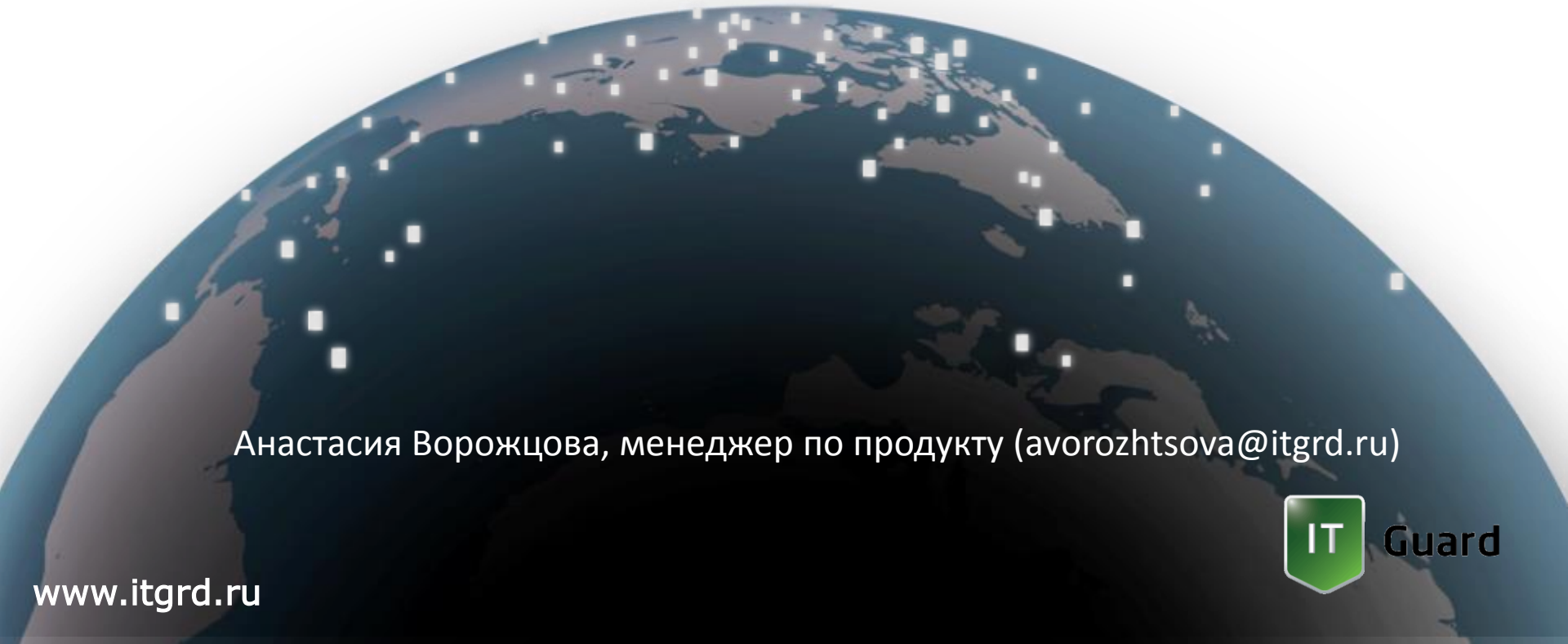
Решения FireEye для эффективной защиты от целенаправленных атак



Анастасия Ворожцова, менеджер по продукту (avorozhtsova@itgrd.ru)

IT Guard

www.itgrd.ru

Крупные инциденты кибер-атак в финансовом секторе в России

Полтора десятка крупных банков-участников **Объединенной расчетной системы (ОРС)** стали жертвами масштабного мошенничества с платежными картами. По данным источников издания, инцидент, имевший место 16 августа 2015 года, причинил ущерб на сумму почти в **500 000 000 рублей**

http://www.securitylab.ru/news/474457.php

Участниками преступной группы были скомпрометированы крупнейшие международные платежные системы. Для осуществления атак на системы дистанционного банковского обслуживания злоумышленники разрабатывали и активно применяли вредоносные программы. Ущерб от деятельности данной преступной группы исчисляется **сотнями миллионов рублей**

https://mvd.ru/news/item/6737350/

ЭНЕРГОБАНК

27 февраля в результате заражения компьютера **Энергобанка** зловредным вирусом тот начал выдавать команды на совершение сделок на валютной бирже, продавая и покупая валюту со значительным убытком.
За 14 минут было совершено 7 сделок, в результате которых банк потерял **250 000 000 рублей**. После этого компьютер отключился и стер всю информацию со своего диска

http://m.business-gazeta.ru/article/297593/

IT Guard

Врага надо знать в лицо

ЭТО “КТО”, А НЕ “ЧТО”

ЗА КАЖДОЙ АТАКОЙ СТОЯТ КОНКРЕТНЫЕ ЛЮДИ

ОНИ АДАПТИРУЮТ АТАКИ ПОД ВАШУ ИНФРАСТРУКТУРУ

ИХ ЦЕЛЬ – ИМЕННО ВЫ

ОНИ ПРОФЕССИОНАЛЬНЫ И ОРГАНИЗОВАНЫ

У НИХ ЕСТЬ ФИНАНСИРОВАНИЕ

ОНИ МОГУТ ИСПОЛЬЗОВАТЬ УНИКАЛЬНЫЙ ИНСТРУМЕНТАРИЙ

ОНИ МОГУТ РАБОТАТЬ ГОДАМИ

ОНИ ПОЧТИ ВСЕГДА ВОЗВРАЩАЮТСЯ

У НИХ ЕСТЬ ЧЕТКО ОПРЕДЕЛЕННЫЕ ЦЕЛИ

ОНИ ДОБИВАЮТСЯ ПОСТОЯННОГО ПРИСУТСТВИЯ

ОНИ ХОТЯТ ОБЕСПЕЧИТЬ БЕСПРЕПЯТСТВЕННЫЙ ДОСТУП В ВАШУ СЕТЬ

FireEye™

IT Guard

Недостатки традиционного подхода

205 ДНЕЙ

СРЕДНЕЕ ВРЕМЯ ОБНАРУЖЕНИЯ УСПЕШНОГО ВЗЛОМА

32 ДНЯ

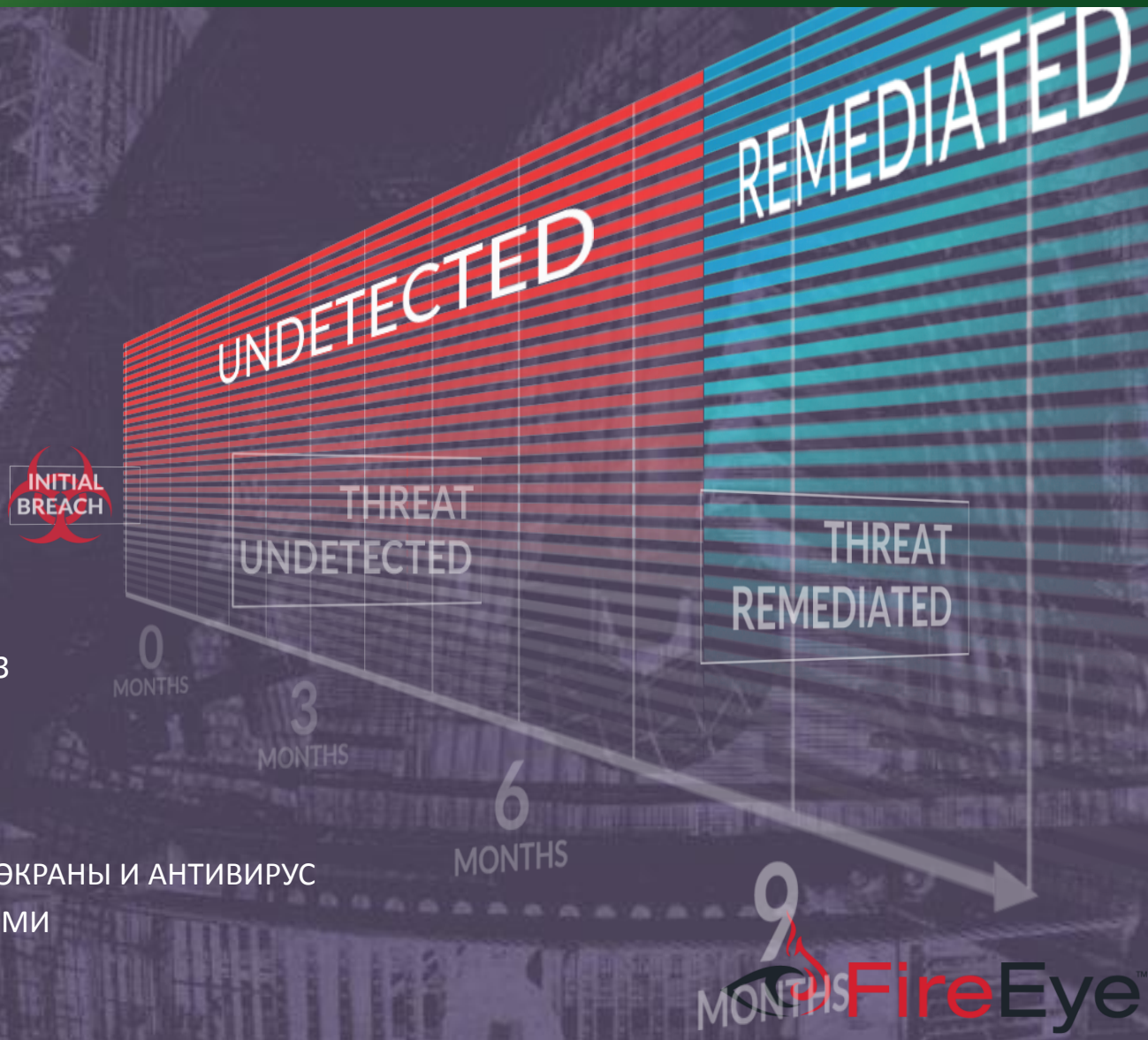
НА УСТРАНЕНИЕ ПОСЛЕДСТВИЙ

69%

УЗНАЛИ О КОМПРОМЕТАЦИИ ИЗ ВНЕШНИХ ИСТОЧНИКОВ

100%

ИСПОЛЬЗОВАЛИ МЕЖСЕТЕВЫЕ ЭКРАНЫ И АНТИВИРУС С АКТУАЛЬНЫМИ ОБНОВЛЕНИЯМИ



FireEye™

SOURCE: MANDIANT M-TRENDS REPORT, PONEMON COST OF DATA BREACH STUDY

FireEye™

“Круговорот атак в природе”

ПРОДУКТЫ FIREEYE

IT Guard

FireEye

IT Guard

Центральная система управления (Central Management System, CMS)

Централизованное управление всеми комплексами
Локальное корпоративное облачное решение DTI

Система веб-защиты от вредоносных программ
Web Malware Protection System (Серия NX)

Защита от вредоносного ПО, загружаемого через Интернет
Обнаружение обратных вызовов и их блокирование

Система защиты файлов от вредоносных программ
File Malware Protection System (Серия FX)

Защита от вредоносного ПО в файловой системе

Система анализа вредоносного ПО
Malware Analysis System (Серия AX)

Предназначено для углубленного анализа вредоносного ПО
Возможность анализа в реальном времени

Система защиты электронной почты от вредоносных программ
Email Malware Protection System (Серия EX)

Защищает от вредоносного ПО, содержащегося в электронных письмах

Облачное решение для динамического анализа угроз (Dynamic Threat Intelligence, DTI)

Основанная на облачных технологиях система сопоставления и агрегации

Анализ выполняется локально при помощи специализированных программно-аппаратных комплексов

FireEye

IT Guard

ГЛОБАЛЬНОЕ СООЩЕСТВО THREAT INTELLIGENCE

ОБМЕН ИНФОРМАЦИЕЙ В РЕАЛЬНОМ ВРЕМЕНИ

ПРИОРИТЕЗАЦИЯ РЕАГИРОВАНИЯ С УЧЕТОМ ВЕЛИЧИНЫ УГРОЗЫ И ЕЕ КОНТЕКСТА

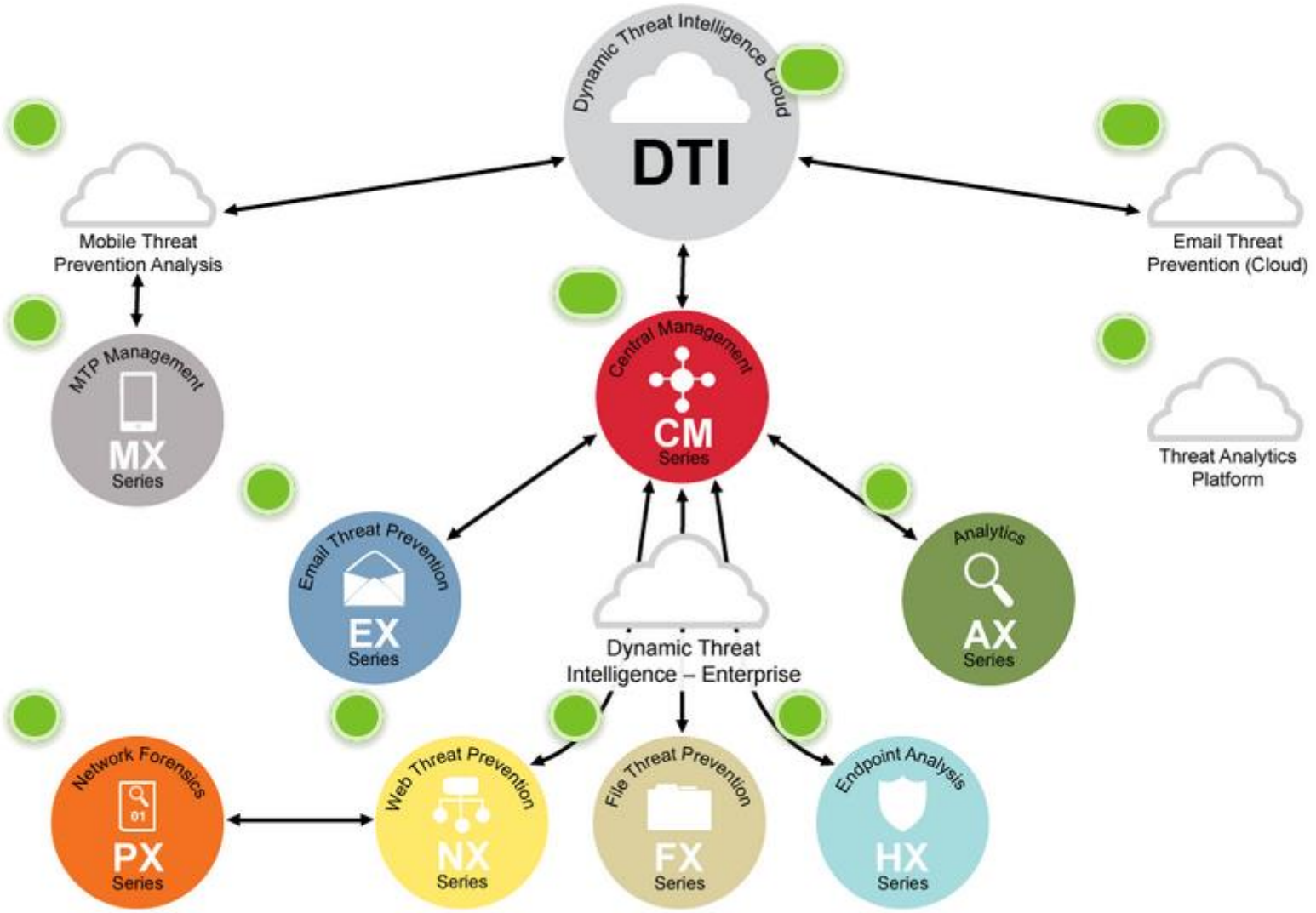
ТАКТИЧЕСКИЕ И СТРАТЕГИЧЕСКИЕ ДАННЫЕ,
ПРИМЕНИМЫЕ ИМЕННО ДЛЯ ВАШЕЙ ОРГАНИЗАЦИИ

3400+ ЗАКАЗЧИКОВ В 67 СТРАНАХ

4M+ ВИРТУАЛЬНЫХ МАШИН
2M+ ОКОНЕЧНЫХ УСТРОЙСТВ

FireEye

IT Guard



FireEye™

“Оригинальное конструктивное решение позволяет вам легко…”

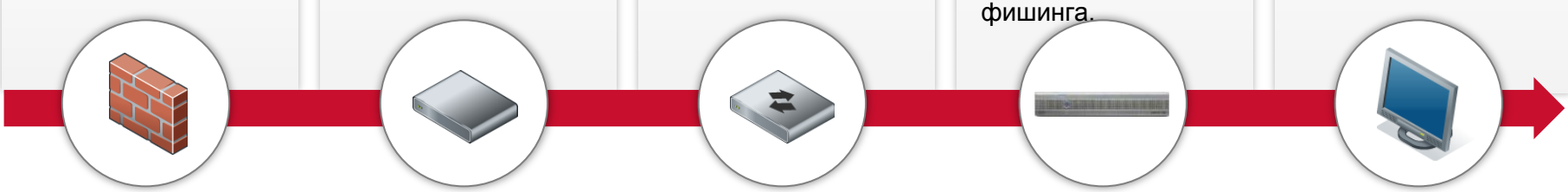
ПРЕИМУЩЕСТВА РЕШЕНИЯ

IT Guard

FireEye

IT Guard

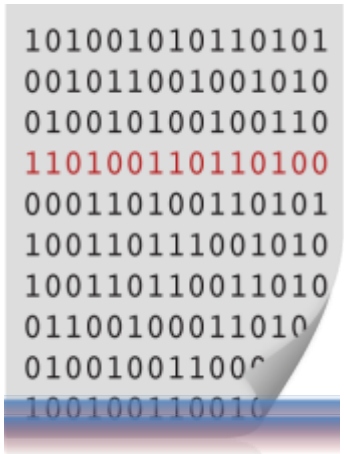
Брандмауэры/ Брандмауэры нового поколения	IPS	Безопасные веб-шлюзы	Анти-спам веб-шлюзы	Антивирусное ПО
Блокировка IP-адресов и портов; управление на уровне приложения; отсутствие возможности контроля эксплойтов; неэффективная защита от современных целевых атак.	Основанная на сигнатурах атак система обнаружения; недостаточно глубокий анализ приложений; частые ложные срабатывания; отсутствие возможности контроля жизненных циклов современных атак.	Неэффективность анализа вредоносных скриптов средствами антивирусного ПО; фильтрация по IP/URL; неэффективная защита от современных целевых атак.	Сильная зависимость от эффективности антивирусного ПО; основанное на сигнатурах обнаружение угроз (частичный анализ поведения); отсутствие полноценной защиты от целевого фишинга.	Основанное на сигнатурах обнаружение (частичный анализ поведения); неэффективная защита от современных целевых атак.



FireEye

IT Guard

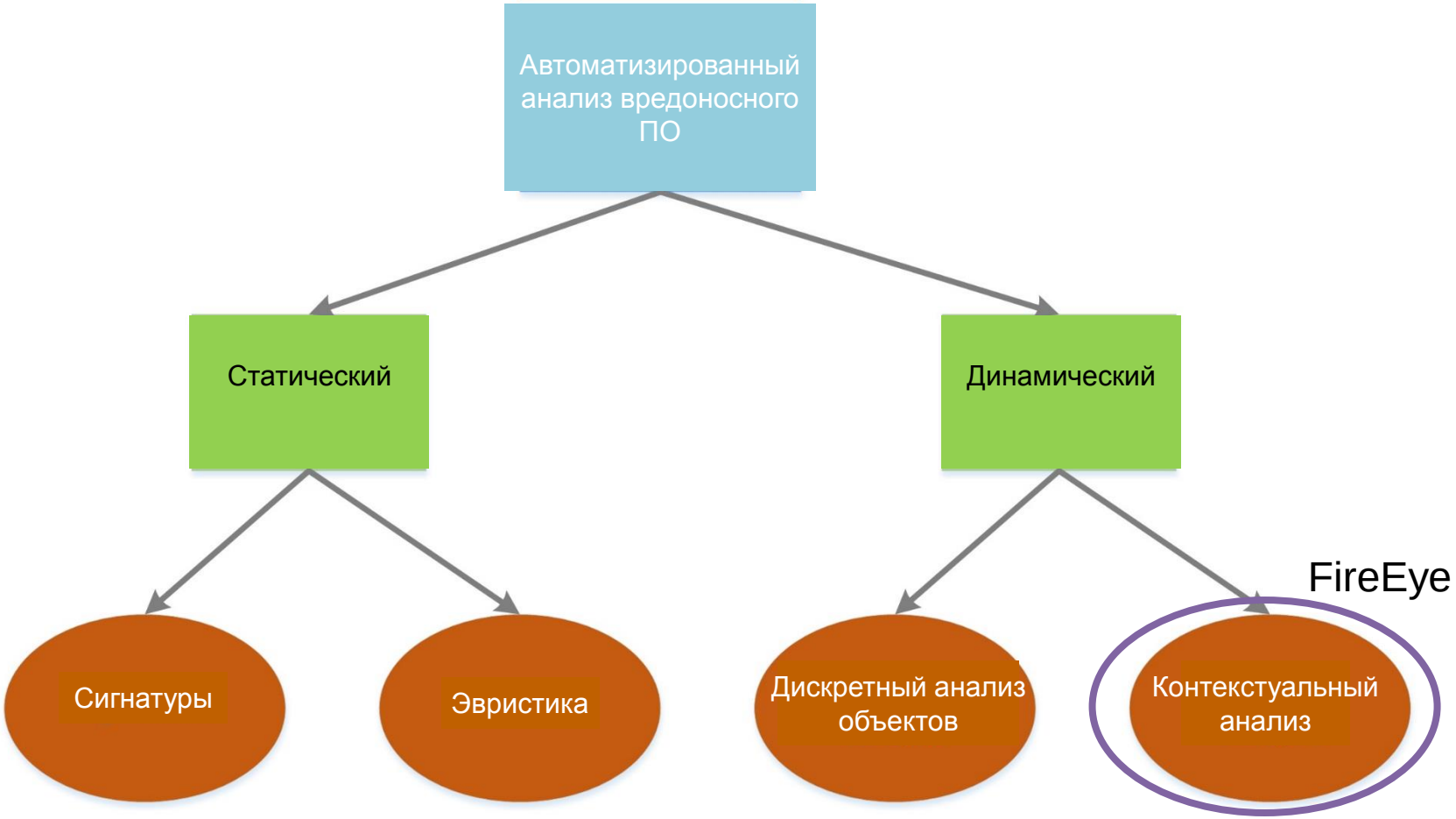
Устаревшая модель обнаружения угроз, основанная на сопоставлении с образцами



- Сигнатуры – черный список – репутация – эвристика
- Реагирует на события
- Только известные угрозы
- Ложные срабатывания

Новая модель обнаружения угроз, основанная на виртуальных машинах

- Без использования сигнатур
- Динамичная, работает в режиме реального времени
- Известные и неизвестные угрозы
- Минимум ложных срабатываний


Автоматизированный анализ вредоносного ПО
Статический
Динамический
Сигнатуры
Эвристика
Дискретный анализ объектов
Контекстуальный анализ
FireEye

FireEye

IT Guard

FireEye Leads in APT Threat Defense

William Blair

2013-07 William Blair - Sec

"We view FireEye as the le
virtual detonation space"

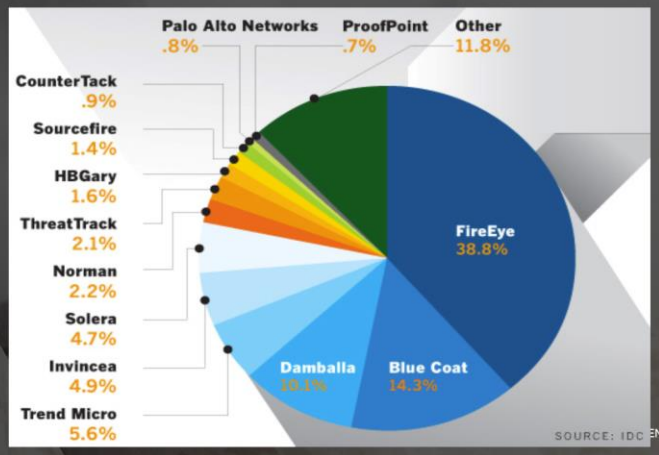
FROST & SULLIVAN

2014-05 Frost ar

APT solution v
vear

NET

IDC: FireEye alone has more than 39% market share worldwide (2013)



FireEye Leads in APT

FireEye

Gartner®

On prevention vs. detection, Gartner says to rebalance purchasing

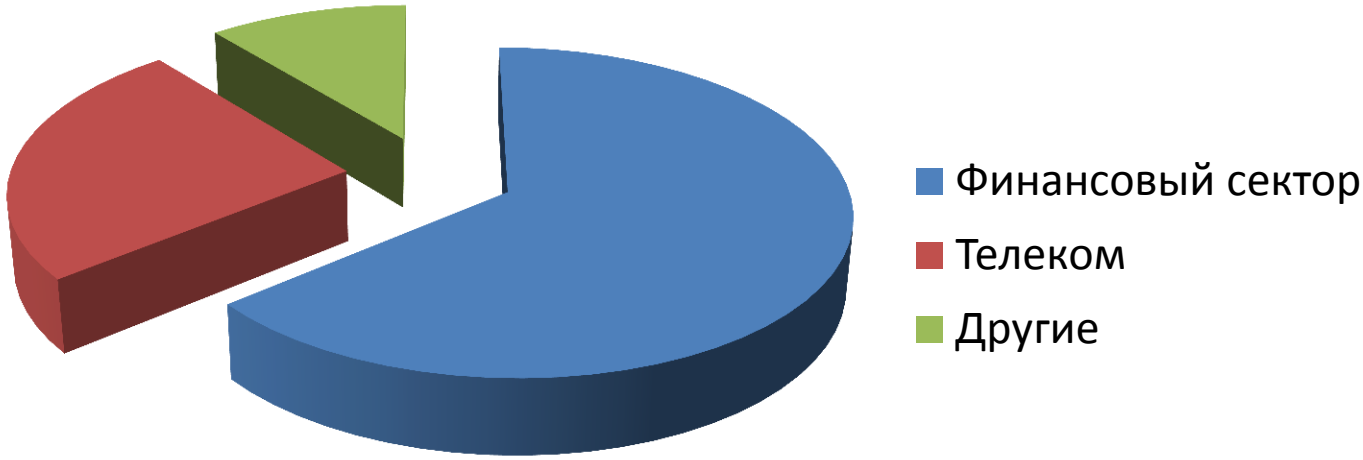
http://searchsecurity.techtarget.com/news/2240223269/On-prevention-vs-detection-Gartner-says-to-rebalance-purchasing

*"Vendors evolving, some more than others […] **FireEye Inc. is at the top of the list**, MacDonald said, not only with its January acquisition of Mandiant , but also recently by adding integrated, low-cost IPS capabilities to its threat prevention platform."*

Neil MacDonald, Vice President and Distinguished Analyst,
20 year Gartner Analyst

Заказчики FireEye в России

Профиль заказчиков FireEye в России



Tinkoff Bank

Ростелеком

открытие
ФИНАНСОВАЯ КОРПОРАЦИЯ

IT Guard

Тестирование FireEye

Web Malware Protection System™ 7400NX /4400NX – производительностью до 1Гбит/с с количеством пользователей до 10 000

Email Malware Protection System™

5400EX/8400EX/ 3400EX – производительностью до 600 000 писем в

Central Management System™ 4400CM/7400CM – для унифицированного управления платформами

Endpoint Security™ 4402HX – с количеством пользователей до 100 000

File Content Security™ 8400FX – проверяет до 160 000 файлов в день

IT Guard

FireEye™

FireEye

IT Guard

Спасибо за внимание!