
McAfee
An Intel Company
Централизованное управление событиями ИБ и организация контрмер
SAFE NEVER SLEEPS.

О компании

- 150 миллионов пользователей McAfee
- 250+ миллионов мобильных устройств с McAfee
- 6 миллионов ПК самое большое внедрение
- 9 Gartner Magic Quadrants в которых есть McAfee
- 480 McAfee зарегистрированных патентов
- 110+ Партнёров McAfee Security Innovation Alliance
- 6,267 работников McAfee
- 120 стран

О компании


Безопасность
+
intel
vPro
Active Management Technology
Advanced Encryption Standard
Virtualization
One Time Password
Secure BIOS
McAfee
Network Security
Cloud Security
Security Management
Endpoint Security
Technology Ecosystem

Эволюция угроз

Прошлое

- Любители
- Самолюбование
- Драйвер - любопытство
- Хаотичность

Настоящее

- Профессионалы
- Скрытность
- Нажива\причинение вреда
- Нацеленные атаки

Эволюция защиты

Эволюция мысли

Шойгу: угроза кибербезопасности сравнима с оружием массового поражения

aif.ru ВЧЕРА, 16:01

Сергей Шойгу.

Фото: РИА Новости

Общество

5 6 7

McAfee Security Connected

McAfee
An Intel Company

БЕЗОПАСНОСТЬ СЕТИ

- High Assurance Firewall
- Network Intrusion Prevention
- Network Access Control
- Network Behavior Analysis

БЕЗОПАСНОСТЬ ДАННЫХ

- Email Security
- Web Security
- Data Loss Prevention
- Encryption
- Identity & Access Mgmt
- API and Web Services Security

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ

- Security Operations Mgmt
- Policy Auditing & Mgmt
- Vulnerability Management
- Risk Management
- Compliance Management

БЕЗОПАСНОСТЬ СТАНЦИЙ

- Malware Protection
- Device Encryption
- Application Whitelisting
- Desktop Firewall
- Device Control
- Email Protection
- Network Access Control
- Endpoint Web Protection
- Host Intrusion Protection
- Mobile Device Management

- Server & Database Protection
- Hardware Assisted Security
- Smartphone and Tablet
- Virtual Machine and VDI
- Embedded Device Protection

СООБЩЕСТВО

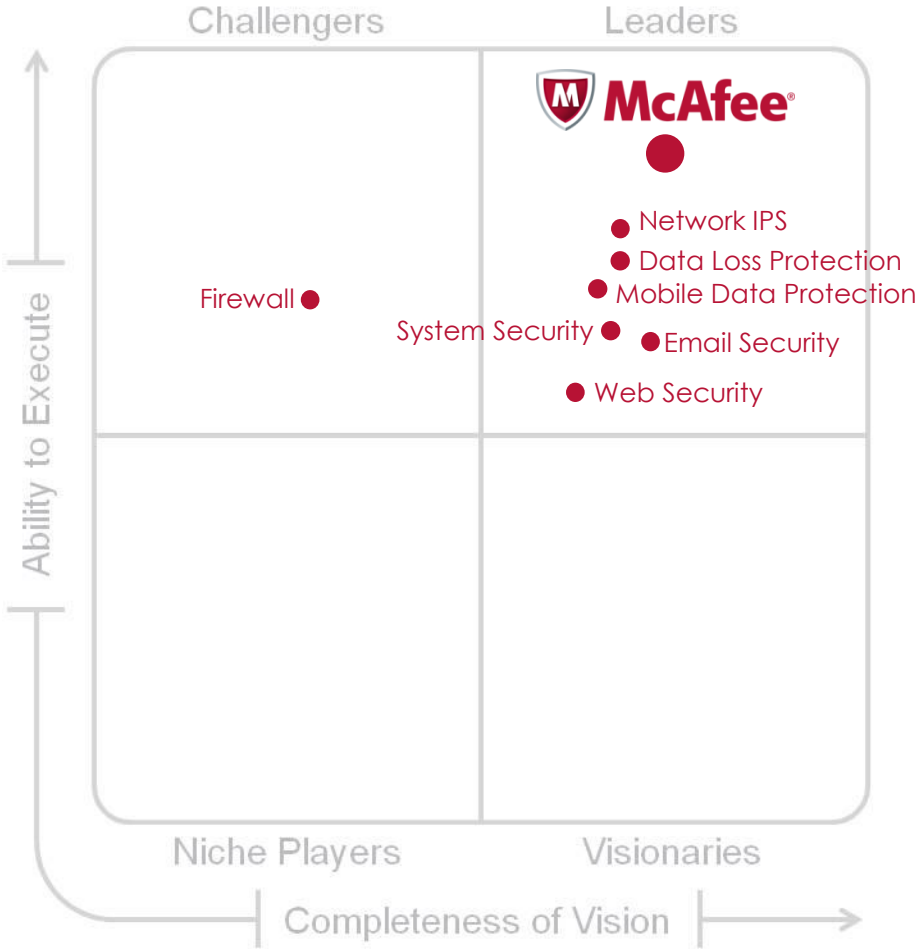
- Security Innovation Alliance
- McAfee Connected
- Global Strategic Alliance

Сертификация

Широкий спектр – лидерство везде

- System Security
- Network IPS
- Email Security
- Web Security
- Data Loss Protection
- Firewall
- Mobile Data Protection
- Network Access Control

Integrated

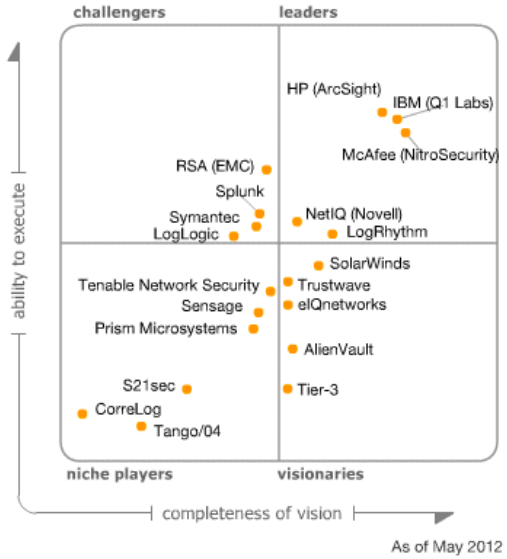


Source: Gartner

Выпуск решения SIEM в конце 2011

- Конец 2011 года – покупка компании Nitro
- Успешная интеграция в экосистему решений McAfee
  - IPS
  - Vulnerability Management
  - Endpoint Protection
  - Database Security
- Результат (середина 2012):
  - Лидерство в Gartner Magic Quadrant
  - №1 по отчету Pike Research “Smart Grid Security” для защиты SCADA

Figure 1. Magic Quadrant for Security Information and Event Management

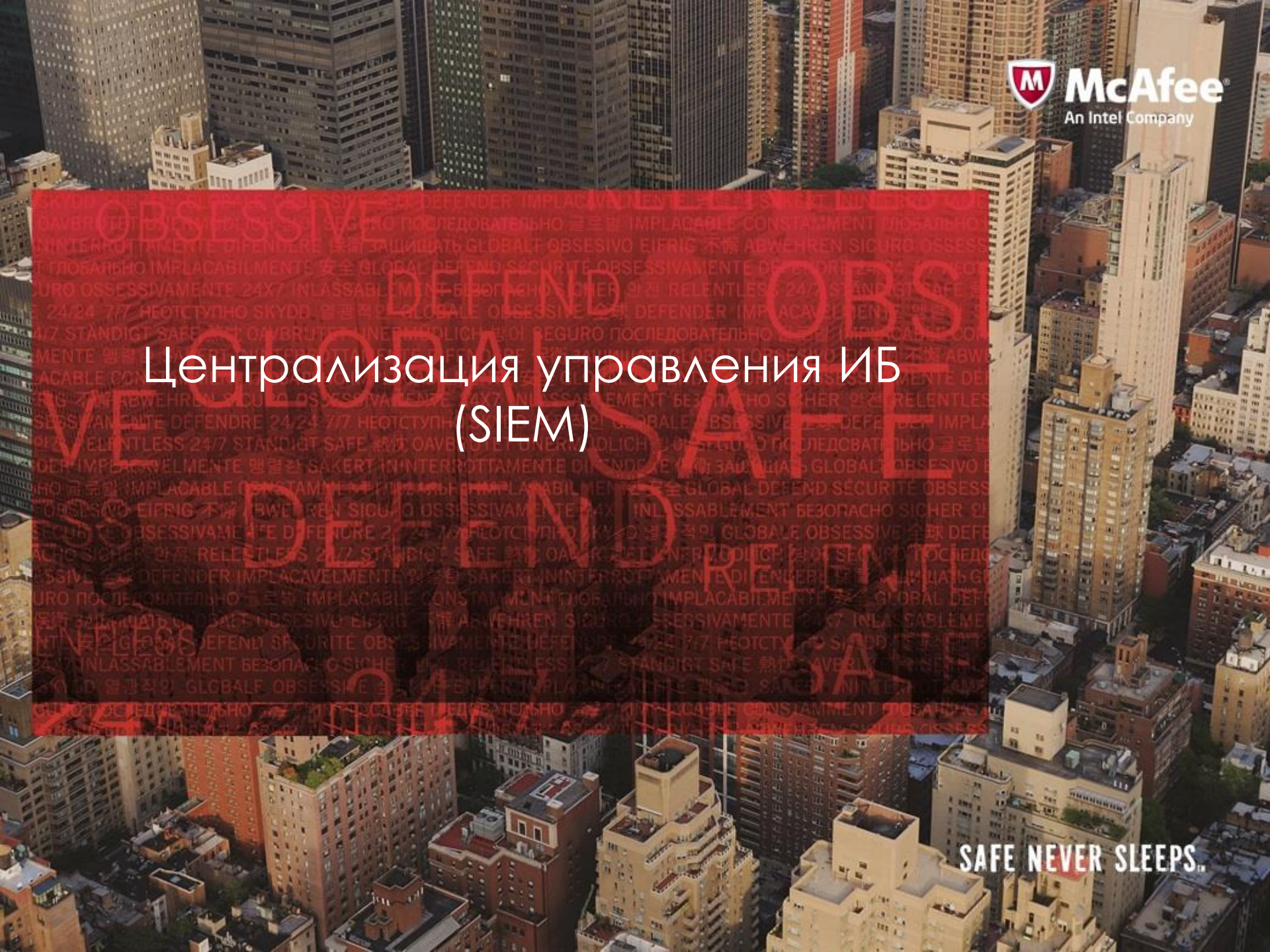


Source: Gartner (May 2012)

Vendor Overall Scores

Rank	Vendor	Total Score
1	McAfee/NitroSecurity	73.7
2	Industrial Defender	71.4
3	RSA	66.9
4	BWise	65.5
5	IBM	64.8
6	Agiliance	61.1
7	Wurldtech	60.7
8	Cisco	60.3
9	Oracle	60.1
10	SUBNET Solutions	56.9
11	SAP	56.4
12	AlienVault	54.6
13	Symantec	51.4
14	AlertEnterprise	50.8

(Source: Pike Research)


McAfee
An Intel Company
Централизация управления ИБ (SIEM)
SAFE NEVER SLEEPS.

Текущее состояние SIEM

McAfee
An Intel Company

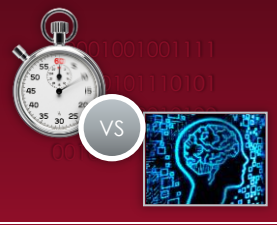
Обещания:

Поддержка данных по безопасности

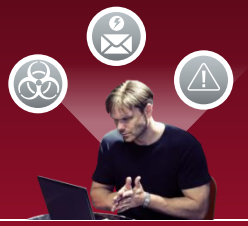
Платформа для глубокого исследования

Управление поддержкой и соответствием

Реальность:



Устаревшая архитектура
Вынужденный выбор между скоростью и информативностью



События сами по себе не помогут справится с современными угрозами

Сложные управление и установка приводят к увеличению расходов

Современные требования

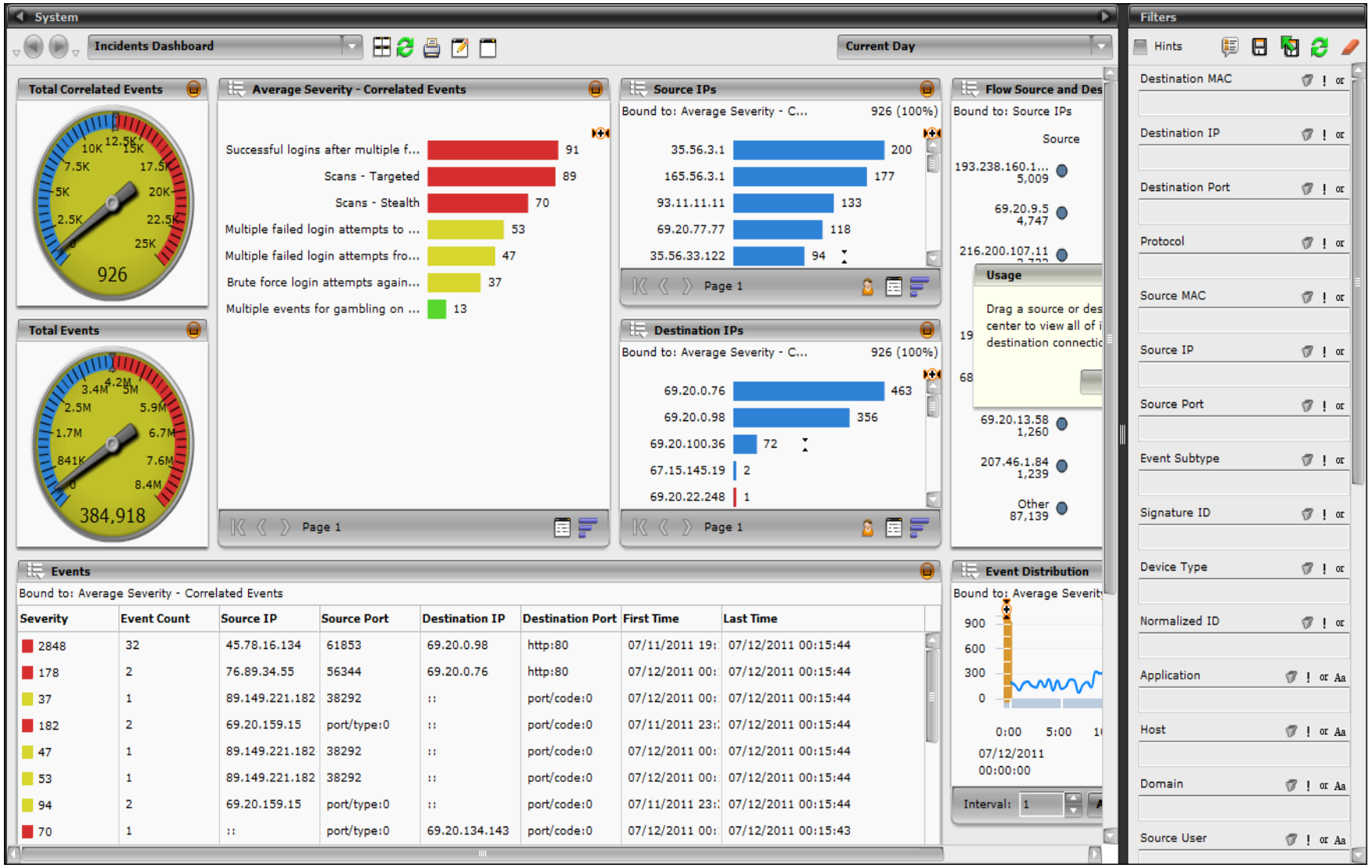
- Наблюдение за частотой записей
- Поиск логов
- Корреляция событий
- Какие данные?
- Кто это сделал?
- Опасные хосты?
- Каков риск системы?
- Каков риск пользователя?

Производительность и масштабируемость

- **Высокая 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)
- **Интеграция**
- **Масштабируемость**
  - Сбор всей релевантной информации
  - Анализ информации за месяцы и годы, включая высокоуровневую информацию о контенте и контексте
  - Работа с миллиардами записей в БД

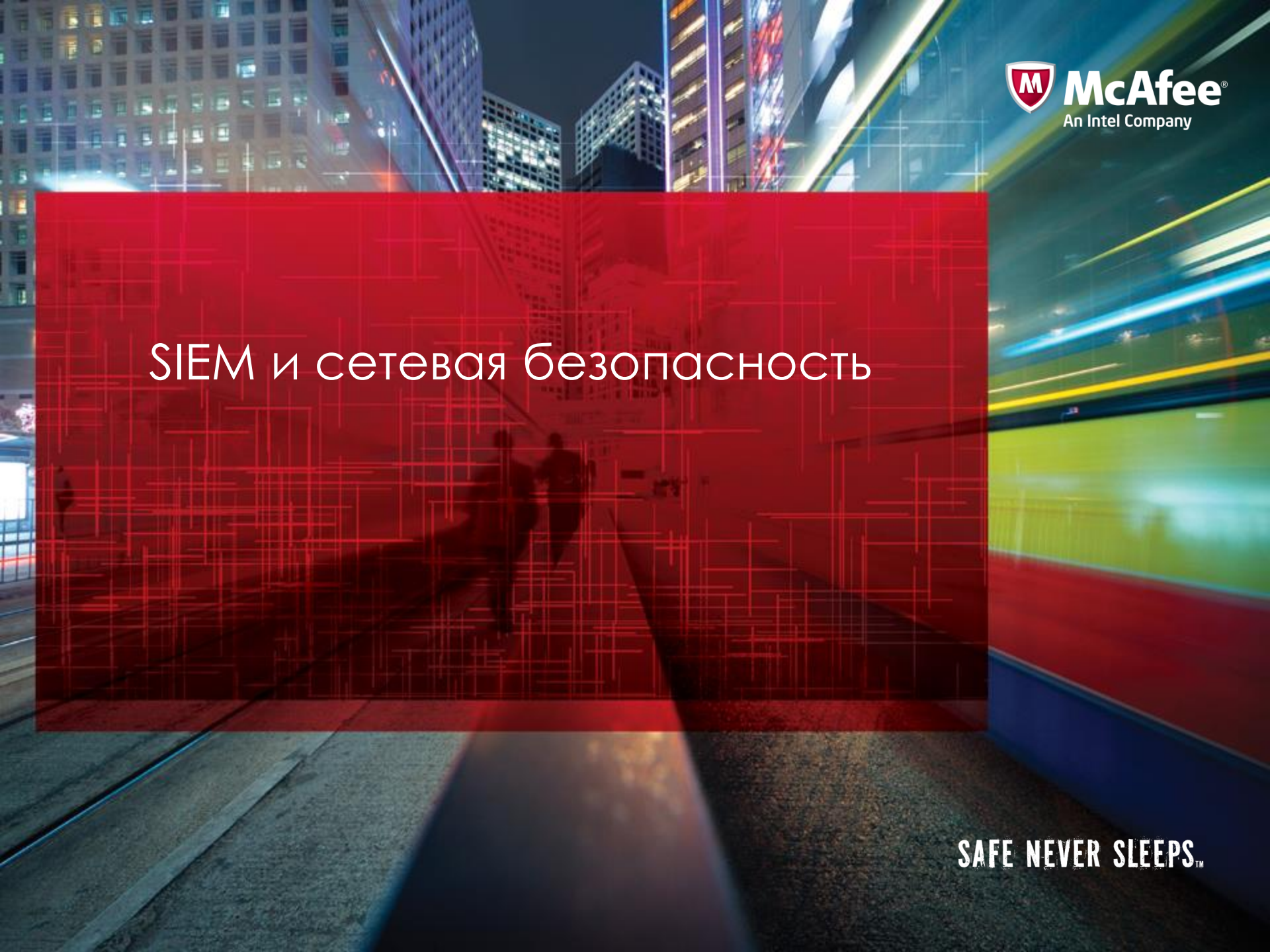
Удобное управление



Гибкая архитектура

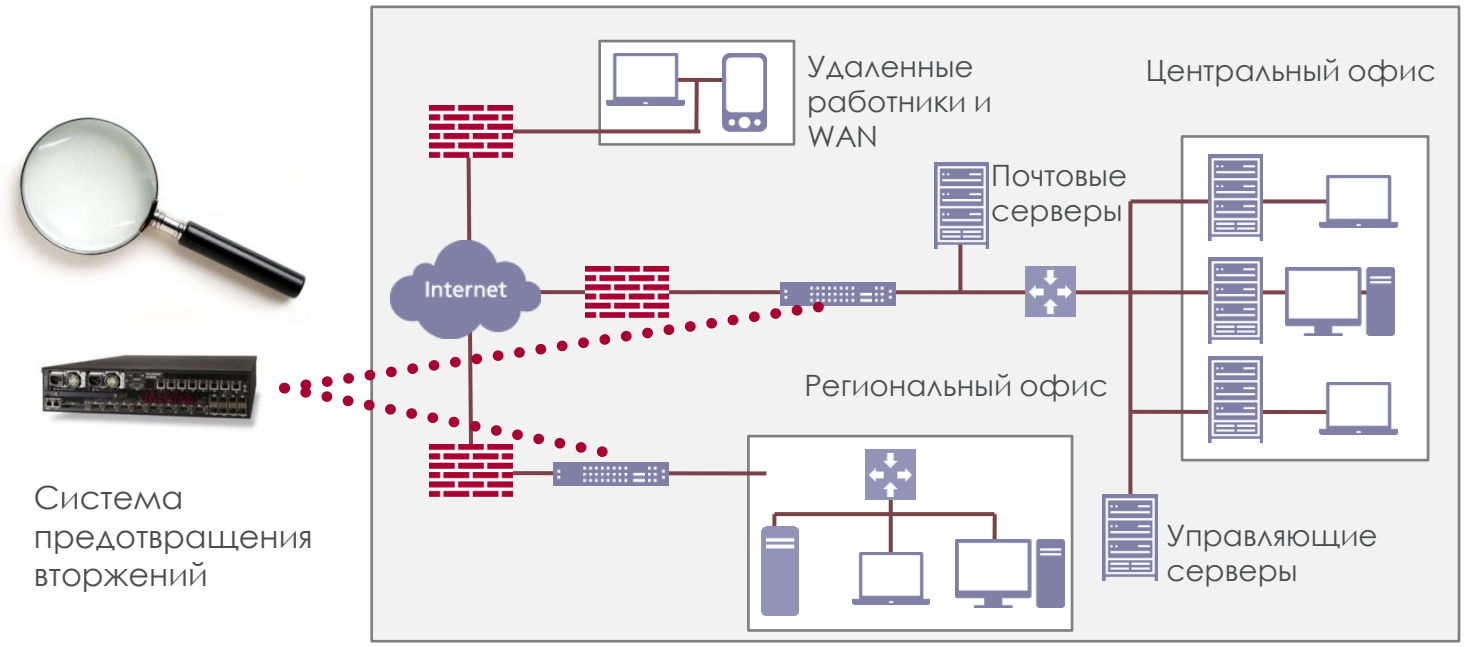
Разведка и операционная деятельность	GTI	ePO	MRA	SIA
Анализ рисков	McAfee Advanced Correlation Engine 			
SIEM и управление логами	McAfee Enterprise Security Manager McAfee Enterprise Log Manager 			
Анализ приложений	McAfee Application Data Monitor 	McAfee Database Event Monitor 		
Производительный коллектор	McAfee Receivers 			

Big Security Data DB


McAfee
An Intel Company
SIEM и сетевая безопасность
SAFE NEVER SLEEPS™

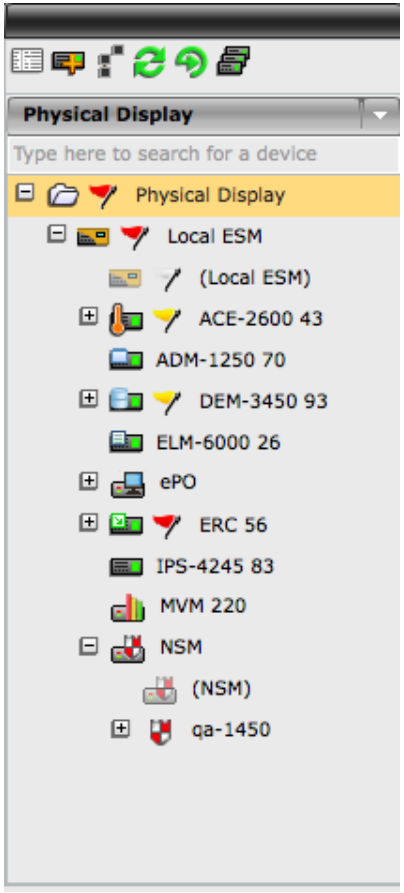
Защита сети на основе McAfee Network Security Platform

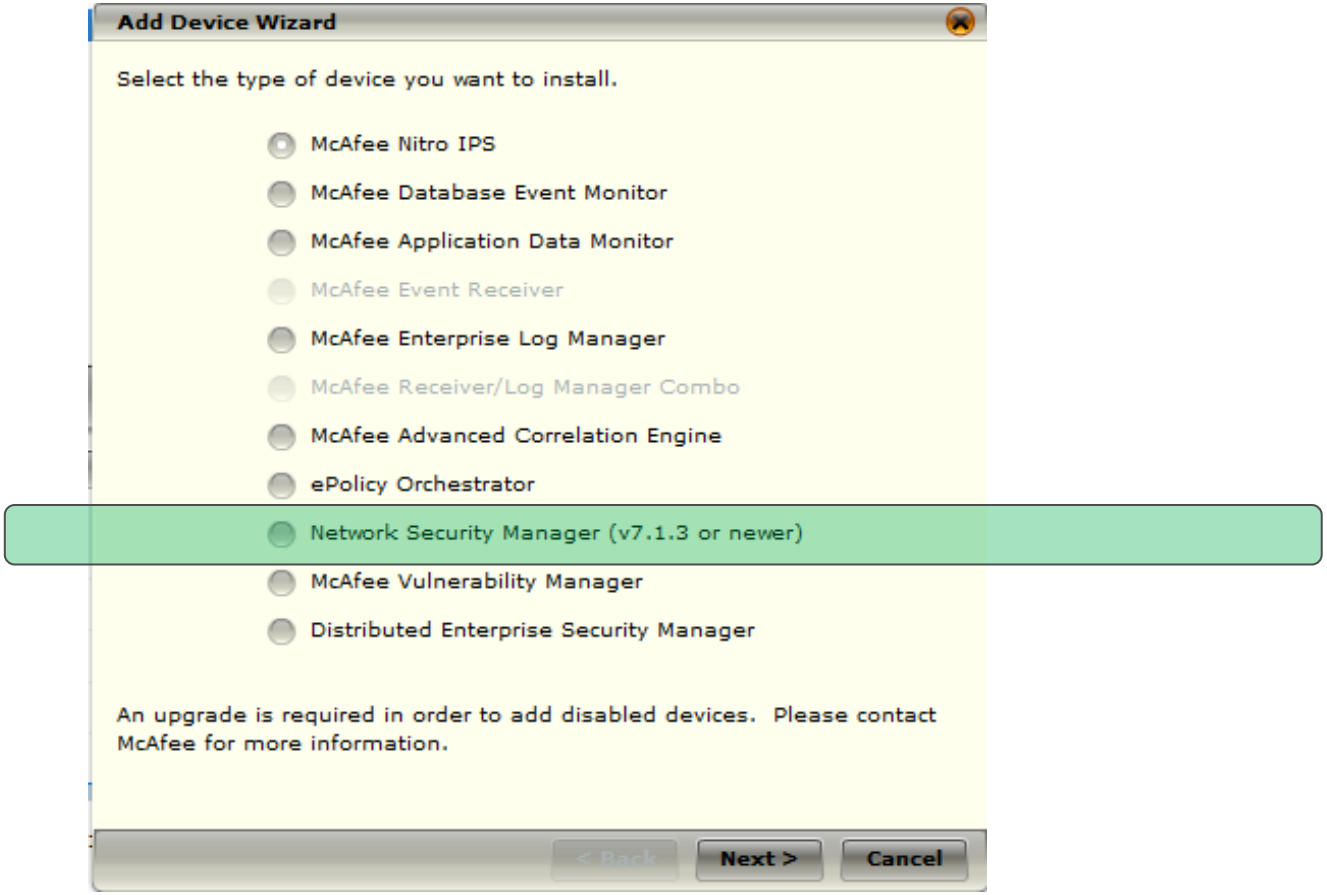
- **McAfee Network Security Platform (IPS):**
  - Инспектирует входящий и исходящий трафик в реальном времени
  - Останавливает вредоносный или нежелательный трафик
  - Категорирует все потенциальные угрозы и составляет отчеты
  - Анализ аномальной сетевой активности и идентификация бот-сетей, сетевых червей, троянов, нежелательного прикладного трафика и пр.



IPS – модуль платформы безопасности

IPS встраивается на уровне общего API в решение McAfee SIEM

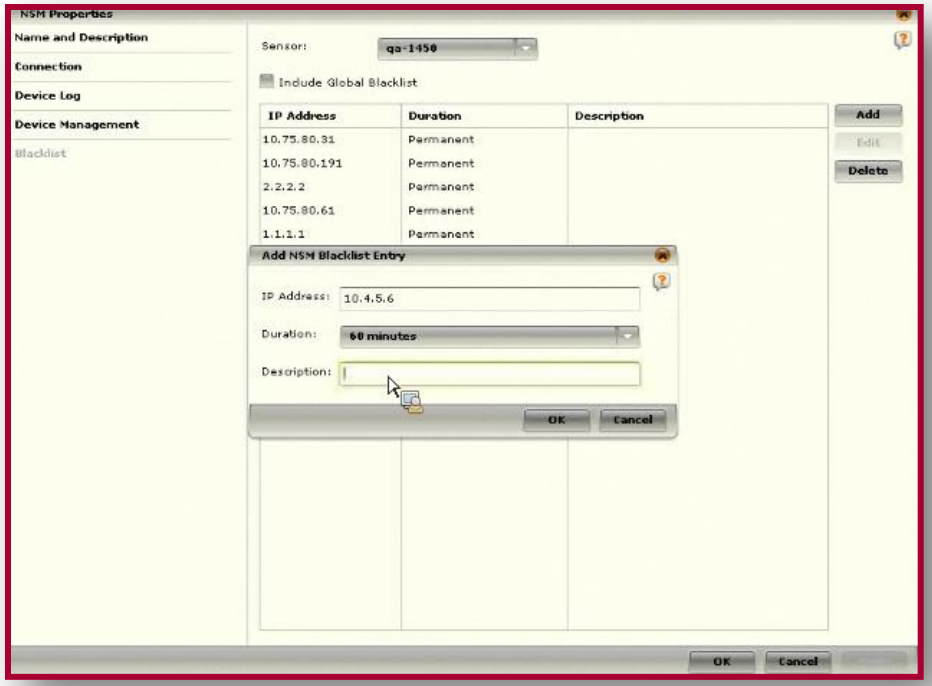




Использование McAfee IPS при обработке инцидента ИБ

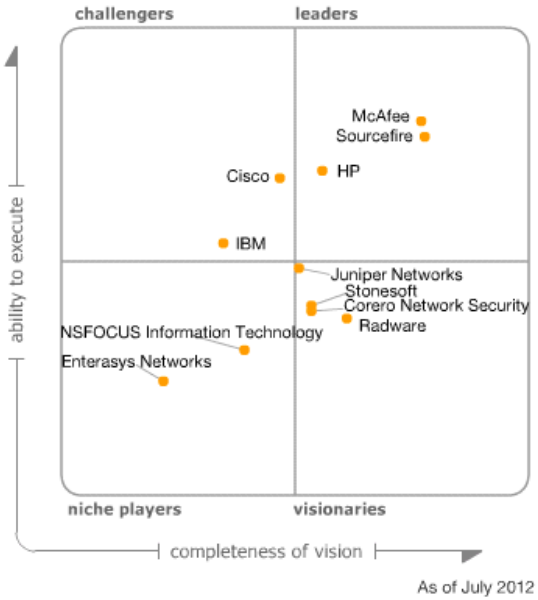
SIEM вызывает специализированные функции IPS в ответ на инциденты

Любой оператор SOC может запустить **ответное действие из SIEM** в ответ на появление в сети вредоносного узла (запуск эксплоитов, запуск вредоносов, аномальный трафик, плохая репутация в облаке GTI). Вредоносный узел перемещается в карантин либо в черный список напрямую из SIEM



Почему именно McAfee IPS?

Figure 1. Magic Quadrant for Intrusion Prevention Systems



Source: Gartner (July 2012)

Product	Overall Protection	Evasion	Throughput
McAfee Network Security Platform (NSP) M-8000 v6.1	95%	100%	12,300 Mbps
Stability & Reliability	Client Protection	Server Protection	
Excellent	99%	91%	

NSS Labs TESTED

AV-TEST

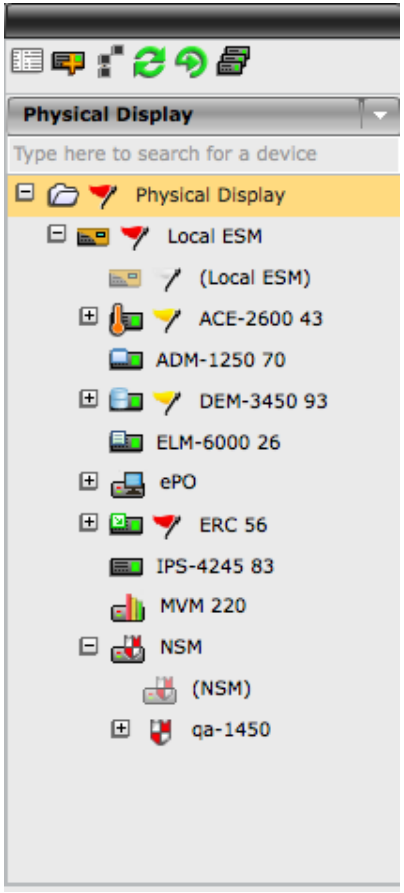
Type of Malware	Number of Samples	Detected Samples	%
Total	113,646	105,803	93.10%
Prevalent Malware	11,072	10,371	93.67%
Backdoors	7,932	7,827	98.68%
Bots	2,329	2,317	99.48%
Rogue Software	1,683	1,659	98.57%
Trojan Horses	81,265	75,655	93.10%
Viruses	4,013	3,485	86.84%
Worms	5,352	4,489	83.88%

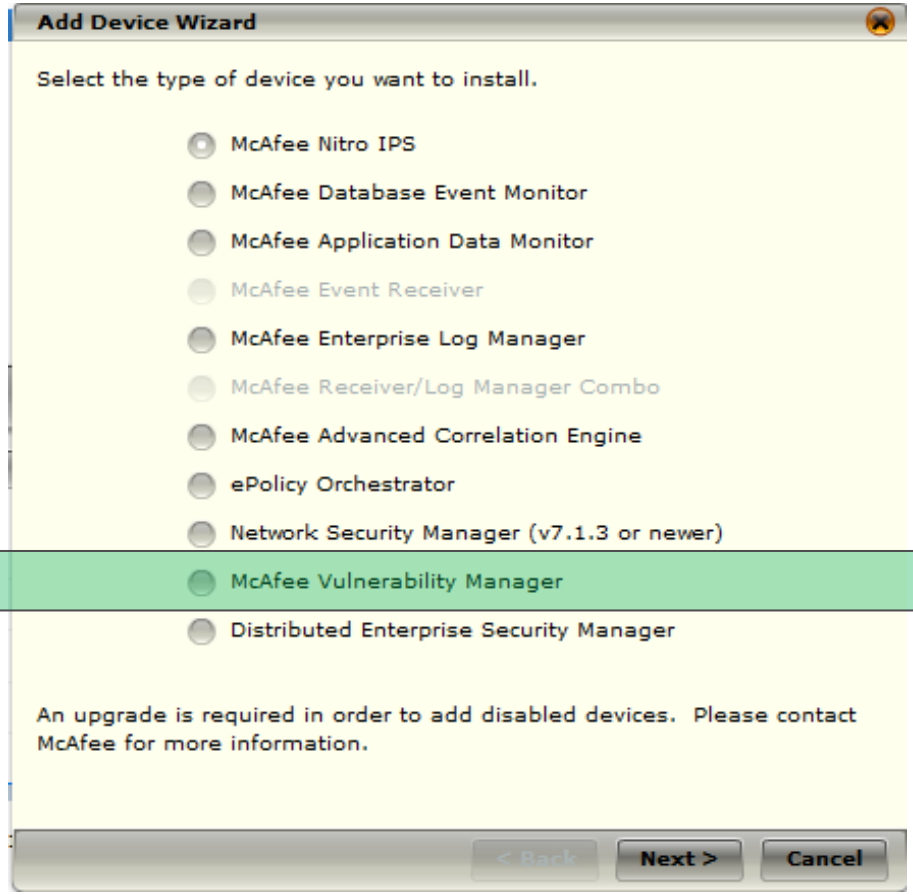
Figure 5: Zoo detection results


McAfee
An Intel Company
SIEM и оценка уязвимостей
SAFE NEVER SLEEPS™

Сканнер уязвимостей – часть платформы безопасности

McAfee Vulnerability Manager встраивается на уровне API в McAfee SIEM



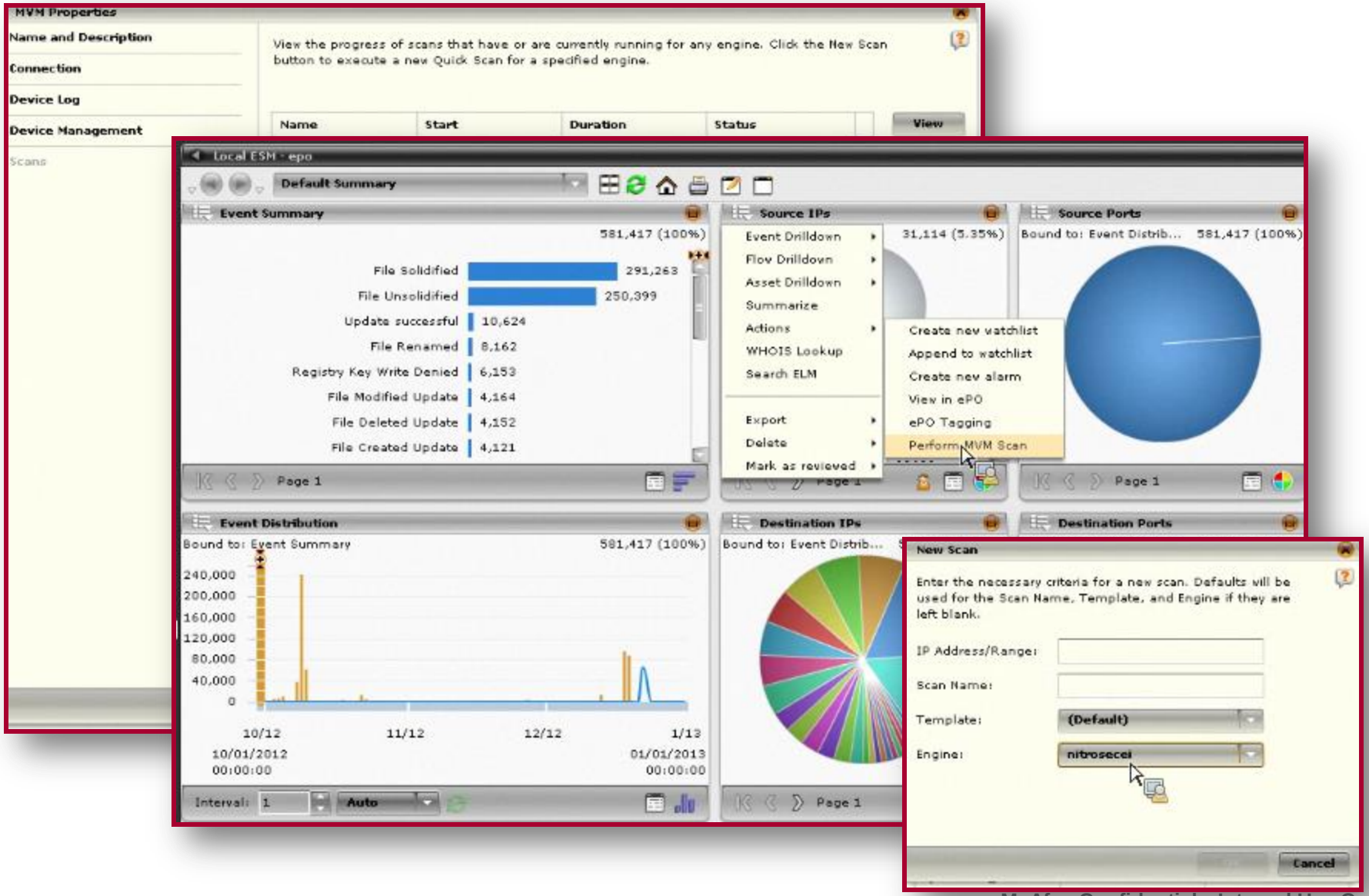


Глубокая интеграция с сканнером уязвимостей

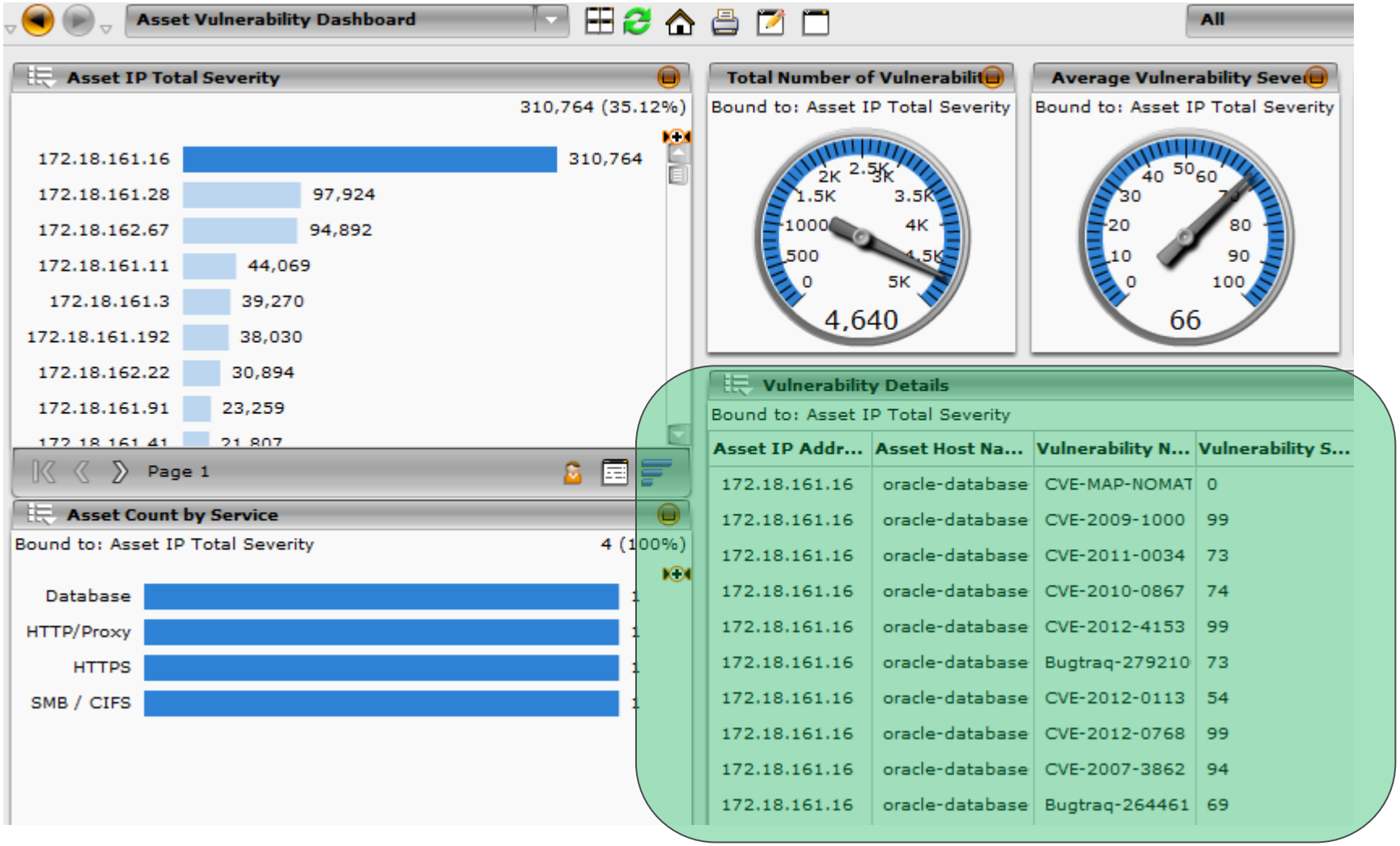
McAfee ESM может сканировать устройства в сети

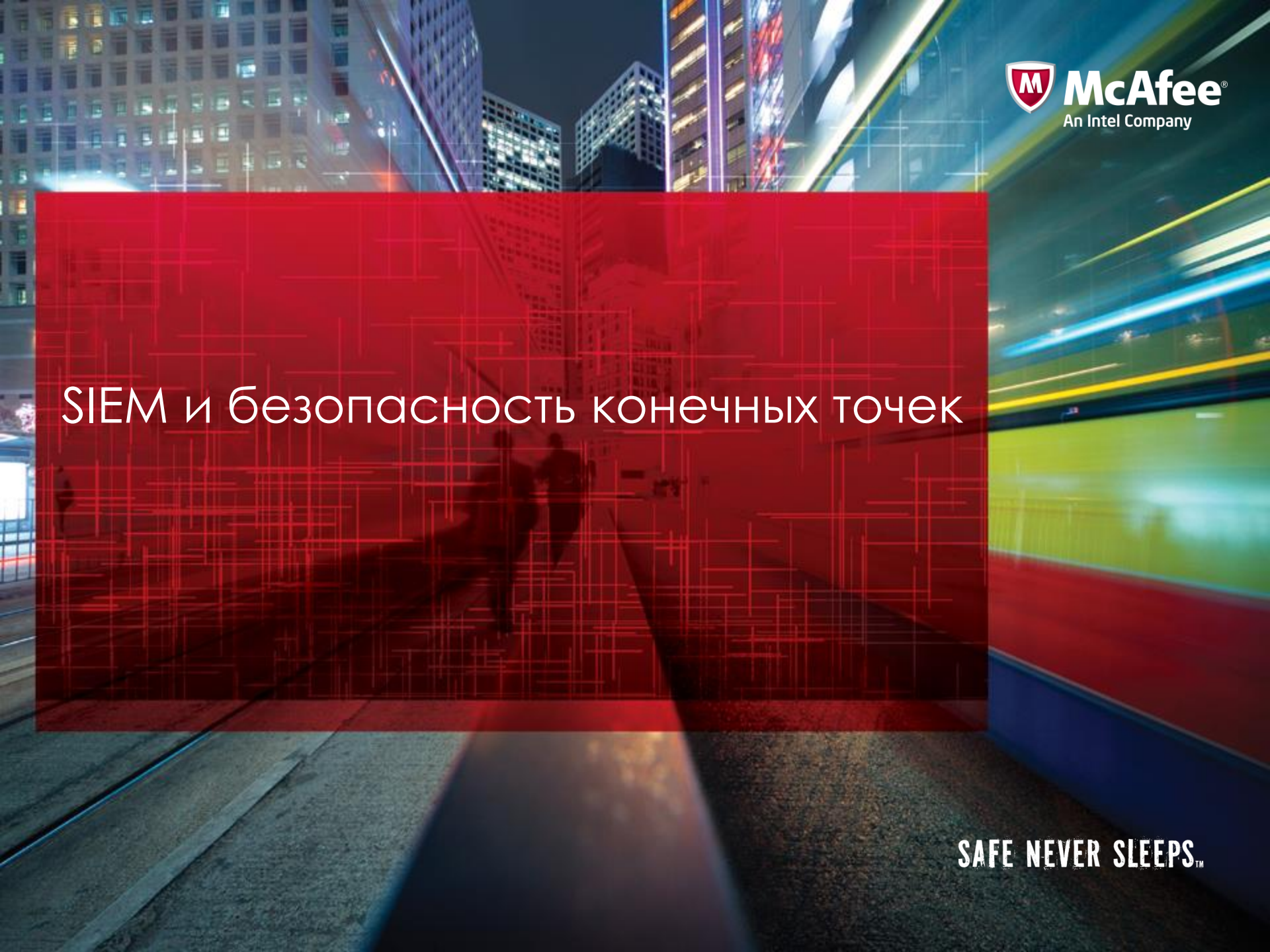
- Операторы SOC могут вызывать сканирование специфичных узлов не покидая консоли SIEM (например, для оценки попыток сетевых вторжений). Информация об активе и его уязвимостях **автоматически добавляется в SIEM.**

Как это работает?



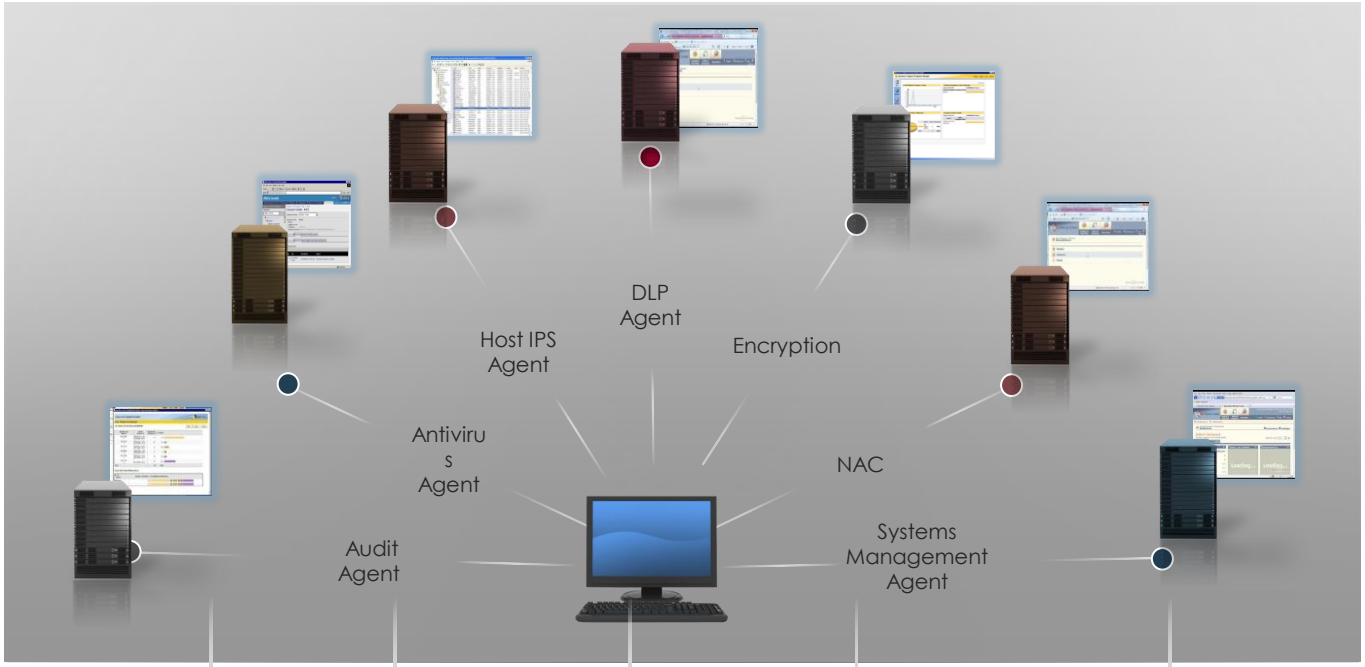
Информация об уязвимостях доступна в SIEM




McAfee
An Intel Company
SIEM и безопасность конечных точек
SAFE NEVER SLEEPS™

Архитектура безопасности

Насколько объединена ваша система безопасности?



КАЖДОЕ **РЕШЕНИЕ** ИМЕЕТ СВОЕГО АГЕНТА

КАЖДЫЙ **АГЕНТ** ИМЕЕТ СВОЮ КОНСОЛЬ

КАЖДАЯ **КОНСОЛЬ** ТРЕБУЕТ ОТДЕЛЬНОГО СЕРВЕРА

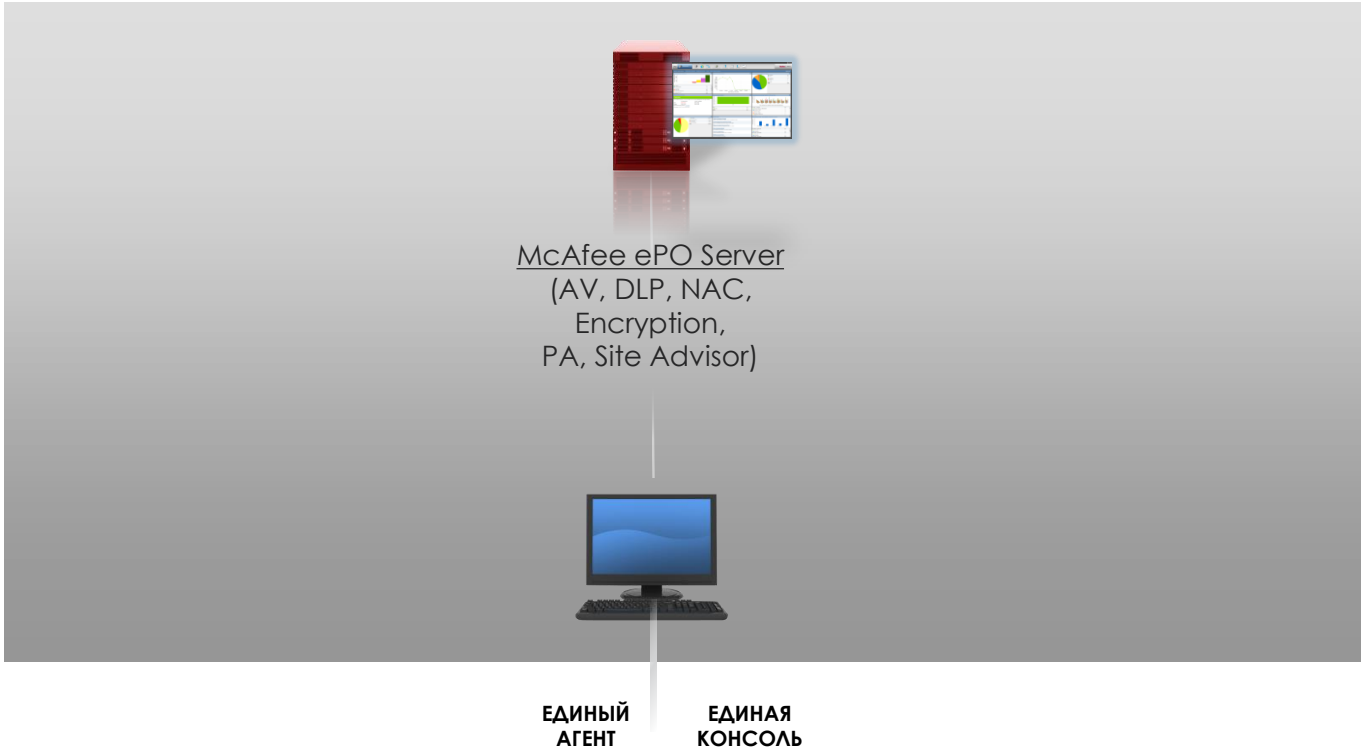
КАЖДЫЙ **СЕРВЕР** ТРЕБУЕТ ОС И БАЗУ ДАННЫХ

КАЖДАЯ **ОС И БАЗА** ДАННЫХ ТРЕБУЕТ ПОДДЕРЖКИ, ЛЮДЕЙ, ПАТЧЕЙ

ГДЕ ЖЕ **КОНЕЦ**?

Платформа McAfee

Насколько объединена ваша система безопасности?



ePolicy Orchestrator

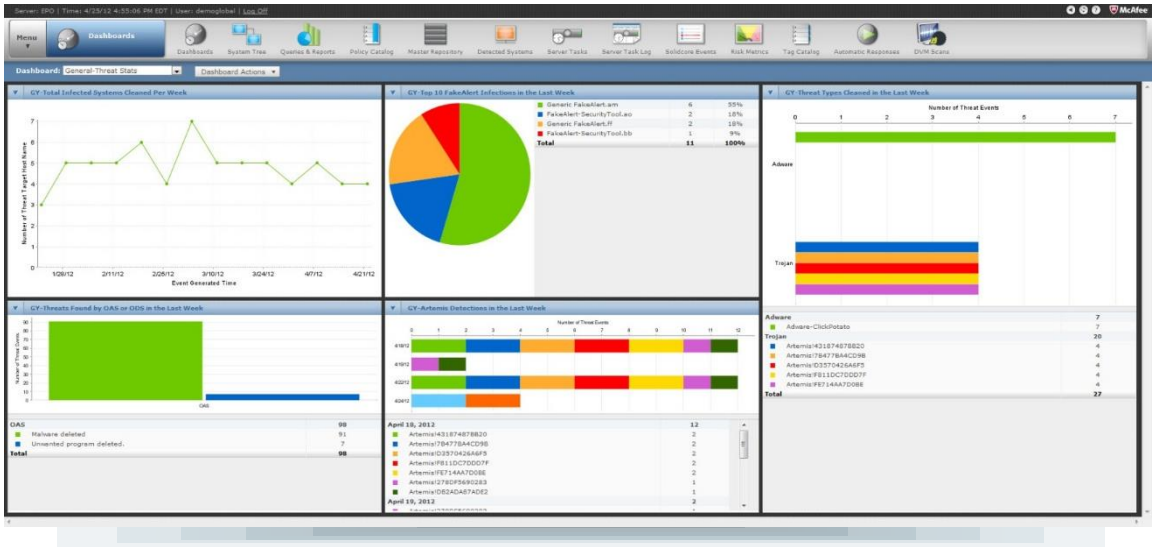
Complete Management

- Командный центр
- Отчеты и настраиваемые панели
- Ролевое управление
- Автоматизация рабочих процессов
- Управление миллионами конечных точек
- Расширения

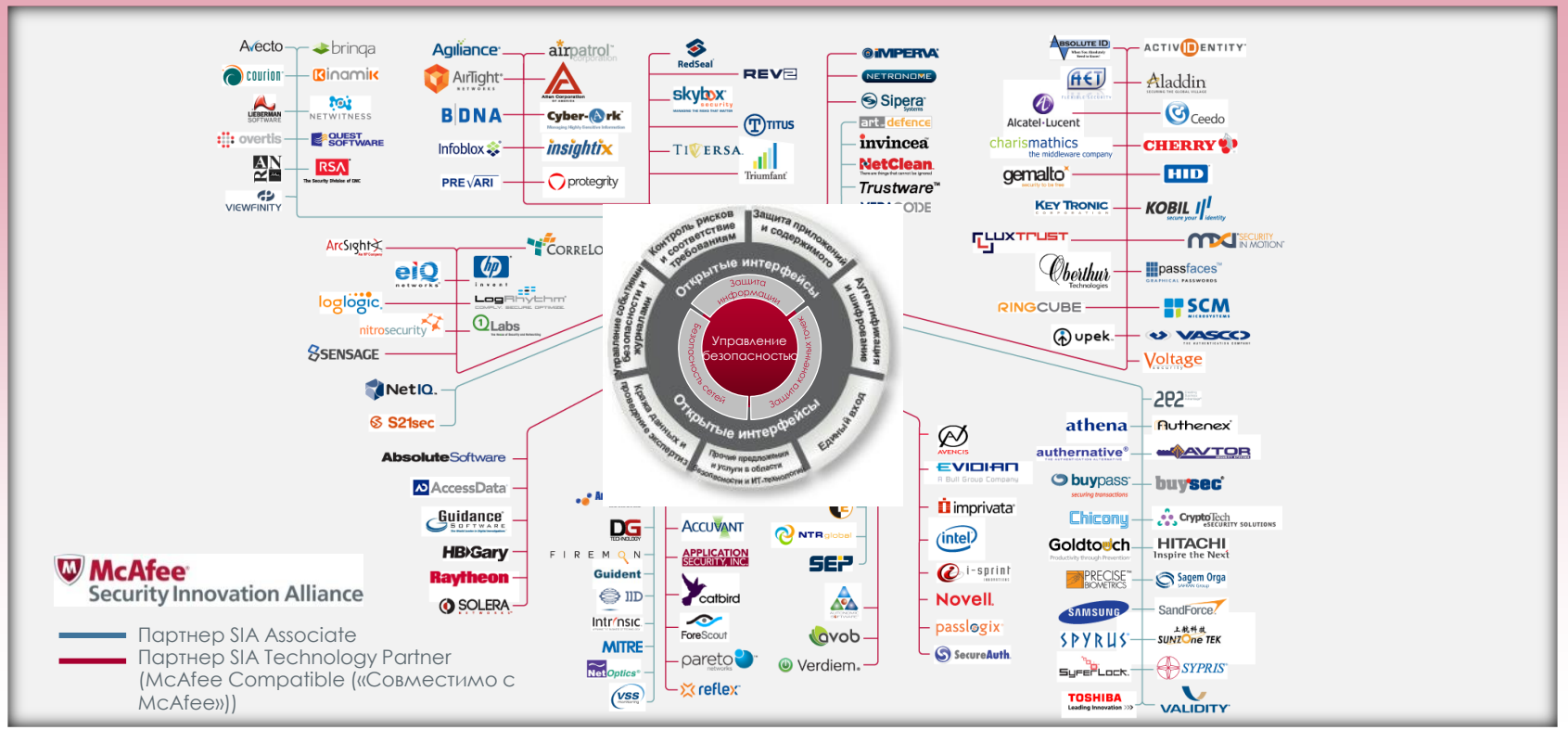
McAfee ePolicy Orchestrator (McAfee ePO)

Унифицированное управление политиками и событиями для защиты на уровне конечных точек, данных, сети

- Полная видимость
- Открытая, расширяемая архитектура
- Доказанная эффективность

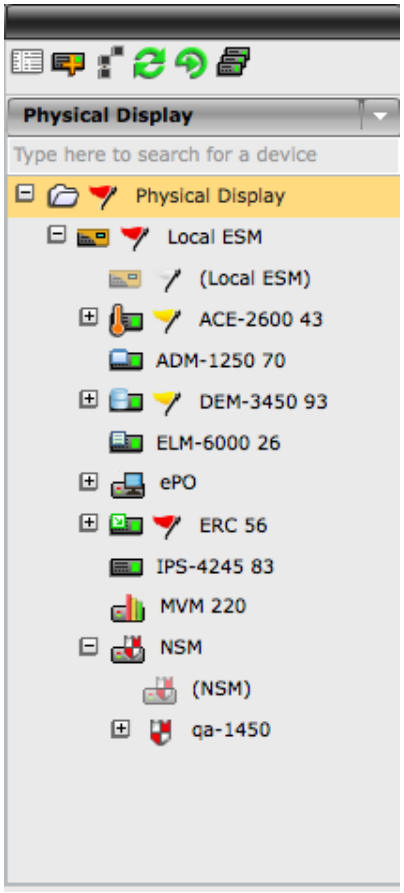


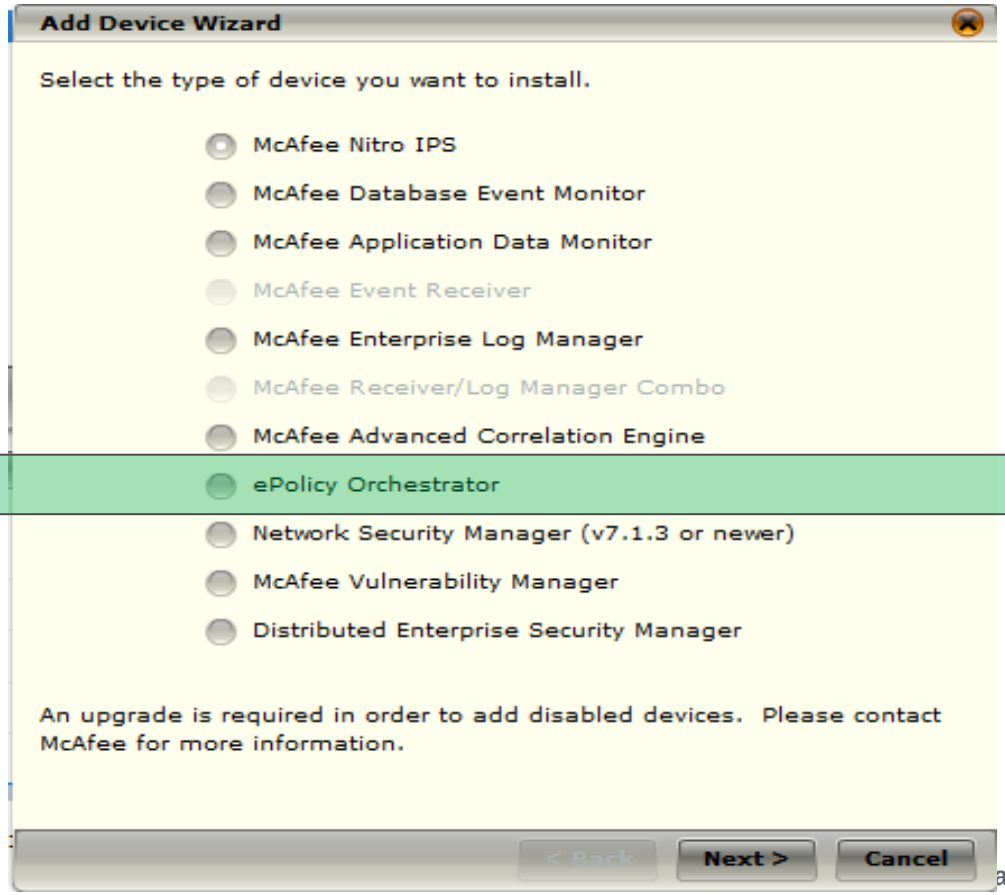
Security Connected: Интеграция сторонних продуктов



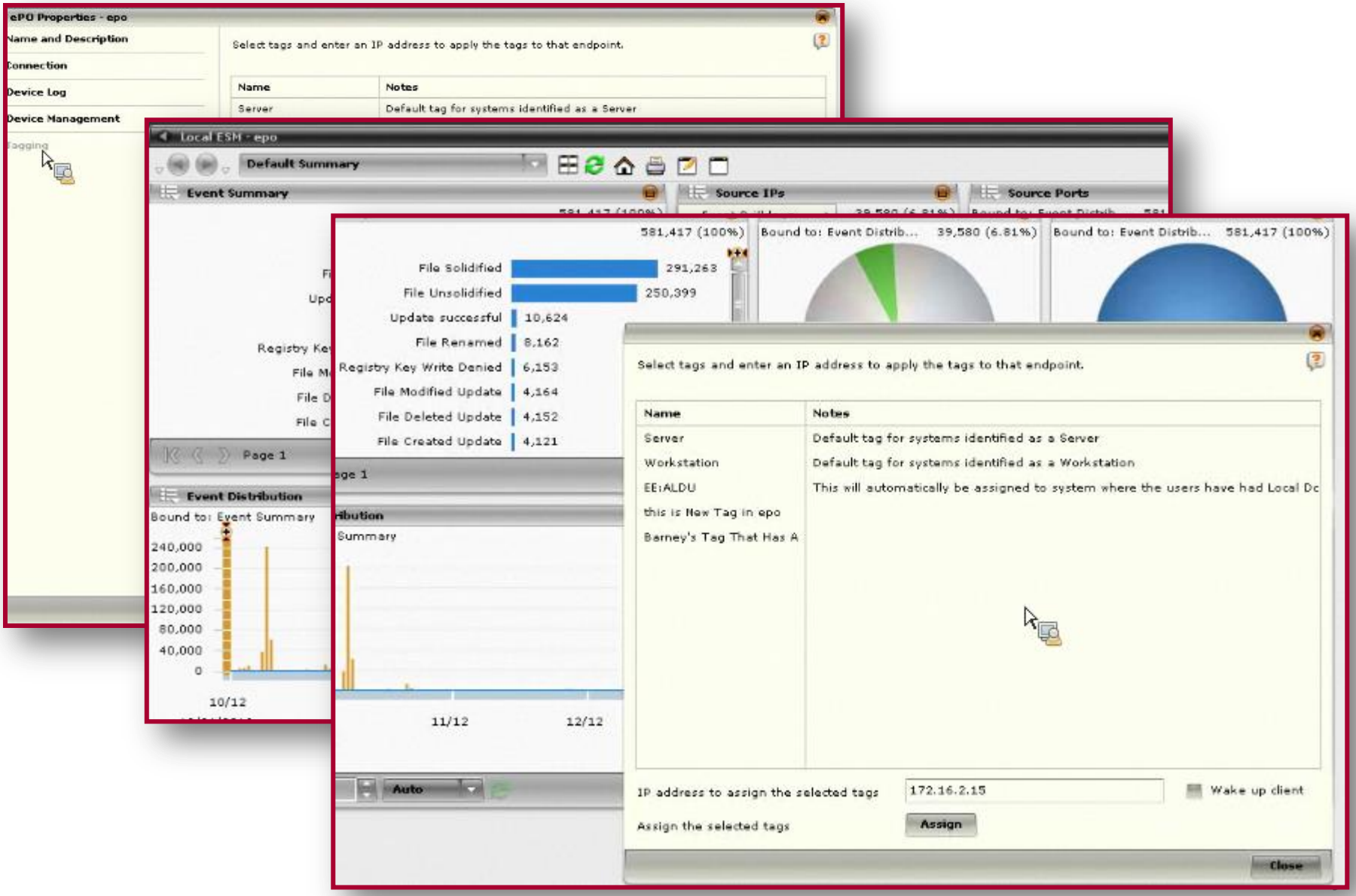
Управление безопасностью APM – часть платформы ИБ

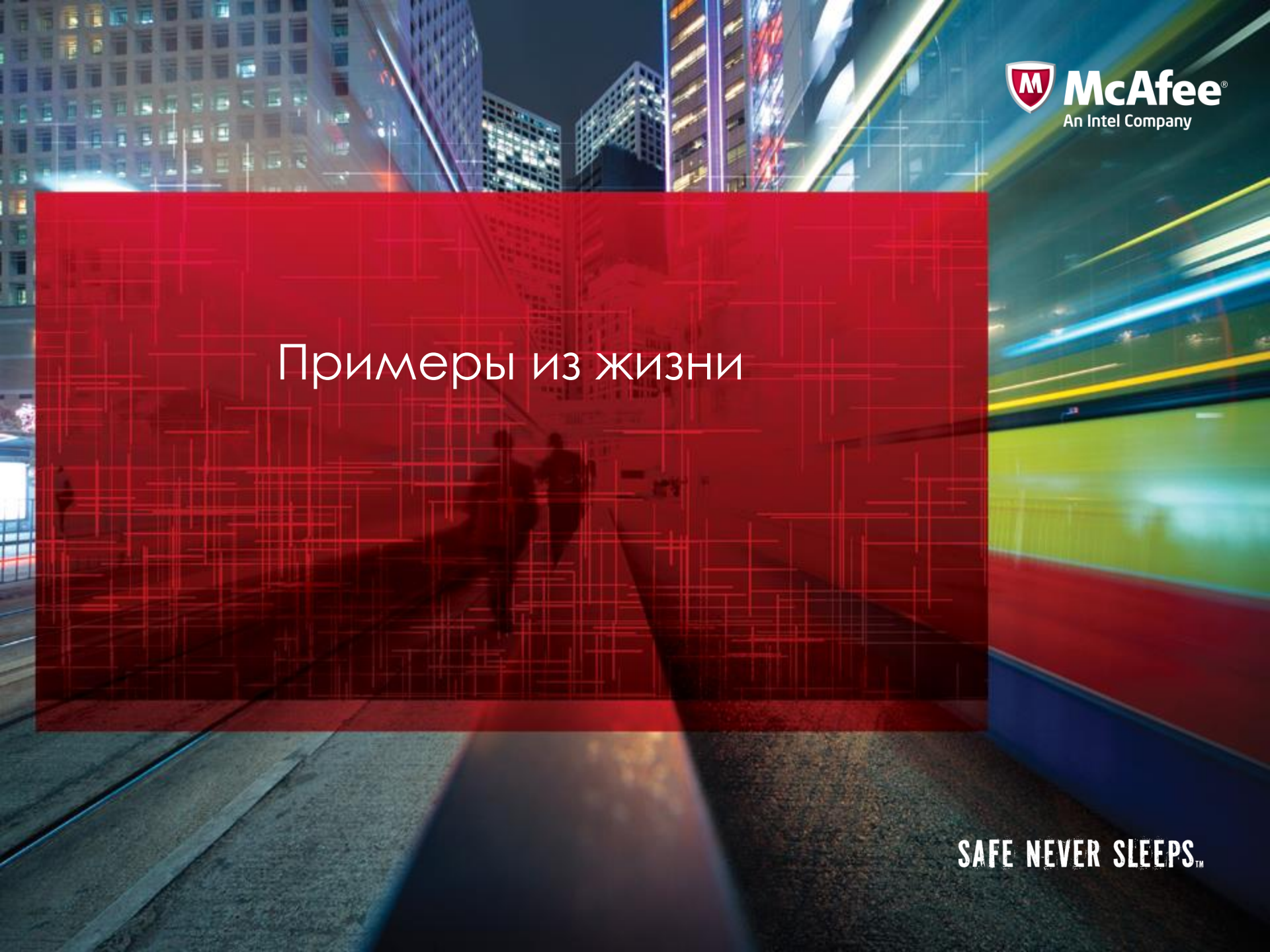
McAfee ePolicy Orchestrator встраивается на уровне API в McAfee SIEM



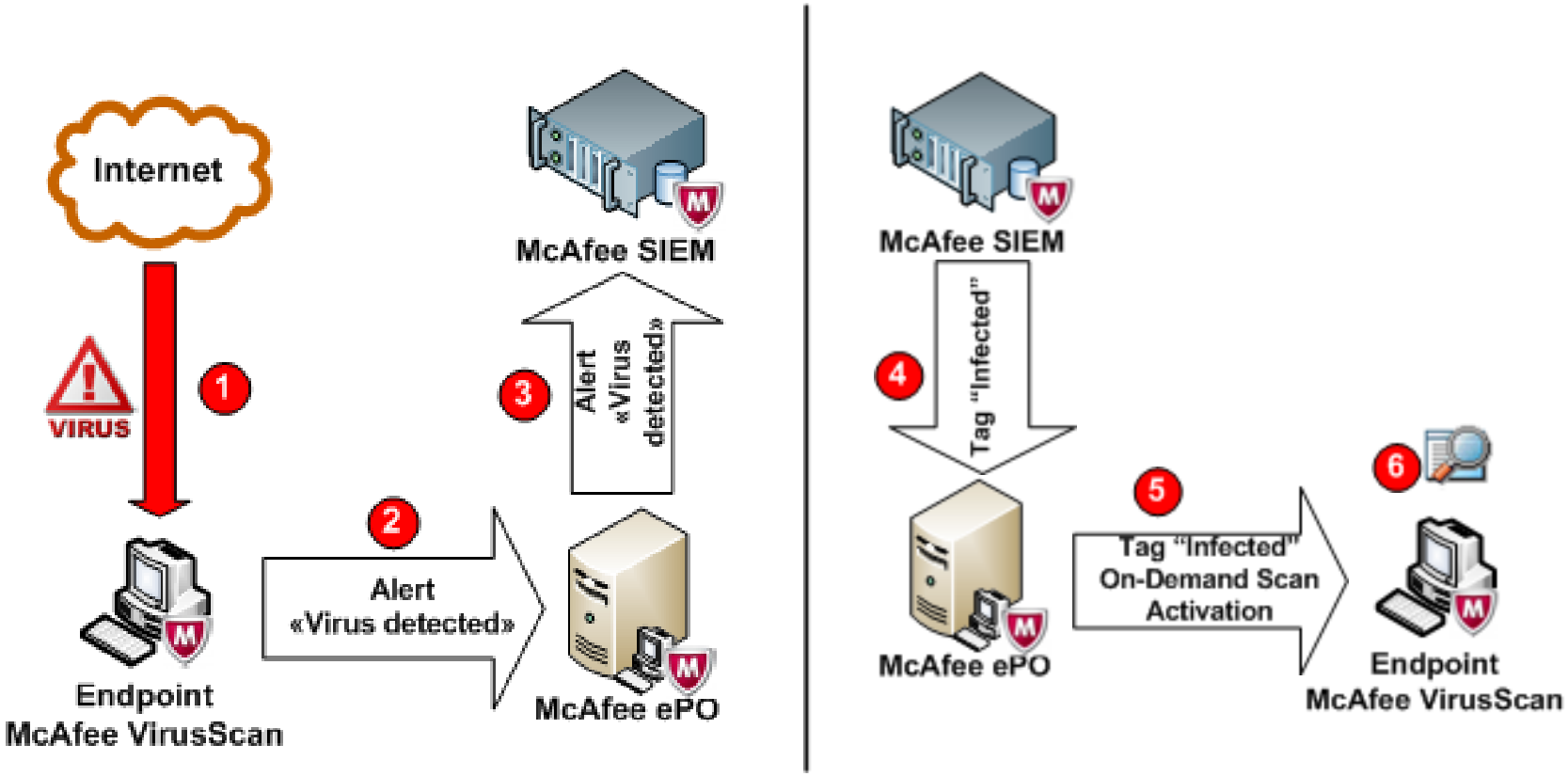


Установка меток ePo в ответ на инцидент

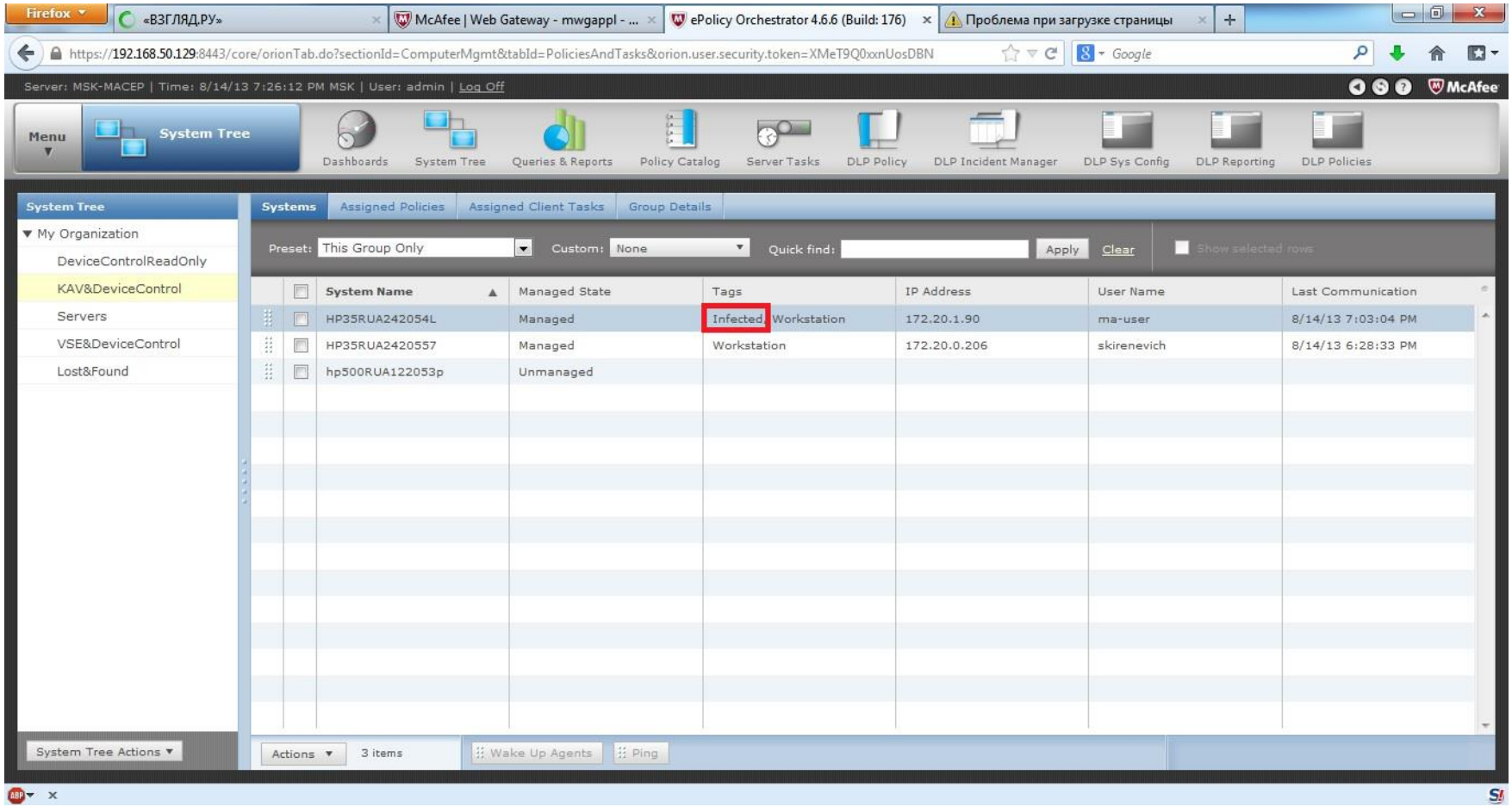



McAfee
An Intel Company
Примеры из жизни
SAFE NEVER SLEEPS™

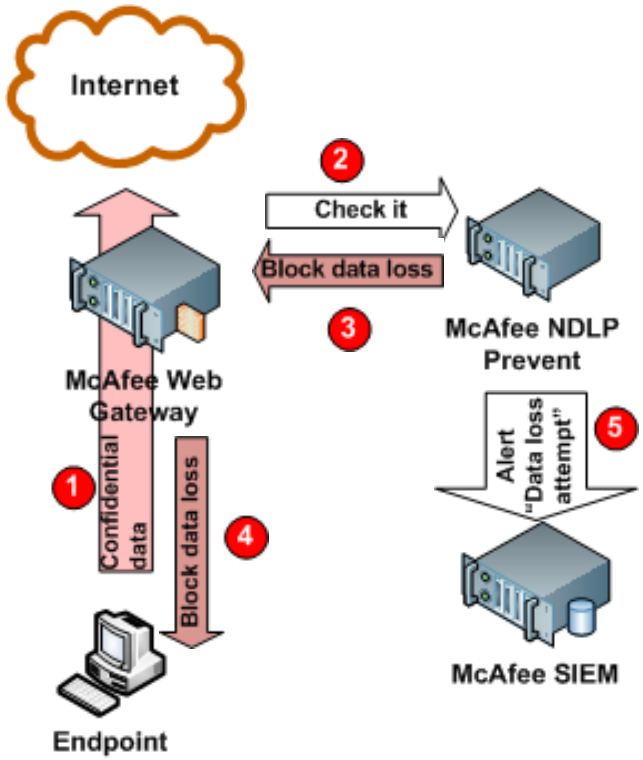
Сценарий работы интегрированной системы защиты Endpoint->SIEM->Endpoint

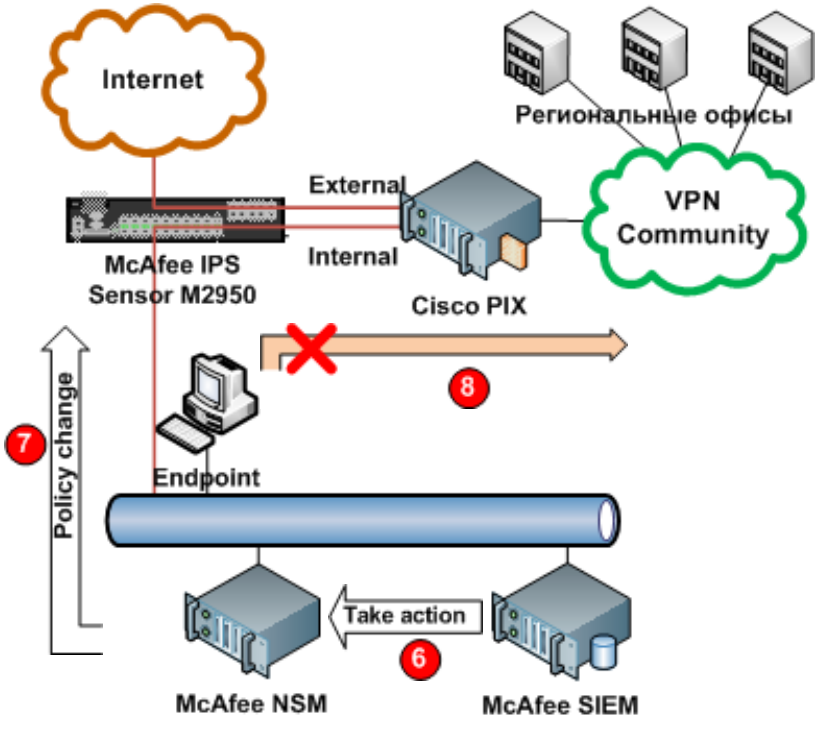


Сценарий работы интегрированной системы защиты Endpoint->SIEM->Endpoint

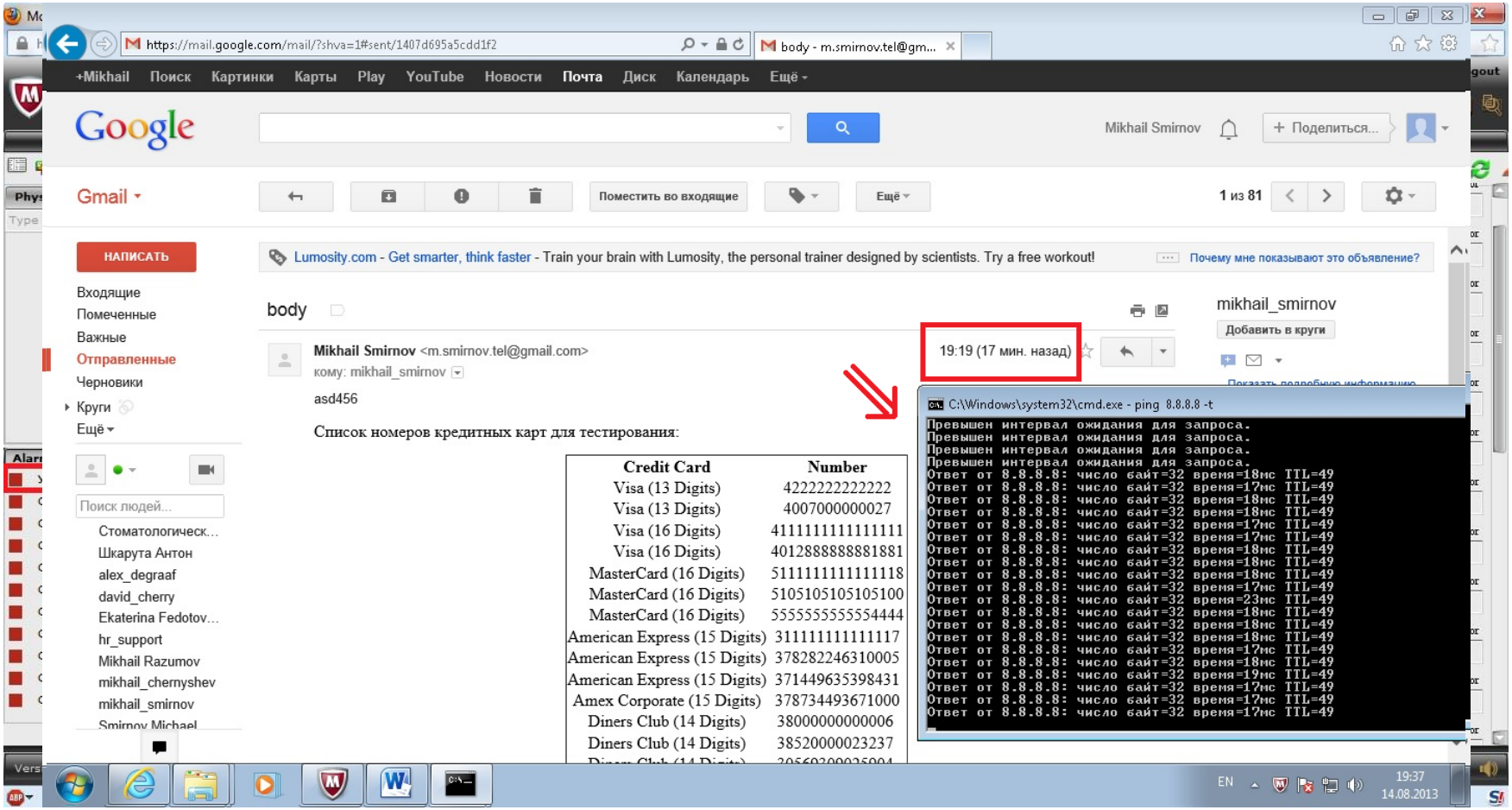


Сценарий работы интегрированной системы защиты Web Gateway->NDLP Prevent->SIEM->IPS

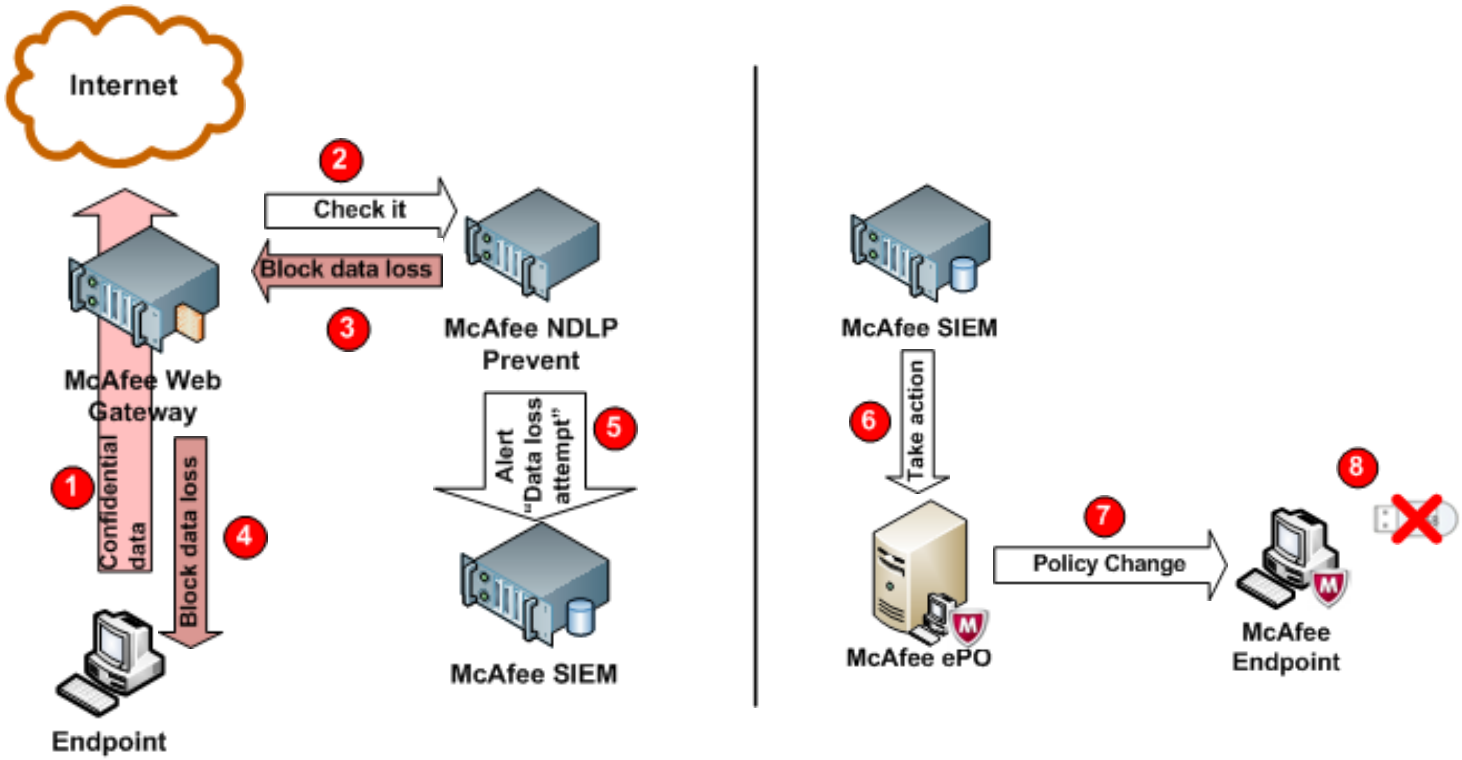




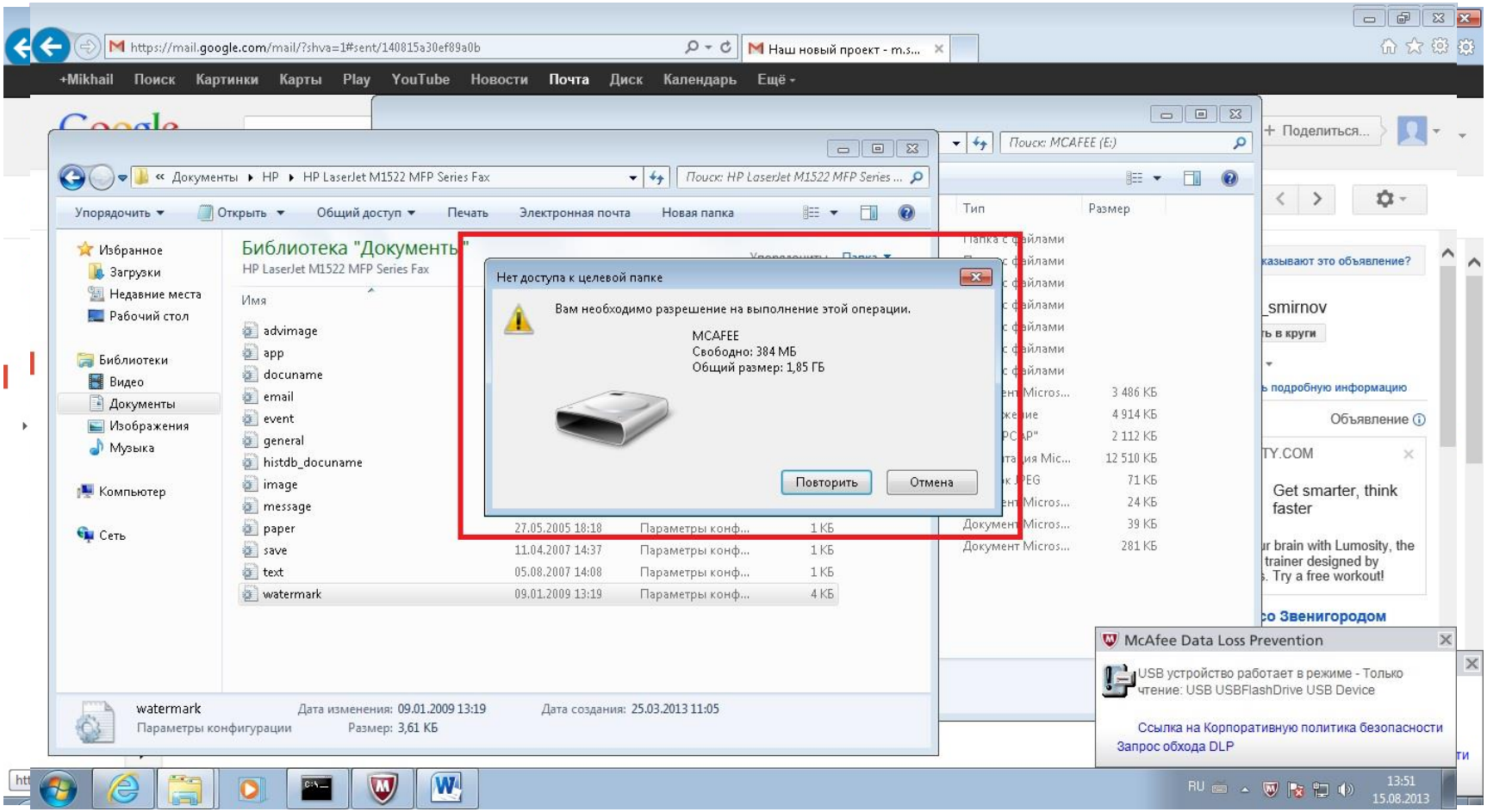
Сценарий работы интегрированной системы защиты Web Gateway->NDLP Prevent->SIEM->IPS



Сценарий работы интегрированной системы защиты Web Gateway->NDLP Prevent->SIEM->Device Control



Сценарий работы интегрированной системы защиты Web Gateway->NDLP Prevent->SIEM->Device Control



Оптимизация позволяет бизнесу экономить

Вы **знаете**, что происходит
Вы **понимаете**, что происходит
Ваше **время реакции** гораздо меньше
Ваша реакция гораздо **точнее**
Ваши **потери минимальны**
Ваши **затраты** существенно **ниже**


McAfee®
An Intel Company