



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



- Current
- Credit c
- Online banking
- Telephone banking

Date	Event
January 2012	January 7: President domain registered via Ukrainian Internet Names for use as transaction server in Kamerun, Russia
February	February 23: Custom Spylife variant PWS-Zbot.gen deployed to collect and gather intelligence on potential targets
March	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 Spylife variant PWS-Zbot.gen deployed to selected victims, beginning in Tipp City, Ohio
April	

КАК?

Оптимизированные средства защиты

Снижение совокупной стоимости владения (ТСО) 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

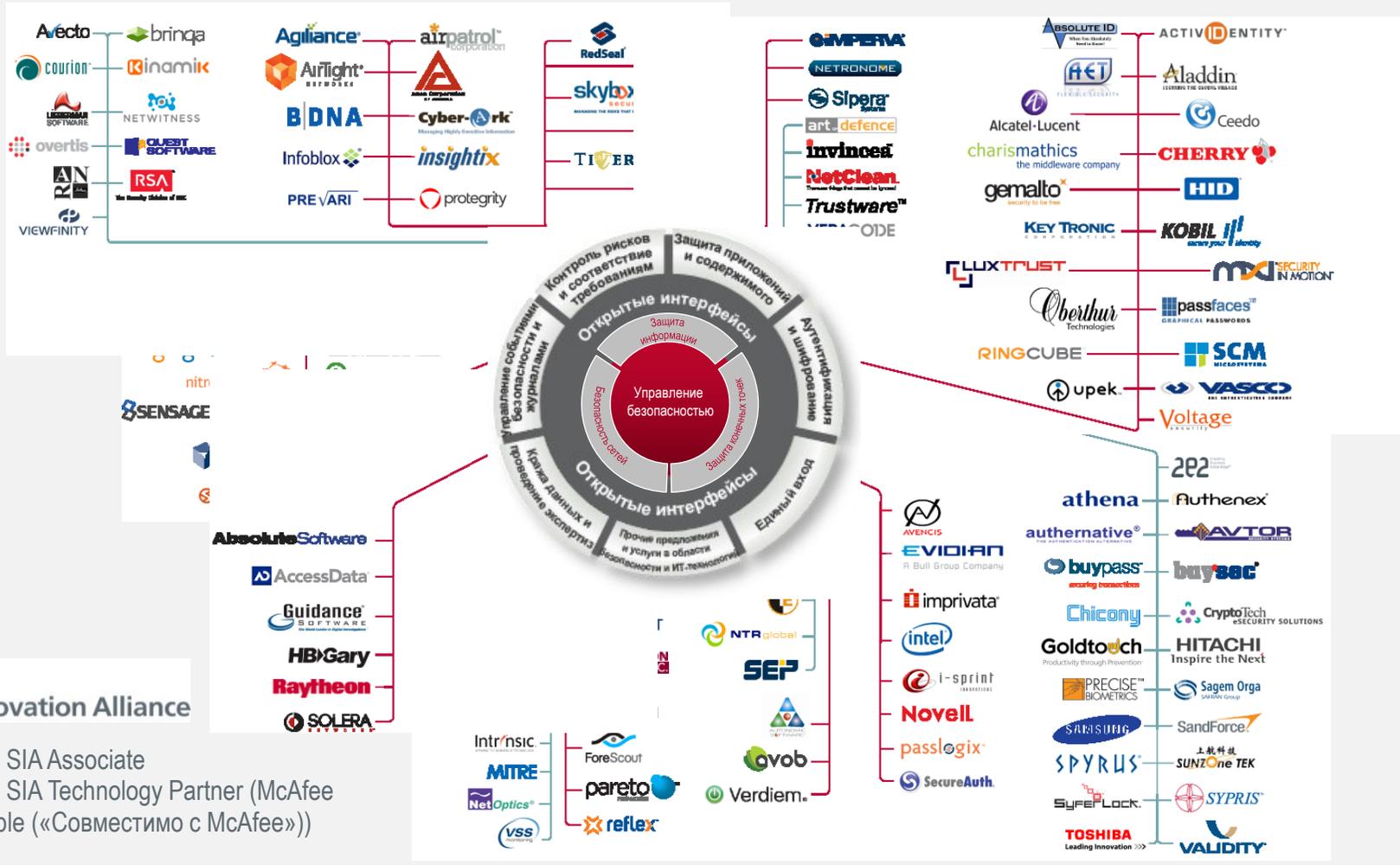


СООБЩЕСТВО ПАРТНЕРОВ



Security Connected: Интеграция сторонних продуктов

Security Innovation Alliance



McAfee
Security Innovation Alliance

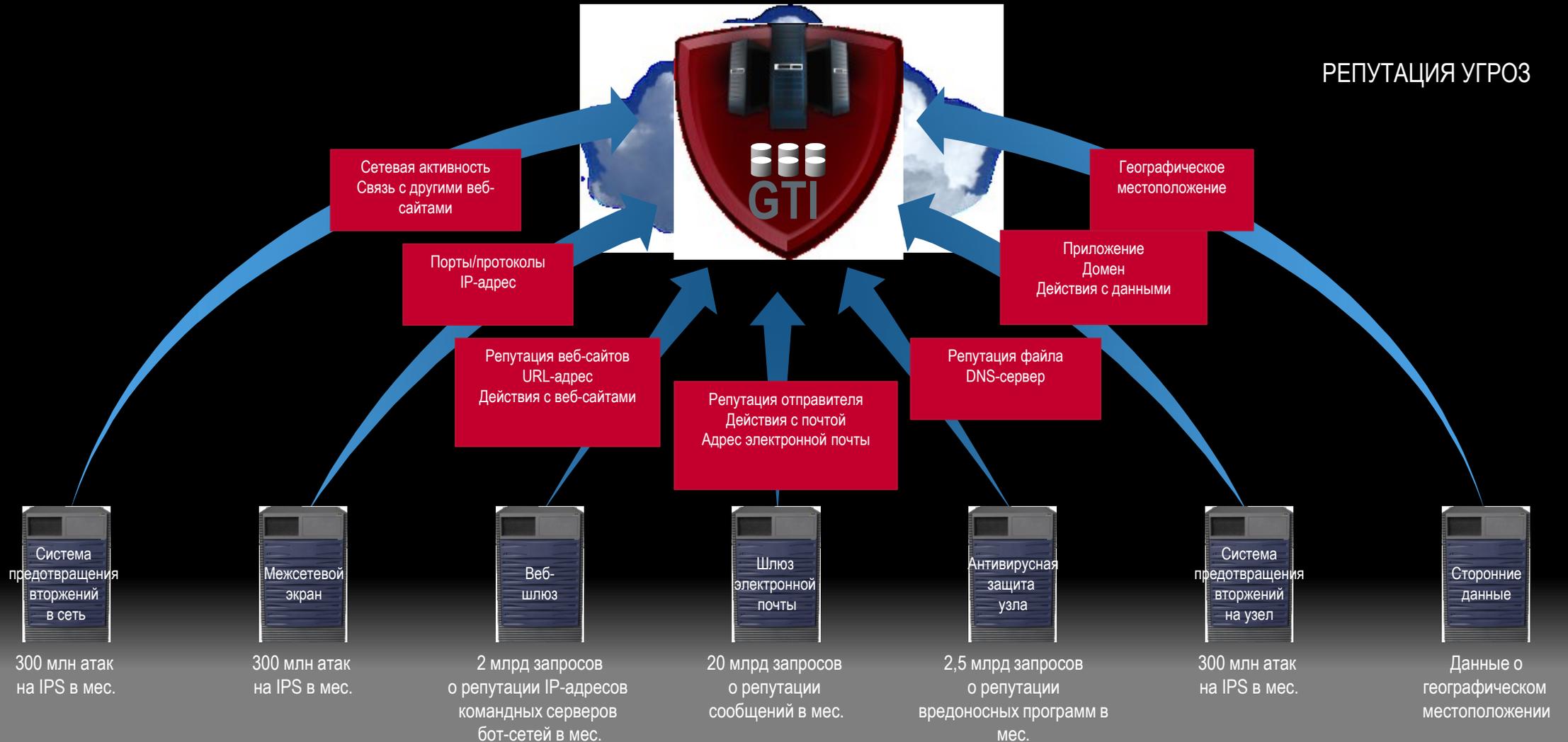
- Партнер SIA Associate
- Партнер SIA Technology Partner (McAfee Compatible («Совместимо с McAfee»))

Security Connected: Глобальный сбор информации об угрозах (GTI)

Что стоит за обеспечением безопасности вашей организации



РЕПУТАЦИЯ УГРОЗ



Security Connected: Глобальный сбор информации об угрозах (GTI)

Что стоит за обеспечением безопасности вашей организации



РЕПУТАЦИЯ УГРОЗ



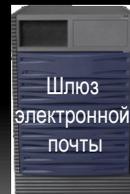
300 млн атак на IPS в мес.



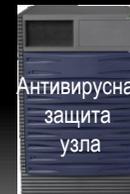
300 млн атак на IPS в мес.



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.



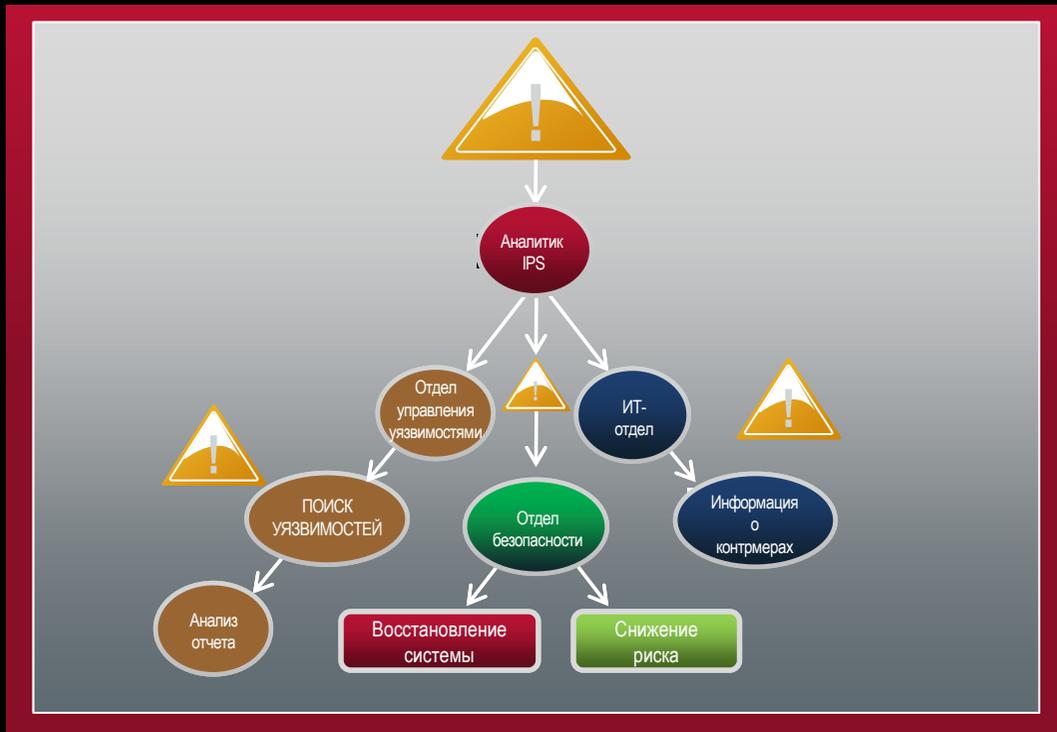
Данные о географическом местоположении

Эволюционирование платформы (ERP с преимуществом открытой системы)



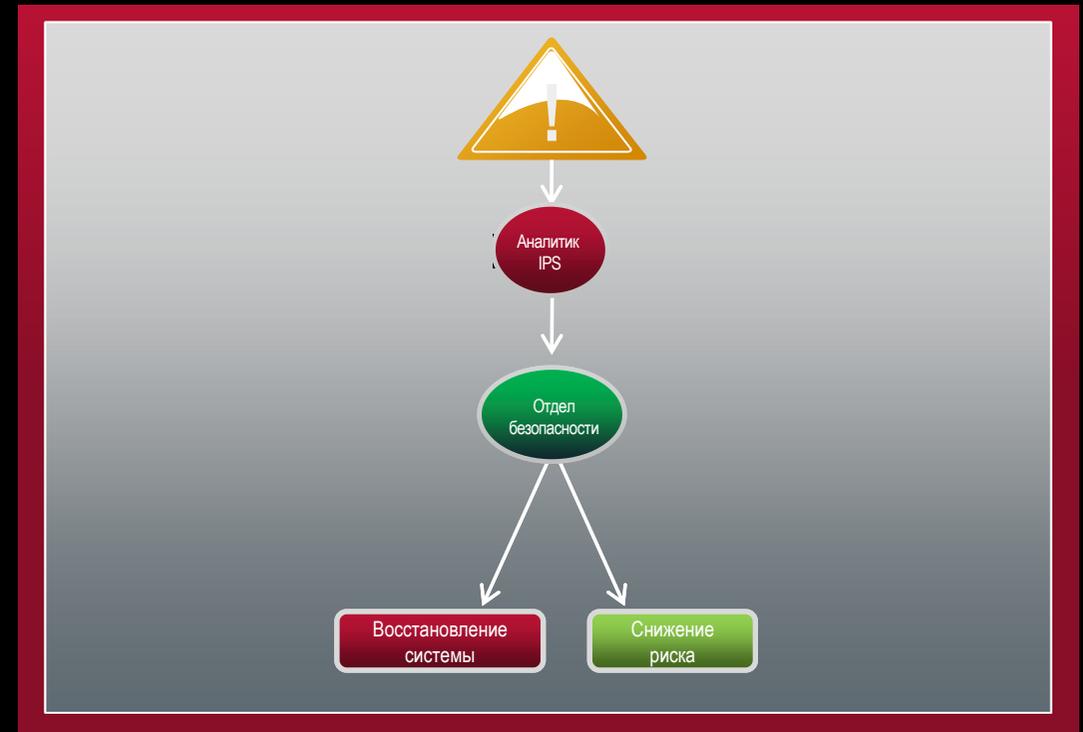
Security Connected: Ощутимая разница

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)



ДАННЫЕ ОБ УГРОЗАХ

Глобальный сбор информации об угрозах (GTI) (GTI)	Локальный сбор информации об угрозах (LTI) (LTI)	Третьи стороны (вертикальная интеграция, геопозиционирование, анализ поведения)	Обогащенные данные
---	--	---	---------------------------

АНАЛИТИКА

McAfee SIEM, личные данные, экспертизы, анализ рисков, анализ поведения

МЕРЫ ПРОТИВОДЕЙСТВИЯ
УПРАВЛЕНИЕ И
КОНТРОЛЬ

«Облачная» защита <ul style="list-style-type: none">Защита от вредоносных программСистема предотвращения вторжений на узелШифрованиеМежсетевой экран для настольного компьютераЗащита баз данных	Безопасность сетей <ul style="list-style-type: none">Контроль за приложениями и контроль за изменениямиЗащита мобильных устройствСистема предотвращения вторженийМежсетевой экранКонтроль доступа	Защита конечных точек <ul style="list-style-type: none">Шлюз электронной почтыВеб-шлюзУправление уязвимостямиУправление идентификационными атрибутами	Глубокая проверка
--	---	--	------------------------------

УПРАВЛЕНИЕ
БЕЗОПАСНОСТЬЮ

ePO + SIEM + сетевая политика

УРОВЕНЬ ДАННЫХ
И АВТОМАТИЗАЦИИ

Репозиторий ePO+ БД SIEM Nitro

Защита с аппаратной поддержкой



СИТУАТИВНАЯ
ОСВЕДОМЛЕННОСТЬ ДЛЯ
ПРИНЯТИЯ
КОНКРЕТНЫХ ДЕЙСТВИЙ
И СНИЖЕНИЕ TCO

McAfee Deep Defender



Использует технологию McAfee DeepSAFE



Защита ядра системы в реальном времени

Защита от ранее скрытых угроз



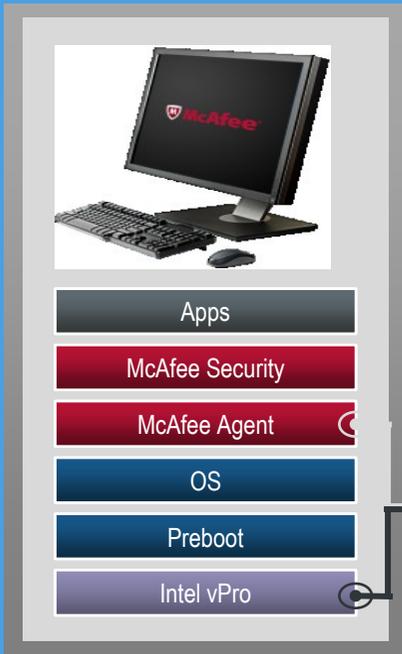
Управляется с помощью ePO

Intel® Core™ i3, i5, i7 | VT-x

McAfee ePO Deep Command



McAfee ePO



- 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

SAFE NEVER SLEEPS™

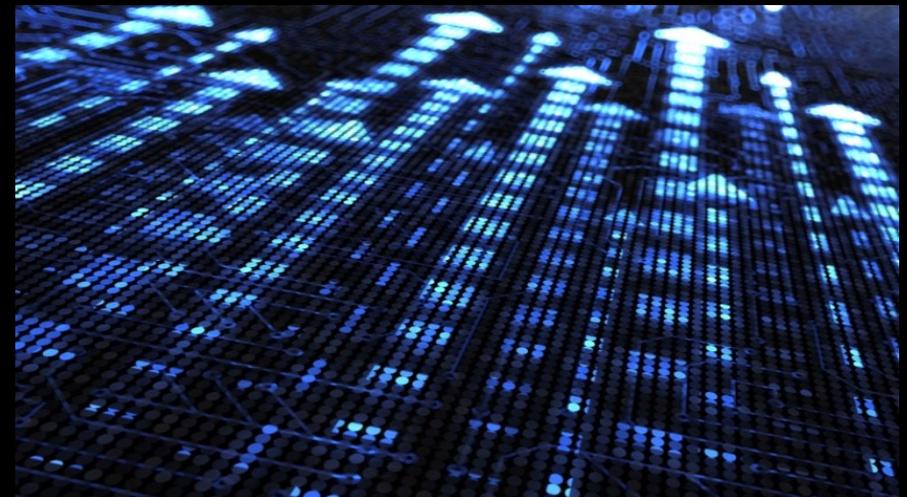
- Недостижимая скорость

- 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)

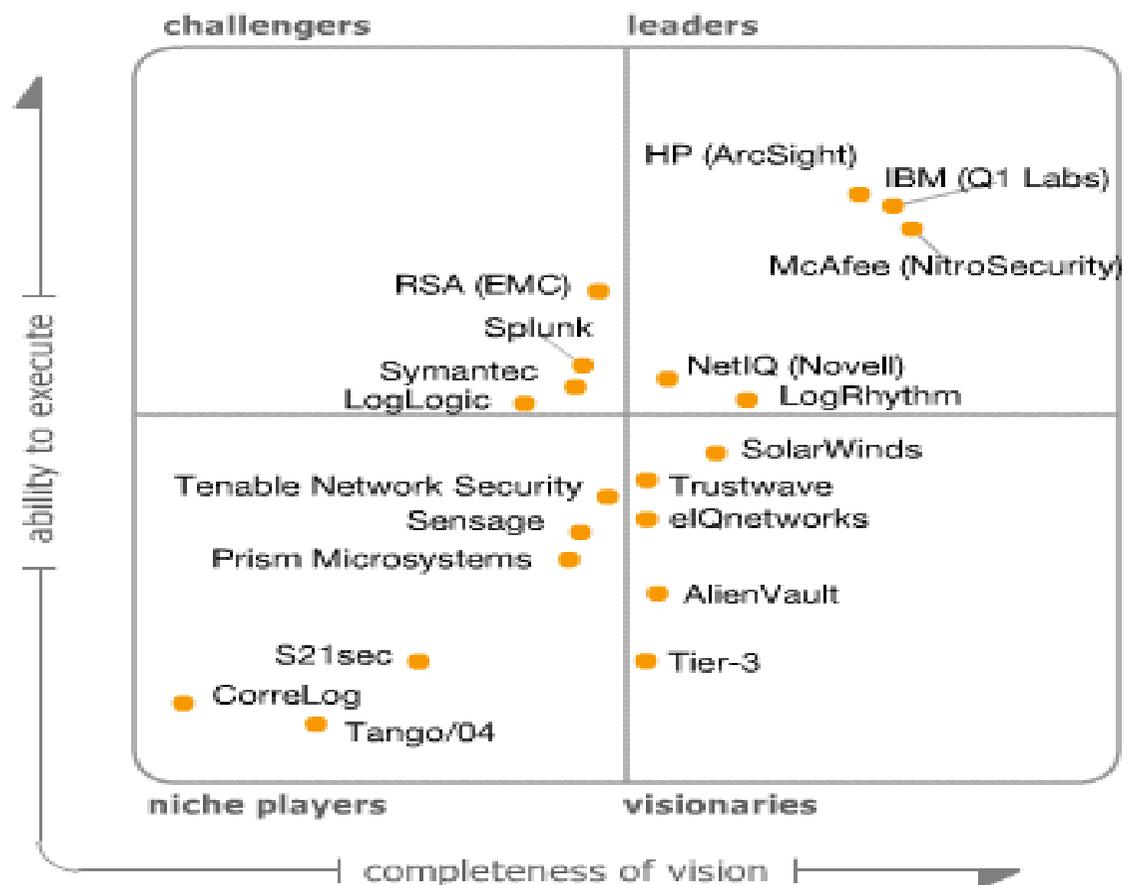


- Недостижимая масштабируемость

- 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

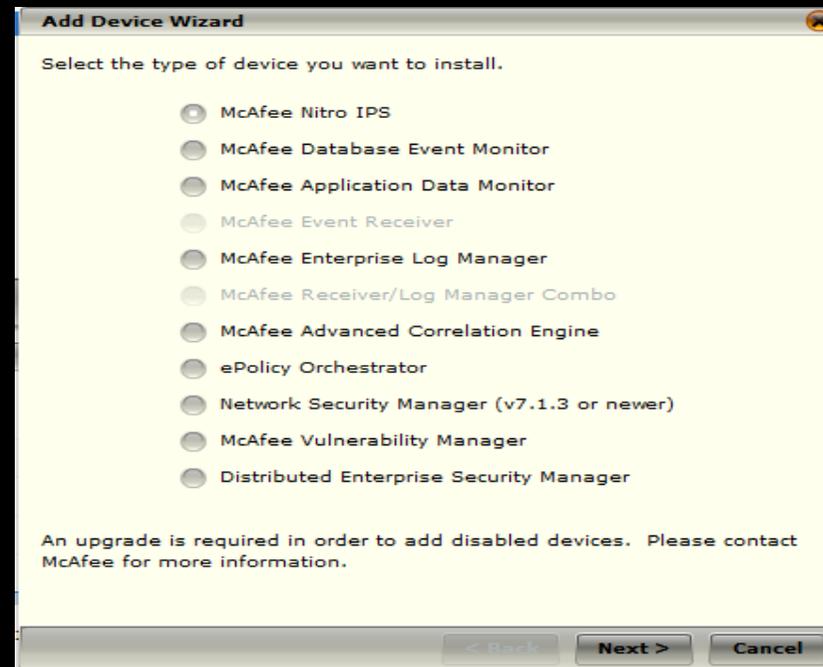
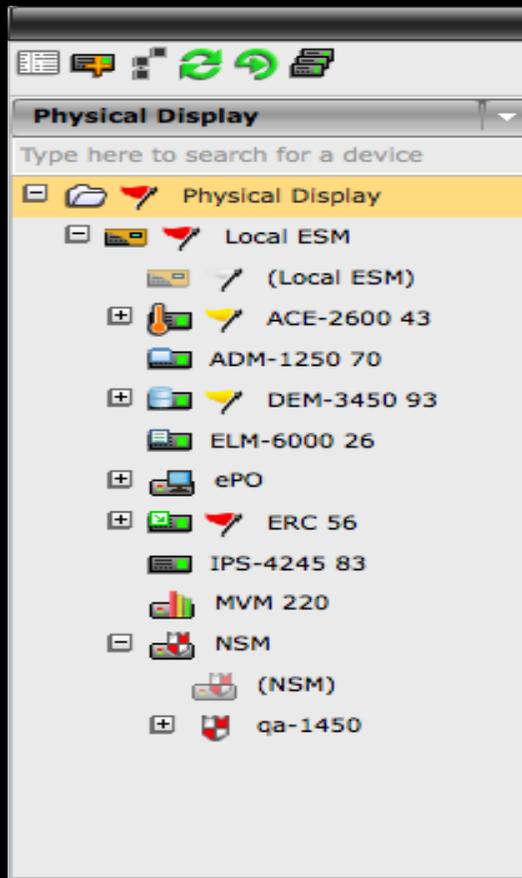


As of May 2012

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



The screenshot displays the ePO console interface, illustrating the execution of various tasks from a single console. The main window shows the 'Local ESM - epo' interface, which includes a 'Default Summary' section with a list of events and their counts, and an 'Event Distribution' section with a bar chart showing event counts over time (10/12, 11/12, 12/12).

Overlaid on the main window are two smaller windows, both titled 'Select tags and enter an IP address to apply the tags to that endpoint.' The top window shows a table of existing tags:

Name	Notes
Server	Default tag for systems identified as a Server

The bottom window shows a table of new tags being added:

Name	Notes
Workstation	Default tag for systems identified as a Workstation
EE:ALDU	This will automatically be assigned to system where the users have had Local Dc
this is New Tag in epo	
Barney's Tag That Has A	

Below the table in the bottom window, there is an input field for the IP address, set to '172.16.2.15', and a 'Wake up client' checkbox. An 'Assign' button is visible at the bottom of the window.

Конфигурация NSM и черные списки IPS



NSM Properties

Sensor: **qs-1450**

Include Global Blacklist

IP Address	Duration	Description
10.75.80.31	Permanent	
10.75.80.191	Permanent	
2.2.2.2	Permanent	
10.75.80.61	Permanent	
1.1.1.1	Permanent	

Add NSM Blacklist Entry

IP Address:

Duration:

Description:

Buttons: Add, Edit, Delete, OK, Cancel

Интеграция с MVM



MVM Properties

Name and Description: View the progress of scans that have or are currently running for any engine. Click the New Scan button to execute a new Quick Scan for a specified engine.

Connection

Device Log

Device Management

Name	Start	Duration	Status	View
------	-------	----------	--------	------

Scans

Local ESM - epo

Default Summary

Event Summary 581,417 (100%)

- File Solidified: 291,263
- File Unsolidified: 250,399
- Update successful: 10,624
- File Renamed: 8,162
- Registry Key Write Denied: 6,153
- File Modified Update: 4,164
- File Deleted Update: 4,152
- File Created Update: 4,121

Source IPs 31,114 (5.35%)

- Event Drilldown
- Flov Drilldown
- Asset Drilldown
- Summarize
- Actions
 - Create new watchlist
 - Append to watchlist
 - Create new alarm
 - View in ePO
 - ePO Tagging
 - Perform MVM Scan
- WHOIS Lookup
- Search ELM

Source Ports Bound to: Event Distrib... 581,417 (100%)

Event Distribution Bound to: Event Summary 581,417 (100%)

240,000
200,000
160,000
120,000
80,000
40,000
0

10/12 11/12 12/12 1/13

10/01/2012 00:00:00 01/01/2013 00:00:00

Interval: 1 Auto

Destination IPs Bound to: Event Distrib...

Destination Ports

New Scan

Enter the necessary criteria for a new scan. Defaults will be used for the Scan Name, Template, and Engine if they are left blank.

IP Address/Range:

Scan Name:

Template: (Default)

Engine: nitrosecel

Cancel

Кабинет администратора ИТ/Безопасности



