Решения McAfee для обеспечения безопасности мобильных пользователей

Чернышев Михаил,
McAfee

Cloud & Mobility CONFERENCE

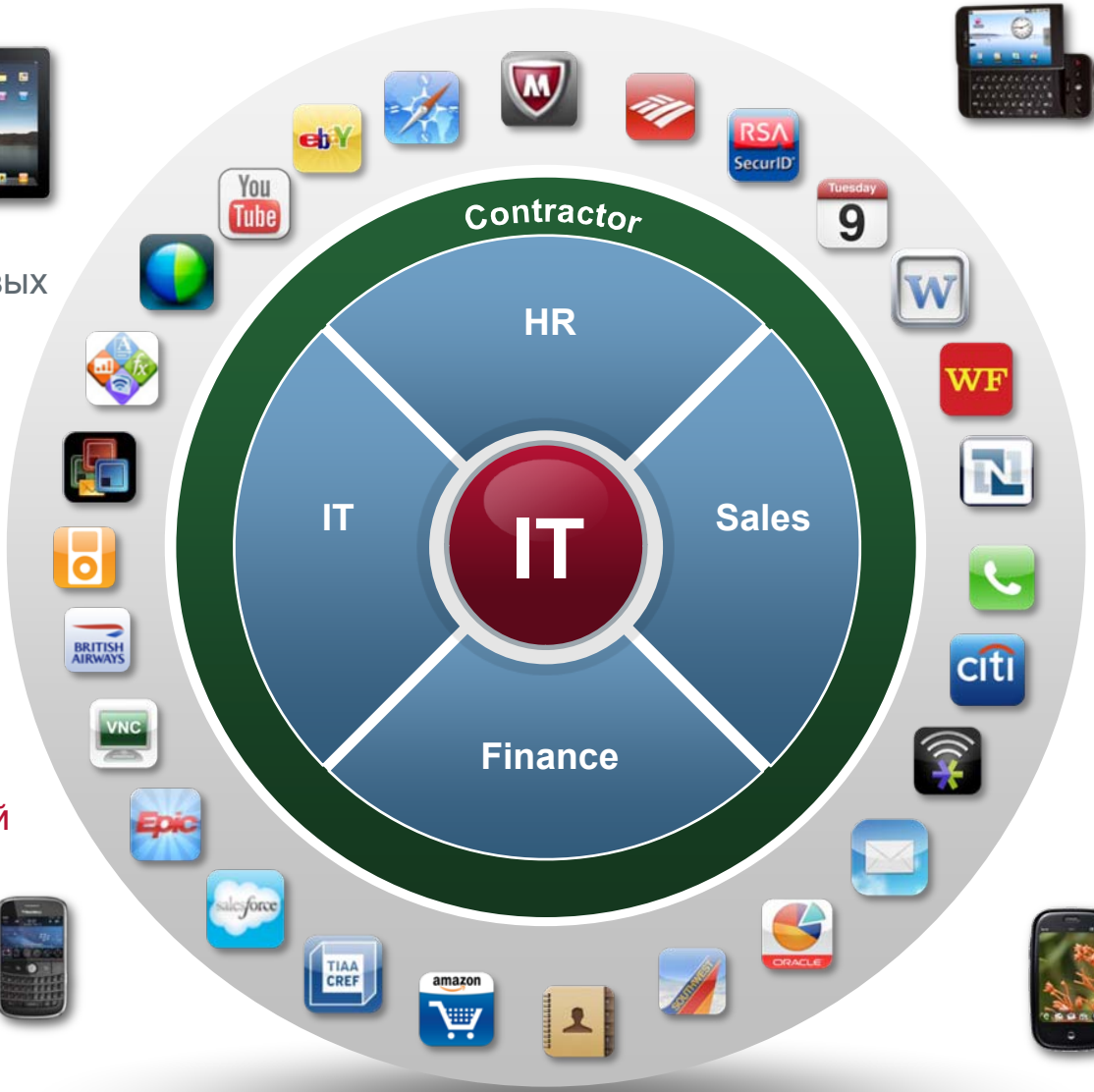
Сообщество развивается!

И продолжает развиваться!

Мобильные пользователи ставят новые задачи для ИТ
Web 2.0, Apps 2.0, Mobility 2.0

Порядка 60,000 новых образцов вирусов/день

Мобильные устройства – новый фронт для атак



Более половины пользователей не блокируют свои наладонники

ИТ обеспокоено **Утерей** данных

Арсенал мобильных пользователей

Мобильные устройства

1

Ноутбуки

2

Требования для безопасного использования мобильных устройств

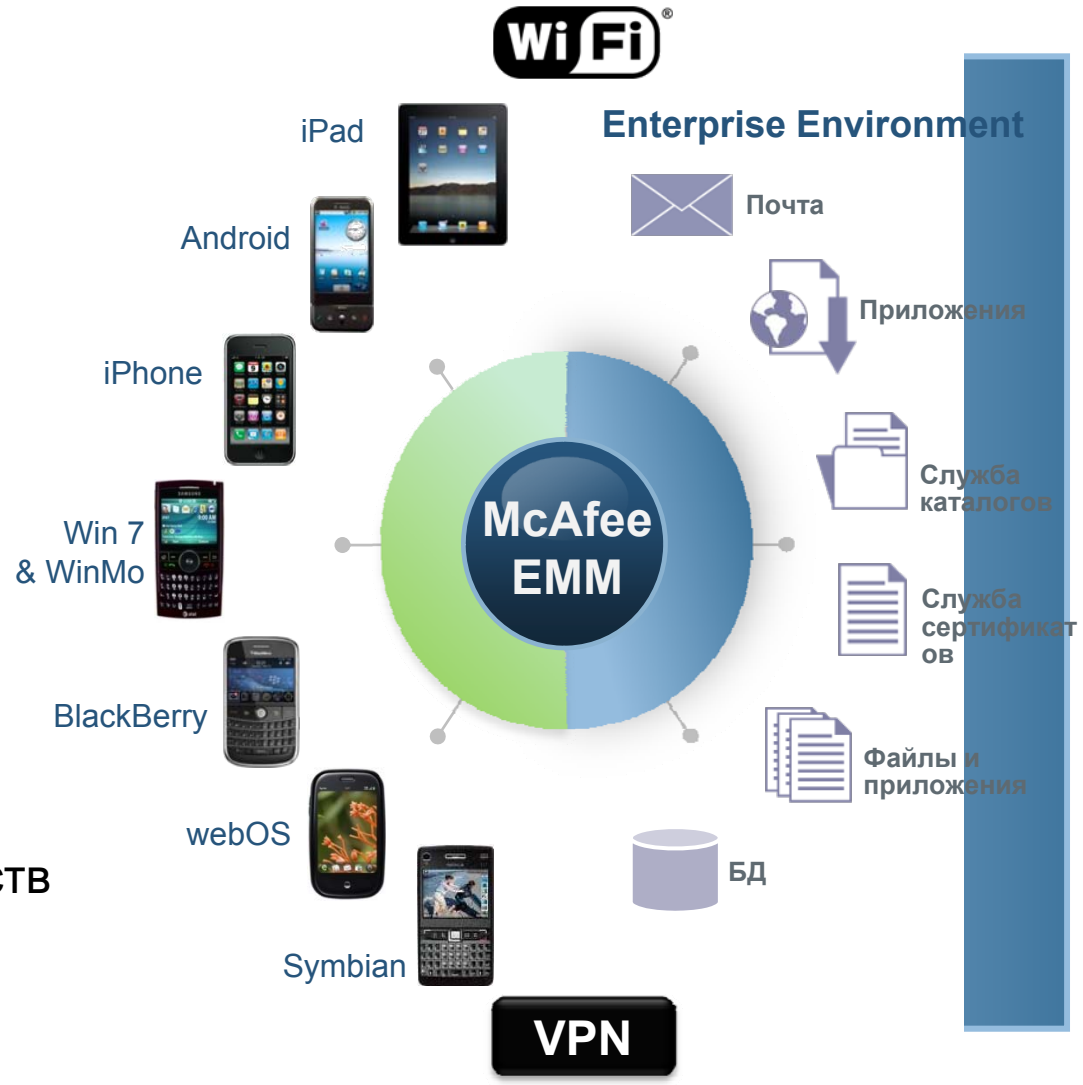
Необходимо:

- Защита данных
- Соответствие
- Аутентификация

- Безопасное управление политиками
- Self-Service
- Управление корпоративными приложениями

Включаем корпоративную мобильность

- **Безопасность**
  - Управление настройками безопасности
  - Подтверждение соответствия
  - Централизация управления (ePo)
  - Интеграция с ИТ инфраструктурой
  - Антивирус
- **Простота**
  - Простое управление из ePo
  - self-service при установке
  - Персонализация устройств
- **Масштаб**
  - От десятков до тысяч устройств
  - Отказоустойчивые и масштабируемые режимы развертывания



Жизненный цикл управления мобильными устройствами

Управление корпоративными приложениями
Безопасный доступ к приложениям **на основе ролей**. Скачивание приложений, ссылки на third-party рынки, и веб-ссылки.

Установка
На основе политик ИБ, доступа по сети и ресурсов; использование self-service для установки.

Служба поддержки
визуализация и управление централизованно из McAfee ePolicy Orchestrator

Безопасность и аутентификация
Поддержка аутентификации в Microsoft CA.
Поддержка двухфакторной аутентификации

Соответствие
автоматическая проверка перед предоставлением доступа

Управление политиками
удаленное распространение задач helpdesk и политик «по-воздуху»

Аутентификация на основе PKI

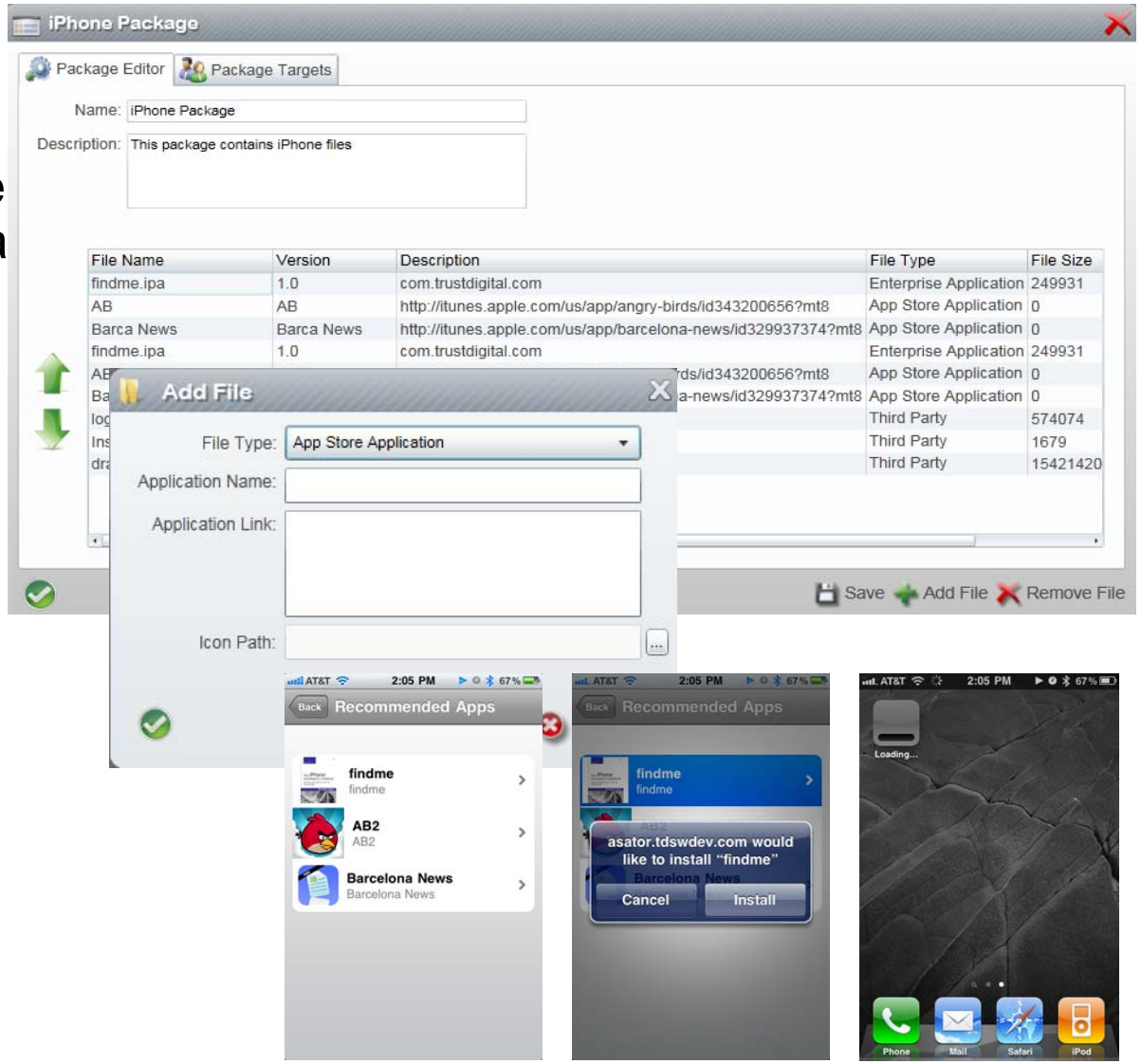
Стандарт безопасности: Microsoft CA

Достоинства:

- Безопасность на основе индустриального стандарта
- Сильная аутентификация при доступе к службам коммуникации VPN, Wi-Fi
- Сильная аутентификация при доступе к эл.почте и другим приложениям
- Поддержка SSO
- Слабое влияние на расход батареи

Корпоративный портал приложений

- Публикация рекомендованных приложений на основе группы, роли, или типа устройства
  - Приложения собственной разработки
  - Third-party приложения (Apple App Store / Android Marketplace)
  - Вебклипы
- Инвентаризация и аудит установленных приложений

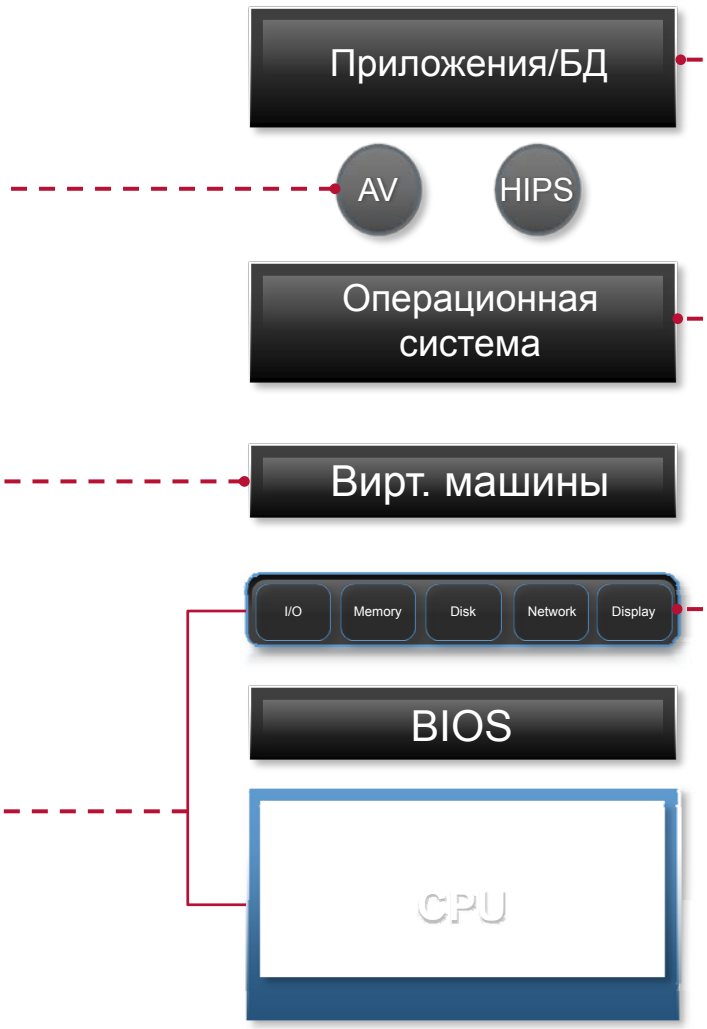


Ноутбуки – «старое» и новое в защите

Традиционные средства защиты McAfee

	EPS	EPA	TEB	TPE
Центральная консоль управления				
Анти-вирус				
Защита почтового сервера				
Настольный брандмауэр				
Безопасный серфинг Web				
Защита от шпионского ПО				
Настольный IPS				
Контроль доступа к сети				
Аудит политик безопасности				
Контроль устройств				
Фильтрация Web				
Шифрование данных				
Кроссплатформенность				

“Stealth” технологии идут в обход



Запуск традиционных видов атак на прикладном уровне

Атака и отключение всех средств традиционной защиты

ОС инфицируется вследствие действий APT

Компрометация всех гостевых виртуальных машин

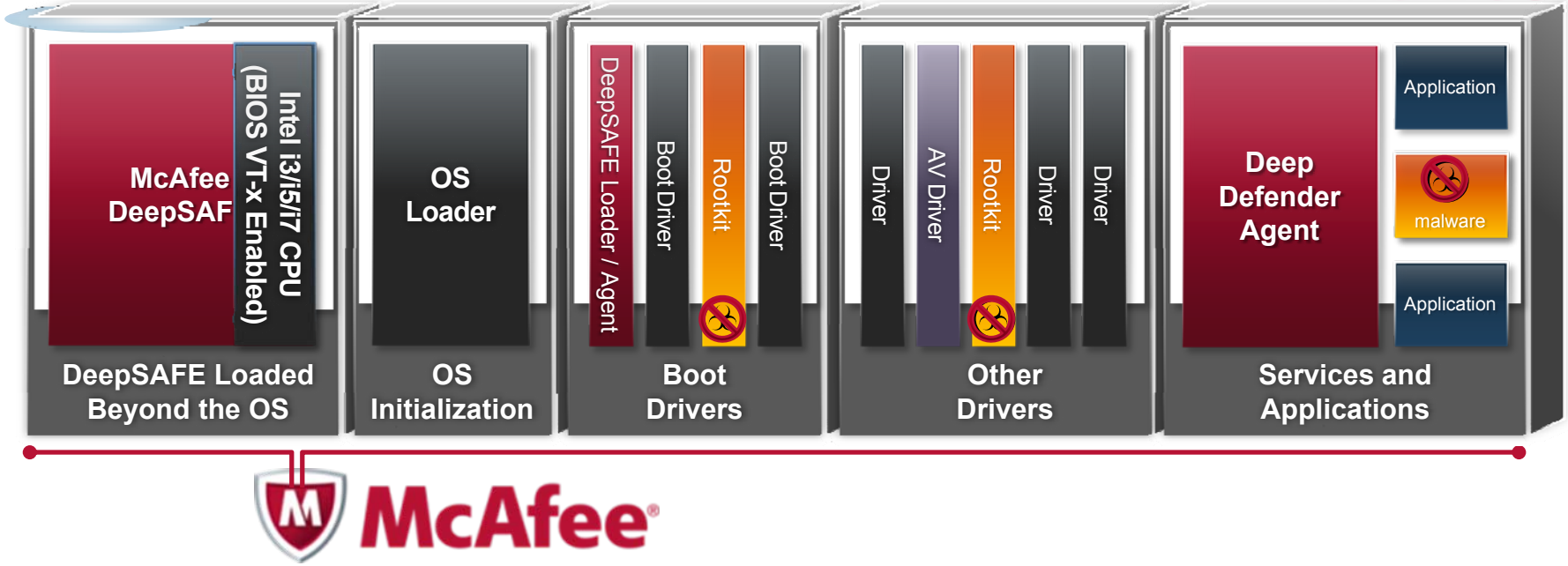
Вредоносное firmware в состоянии обойти все меры безопасности

“Точечные APT атаки” компрометируют устройства в момент поставки или до нее

Немного статистики по «невидимкам»

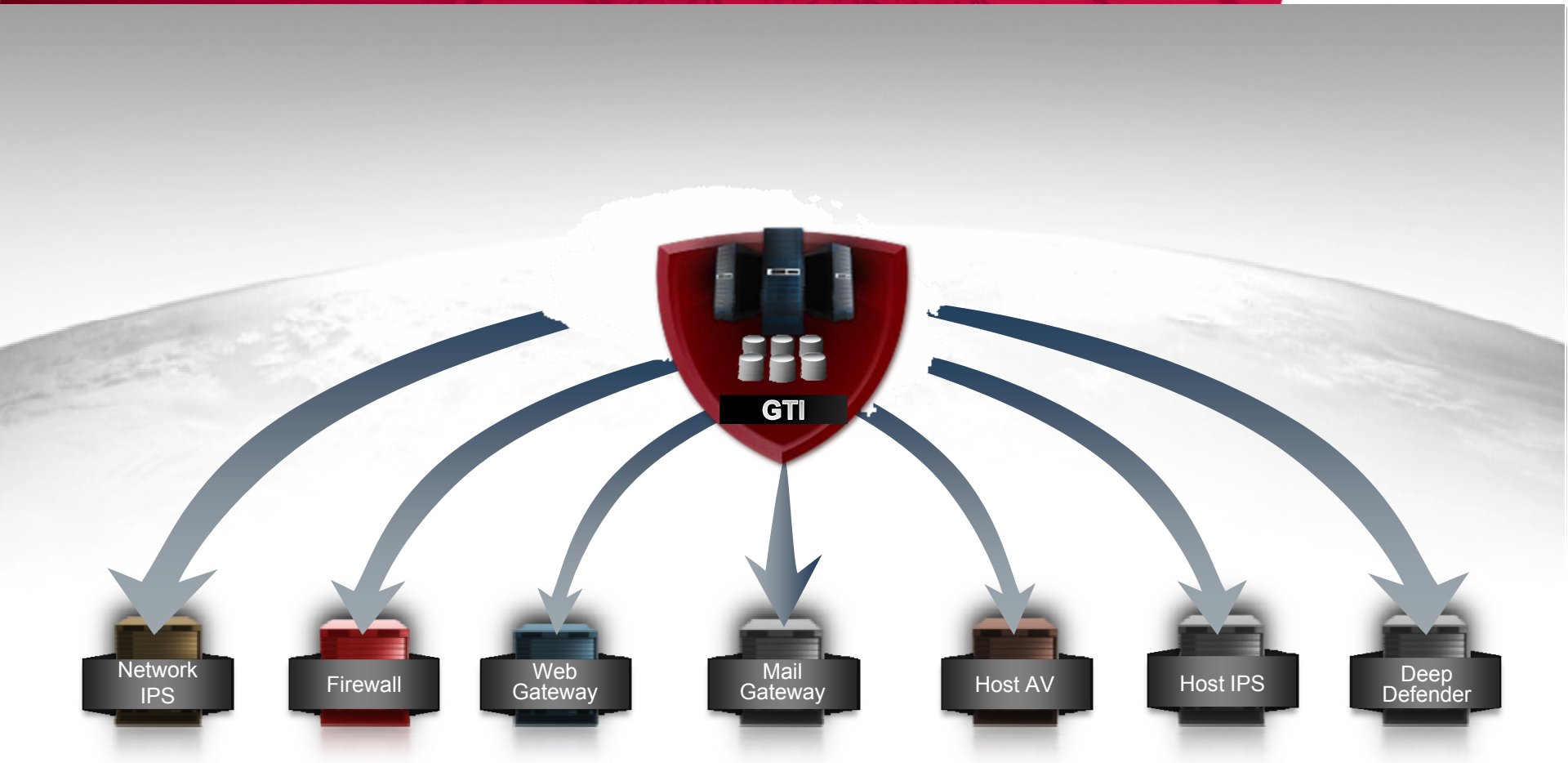
- «Невидимки» подсаживают вредоносное ПО
- Спроектированы так, чтобы быть незаметными для традиционных средств
- Используются кибер-преступниками для кражи данных
  - 110,000 новых руткитов/квартал
  - 1,200 новых руткитов/день
- Большинство вредоносного ПО использует руткиты для скрытия
  - Stuxnet (Иран. Индия)
  - Koobface быстро превращает систему в бота
  - SpyEye - инструментарий для разработки собственных руткитов
  - TDSS – семейство руткитов, которое не детектируется на всех ОС независимо от средств безопасности

Deep Defender— остановка для Stealth'ов



- Мониторинг памяти на уровне ядра в реальном времени
- Идентификация руткитов на уровне ядра
- Предотвращение загрузки фальшивых драйверов
- DeepSAFE технология загружается до ОС
- DeepSAFE информирует Deep Defender о подозрительном поведении

Deep Defender дополняет Global Threat Intelligence



Это только часть комплексного подхода McAfee

Управление ИБ

Управление политиками
Отчетность
Управление моб.устройствами
Управление уязвимостями
Управление рисками
Соответствие

Безопасность сети

МСЭ нового поколения
Предотвращение вторжений
Шлюз NAC
Мониторинг аномальных действий пользователей
Сетевой мониторинг угроз

Безопасность контента

Email Gateway
Web Gateway
Data Loss Prevention
Encryption

Защита конечных точек

Mac, UNIX/Linux AV
Virtual Desktop
Virtual Server
Mobile Devices

Anti-Virus & Anti-Spyware
Host Intrusion Prevention
Endpoint Encryption
Application Whitelisting

Desktop Firewall
Device Control
Policy Auditing
NAC Endpoint

Email Server AV & Anti-Spam
SharePoint Protection
Website Reputation

реализация
ПО
Устройства
SaaS
Виртуализация

Open Security Platform
Security Innovation Alliances
Global Strategic Alliances
McAfee Connected
Security Alliances


McAfee®