

Централизованное управление  
событиями ИБ и организация  
контрмер



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

## Безопасность



---

vPro  
Active Management  
Technology  
Advanced Encryption Standard  
Virtualization  
One Time Password  
Secure BIOS



---

Network Security  
Cloud Security  
Security Management  
Endpoint Security  
Technology Ecosystem

## Прошлое



- Любители
- Самолюбование
- Драйвер - любопытство
- Хаотичность



## Настоящее



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



# Шойгу: угроза кибербезопасности сравнима с оружием массового поражения

aif.ru ВЧЕРА, 16:01



Сергей Шойгу.

Фото: РИА Новости

Общество



# McAfee Security Connected



## 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



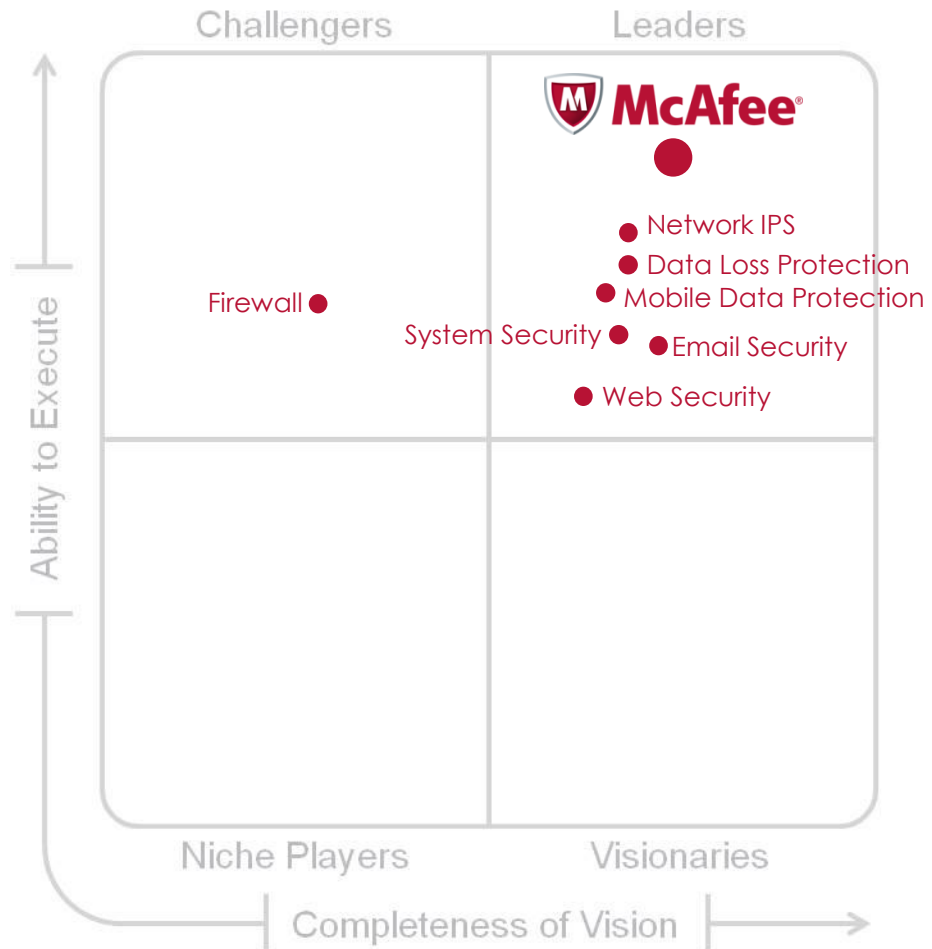


# Широкий спектр – лидерство везде



Integrated

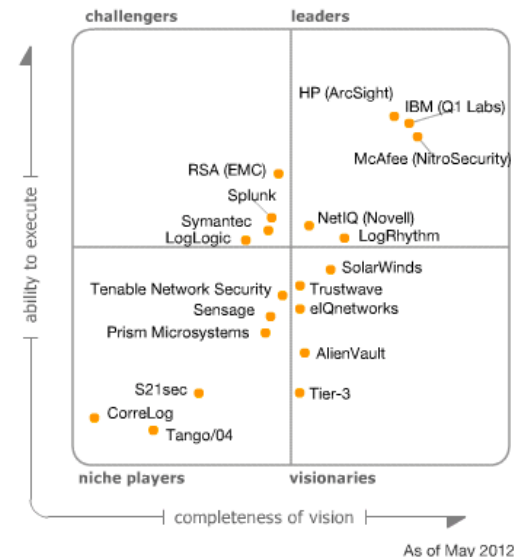
Source: Gartner



# 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

Figure 1. Magic Quadrant for Security Information and Event Management



Source: Gartner (May 2012)

- Результат (середина 2012):
  - Лидерство в Gartner Magic Quadrant
  - №1 по отчету Pike Research “Smart Grid Security” для защиты SCADA

## 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	Agilience	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)

# Централизация управления ИБ (SIEM)

# Текущее состояние SIEM

## Обещания:



Поддержка данных по безопасности

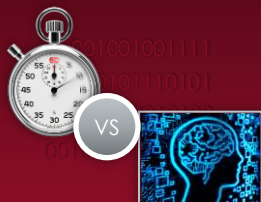


Платформа для глубокого исследования



Управление поддержкой и соответствием

## Реальность:



Устаревшая архитектура  
Вынужденный выбор между скоростью и информативностью



События сами по себе не помогут справиться с современными угрозами



Сложные управление и установка приводят к увеличению расходов

# Современные требования

Визуализация, Исследование и Ответ

Корреляционный модуль

GLOBAL THREAT  
LANDSCAPE

- Информация об угрозах
- Немедленные алармы
- Анализ истории



ENTERPRISE RISK  
LANDSCAPE

- Уязвимости
- Контрмеры
- Лица

Risk  
Advisor

ePolicy  
Orchestrator



Динамическое содержание



Основа на содержании



Традиционный контекст



Управление логами



- 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

System Incidents Dashboard Current Day

### Total Correlated Events

926

### Average Severity - Correlated Events

Successful logins after multiple f...	91
Scans - Targeted	89
Scans - Stealth	70
Multiple failed login attempts to ...	53
Multiple failed login attempts fro...	47
Brute force login attempts again...	37
Multiple events for gambling on ...	13

### Source IPs

Bound to: Average Severity - C... 926 (100%)

35.56.3.1	200
165.56.3.1	177
93.11.11.11	133
69.20.77.77	118
35.56.33.122	94

### Flow Source and Des

Bound to: Source IPs

193.238.160.1...	5,009
69.20.9.5	4,747
216.200.107.11	3,733

### Total Events

384,918

### Destination IPs

Bound to: Average Severity - C... 926 (100%)

69.20.0.76	463
69.20.0.98	356
69.20.100.36	72
67.15.145.19	2
69.20.22.248	1

### Event Distribution

Bound to: Average Severit

Interval: 1

### Events

Bound to: Average Severity - Correlated Events

Severity	Event Count	Source IP	Source Port	Destination IP	Destination Port	First Time	Last Time
2848	32	45.78.16.134	61853	69.20.0.98	http:80	07/11/2011 19:	07/12/2011 00:15:44
178	2	76.89.34.55	56344	69.20.0.76	http:80	07/12/2011 00:	07/12/2011 00:15:44
37	1	89.149.221.182	38292	::	port/code:0	07/12/2011 00:	07/12/2011 00:15:44
182	2	69.20.159.15	port/type:0	::	port/code:0	07/11/2011 23:	07/12/2011 00:15:44
47	1	89.149.221.182	38292	::	port/code:0	07/12/2011 00:	07/12/2011 00:15:44
53	1	89.149.221.182	38292	::	port/code:0	07/12/2011 00:	07/12/2011 00:15:44
94	2	69.20.159.15	port/type:0	::	port/code:0	07/11/2011 23:	07/12/2011 00:15:44
70	1	::	port/type:0	69.20.134.143	port/code:0	07/12/2011 00:	07/12/2011 00:15:43

### Filters

Hints

- Destination MAC
- Destination IP
- Destination Port
- Protocol
- Source MAC
- Source IP
- Source Port
- Event Subtype
- Signature ID
- Device Type
- Normalized ID
- Application
- Host
- Domain
- Source User

# 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



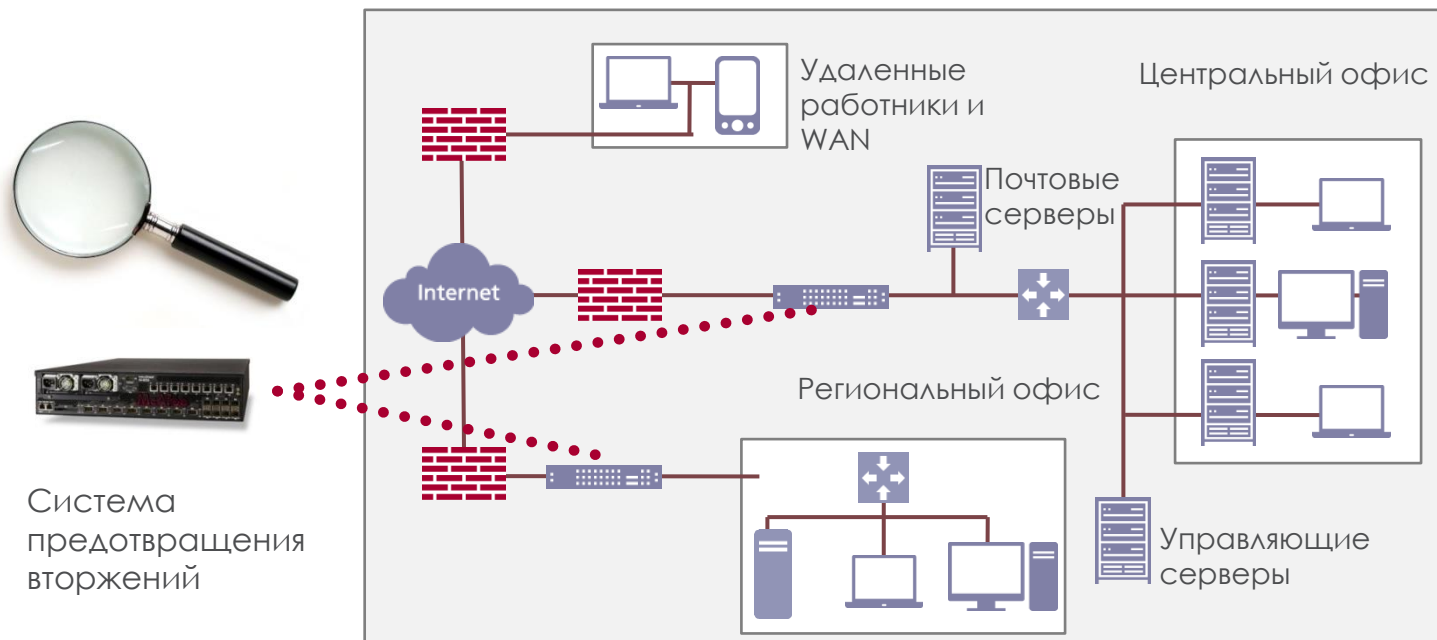
# SIEM и сетевая безопасность

# Защита сети на основе McAfee Network Security Platform



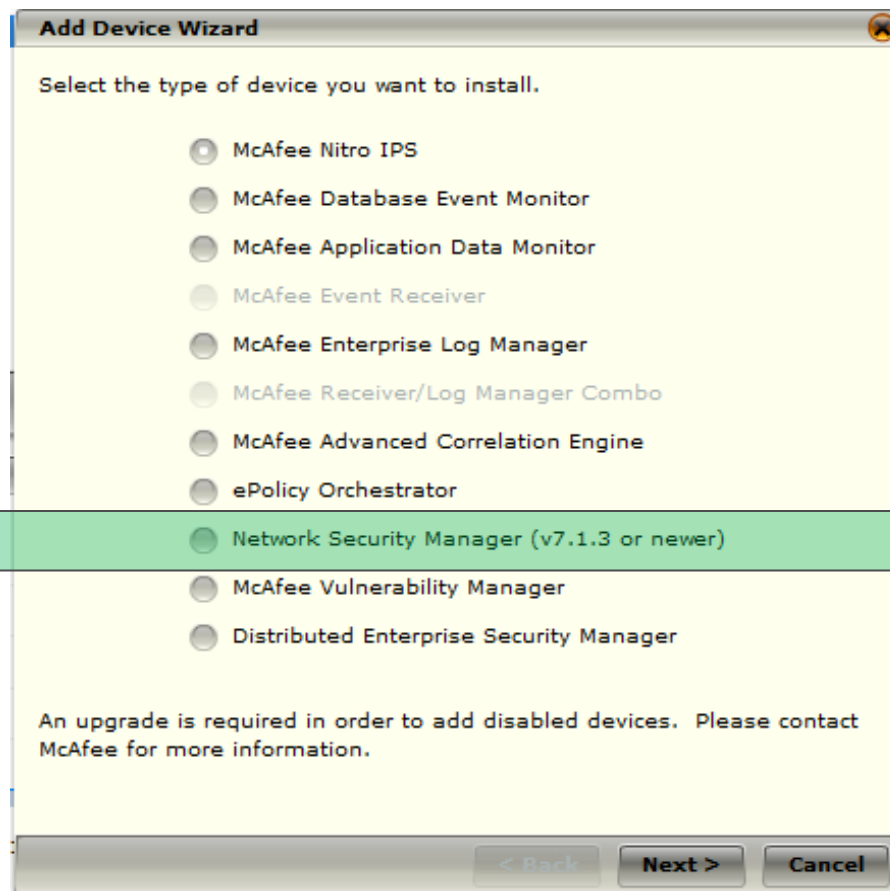
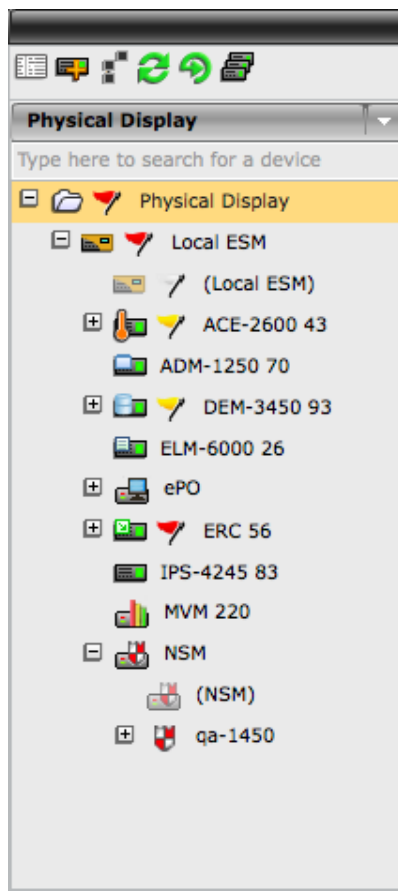
## • McAfee Network Security Platform (IPS):

- Инспектирует входящий и исходящий трафик в реальном времени
- Останавливает вредоносный или нежелательный трафик
- Категоризирует 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

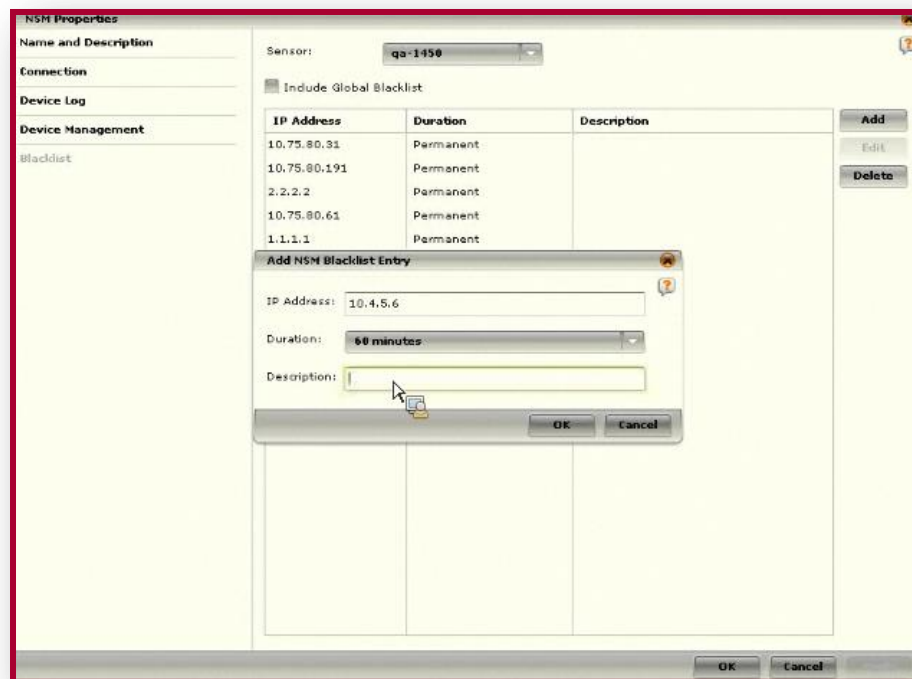
## IPS встраивается на уровне общего API в решение McAfee SIEM



# Использование McAfee IPS при обработке инцидента ИБ

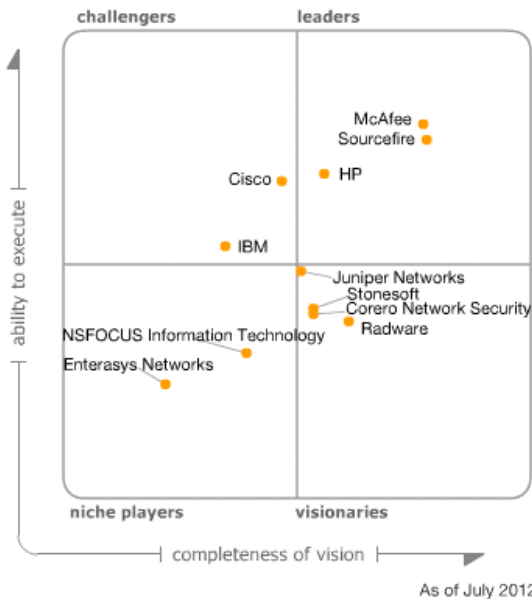
## SIEM вызывает специализированные функции IPS в ответ на инциденты

Любой оператор SOC может запустить **ответное действие из SIEM** в ответ на появление в сети вредоносного узла (запуск эксплоитов, запуск вредоносных, 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
<b>McAfee Network Security Platform (NSP) M-8000 v6.1</b>	95%	100%	12,300 Mbps
Stability & Reliability	Client Protection	Server Protection	
Excellent	99%	91%	



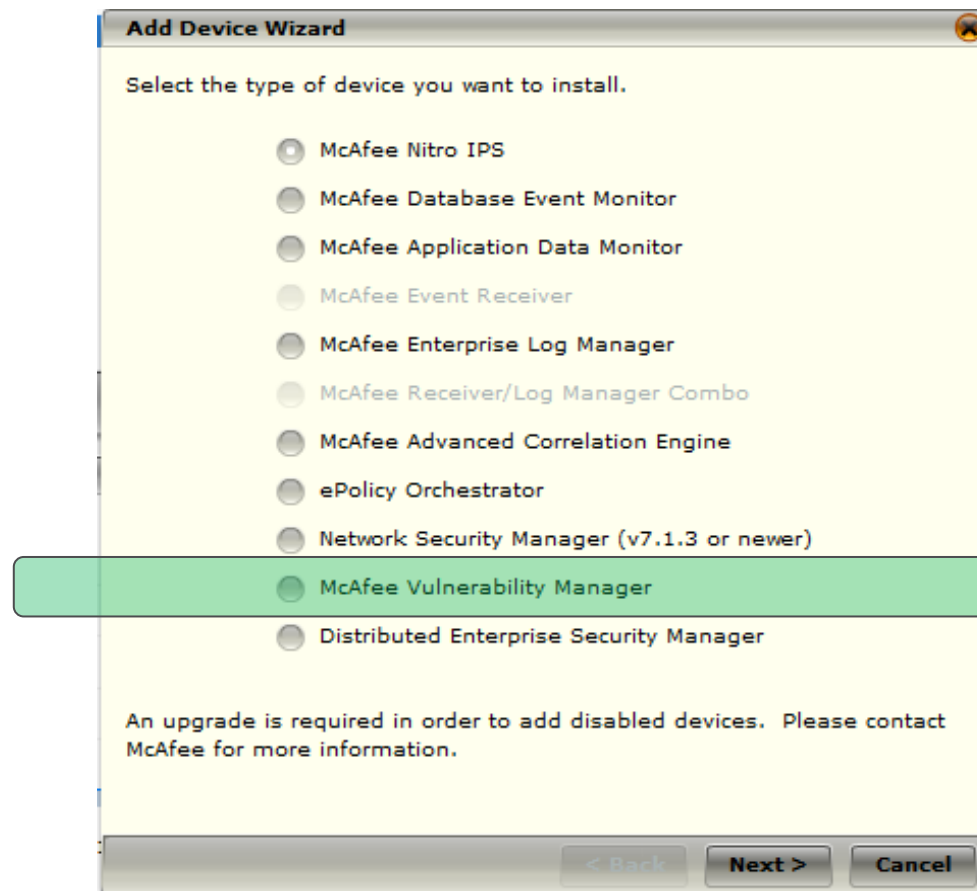
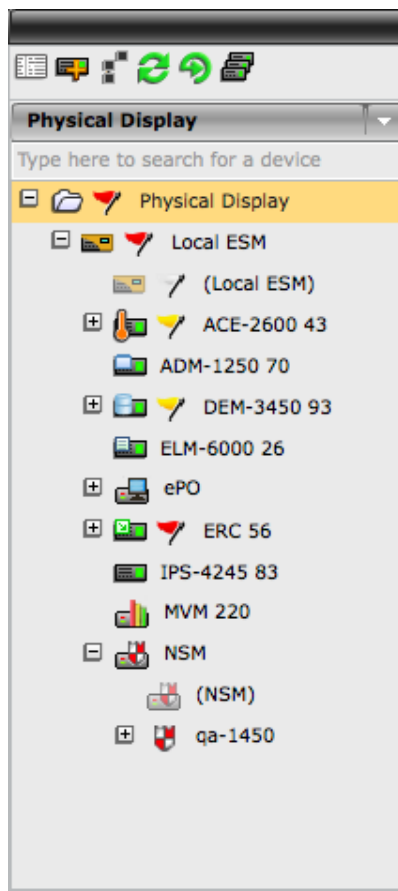
Type of Malware	Number of Samples	Detected Samples	%
<b>Total</b>	113,646	105,803	93.10%
<b>Prevalent Malware</b>	11,072	10,371	93.67%
<b>Backdoors</b>	7,932	7,827	98.68%
<b>Bots</b>	2,329	2,317	99.48%
<b>Rogue Software</b>	1,683	1,659	98.57%
<b>Trojan Horses</b>	81,265	75,655	93.10%
<b>Viruses</b>	4,013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

Figure 5: Zoo detection results

# SIEM и оценка уязвимостей

# Сканнер уязвимостей – часть платформы безопасности

## McAfee Vulnerability Manager встраивается на уровне API в McAfee SIEM

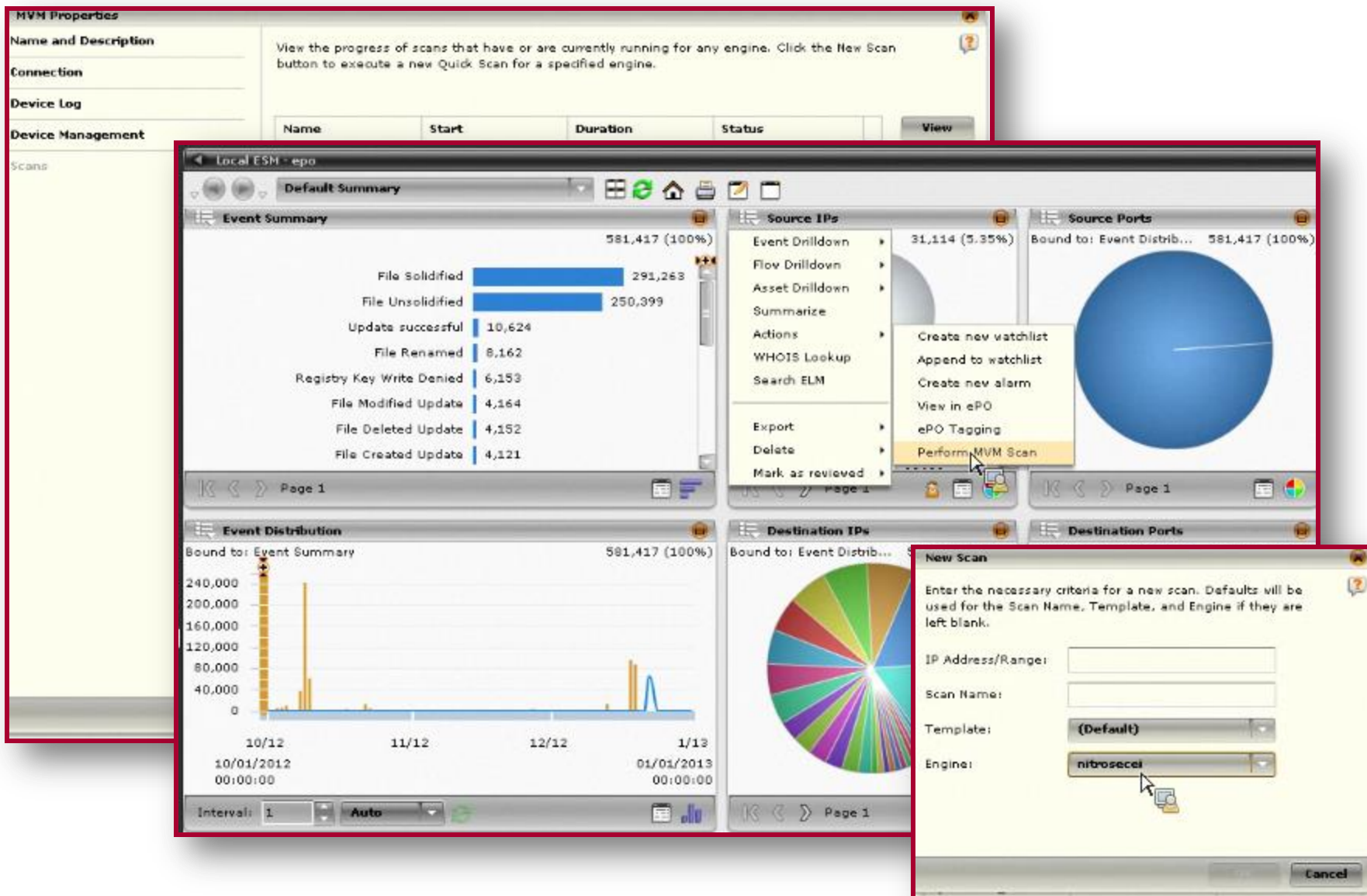


## McAfee ESM может сканировать устройства в сети

- 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?



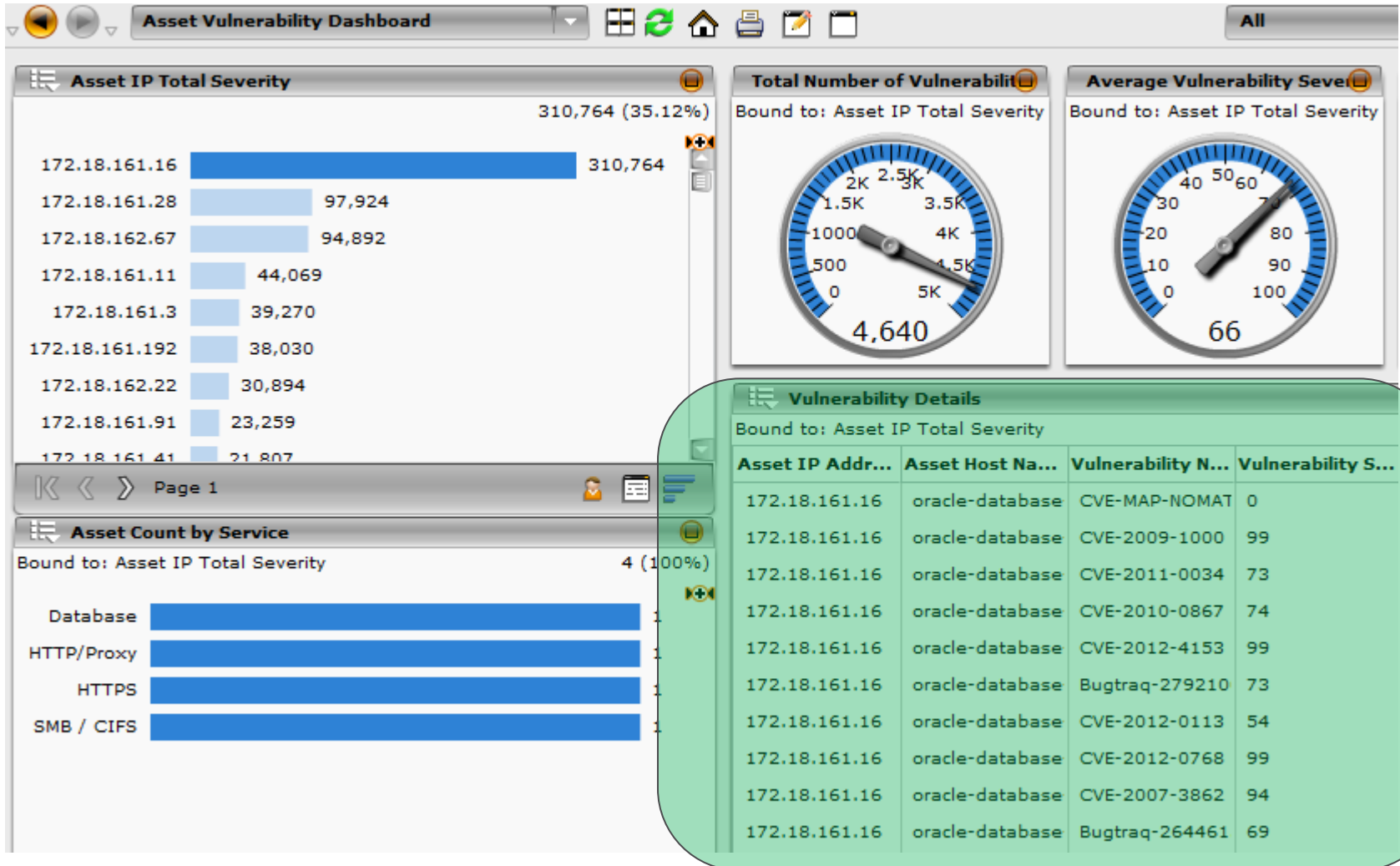
The screenshot displays the McAfee MVM (McAfee Virus Management) interface. The main window shows a 'Default Summary' for 'Local ESM - epo' with 581,417 events. The 'Event Summary' section includes a bar chart with the following data:

Event Type	Count
File Solidified	291,268
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

The 'Source IPs' section shows 31,114 (5.35%) with a context menu open, highlighting 'Perform MVM Scan'. The 'Event Distribution' chart shows a peak in early 2012. The 'New Scan' dialog box is open, showing the following configuration:

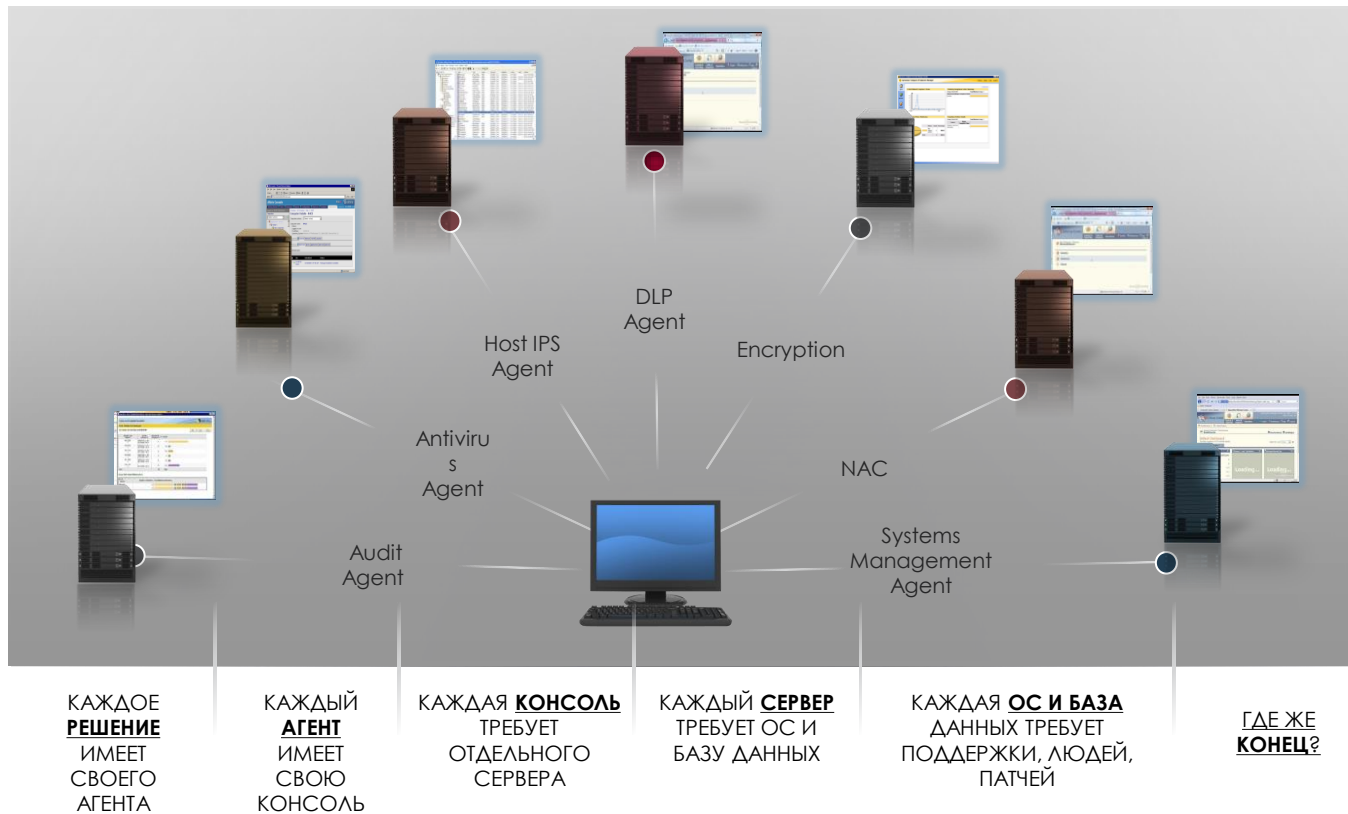
- IP Address/Range: [Empty]
- Scan Name: [Empty]
- Template: (Default)
- Engine: nitroscan

# Информация об уязвимостях доступна в SIEM

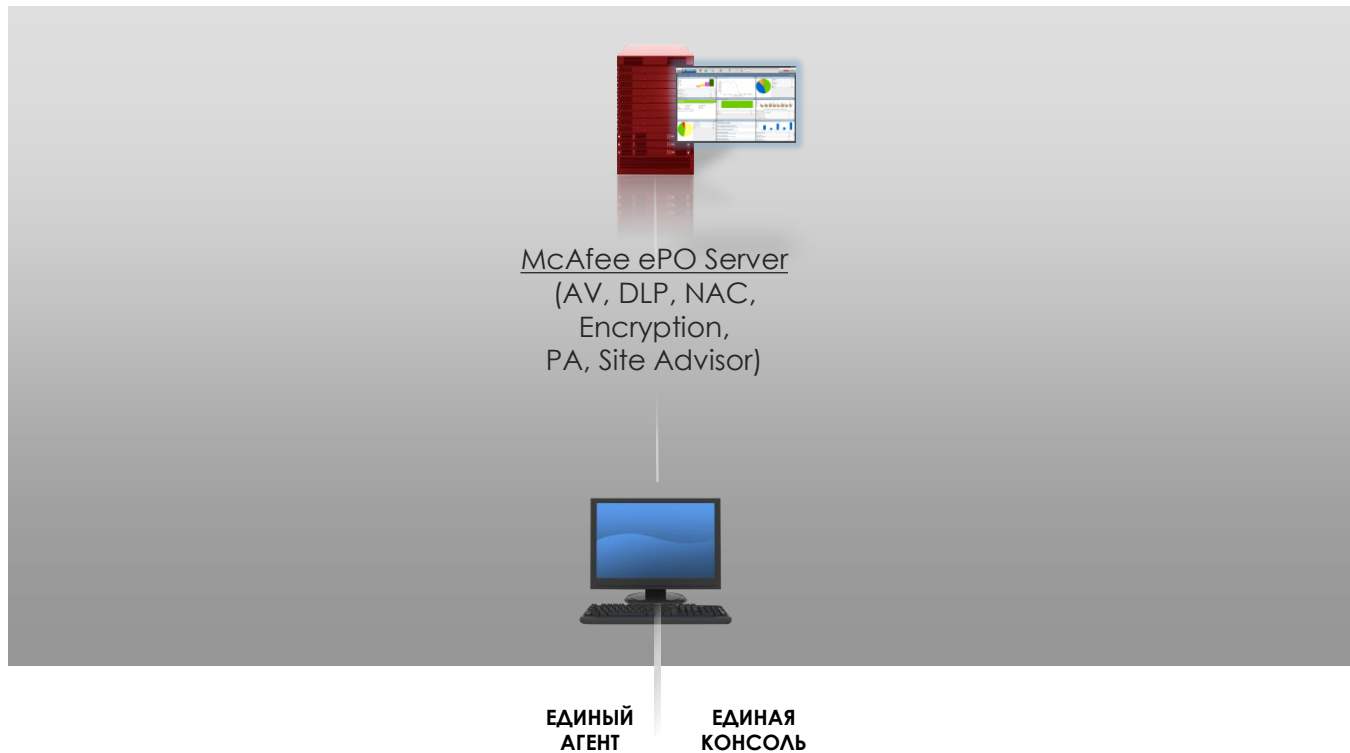


# SIEM и безопасность конечных точек

## Насколько объединена ваша система безопасности?



## Насколько объединена ваша система безопасности?





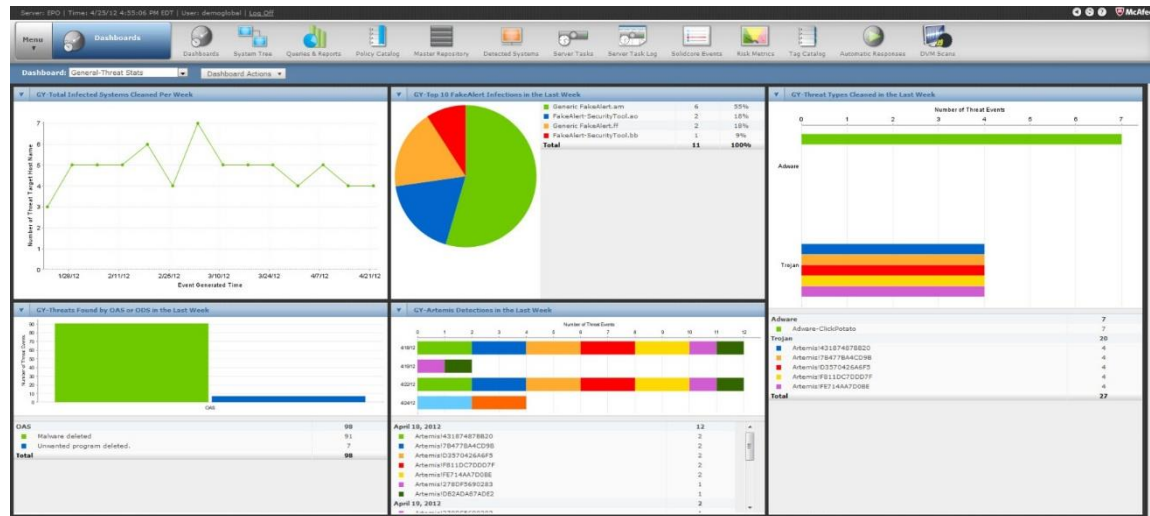
## McAfee ePolicy Orchestrator (McAfee ePO)

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

- Полная видимость
- Открытая, расширяемая архитектура
- Доказанная эффективность

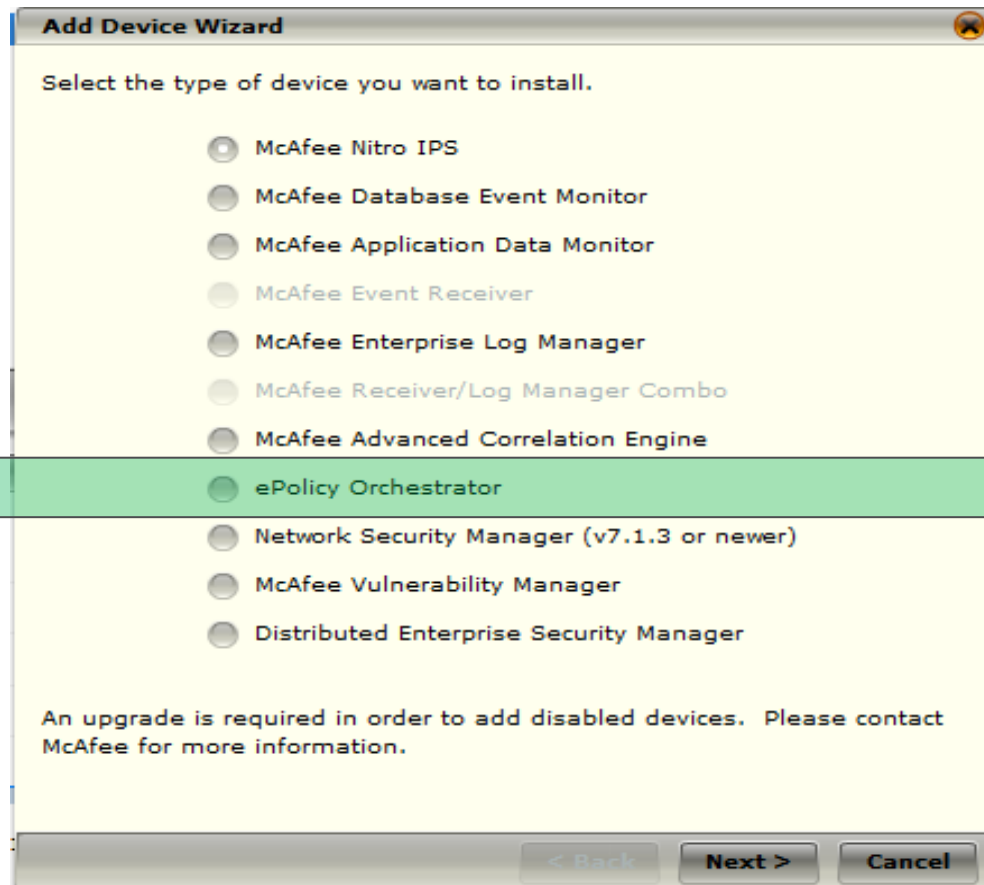
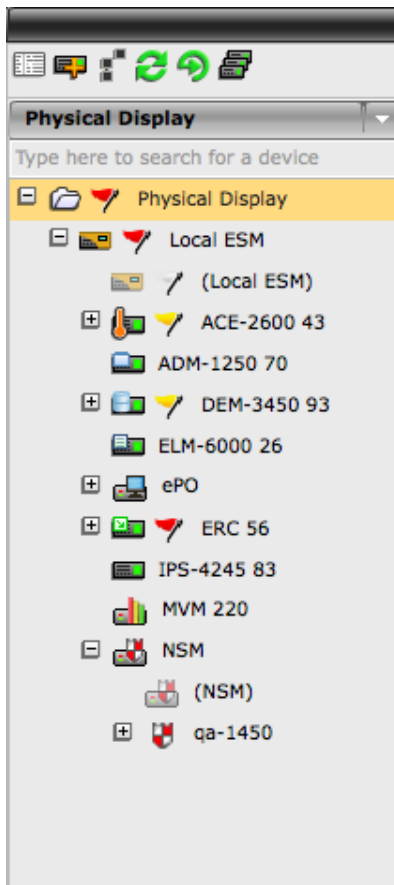
### Complete Management

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



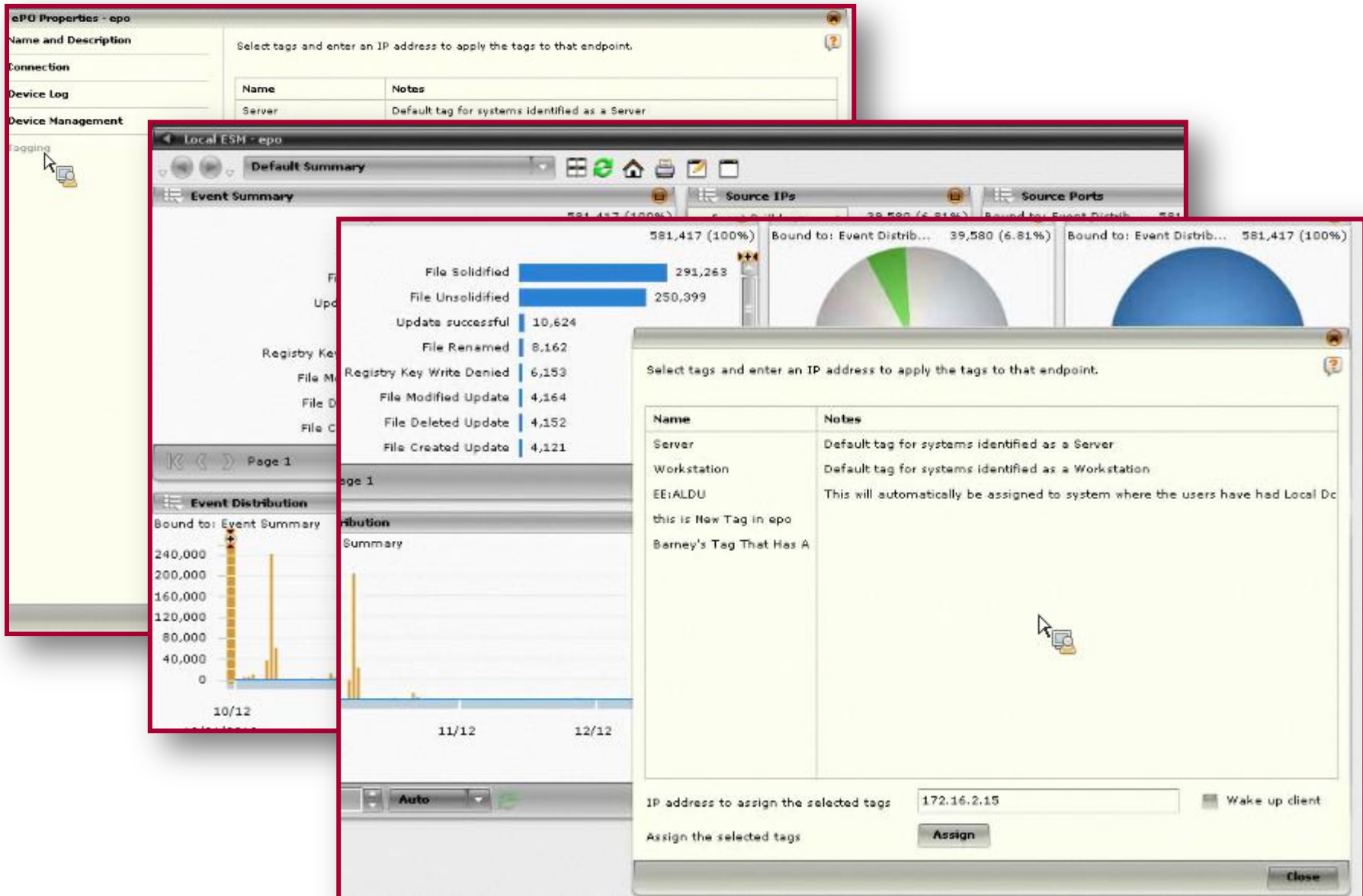


## McAfee ePolicy Orchestrator встраивается на уровне API в McAfee SIEM





# Установка меток ePo в ответ на инцидент



The screenshot illustrates the process of installing ePo tags in response to an incident. It features several overlapping windows from the McAfee ePO console:

- Local ESM - epo**: Shows a "Default Summary" with tabs for "Event Summary", "Source IPs", and "Source Ports". It includes a table of event counts and a bar chart for "Event Distribution".
- Event Summary**: A detailed view of event counts for various categories:

Event Category	Count
File Solidified	291,268
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

- Event Distribution**: A bar chart showing event counts over time, with a peak in 10/12.
- Tag Assignment Dialog**: A window titled "Select tags and enter an IP address to apply the tags to that endpoint." It contains a table of existing tags:

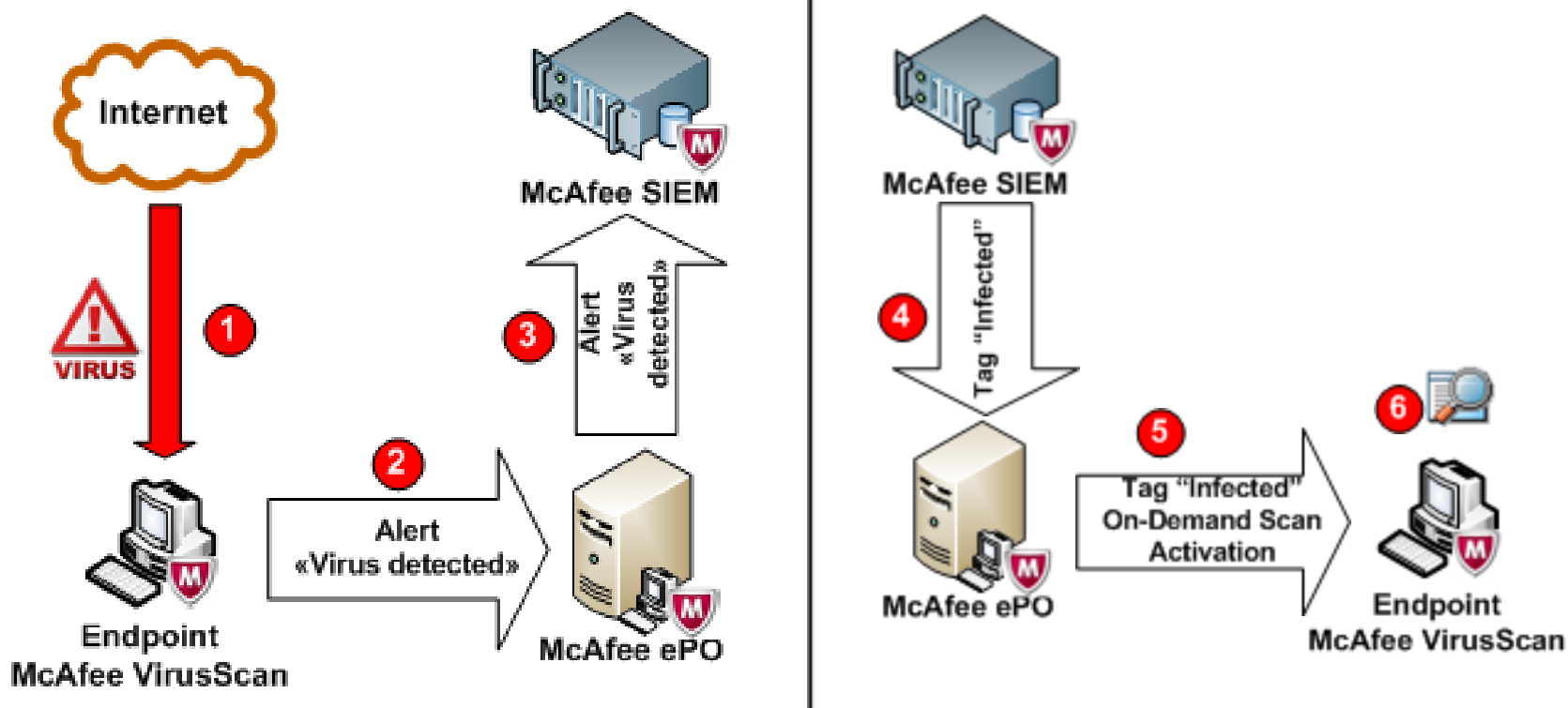
Name	Notes
Server	Default tag for systems identified as a Server
Workstation	Default tag for systems identified as a Workstation
EE:ALDU	This will automatically be assigned to system where the users have had Local Dc
this is New Tag in epo	
Barney's Tag That Has A	

At the bottom of the dialog, there is a field for "IP address to assign the selected tags" with the value "172.16.2.15" and a "Wake up client" checkbox. An "Assign" button is visible.

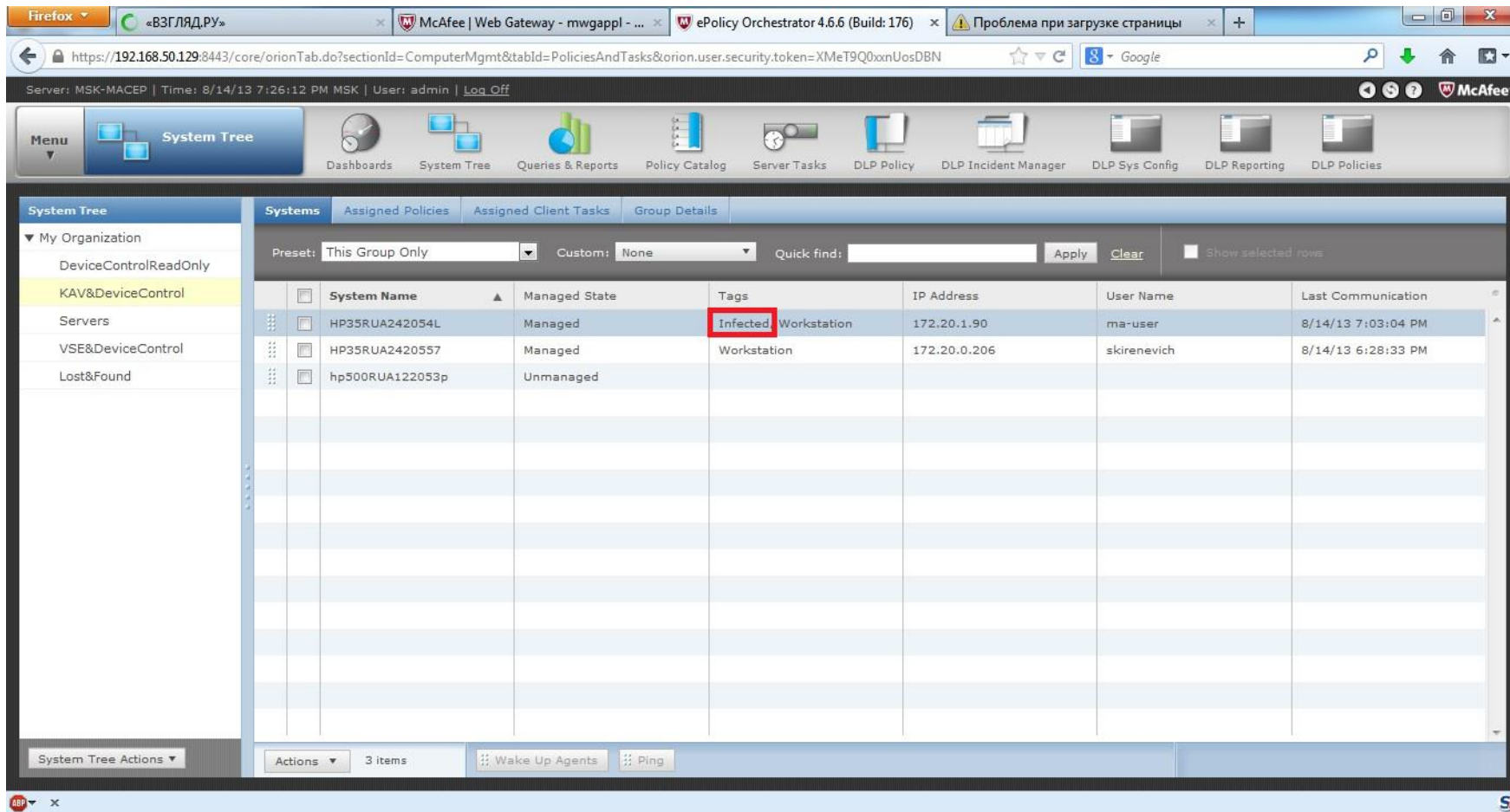
Примеры из жизни

**SAFE NEVER SLEEPS.**<sup>™</sup>

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



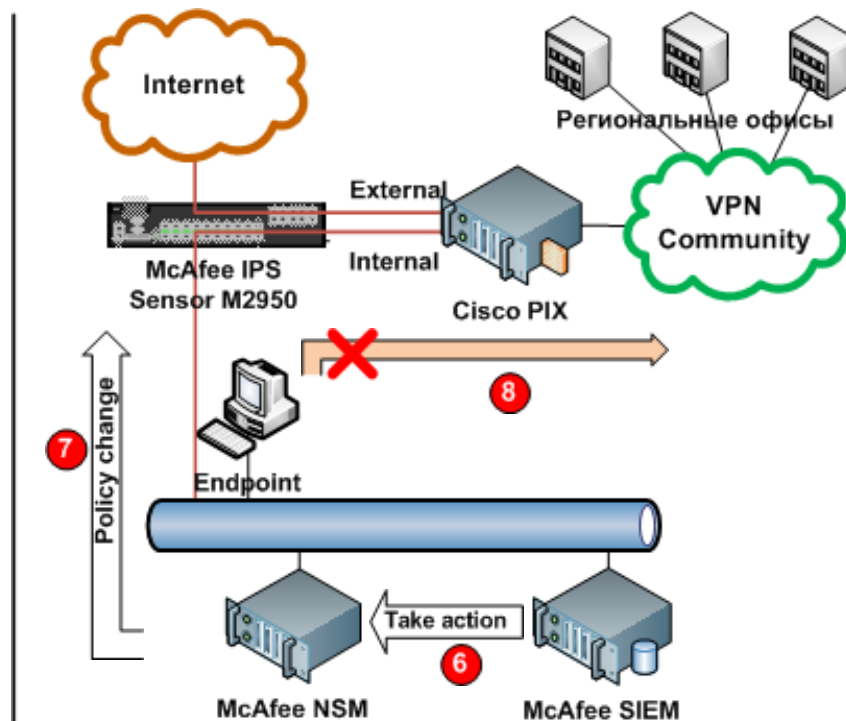
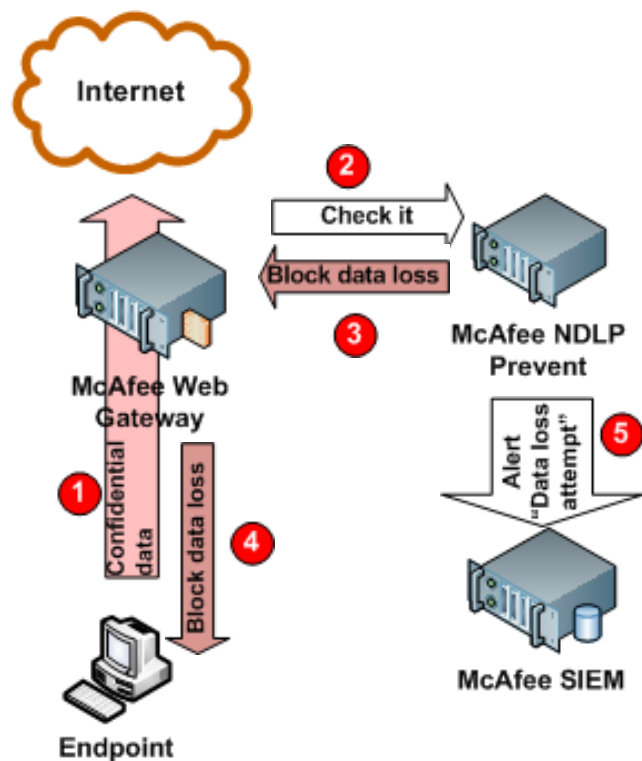
# Сценарий работы интегрированной системы защиты Endpoint->SIEM->Endpoint



The screenshot displays the McAfee ePolicy Orchestrator (EPO) 4.6.6 web interface. The browser address bar shows the URL: <https://192.168.50.129:8443/core/orionTab.do?sectionId=ComputerMgmt&tabId=PoliciesAndTasks&orion.user.security.token=XMeT9Q0xxnUosDBN>. The interface includes a navigation menu with options like System Tree, Dashboards, and Policy Catalog. The main content area shows the 'Systems' tab with a table of managed systems. The 'KAV&DeviceControl' folder is selected in the left-hand System Tree.

System Name	Managed State	Tags	IP Address	User Name	Last Communication
HP35RUA242054L	Managed	Infected, Workstation	172.20.1.90	ma-user	8/14/13 7:03:04 PM
HP35RUA2420557	Managed	Workstation	172.20.0.206	skirenevich	8/14/13 6:28:33 PM
hp500RUA122053p	Unmanaged				

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



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



**body**

Mikhail Smirnov <m.smirnov.tel@gmail.com>  
кому: mikhail\_smirnov  
asd456

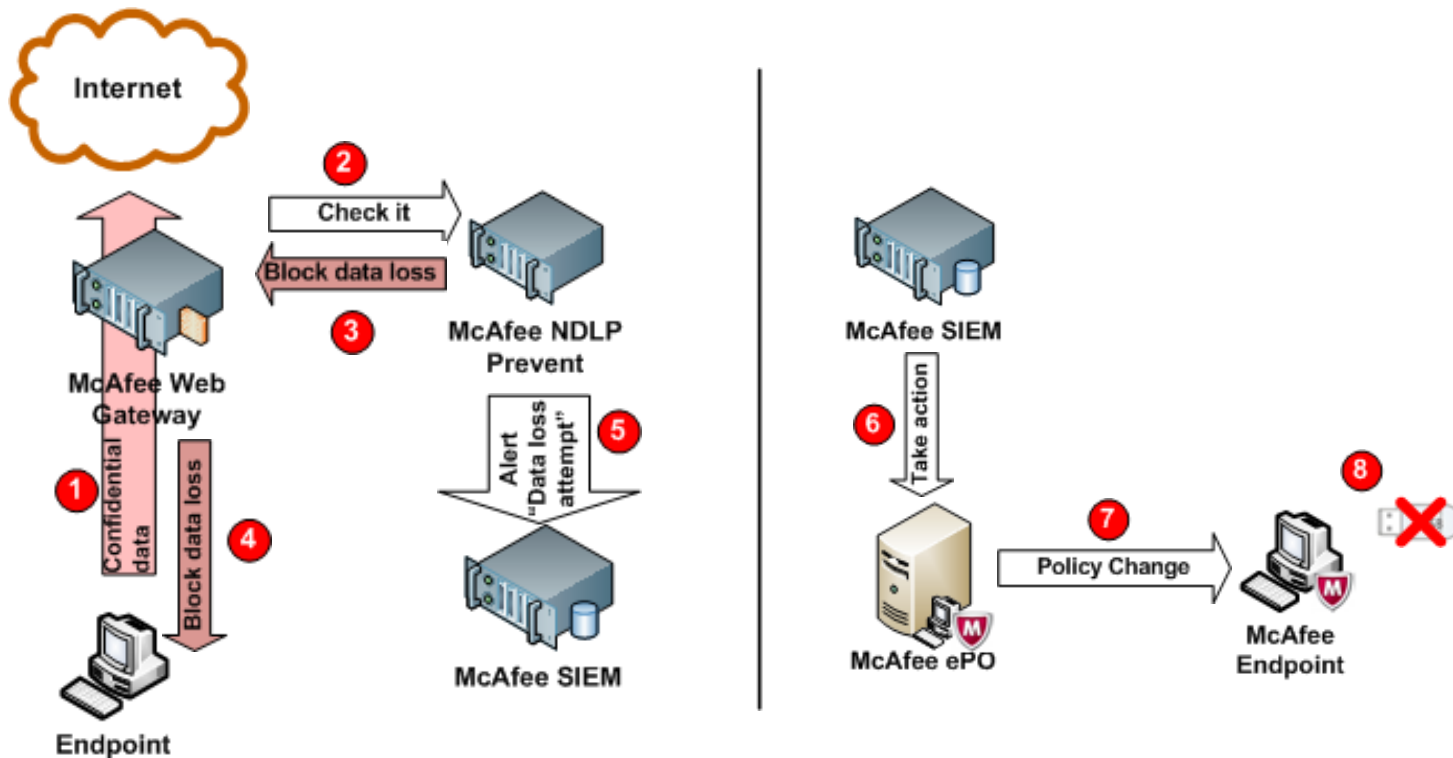
Список номеров кредитных карт для тестирования:

Credit Card	Number
Visa (13 Digits)	4222222222222
Visa (13 Digits)	4007000000027
Visa (16 Digits)	411111111111111
Visa (16 Digits)	4012888888881881
MasterCard (16 Digits)	5111111111111118
MasterCard (16 Digits)	5105105105105100
MasterCard (16 Digits)	5555555555554444
American Express (15 Digits)	3111111111111117
American Express (15 Digits)	378282246310005
American Express (15 Digits)	371449635398431
Amex Corporate (15 Digits)	378734493671000
Diners Club (14 Digits)	38000000000006
Diners Club (14 Digits)	38520000023237
Diners Club (14 Digits)	2056000025004

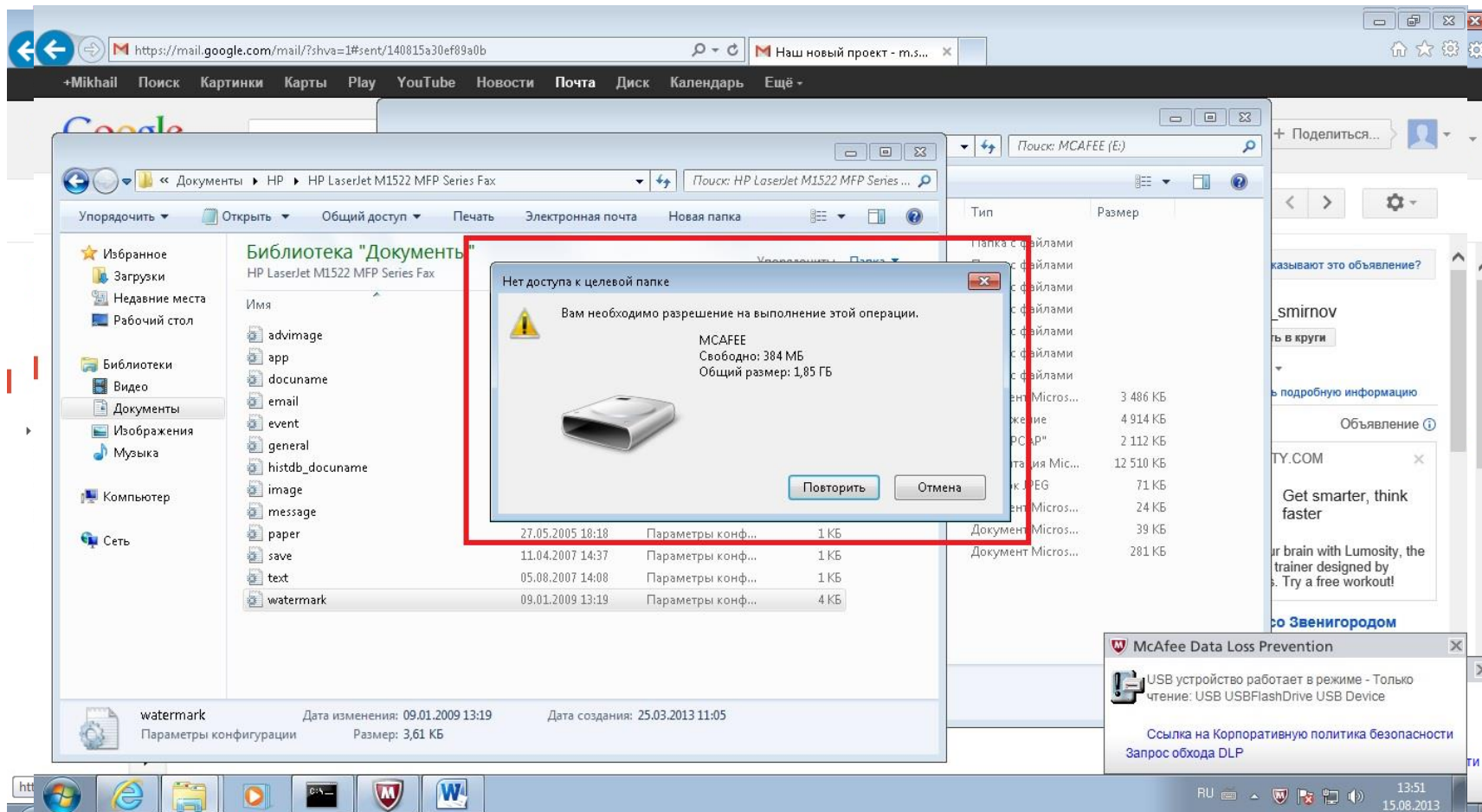
19:19 (17 мин. назад)

```
C:\Windows\system32\cmd.exe - ping 8.8.8.8 -t
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Ответ от 8.8.8.8: число байт=32 время=18мс TTL=49
Ответ от 8.8.8.8: число байт=32 время=17мс TTL=49
Ответ от 8.8.8.8: число байт=32 время=18мс TTL=49
Ответ от 8.8.8.8: число байт=32 время=18мс TTL=49
Ответ от 8.8.8.8: число байт=32 время=17мс TTL=49
Ответ от 8.8.8.8: число байт=32 время=17мс TTL=49
Ответ от 8.8.8.8: число байт=32 время=18мс TTL=49
Ответ от 8.8.8.8: число байт=32 время=18мс TTL=49
Ответ от 8.8.8.8: число байт=32 время=18мс TTL=49
Ответ от 8.8.8.8: число байт=32 время=18мс TTL=49
Ответ от 8.8.8.8: число байт=32 время=18мс TTL=49
Ответ от 8.8.8.8: число байт=32 время=17мс TTL=49
Ответ от 8.8.8.8: число байт=32 время=18мс TTL=49
Ответ от 8.8.8.8: число байт=32 время=18мс TTL=49
Ответ от 8.8.8.8: число байт=32 время=18мс TTL=49
Ответ от 8.8.8.8: число байт=32 время=17мс TTL=49
Ответ от 8.8.8.8: число байт=32 время=17мс TTL=49
Ответ от 8.8.8.8: число байт=32 время=17мс TTL=49
Ответ от 8.8.8.8: число байт=32 время=17мс TTL=49
```

# 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**

