FireEye – эффективное решение
для защиты от целевых атак

ДиалогНаука

Обо мне

Николай Петров, CISSP

Заместитель генерального директора, ДиалогНаука

Первым в России был удостоен звания CISSP

На протяжении многих лет являюсь единственным сертифицированным инструктором (ISC)2 в России

Работал в компаниях Philip Morris, Kerberus,

MIS Training Institute, (ISC)2, Ernst & Young

План презентации

1. Целевые атаки
2. Решение FireEye

Продолжительность 25-30 мин

Целевые атаки

- Operation Aurora
- F-35 и F-22
- Stuxnet
- RSA
- Citigroup
- Globalpayments
- NY Times
- Red October
- NetTraveler

Известные атаки

2009

Operation Aurora

- август- декабрь Китай взламывает Google для доступа к почтовым ящикам китайских правозащитников.
- уязвимость 0-дня в Microsoft IE & SSL соединение с серверами управления в Иллинойсе, Техасе и Тайване.
- Yahoo, Symantec, Northrop Grumman, Morgan Stanley, и Dow Chemical так же пострадали от этой атаки

F-35 и F-22

- Китай посредством успешной атаки похищает техническую документацию на новые истребители F-35 и F-22

Известные атаки

2015

Апрель 2015 Топ-5 банк РФ – атака на мобильные устройства клиентов

Телефон все время находился в руках абонента. По его словам, он ничего не делал, никакие смс не отправлял, но деньги с банковского счета все равно исчезли

- Клиент устанавливает проигрыватель Flash злоумышленника
- Вредоносный код посылает СМС на короткий номер «Баланс»
- Если получен ответ, значит телефонный номер привязан к банковскому счету
- Осуществляется перевод денежных средств
- Весь СМС обмен с банком стирается, включая СМС подтверждения операций

Известные атаки

2015

Весна 2015 осуществлена атака на ЛК

- Объявлено 10 июня в корпоративном блоге, и на пресс-конференции Е Касперского в Лондоне
- По заявлению ЛК злоумышленники создали инновационную вредоносную киберплатформу и использовали несколько уязвимостей нулевого дня.
- Мишенью хакеров была информация об инструментах обеспечения корпоративной безопасности и предотвращения ответных направленных атак, защищающая банки от мошеннических операций платформа Kaspersky Fraud Prevention, и другое

Отчет Gartner

“Все согласны с тем, что целенаправленные атаки обходят традиционные средства защиты и остаются необнаруженными в течение длительного времени. Угроза реальна. Ваши сети скомпрометированы независимо от того, знаете Вы об этом или нет.”

Отчет Gartner 2012

Особенности APT

Особенности APT

APT - целенаправленная сетевая атака, при которой атакующий получает неавторизованный доступ в сеть и остается необнаруженным в течении длительного времени

Термин APT введен U.S. Air Force в 2006

- **Advanced:** Атакующий является экспертом и использует свои собственные, неизвестные другим инструменты для эксплуатации уязвимостей
- **Persistent:** Атакующий не ограничен во времени, т е он будет тратить столько времени, сколько нужно, чтобы получить доступ и остаться незамеченным
- **Threat:** Атакующий организован, мотивирован, обладает необходимыми финансовыми ресурсами

APT

- не вредоносное ПО
- спланированная атака, мотивированная деньгами, политикой/национальными интересами и направленная для достижения определенной цели

Особенности APT

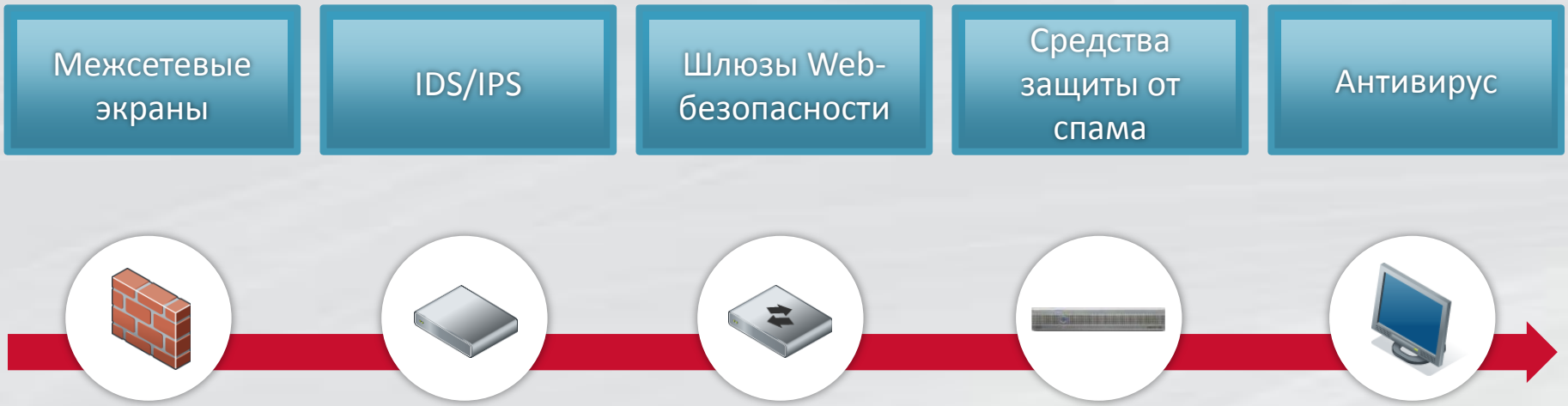
Обход защиты основанной на анализе сигнатур

- Традиционные продукты, такие как IDS/IPS, межсетевые экраны следующего поколения (NGFW), шлюзы Web-безопасности (secure Web gateways), антивирусное ПО— анализируют сигнатуры для обнаружения известным им атак, и в некоторых случаях, неизвестных атак, которые используют известные им уязвимости

Обход защиты основанной на анализе аномалий

- Продвинутые IDS/IPS и решения анализирующие сетевые аномалии могут обнаруживать APT. Они собирают траффик (e.g., NetFlow, sFlow, cFlow) с сетевых устройств и сравнивают его с “обычным” сетевым трафиком в имевшем место в течении дня, недели, месяца
- Однако такие решения подвержены ошибкам 1-го и 2-го рода. False positives – когда нормальный трафик принимается за атаку, и наоборот, false negatives – когда атака воспринимается как нормальный трафик

Особенности APT



Традиционные технологии не могут остановить APT

Решение FireEye

ДиалогНаука

Решение FireEye

- Компания FireEye с 2004 г в США
- Поставляет продукты с 2006 г
- Мировой лидер – FireEye используют 40% компаний Fortune 100

Результаты тестирования

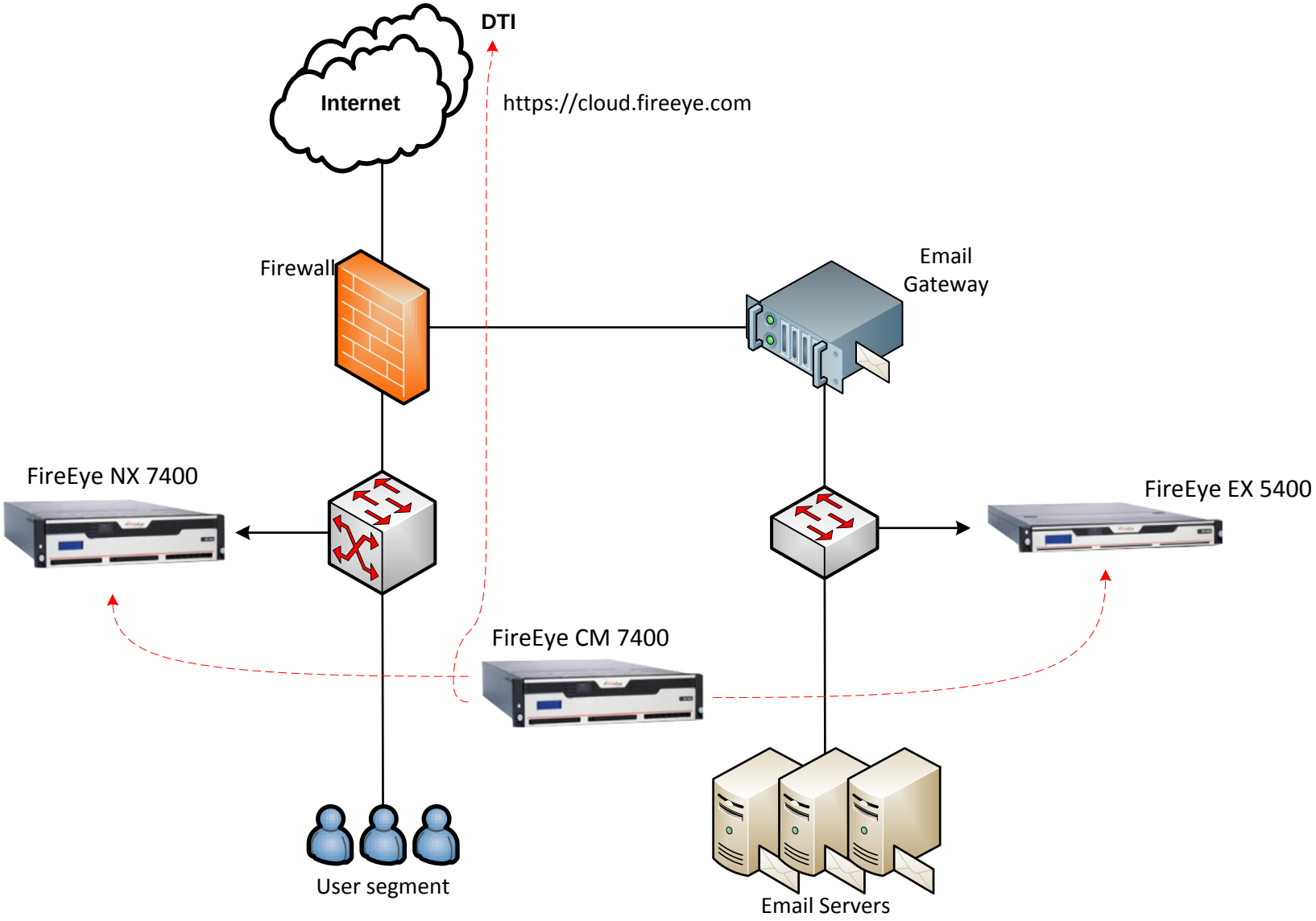
Мы провели более 10 пилотных проектов

В результате пилотного тестирования, FireEye обнаружил:

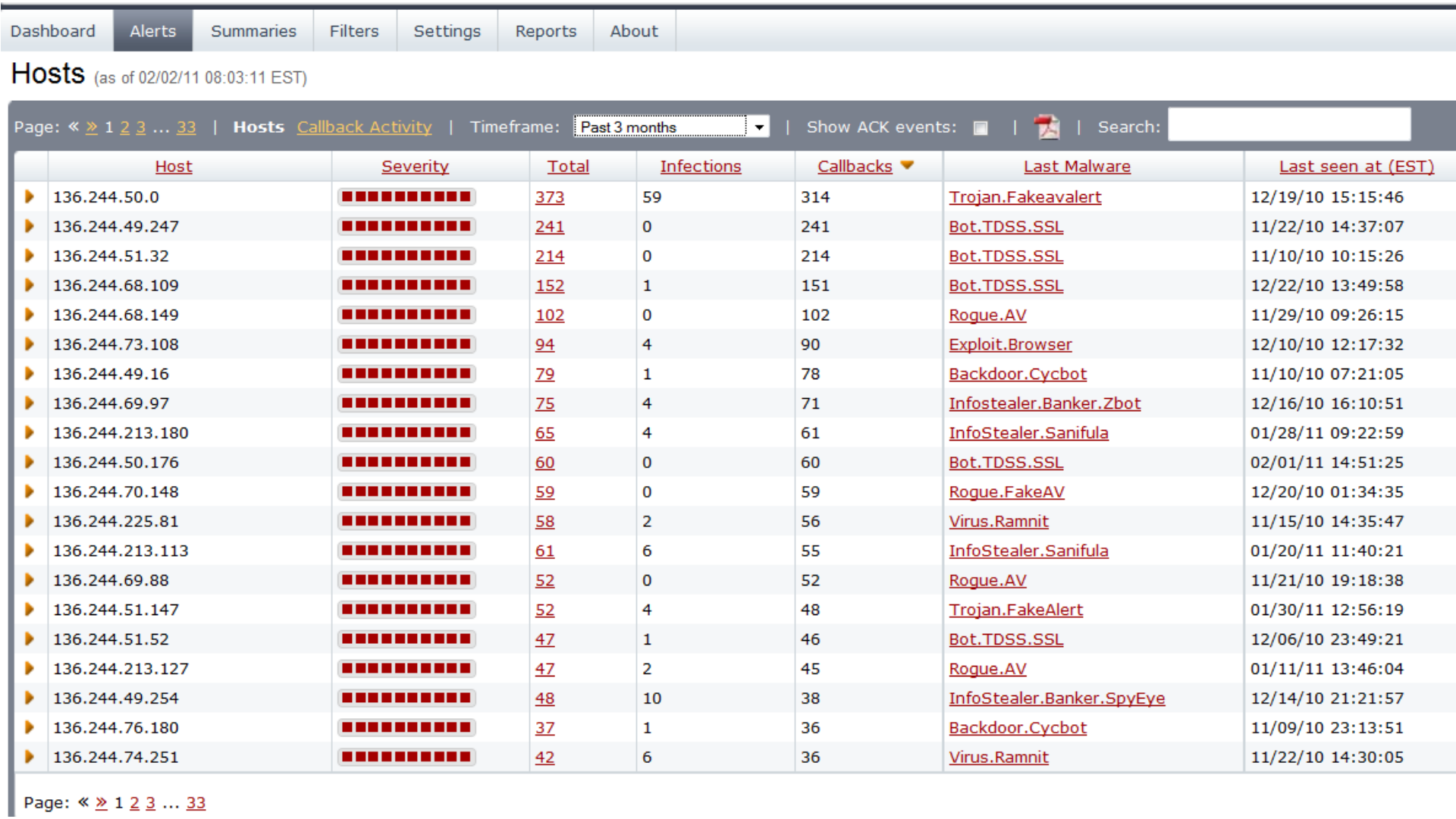
- Не менее 8 рабочих станций контролируются злоумышленниками извне Компании
- Не менее 24 рабочих станций потенциально заражены троянскими программами и могут контролироваться злоумышленниками извне Компании
- Основные каналы распространения WEB и электронная почта

Количество рабочих станций у клиента - 2000

Схема тестирования



Экран системы



Dashboard | Alerts | Summaries | Filters | Settings | Reports | About

Hosts (as of 02/02/11 08:03:11 EST)

Page: « » 1 2 3 ... 33 | **Hosts** Callback Activity | Timeframe: Past 3 months | Show ACK events: | Search:

Host	Severity	Total	Infections	Callbacks	Last Malware	Last seen at (EST)
136.244.50.0		373	59	314	Trojan.Fakeavalert	12/19/10 15:15:46
136.244.49.247		241	0	241	Bot.TDSS.SSL	11/22/10 14:37:07
136.244.51.32		214	0	214	Bot.TDSS.SSL	11/10/10 10:15:26
136.244.68.109		152	1	151	Bot.TDSS.SSL	12/22/10 13:49:58
136.244.68.149		102	0	102	Rogue.AV	11/29/10 09:26:15
136.244.73.108		94	4	90	Exploit.Browser	12/10/10 12:17:32
136.244.49.16		79	1	78	Backdoor.Cycbot	11/10/10 07:21:05
136.244.69.97		75	4	71	Infostealer.Banker.Zbot	12/16/10 16:10:51
136.244.213.180		65	4	61	InfoStealer.Sanifula	01/28/11 09:22:59
136.244.50.176		60	0	60	Bot.TDSS.SSL	02/01/11 14:51:25
136.244.70.148		59	0	59	Rogue.FakeAV	12/20/10 01:34:35
136.244.225.81		58	2	56	Virus.Ramnit	11/15/10 14:35:47
136.244.213.113		61	6	55	InfoStealer.Sanifula	01/20/11 11:40:21
136.244.69.88		52	0	52	Rogue.AV	11/21/10 19:18:38
136.244.51.147		52	4	48	Trojan.FakeAlert	01/30/11 12:56:19
136.244.51.52		47	1	46	Bot.TDSS.SSL	12/06/10 23:49:21
136.244.213.127		47	2	45	Rogue.AV	01/11/11 13:46:04
136.244.49.254		48	10	38	InfoStealer.Banker.SpyEye	12/14/10 21:21:57
136.244.76.180		37	1	36	Backdoor.Cycbot	11/09/10 23:13:51
136.244.74.251		42	6	36	Virus.Ramnit	11/22/10 14:30:05

Page: « » 1 2 3 ... 33

Решение FireEye

1

Аппаратный гипервизор FireEye

- Специализированный гипервизор
- Разработан для анализа угроз

2

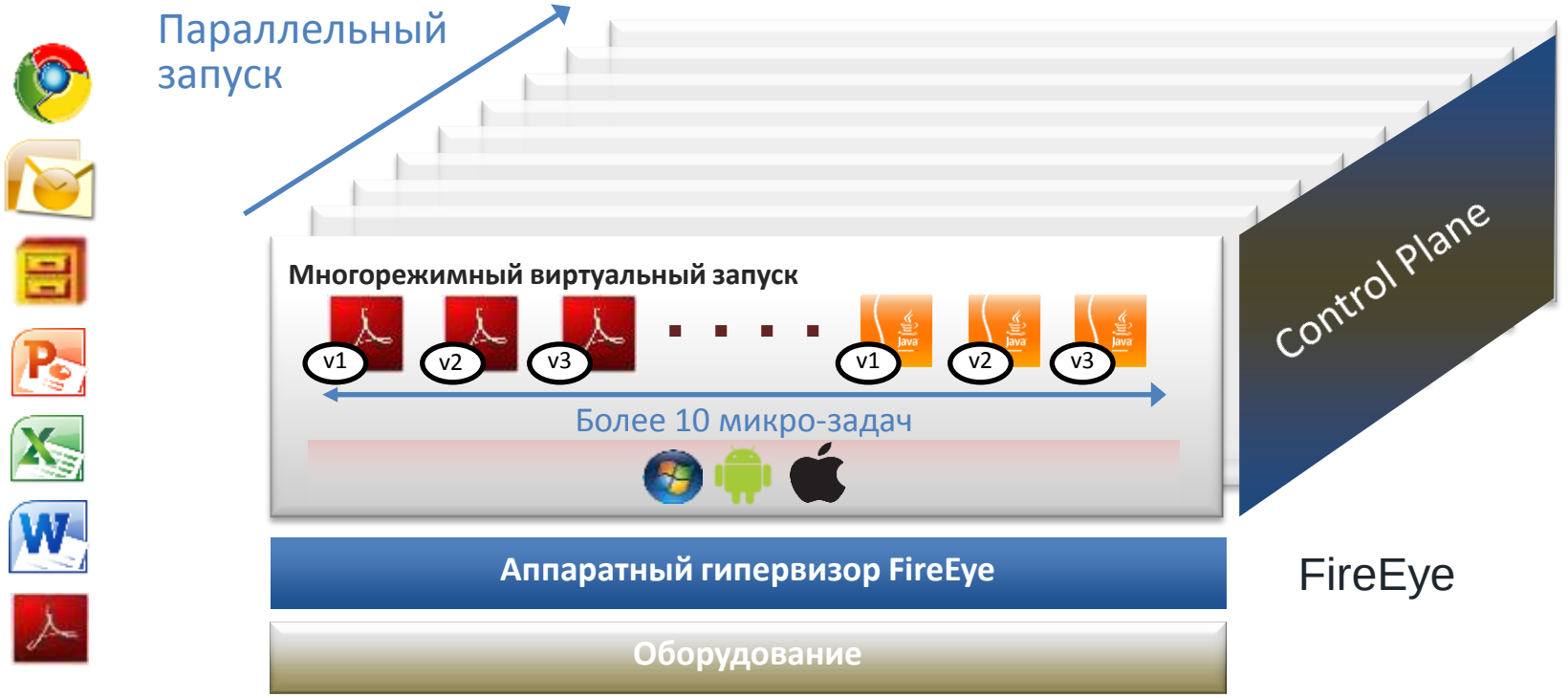
Многопоточный виртуальный запуск

- Разные ОС
- Разные сервис-паки
- Разные приложения
- Разные типы файлов

3

Защита от угроз в масштабе

- Параллельный запуск
- Многоуровневый анализ



Передача информации об атаках

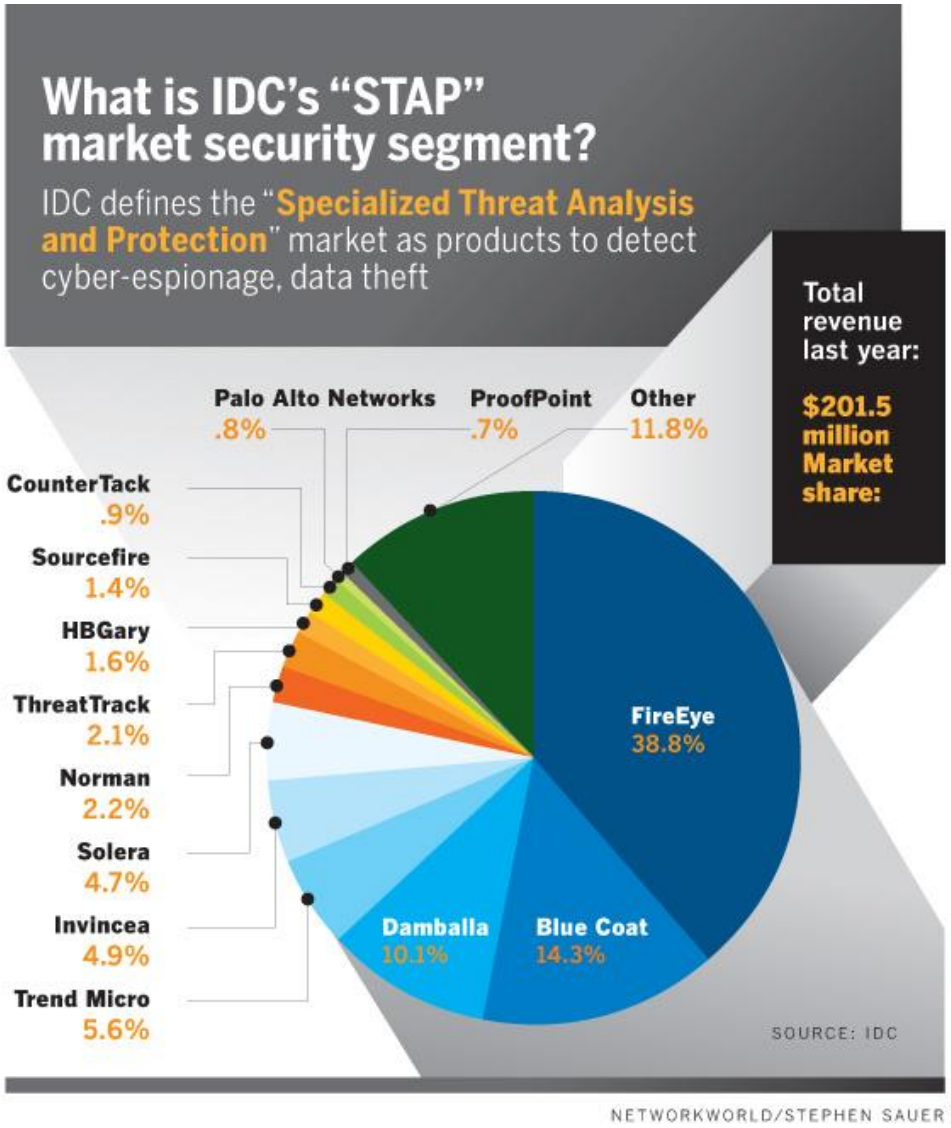
Передача информации об атаках

- Файлы из вашей сети не передаются в Облако (Персональные данные, конфиденциальная информация)
- Идентификаторы вредоносного ПО со всего мира
- Возможность выбрать вариант обмена информацией

Почему FireEye?

- **16 из 22** уязвимостей нулевого дня (Zero Day) в 2013-2014 году были обнаружены FireEye
- Выполняет анализ не только исполняемых файлов и MS Office, но и других (более 30 типов файлов, включая графические, аудио, видео)
- Выполняется анализ веб-сессии целиком, а не отдельного файла
- Обладает специализированым гипервизором для анализа угроз и позволяет обнаруживать неизвестные угрозы
- Обеспечивает **близкое к реальному времени** скорость анализа (не более 5 мин)
- Позволяет блокировать вредоносную активность на каждой стадии атаки
- Выявляет вредоносный код в системах Windows и Mac OS и мобильных устройствах iOS и Android

Доля рынка


What is IDC's "STAP" market security segment?
IDC defines the "Specialized Threat Analysis and Protection" market as products to detect cyber-espionage, data theft
Total revenue last year:
$201.5 million
Market share:
Palo Alto Networks .8%
ProofPoint .7%
Other 11.8%
CounterTack .9%
Sourcefire 1.4%
HBGary 1.6%
ThreatTrack 2.1%
Norman 2.2%
Solera 4.7%
Invincea 4.9%
Trend Micro 5.6%
FireEye 38.8%
Damballa 10.1%
Blue Coat 14.3%
SOURCE: IDC
NETWORKWORLD/STEPHEN SAUER

Дополнительная информация – мои статьи

«Защищаемся от целенаправленных атак»
Национальный Банковский Журнал, №2 февраль 2014

«Целенаправленные атаки – обнаружение и защита»
Информационная безопасность, №2 май 2014

«Расследование целевых атак»
Безопасность Деловой Информации, №06 II квартал 2014

«Защита от вредоносного кода на мобильных устройствах»
Информационная безопасность банков, 03 / 2015

Вопросы?

ДиалОгНаука