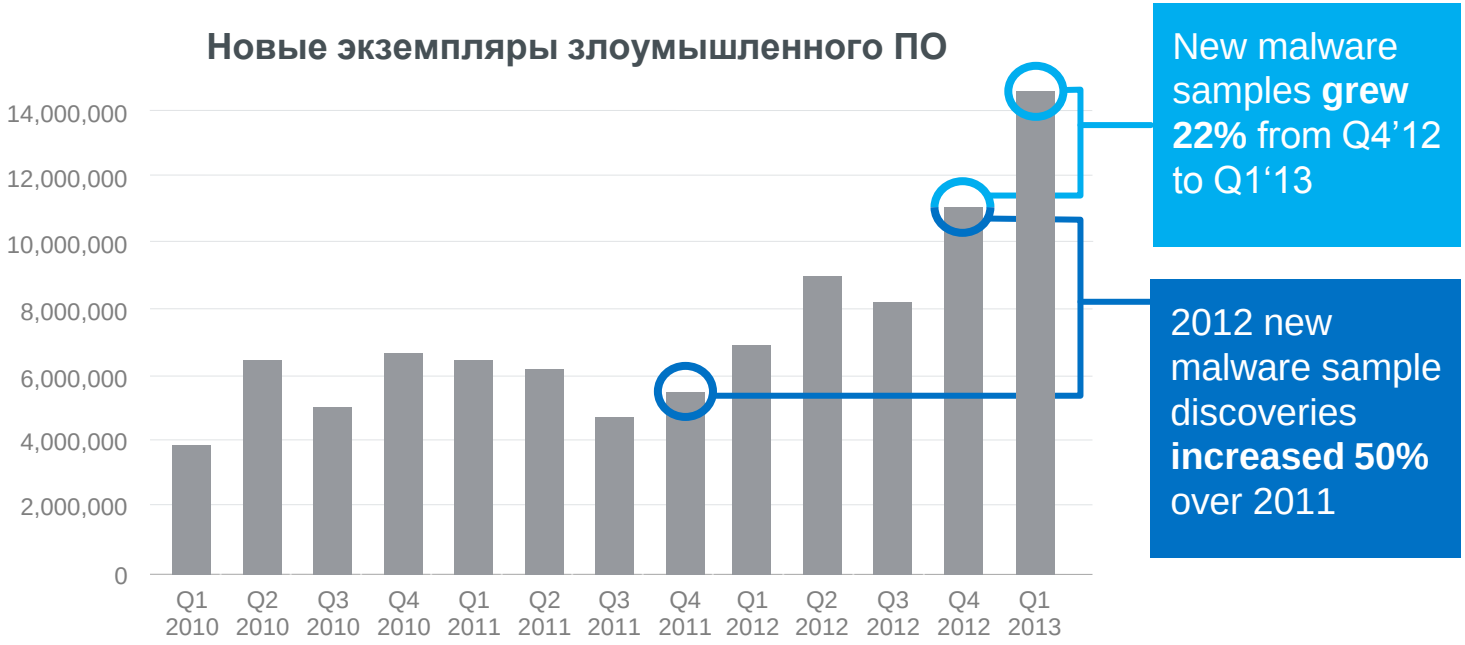
Complete Endpoint Protection

mcafee@softprom.com

TM

Количество зловредов растёт…

… и совершенствуется



Source: McAfee Labs, 2013

Четыре фазы атаки

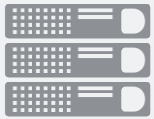
Пример: Fake AV

Эволюция конечных точек

Настольные ПК

Ноутбуки

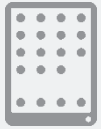
Съёмные носители



Серверы
(Физические и виртуальные)

Базы данных

Хранилища



Таблетки

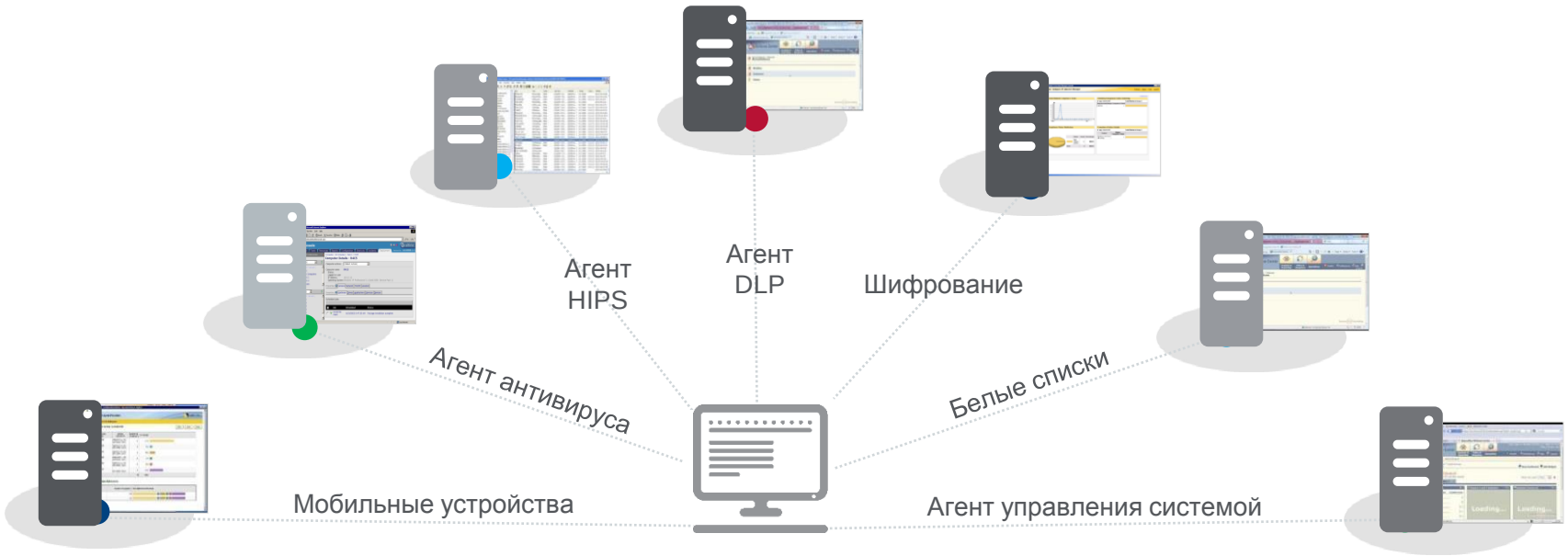
Смартфоны

Банкоматы

Медицинские устройства

РАБОЧЕЕ МЕСТО | ДАТАЦЕНТР | МОБИЛЬНЫЕ И СПЕЦ.УСТРОЙСТВА

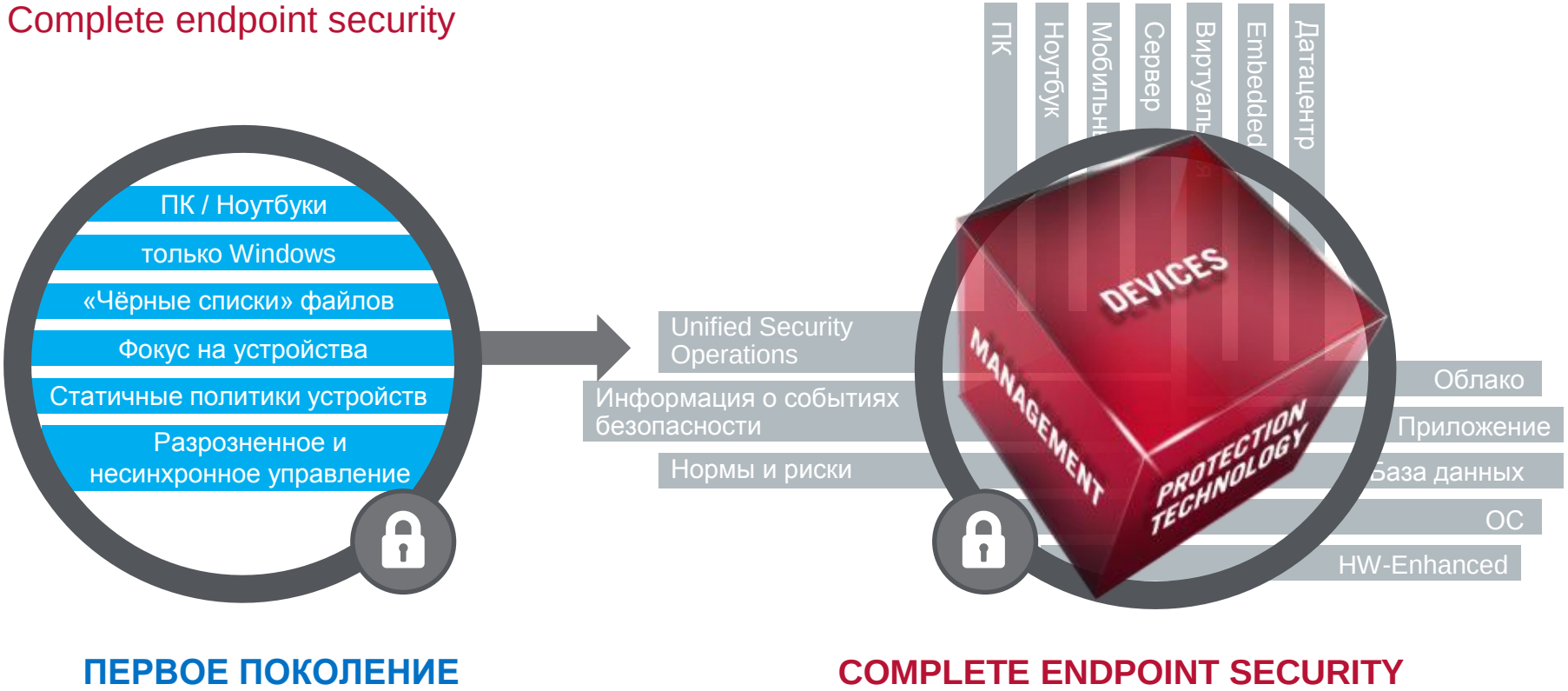
Традиционная архитектура безопасности конечных точек



У каждого **РЕШЕНИЯ** своя **КОНСОЛЬ** → Каждой **КОНСОЛИ** нужен **СЕРВЕР** → Каждому **СЕРВЕРУ** нужна **ОС** и **БАЗА ДАННЫХ** → Каждая **ОС/БД** требует **ЛЮДЕЙ**, **ОБСЛУЖИВАНИЯ**, **НАСТРОЙКИ** → **КОГДА ЭТО ЗАКОНЧИТСЯ?**

McAfee Endpoint Protection Platform Strategy

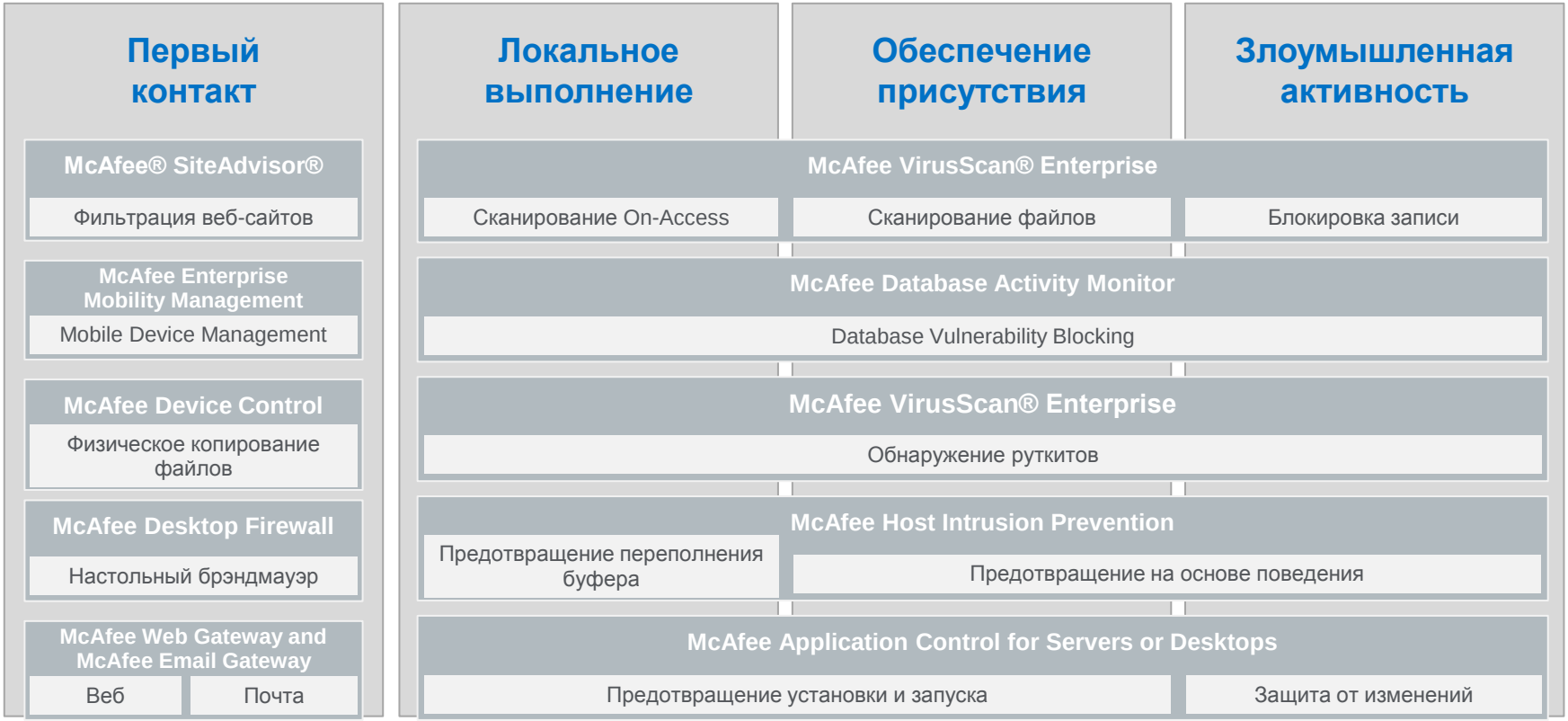
Complete endpoint security



ПЕРВОЕ ПОКОЛЕНИЕ

COMPLETE ENDPOINT SECURITY

Четыре фазы:


Первый контакт
Локальное выполнение
Обеспечение присутствия
Злоумышленная активность
McAfee® SiteAdvisor®
Фильтрация веб-сайтов
McAfee Enterprise Mobility Management
Mobile Device Management
McAfee Device Control
Физическое копирование файлов
McAfee Desktop Firewall
Настольный брэндмауэр
McAfee Web Gateway and McAfee Email Gateway
Веб
Почта
McAfee VirusScan® Enterprise
Сканирование On-Access
Сканирование файлов
Блокировка записи
McAfee Database Activity Monitor
Database Vulnerability Blocking
McAfee VirusScan® Enterprise
Обнаружение руткитов
McAfee Host Intrusion Prevention
Предотвращение переполнения буфера
Предотвращение на основе поведения
McAfee Application Control for Servers or Desktops
Предотвращение установки и запуска
Защита от изменений

Intel Security – лидер защиты конечных точек

Семь лет лидерства в Gartner Magic Quadrant!

- Лидер в *Completeness of Vision*
- Лучшее управление с помощью ePO
- Следующее поколение защиты
- Security Connected Vision
- Высокие рейтинги защиты
- Полнофункциональное решение
- Совместное преимущество Intel / McAfee

Complete Endpoint Protection – Enterprise

Удобство

- Унифицированное и открытое управление конечными точками
- Единое решение для ПК, Mac, Linux, мобильных и виртуальных
- Несложная установка за несколько минут
- Единая консоль – меньше ресурсов для управления

Производительность

- Производительные средства защиты, оптимизированные для разных платформ
- Динамические «белые списки» снижают нагрузку на конечные точки
- Реагирование в режиме реального времени (быстрее, чем обычно, от 10 до 1000 раз)
- Технология сканирования оптимизирует использование CPU и памяти

Защита

- Самый функциональный набор решений на рынке
- Известный лидер по блокированию и обнаружению скрытых угроз
- Использование Application Whitelisting обеспечивает защиту на 100%

Защита конечных точек	
Windows & Unix AV	✓
Mac & Linux AV	✓
Endpoint Firewall	✓
Host Intrusion Prevention	✓
Application Blocking	✓
Application Control – Desktop	✓
Почта/Веб, мобильные устройства	
SiteAdvisor with Web Filter	✓
Anti-malware Email	✓
Mobile Device Management	✓
Защита данных	
Device Control	✓
Развёртывание и управление	
ePO	✓

Complete Endpoint Protection – Business

Удобство

- Унифицированное и открытое управление конечными точками
- Единое решение для ПК, Mac, Linux, мобильных и виртуальных
- Несложная установка за несколько минут
- Единая консоль – меньше ресурсов для управления

Производительность

- Производительные средства защиты, оптимизированные для разных платформ
- Реагирование в режиме реального времени (быстрее, чем обычно, от 10 до 1000 раз)
- Технология сканирования оптимизирует использование CPU и памяти

Защита

- Самый функциональный набор решений на рынке
- Известный лидер по блокированию и обнаружению скрытых угроз

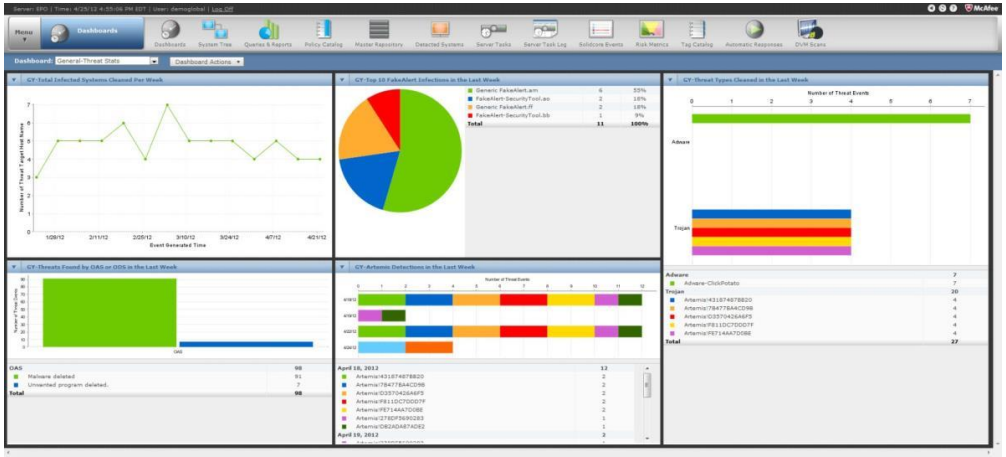
Endpoint Protection	
Windows & Unix AV	✓
Mac & Linux AV	✓
Storage Server AV	✓
SharePoint AV	✓
Endpoint Firewall	✓
Intrusion Prevention	✓
Application Blocking	✓
Web/Messaging Security and Mobile	
Antimalware Email	✓
SiteAdvisor with Web Filtering	✓
Mobile Device Management	✓
Data Protection	
Device Control	✓
Drive Encryption	✓
File & Removable Media Protection	✓
Management & Deployment	
ePO	✓

ePolicy Orchestrator

McAfee ePolicy Orchestrator (McAfee ePO)

Платформа для унифицированного управления информационной безопасностью на уровне конечных точек, сети и данных.

- Прозрачность на всех уровнях
- Открытая, расширяемая архитектура
- Доказанная эффективность



Полноценное управление

- Персонализированный центр управления
- Интерактивные отчёты и конфигурируемые панели
- Ролевой доступ
- Мощные рабочие процессы
- Корпоративный уровень
- Расширяемая платформа

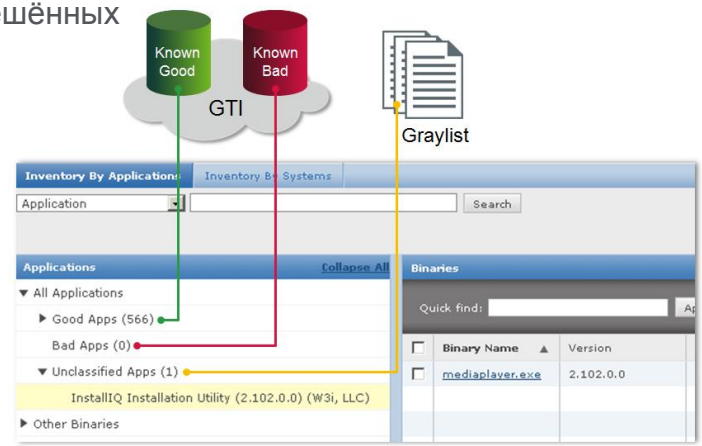
McAfee Application Control for Desktop

Всеобъемлющая защита конечных точек

- Защита от известных и неизвестных угроз
- Использование «белых списков», чтобы разрешить запуск только отдельных приложений
- Интеграция с консолью McAfee ePO для централизованного управления ИТ-средой
- Защита устаревших систем, например, Microsoft Windows NT and 2000

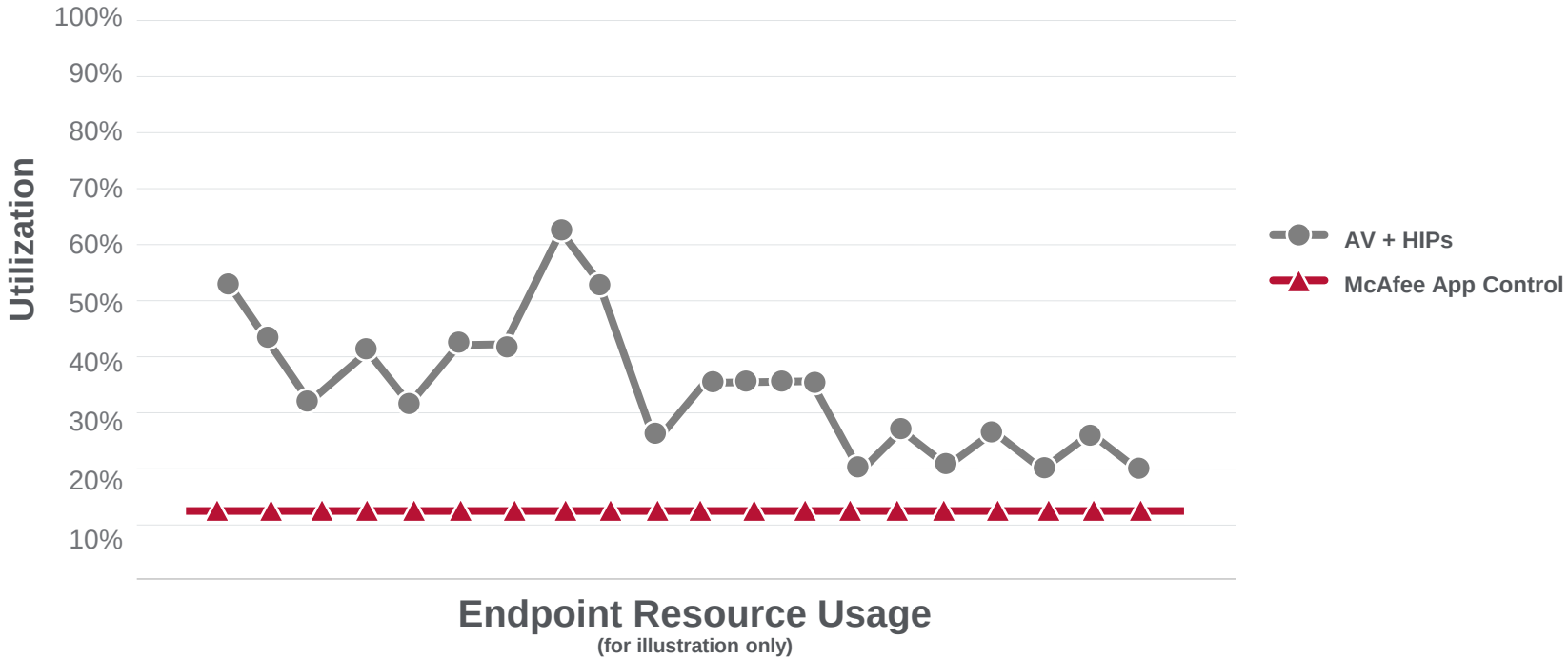
McAfee Application Control обеспечивает полную защиту от нежелательных приложений и кода (блокирует угрозы без необходимости обновлять сигнатуры.

- Защита против «атак нулевого дня» без обновления сигнатур
- Усиление безопасности и снижение затрат с использованием динамических «белых списков»
- Автоматическое доверие к новому ПО, добавленного легитимным путём
- Гибкость для пользователей: возможность добавлять новые приложения в список разрешённых



Быстродействие

McAfee application control = low performance impact



McAfee VirusScan Enterprise

Всеобъемлющая защита конечных точек

- Защита от вирусов, червей, руткитов, Троянов и других угроз
- Проактивная защита от новых и неизвестных эксплойтов (переполнение буфера), которые нацелены на уязвимости в приложениях Microsoft
- Удобная настройка политик для управления и удаления элементов в карантине
- Поддержка пользователей Microsoft Outlook иLotus Notes
- Поддержка настольных Windows (2000, XP, Vista, 7, 8) и Windows Server (2000, 2003, 2008, 2012)

McAfee VirusScan Enterprise проактивно пресекает и удаляет угрозы, расширяет защиту на новые угрозы безопасности, снижая стоимость владения.

- Надёжное обнаружение и удаление зловредов
- Проактивная защита от атак «нулевого дня»
- Интеграция с McAfee GTI для защиты в режиме реального времени
- Управляется с помощь. ePO для развёртывания, настройки, применения и отчётов
- Оптимизировано для быстродействия и снижения нагрузки на систему

Combined Detection Rates

	Exploit	Evasion	Combined
McAfee	97%	100%	99%
Symantec	91%	100%	96%
Sophos	88%	97%	93%
Kaspersky	92%	92%	92%
F-Secure	79%	88%	84%
Microsoft	65%	100%	83%
AVG	76%	88%	82%
ESET	71%	92%	82%
Trend	73%	53%	63%
Norman	47%	75%	61%
Panda	41%	75%	58%

NSS Labs Protection & Evasion Test 2013: (VSE/HIPS/SAE)

McAfee Host IPS

Всеобъемлющая защита конечных точек

- Поведенческий анализ – защита от атак «нулевого дня»
- Снижает необходимость срочной установки патчей
- Обеспечение выполнения приложениями только легитимных действий
- Возможности защиты от уязвимостей практически на 100% защищают возможные уязвимости в инфраструктуре Microsoft

McAfee Host Intrusion Prevention for Desktop предоставляет невероятный уровень защиты от известных и неизвестных угроз типа «нулевого дня», комбинируя использование сигнатуры и поведенческой системы предотвращения.

- Назначьте полноценную защиту IPS покрытие угроз «нулевого дня» на всех уровнях: сеть, приложения и исполняемый код
- Расширенная защита от угроз на основе мощного настольного межсетевого экрана
- Единое и унифицированное управление с помощью ePO
- Установка патчей – не такая уж сложная и срочная задача
- Правила могут обнаруживать угрозы на основе географического расположения


intel
Security