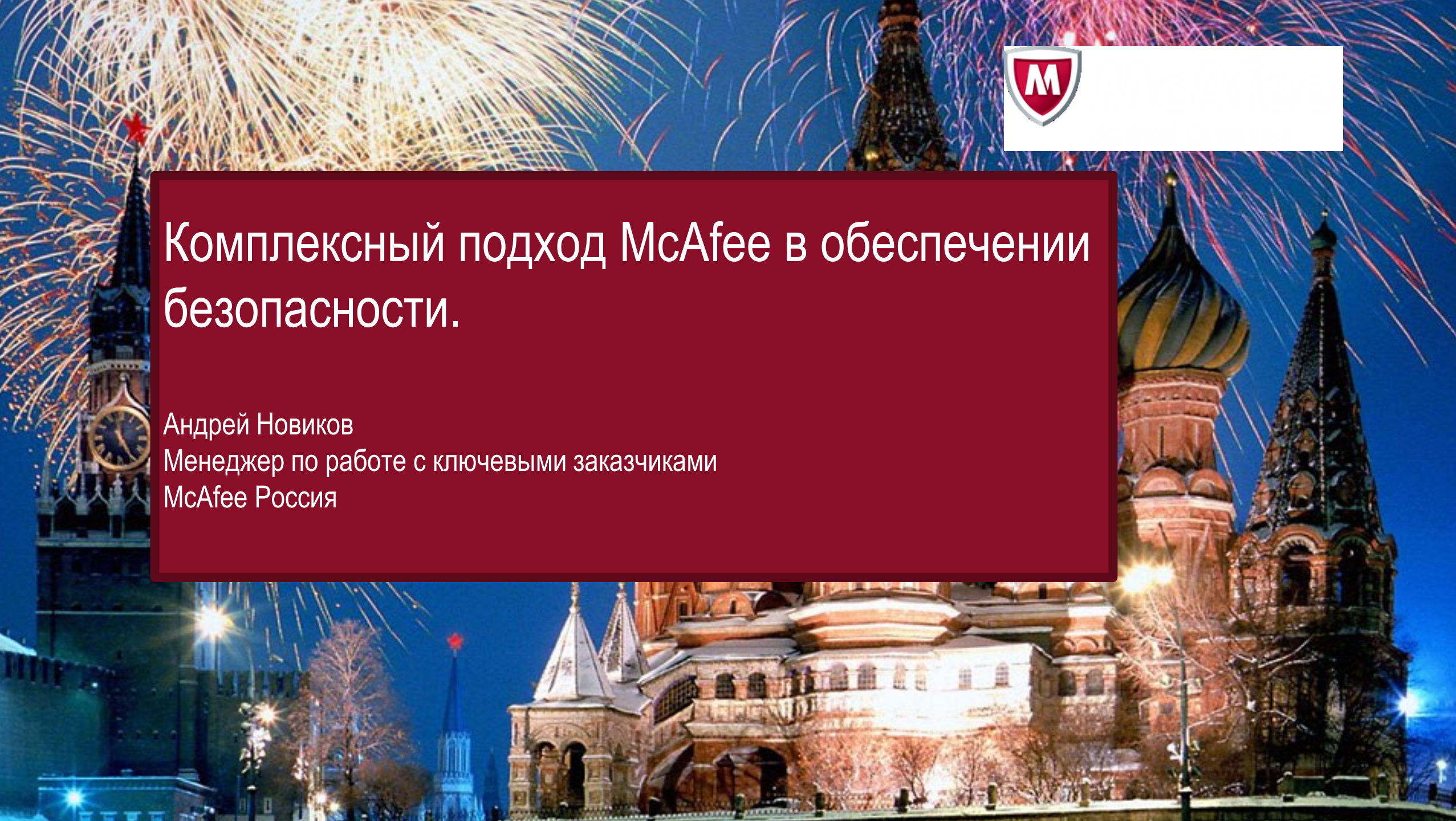


# Комплексный подход McAfee в обеспечении безопасности.

Андрей Новиков
Менеджер по работе с ключевыми заказчиками
McAfee Россия

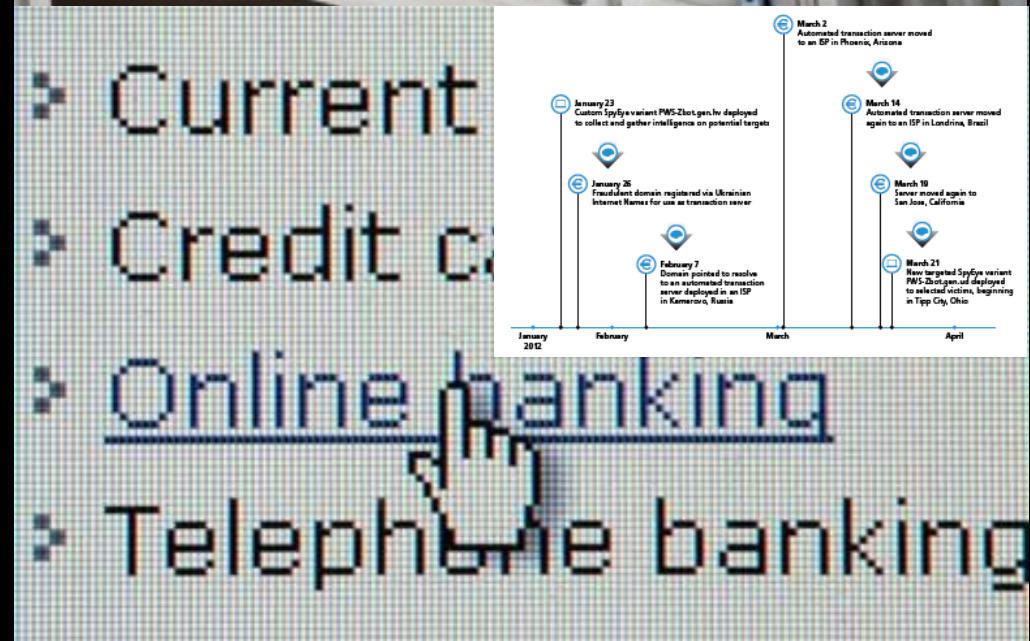
# Война и мир?


ВОЙНА и МИРЪ.


WE ARE
ANONYMOUS


CYBER
ATTACKS
AHEAD
BANK




Current
Credit c
Online banking
Telephone banking


January 23
Custom SpyEye variant PWS-Zbot.gen.hv deployed to collect and gather intelligence on potential targets
January 26
Fraudulent domain registered via Ukrainian Internet Names for use as transaction server
February 7
Domain pointed to resolve to an automated transaction server deployed in an ISP in Kemerovo, Russia
March 2
Automated transaction server moved to an ISP in Phoenix, Arizona
March 14
Automated transaction server moved again to an ISP in Londrina, Brazil
March 19
Server moved again to San Jose, California
March 21
New targeted SpyEye variant PWS-Zbot.gen.ud deployed to selected victims, beginning in Tipp City, Ohio
January 2012
February
March
April

# Ситуация в сфере корпоративной безопасности

КАК?

# Оптимизированные средства защиты

Снижение совокупной стоимости владения (TCO) и повышение уровня безопасности

## ТЕКУЩЕЕ ПОЛОЖЕНИЕ ДЕЛ

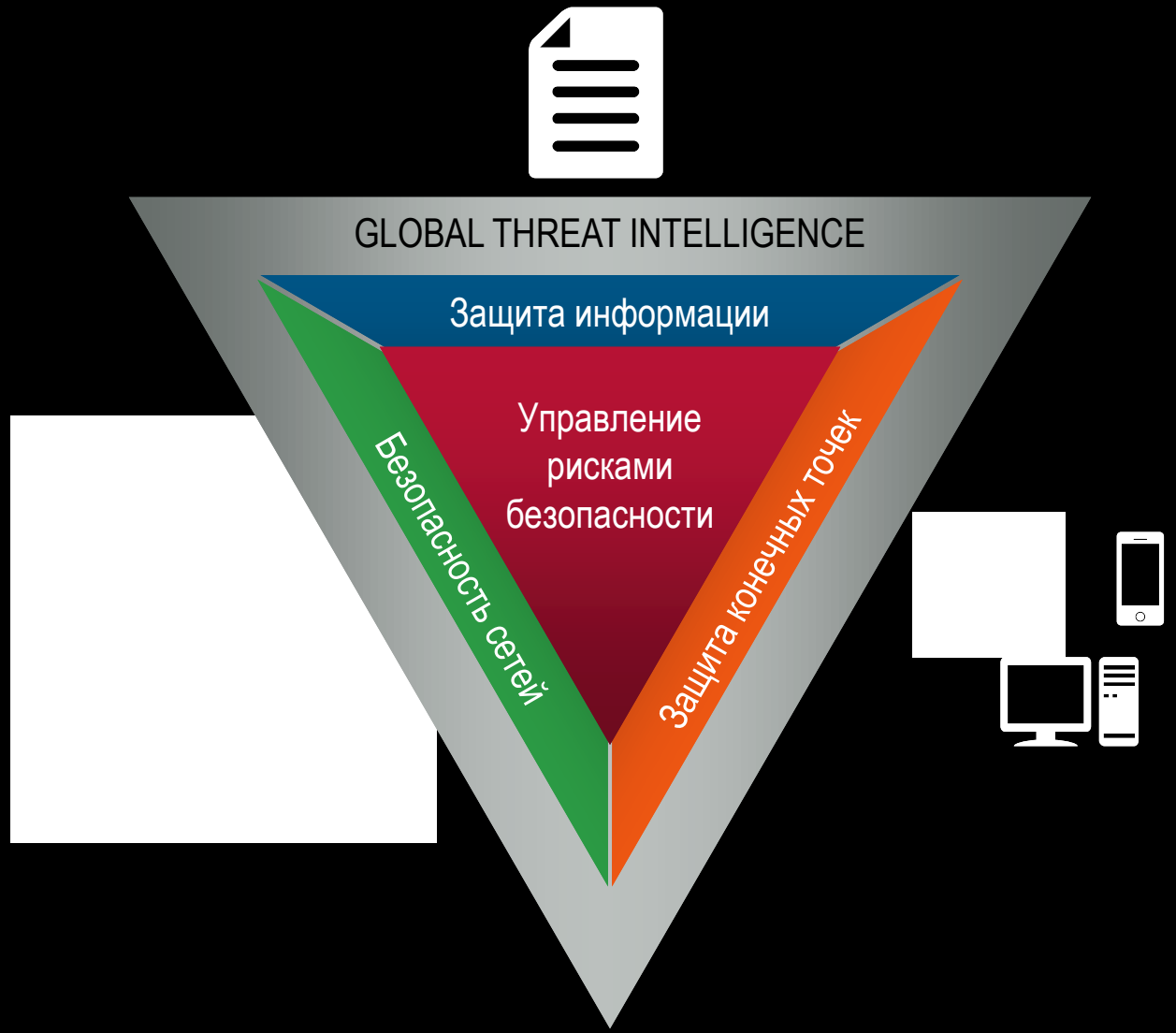
- **НЕСТАНДАРТИЗИРОВАННЫЕ СРЕДСТВА ЗАЩИТЫ:** ручные процессы, неэффективность и сложность ресурсов, и в результате — повышение стоимости владения и высокий уровень риска
- **ПОДХОД, ОСНОВАННЫЙ НА РЕАГИРОВАНИИ** отражает зацикленность на проблемах вчерашнего дня вместо подготовки к отражению изощренных угроз завтрашнего дня
- **НЕСООТВЕТСТВИЕ СТРАТЕГИЯМ БИЗНЕСА** означает ориентацию на ИТ-операции, а не на стратегические задачи бизнеса

## БУДУЩЕЕ ПОЛОЖЕНИЕ ДЕЛ

- **ИНТЕГРАЦИЯ** и консолидация решений в сфере безопасности
- **УПРЕЖДАЮЩАЯ ЗАЩИТА** от изощренных атак «нулевого дня»
- **НЕПРЕРЫВНОЕ ОБЕСПЕЧЕНИЕ** соответствия отраслевым и законодательным нормам
- **ПОЛНАЯ ОСВЕДОМЛЕННОСТЬ** об информационном риске
- **СНИЖЕНИЕ ИЗДЕРЖЕК БИЗНЕСА** при повышении уровня безопасности

# Наша стратегия: Security Connected

Защита конечных точек, сетей и данных, управление, глобальный сбор информации об угрозах



# Наша стратегия: Security Connected

Защита конечных точек, сетей и данных, управление, глобальный сбор информации об угрозах

# Наша стратегия: Security Connected

Защита конечных точек, сетей и данных, управление, глобальный сбор информации об угрозах

## БЕЗОПАСНОСТЬ СЕТЕЙ

## ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

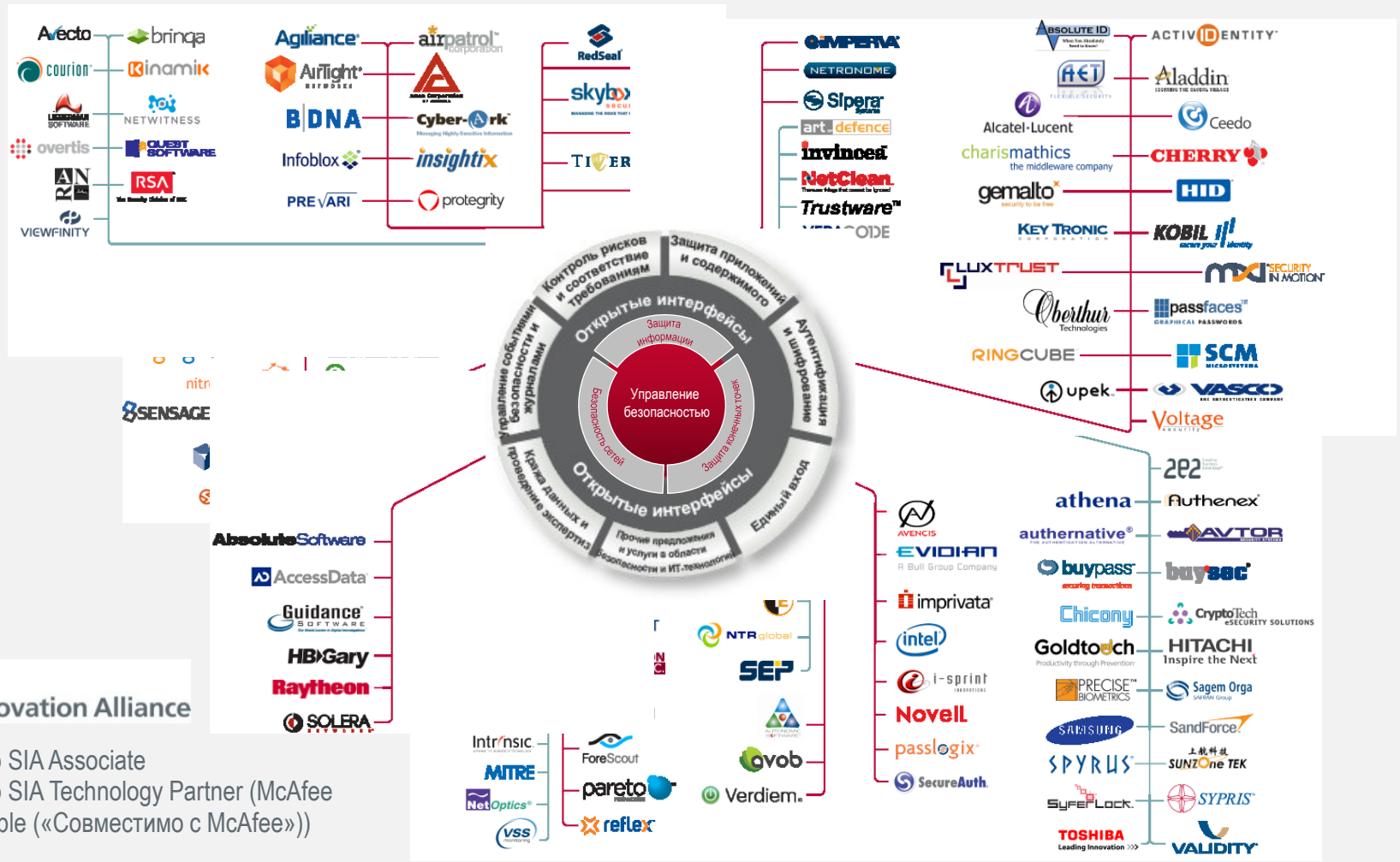
## УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ


## ЗАЩИТА КОНЕЧНЫХ ТОЧЕК

## СООБЩЕСТВО ПАРТНЕРОВ

# Security Connected: Интеграция сторонних продуктов

## Security Innovation Alliance



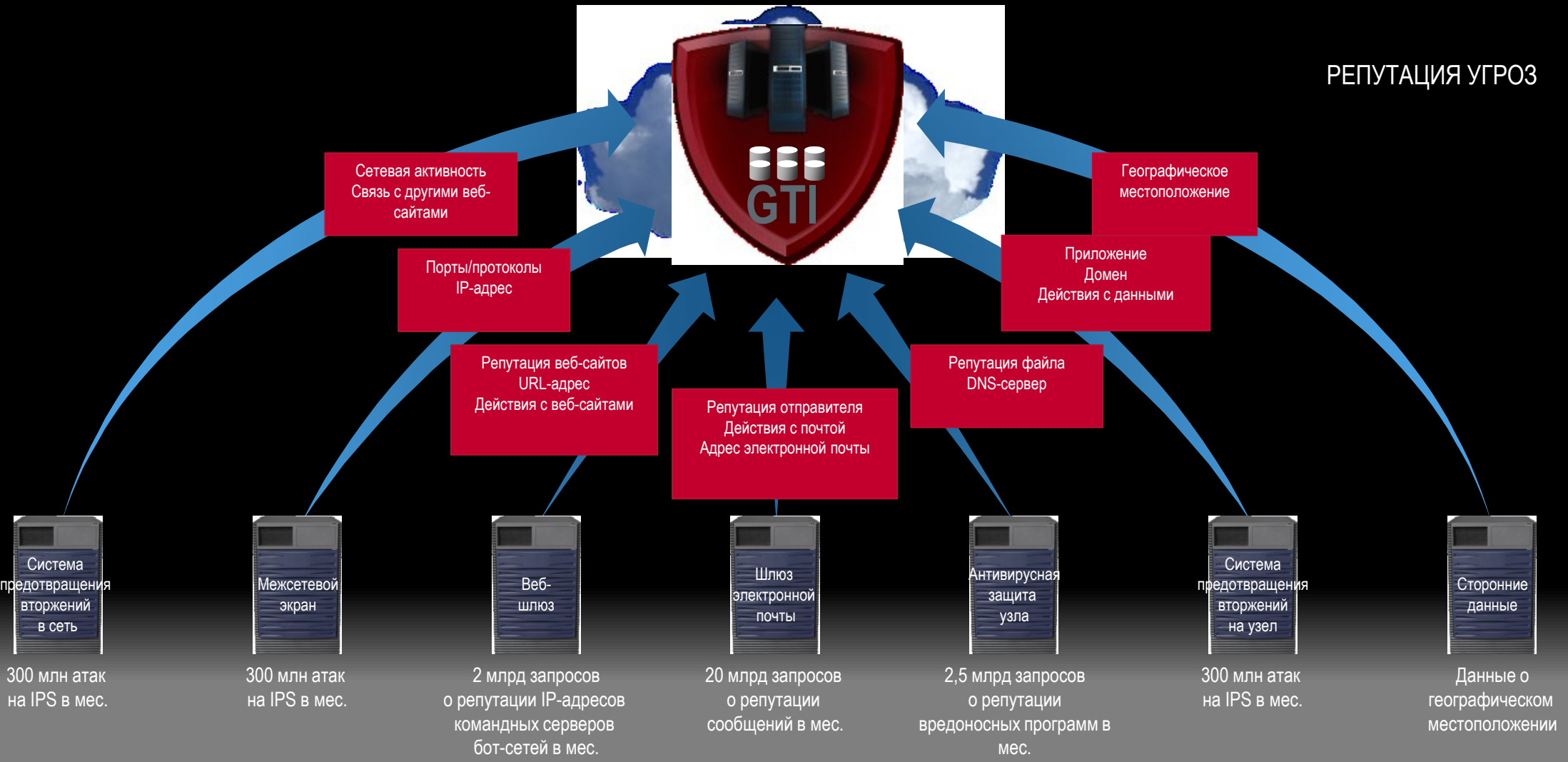

McAfee Security Innovation Alliance

Партнер SIA Associate

Партнер SIA Technology Partner (McAfee Compatible («Совместимо с McAfee»))

# Security Connected: Глобальный сбор информации об угрозах (GTI)

## Что стоит за обеспечением безопасности вашей организации



# Security Connected: Глобальный сбор информации об угрозах (GTI)

## Что стоит за обеспечением безопасности вашей организации


РЕПУТАЦИЯ УГРОЗ

| Система предотвращения вторжений в сеть | Межсетевой экран | Веб-шлюз | Шлюз электронной почты | Антивирусная защита узла | Система предотвращения вторжений на узел | Сторонние данные |
|---|---|---|---|---|---|---|
| 300 млн атак на IPS в мес. | 300 млн атак на IPS в мес. | 2 млрд запросов о репутации IP-адресов командных серверов бот-сетей в мес. | 20 млрд запросов о репутации сообщений в мес. | 2,5 млрд запросов о репутации вредоносных программ в мес. | 300 млн атак на IPS в мес. | Данные о географическом местоположении |

# Эволюционирование платформы (ERP с преимуществом открытой системы)

Совершенствование процесса

Отчетность

Интеграции

Автоматизация
(сокращение затрат, повышение эффективности)

Сбор и анализ данных

ТЕХНОЛОГИЯ РЕАЛИЗАЦИИ:
ПЛАТФОРМА

Катализатор:
проблема
2000 года

Катализатор:
Flame, вирус
сезона…

**ПРОЦЕСС:**
Модели оптимизации, распространение стандартных операционных сред (SOE)

**ОТЧЕТНОСТЬ:**
ePO, MRA и т. д.

**ИНТЕГРАЦИЯ:**
Консолидация в рамках Security Connected

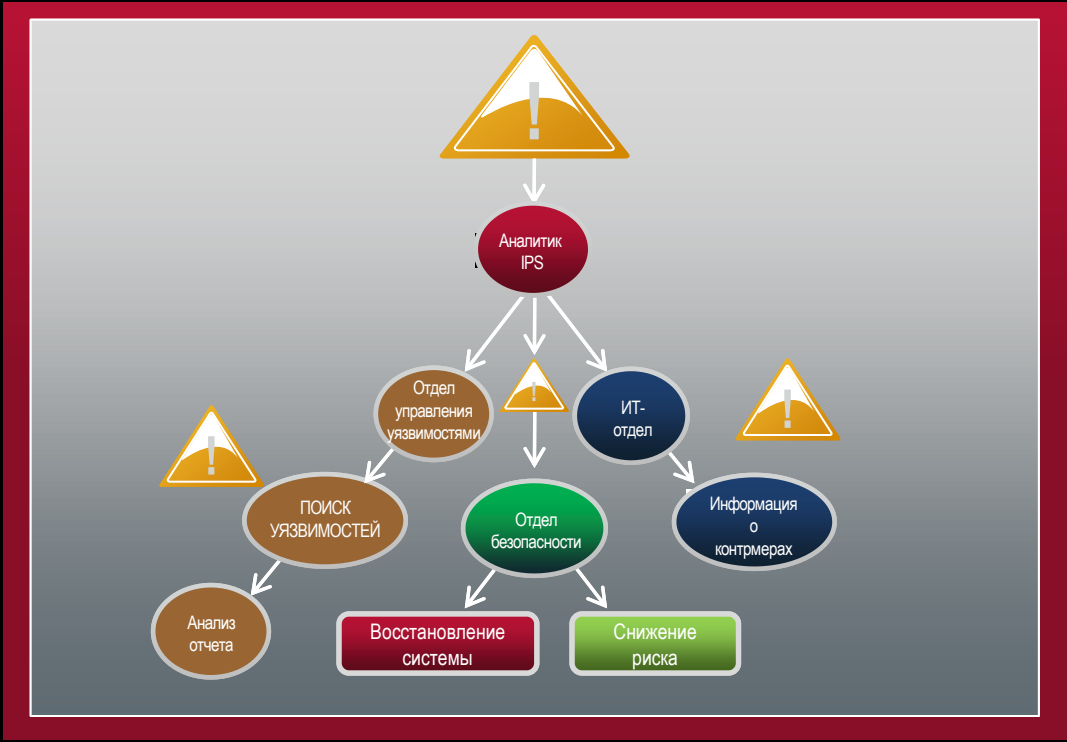
**АВТОМАТИЗАЦИЯ:**
ePO, SIEM, контрмеры

**СБОР И АНАЛИЗ ДАННЫХ:**
SIEM, GTI, LTI, «большие данные»

**ПЛАТФОРМА:**
Платформа Security Connected

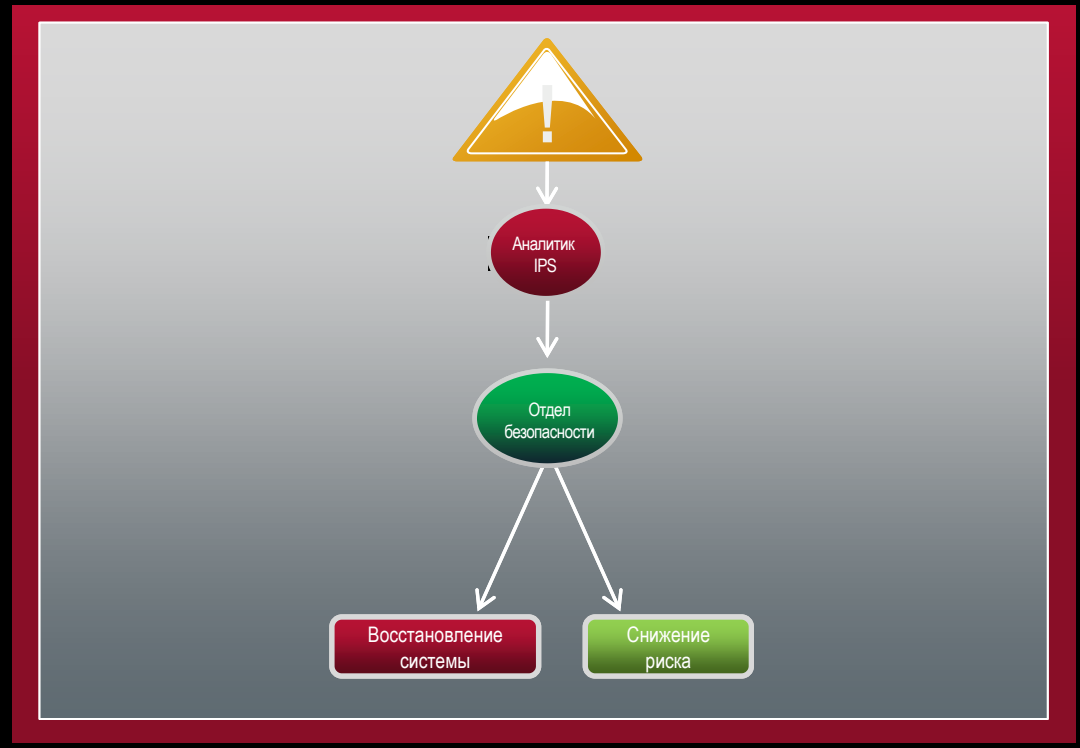
# Security Connected: Ощутимая разница

## Конкретный пример: Обнаружение и блокирование атаки Conficker




### НЕОПТИМИЗИРОВАННАЯ ЗАЩИТА

- 7,5 ЧАСОВ проходит до принятия окончательного решения по событию
- 5 КОНСОЛЕЙ необходимы для проверки актуальности уведомления
- 4 РАЗНЫХ ВНУТРЕННИХ ПРОЦЕССА необходимы для принятия окончательного решения



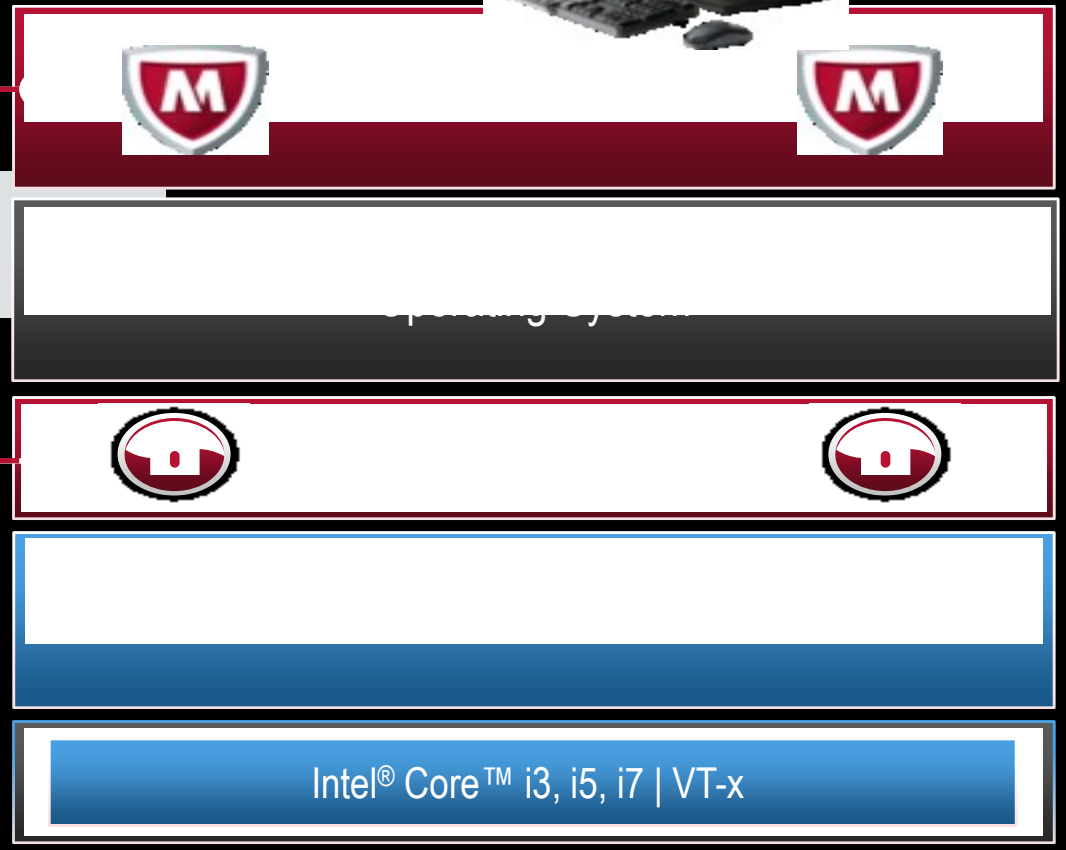

### ОПТИМИЗИРОВАННАЯ ЗАЩИТА

- 36 МИНУТ проходит до принятия окончательного решения по событию
- 2 КОНСОЛИ необходимы для проверки актуальности уведомления
- 2 РАЗНЫХ ВНУТРЕННИХ ПРОЦЕССА необходимы для принятия окончательного решения

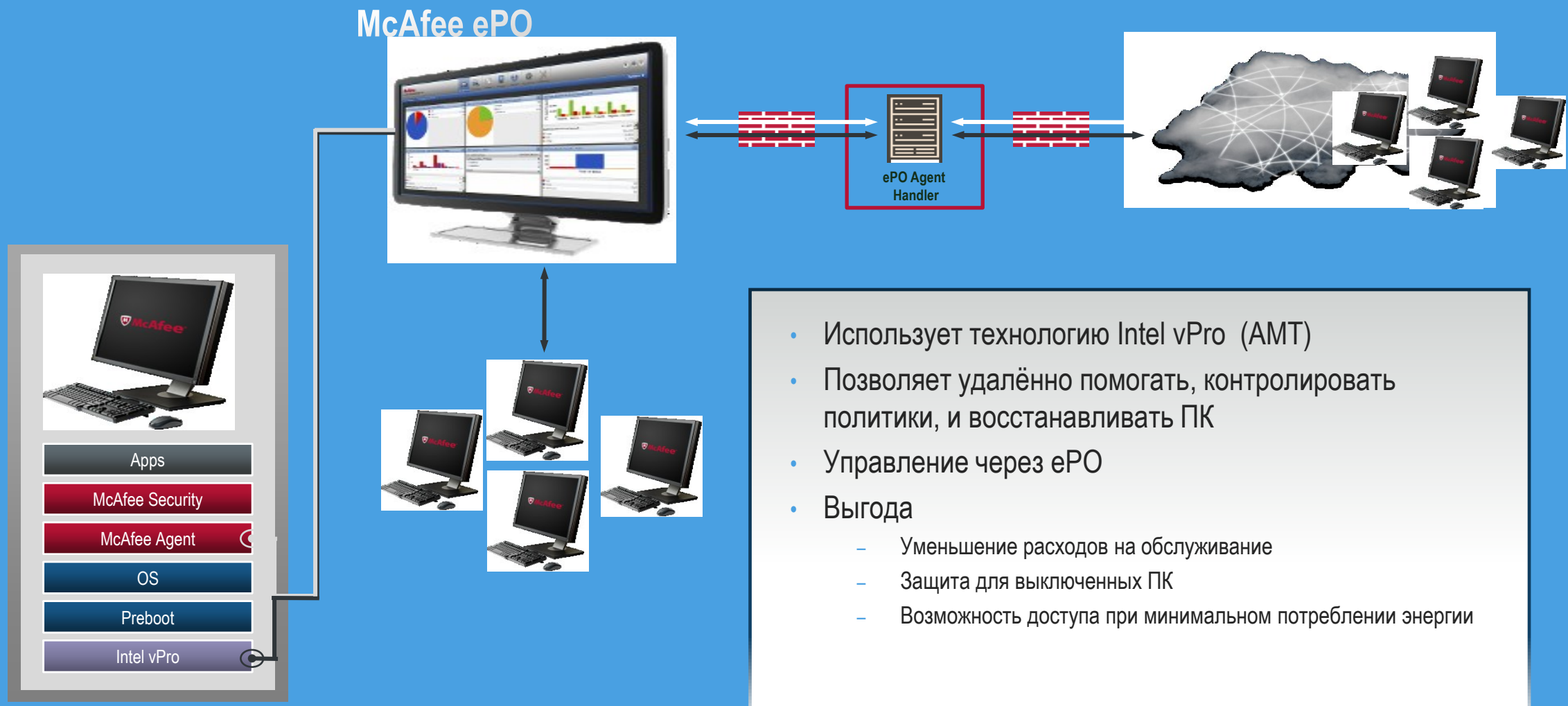
# Платформа Security Connected (SCP)

# McAfee Deep Defender

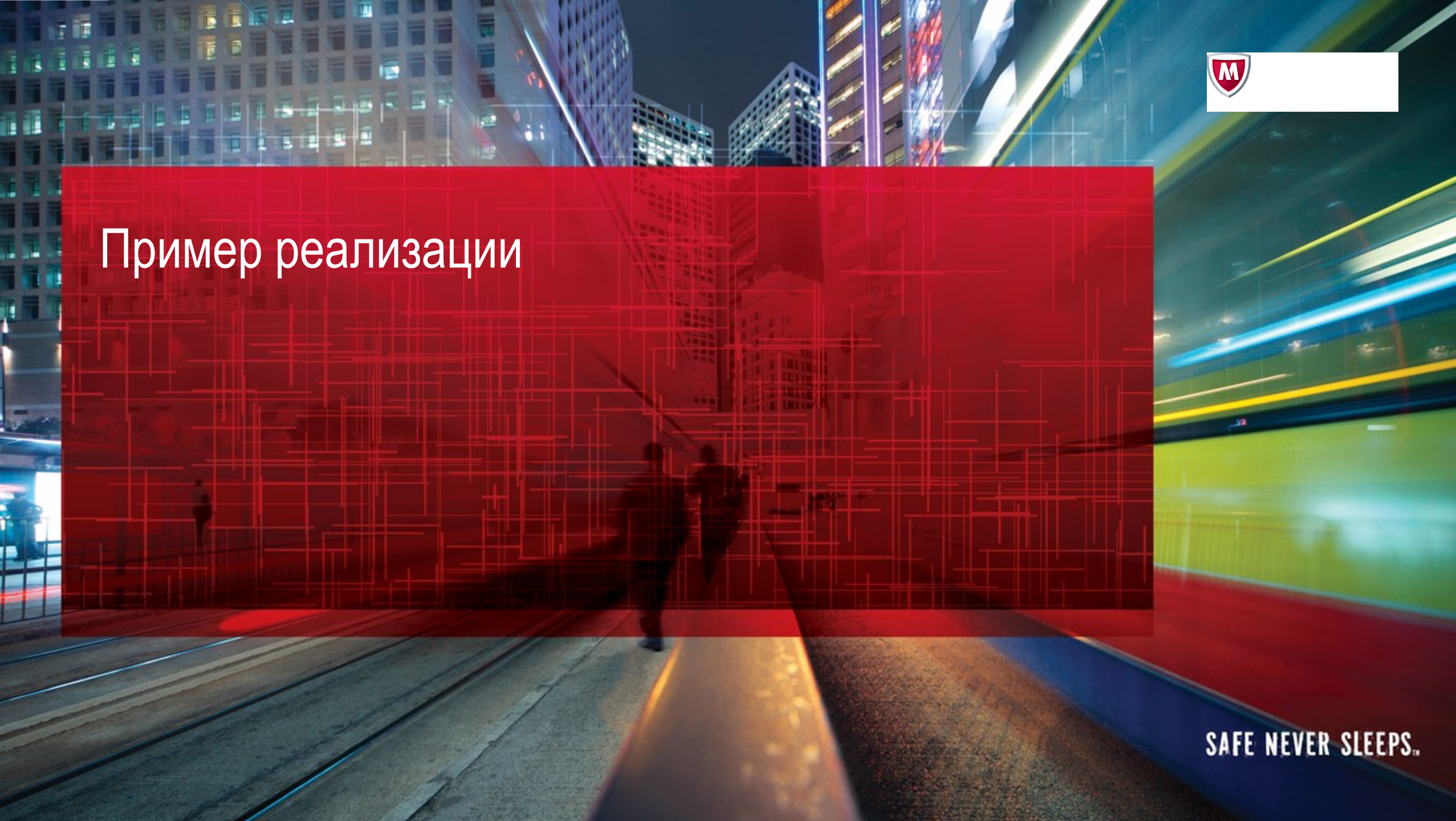
- Использует технологию McAfee DeepSAFE
- Защита ядра системы в реальном времени
- Защита от ранее скрытых угроз
- Управляется с помощью ePO



# McAfee ePO Deep Command




- Использует технологию Intel vPro (AMT)
- Позволяет удалённо помогать, контролировать политики, и восстанавливать ПК
- Управление через ePO
- Выгода
  - Уменьшение расходов на обслуживание
  - Защита для выключенных ПК
  - Возможность доступа при минимальном потреблении энергии



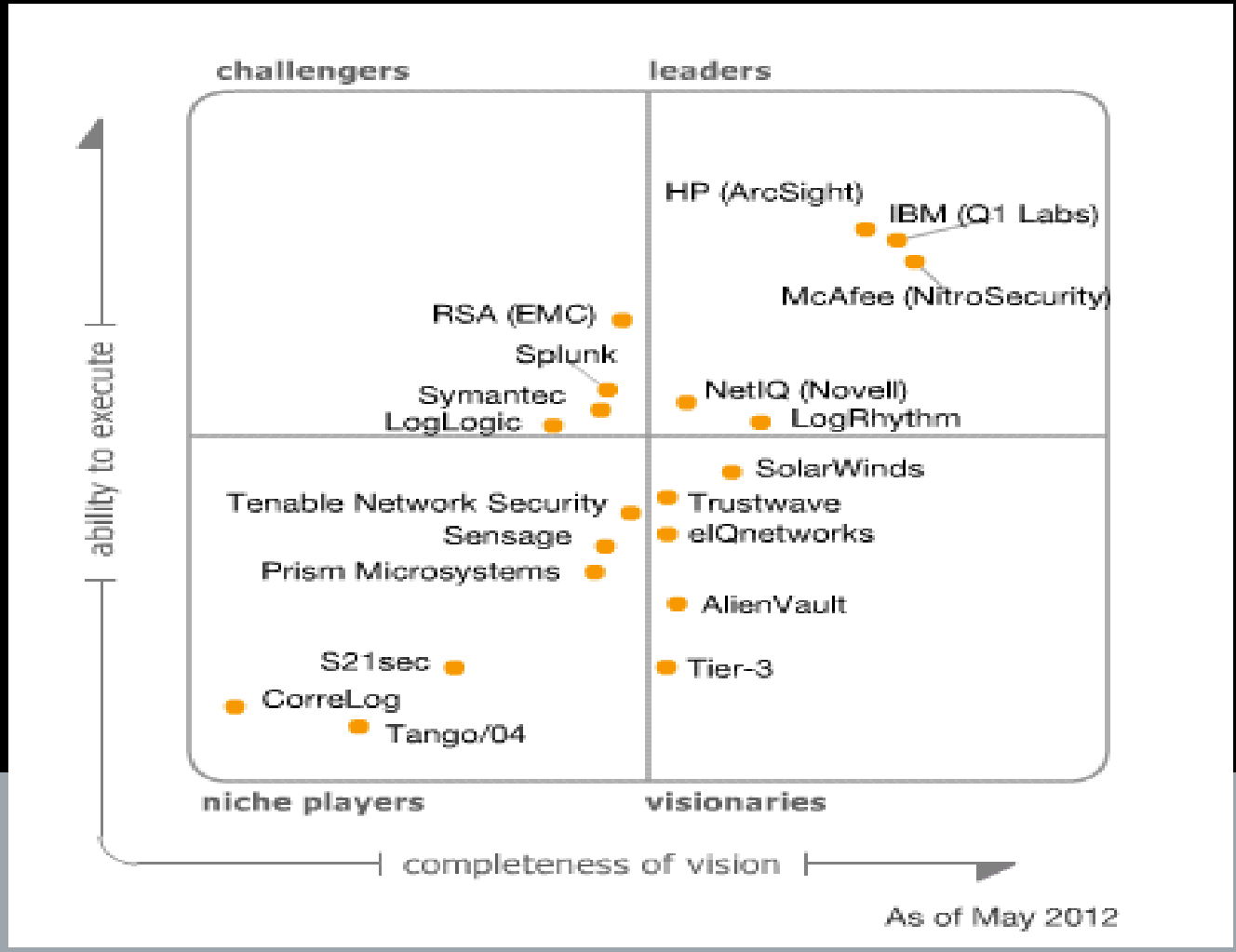

# Пример реализации

# Производительность и масштабируемость

- Недостижимая скорость
  - Наиболее производительный SIEM на рынке
  - В сотни (а часто и в тысячи) раз быстрее аналогичных решений конкурентов
  - Запросы, корреляция и анализ за секунды (а не минуты или часы)

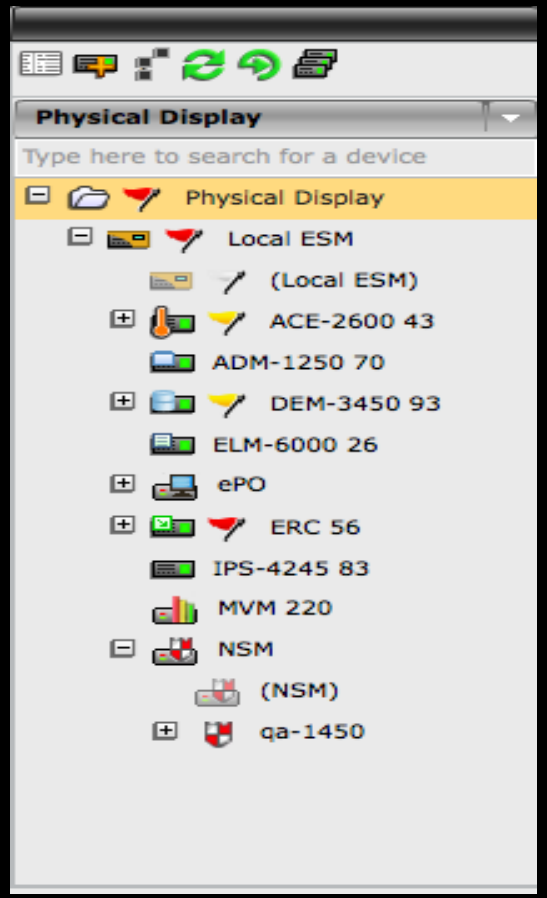
- Недостижимая масштабируемость
  - Сбор всей релевантной информации
  - Анализ информации за месяцы и годы, включая высокоуровневую информацию о контенте и контексте
  - Работа с миллиардами записей в БД

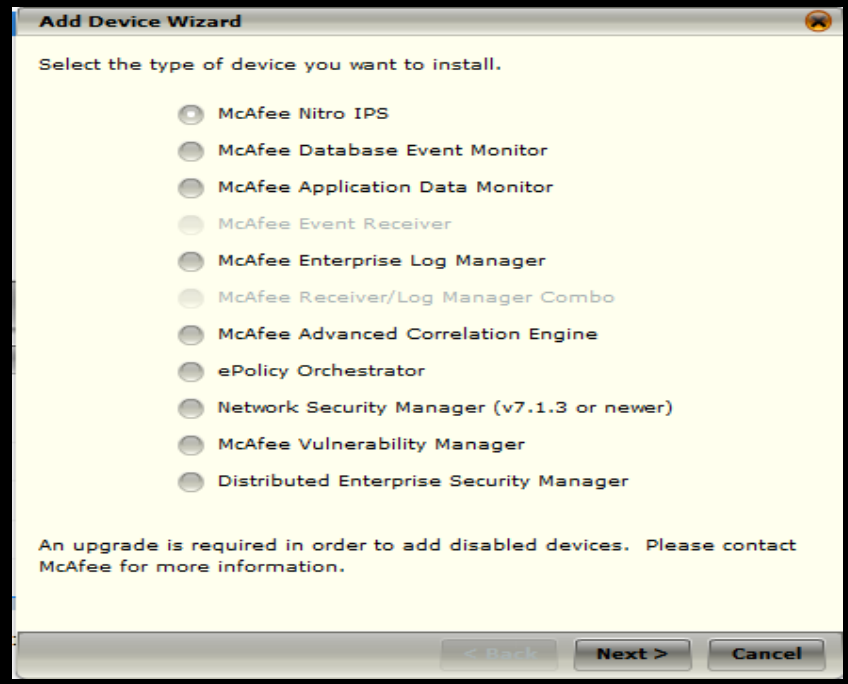
# Лидер на рынке SIEM



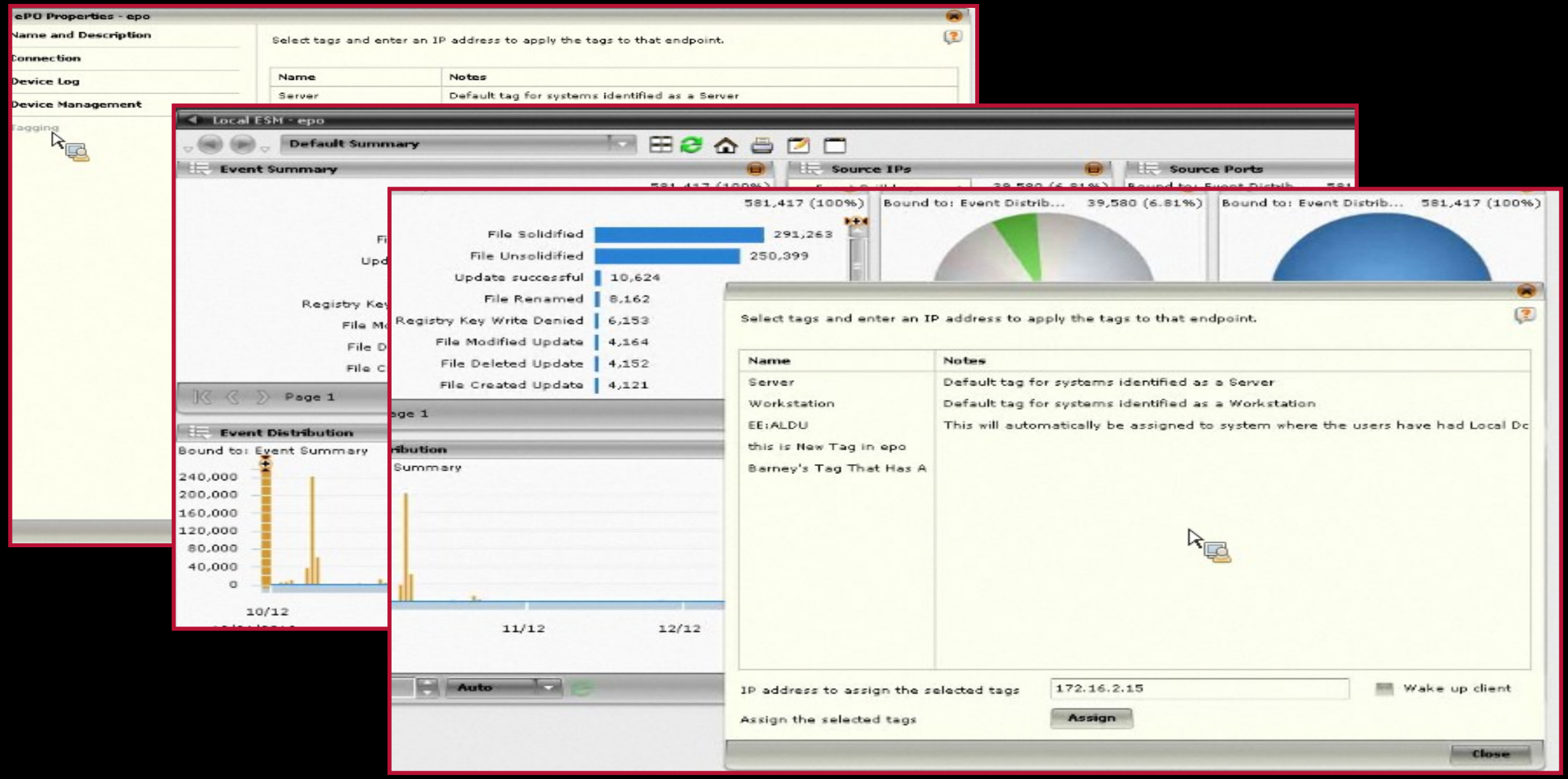
# Новые устройства в SIEM: ePO, NSM, MVM

- ePO, NSM, MVM стали нативными устройствами McAfee SIEM
  - Глубокая интеграция позволит получить ещё больший эффект от внедрения продуктов McAfee

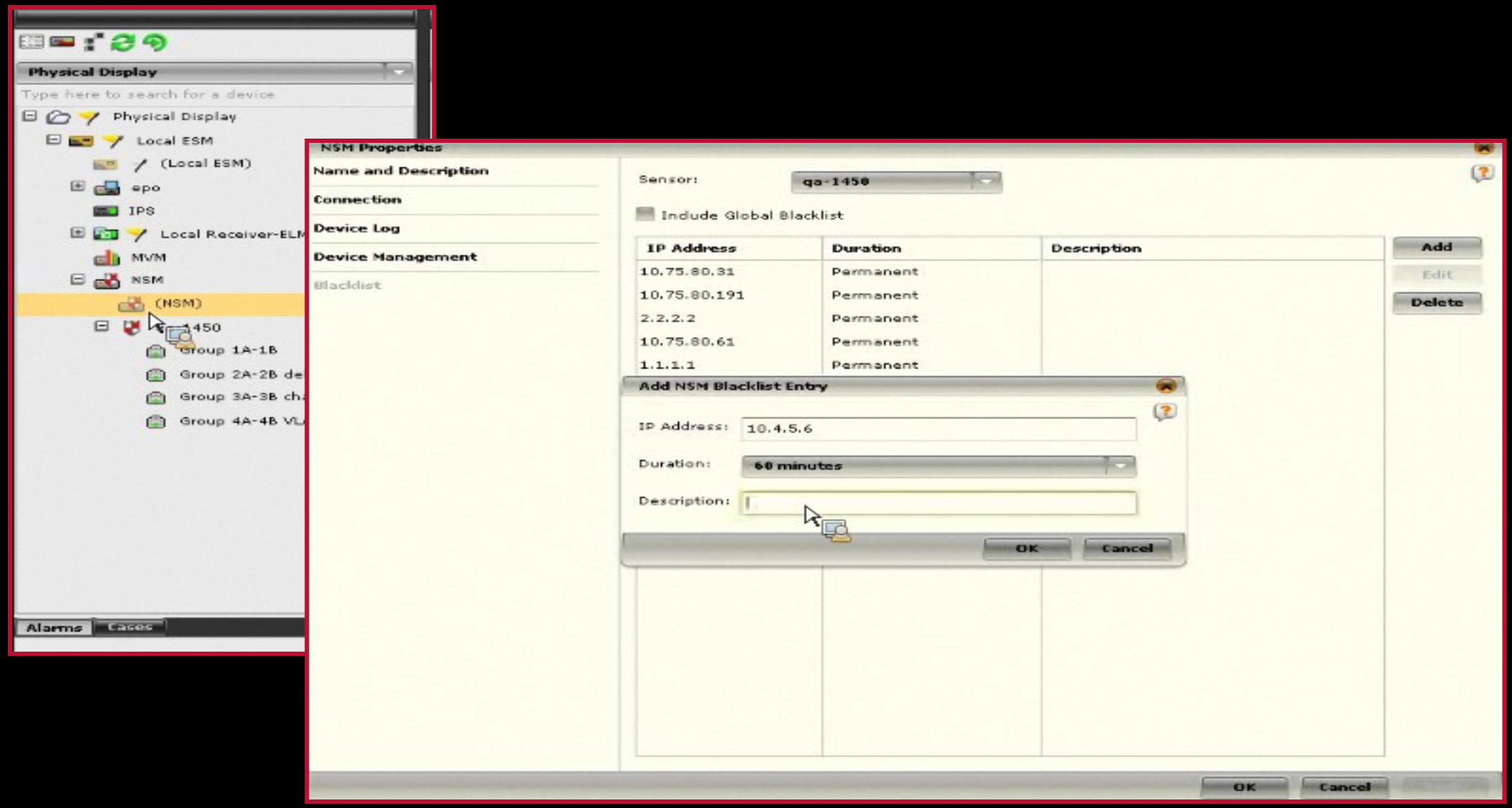


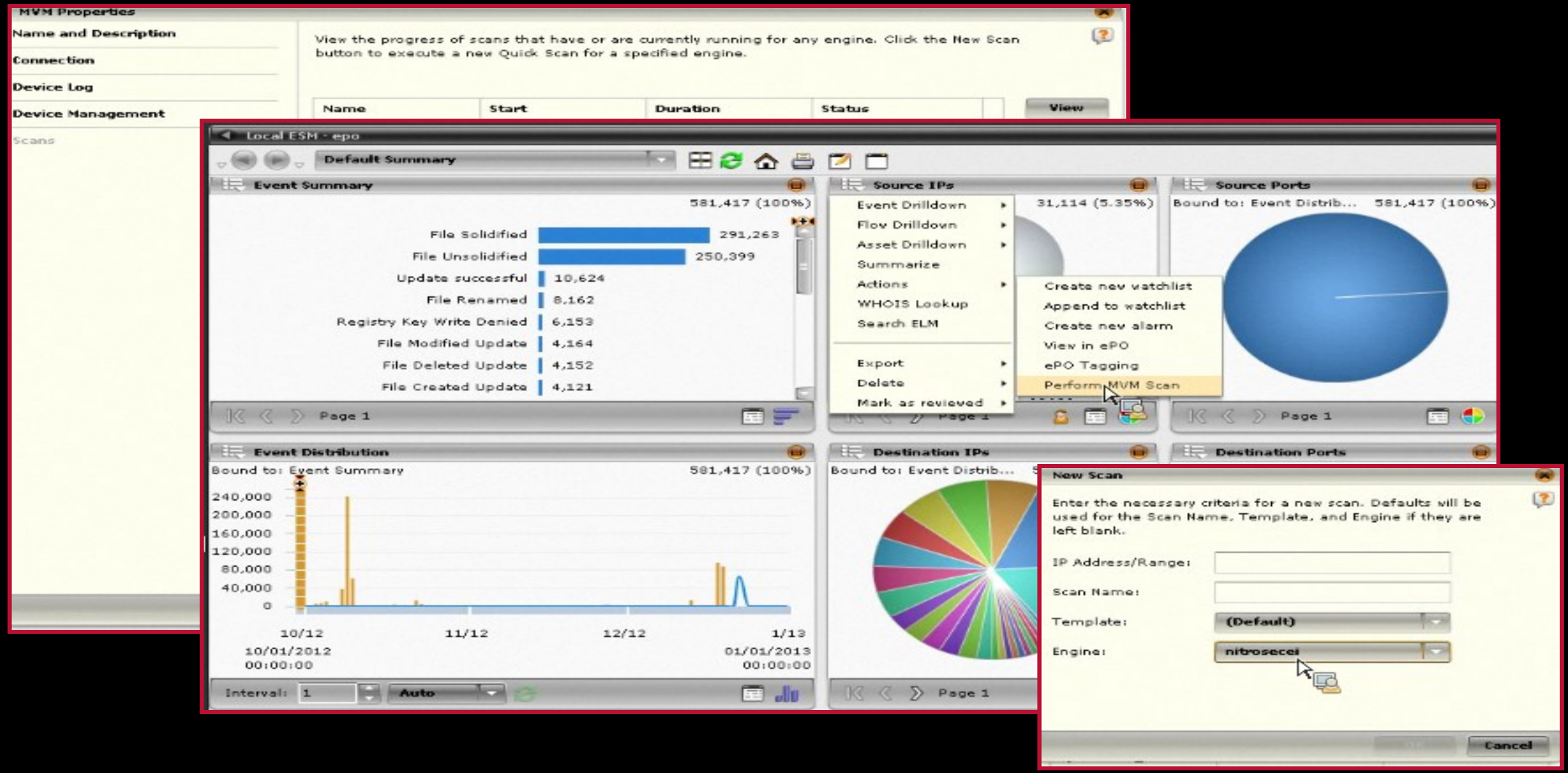
# Выполнение различных задач из единой консоли



# Конфигурация NSM и черные списки IPS



# Интеграция с MVM



# Кабинет администратора ИТ/Безопасности