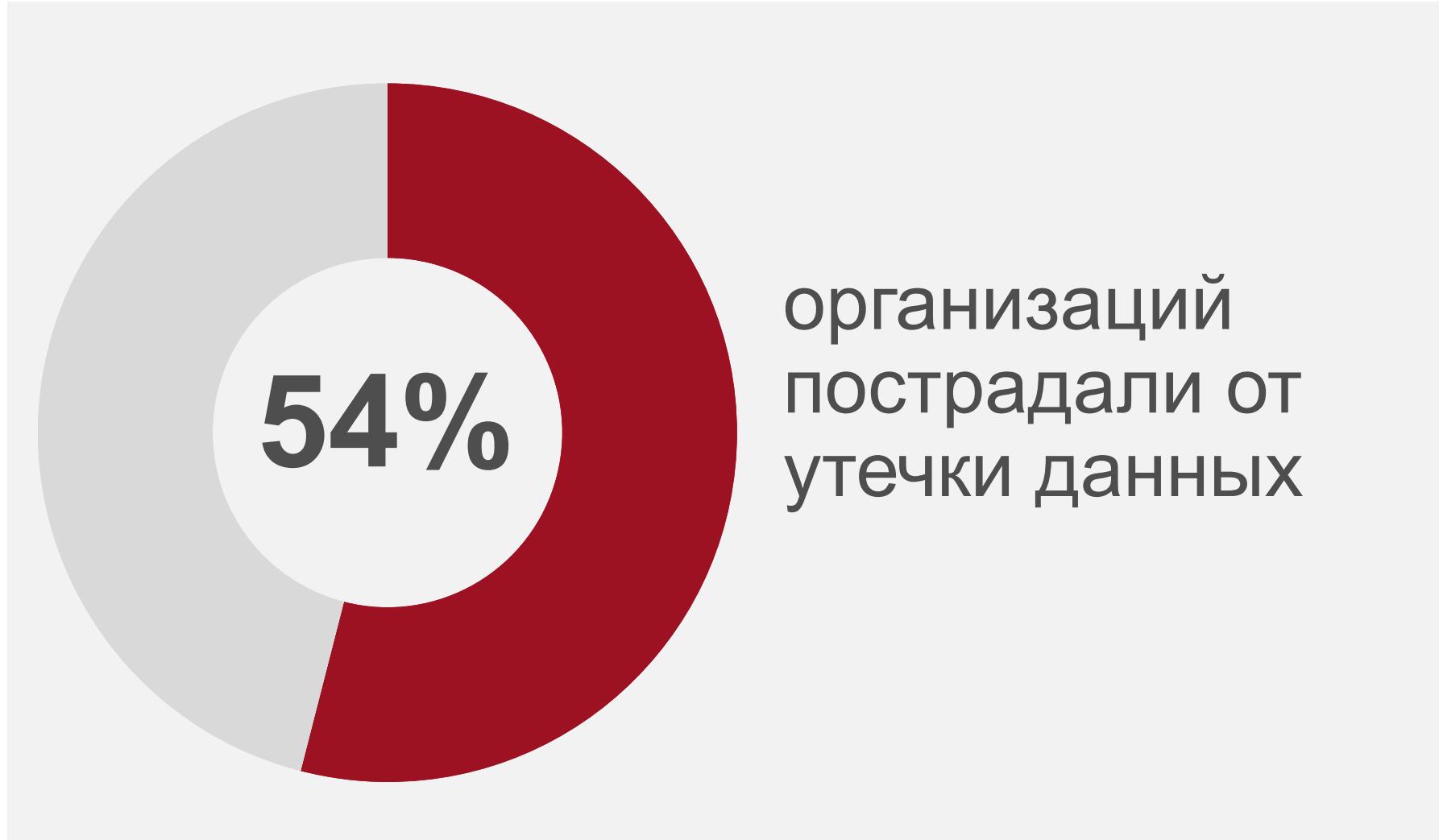


Утечка данных



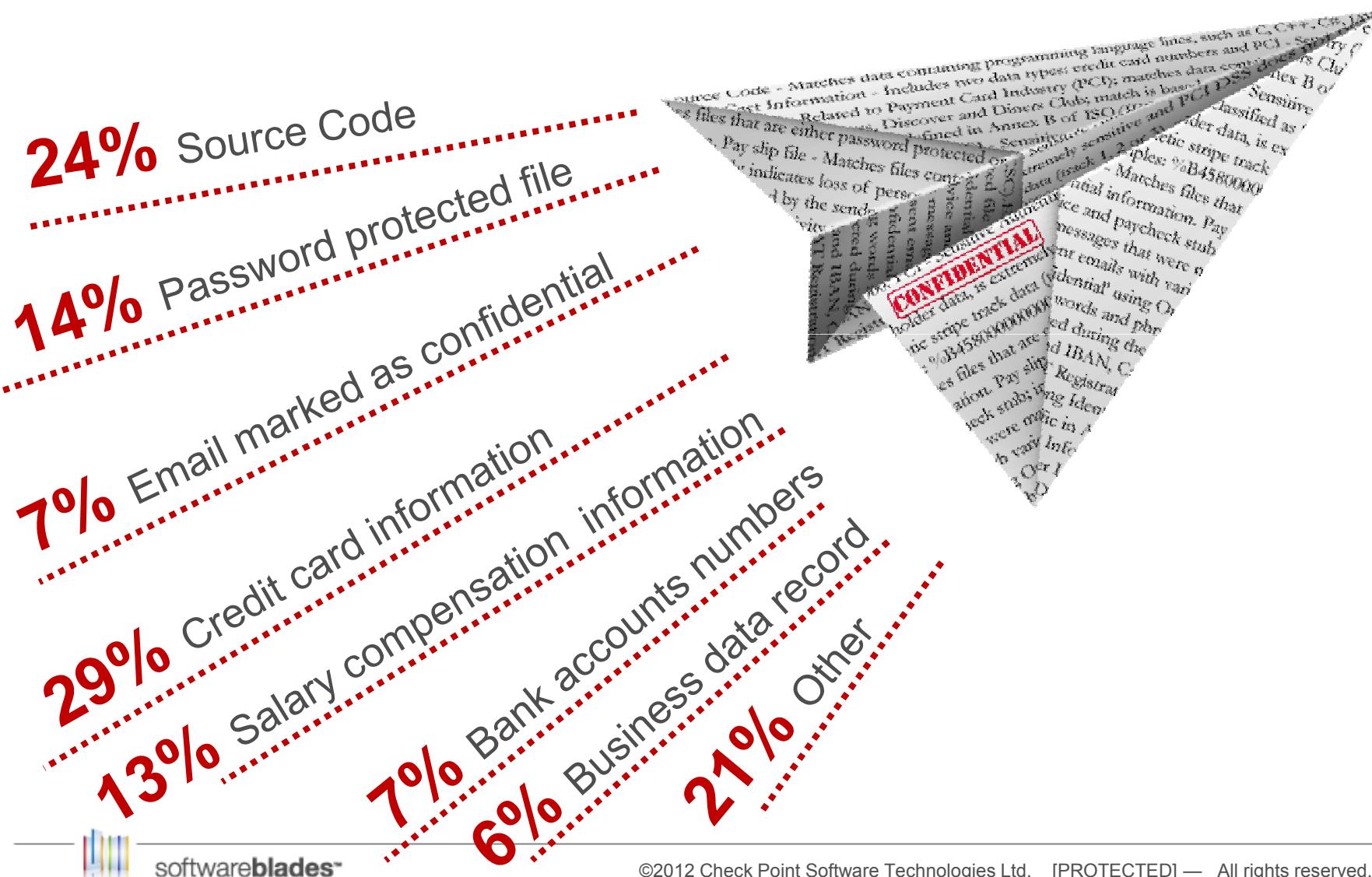
softwareblades™

Как часто это происходит?



softwareblades™

Что же мы нашли?



Все встречаются с этой проблемой!



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



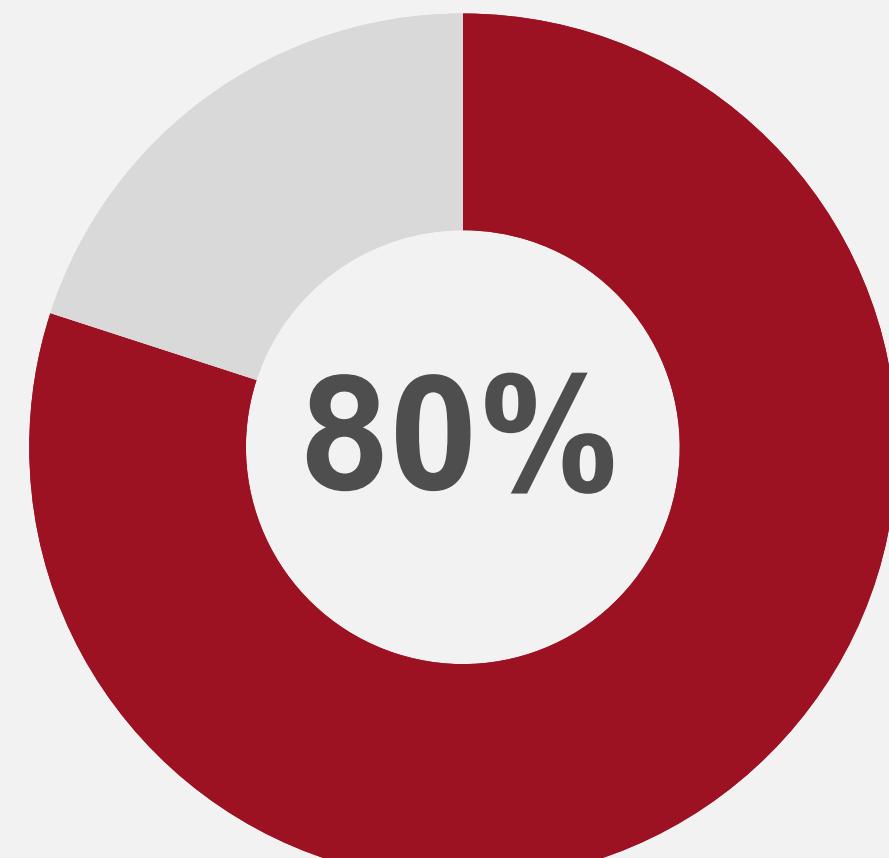
Dropbox?



YouSendIt?



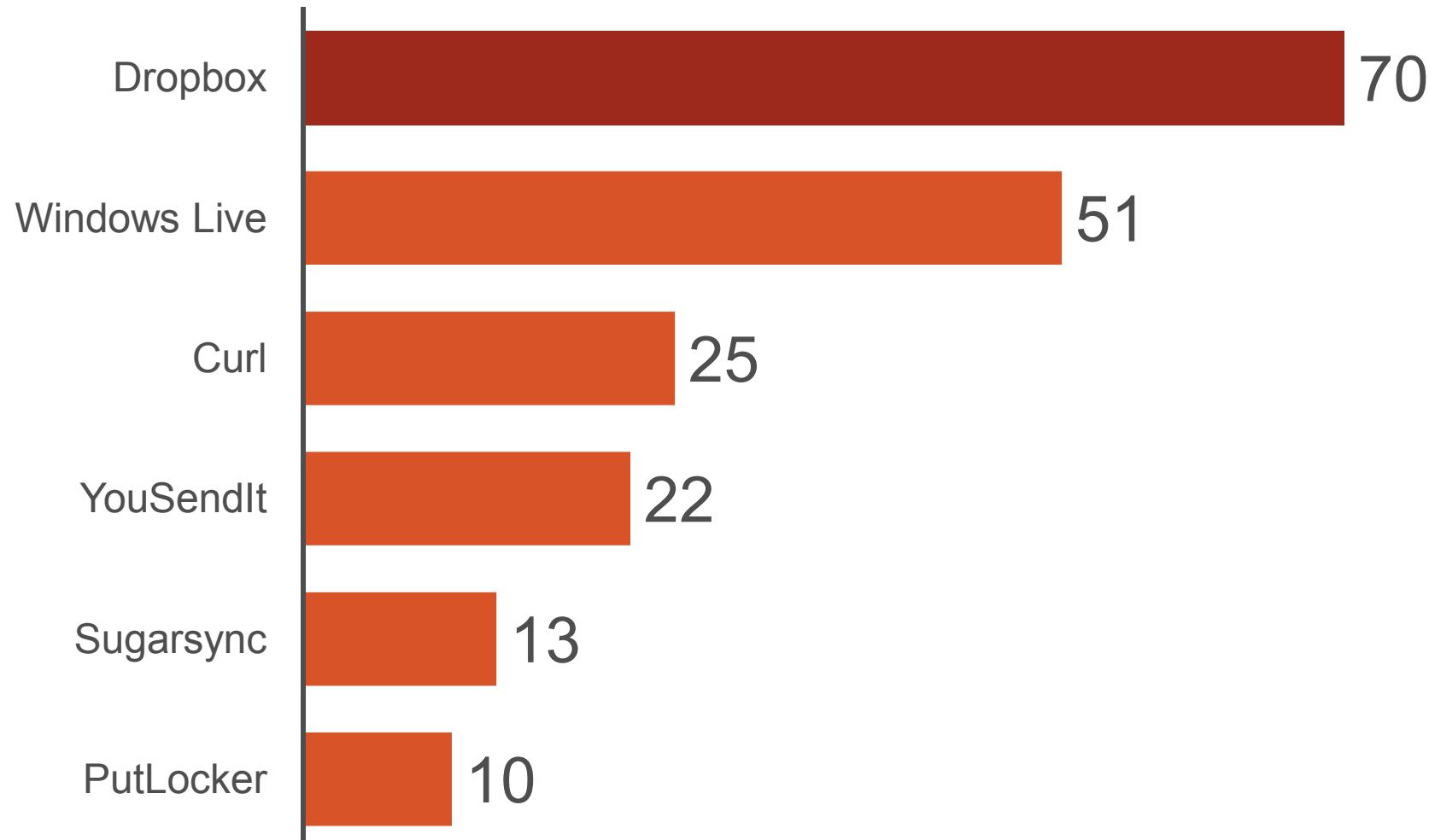
Windows Live?



Организаций
использовали
сервисы внешнего
хранения файлов



Мы нашли:



Что нужно помнить?



Угрозы
организации

Риски
приложений

Утечка данных

63%

47%

54%

Инфицированы
ботнетами

Использовали
анонимайзеры

Столкнулись с
утечкой данных

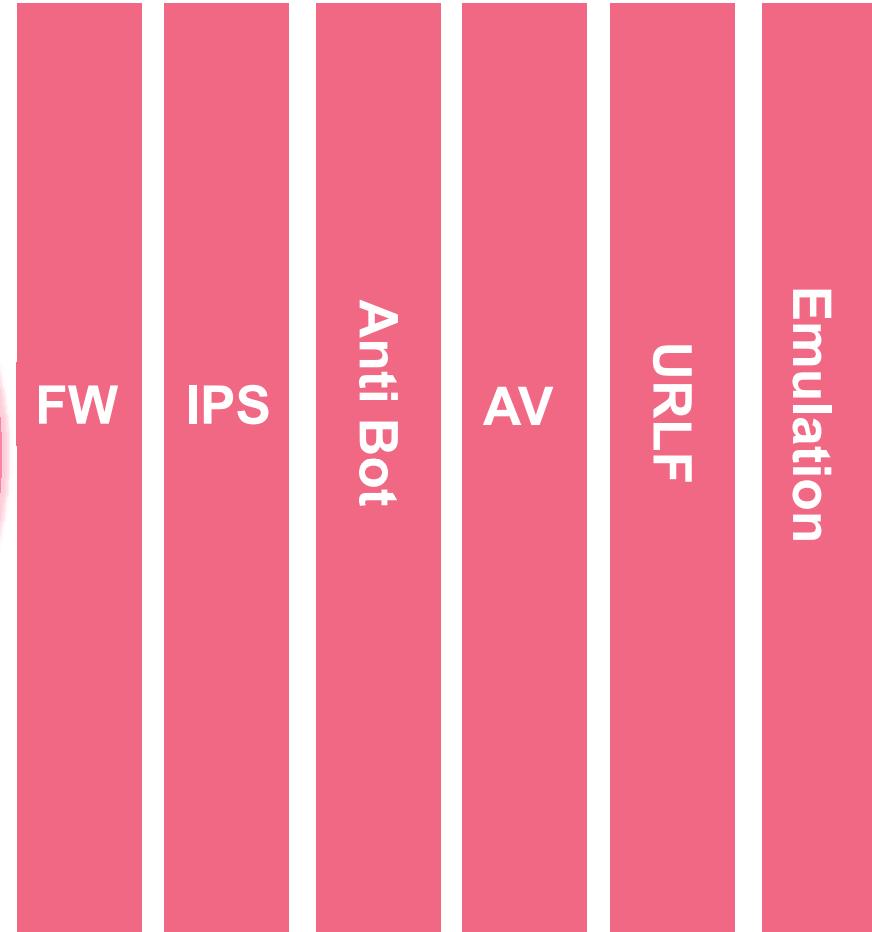


softwareblades™

Как заблокировать атаку?



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

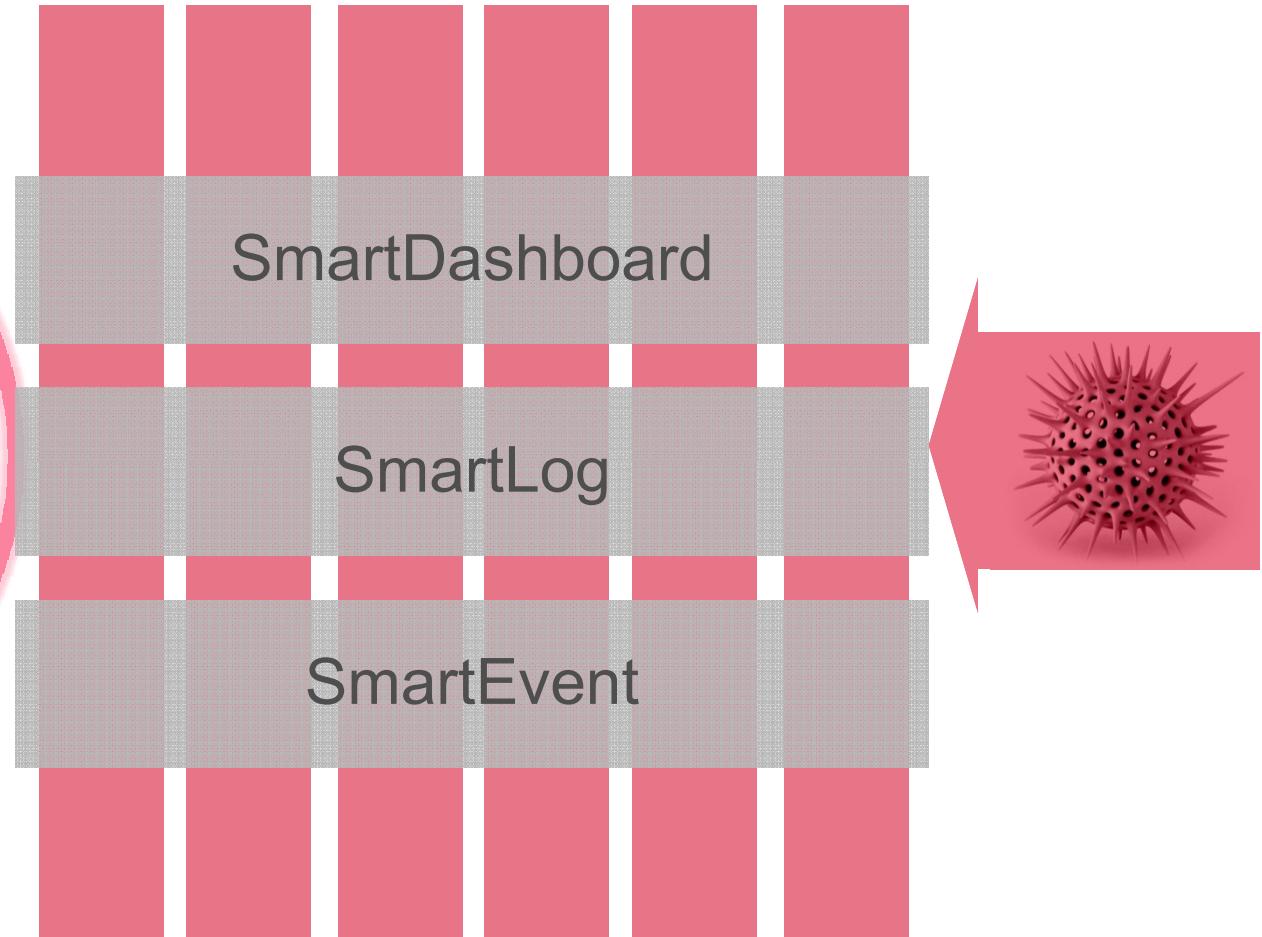


softwareblades™

Постоянный мониторинг



R76
Multi Domain
Management



softwareblades™

Глобальное взаимодействие для моментальной реакции



Real-time Security Intelligence
Шлюзы постоянно обновлены



Threat Cloud™ растет



Свыше **250 миллионов**
адресов

Свыше **12**
миллионов malware

Свыше **1 миллиона**
malware-infested

1,000 URL обновлений в день!
50,000 сигнатур обновляется за день!



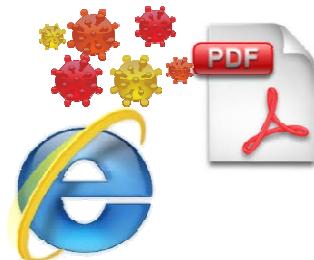
softwareblades™

Многоуровневое решение



IPS

Prevent exploit
of known vulnerabilities



Antivirus

Block download of
known malware



Anti-Bot

Block Bot
Communication



Emulation

Unknown Threats



softwareblades™

IPS



Network Threat Prevention

Mobile Access



Remote VPN – Mobile Access

DLP



Prevent leakage of corporate Data

Application Control & URL Filtering



Control access to Application and URLs

Identity Awareness



New User based Policies

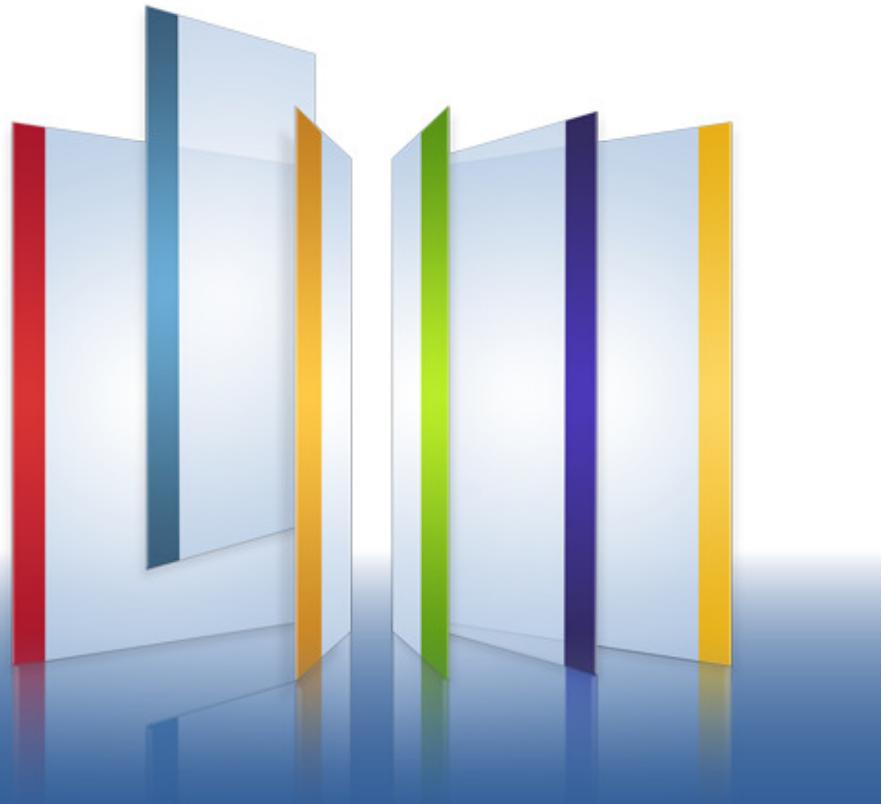


softwareblades™



We Secure the Internet.

Спасибо!



Георгий Цициашвили
Директор по работе с партнерами в России и СНГ
Check Point Software Technologies