McAFEE Security | SNIFFER Technologies | MAGIC Solutions

networkassociates.com

Безопасность и эффективность работы корпоративных сетей – комплексные решения Network Associates

Сергей Савинов, директор по маркетингу компании Обинко Технологии

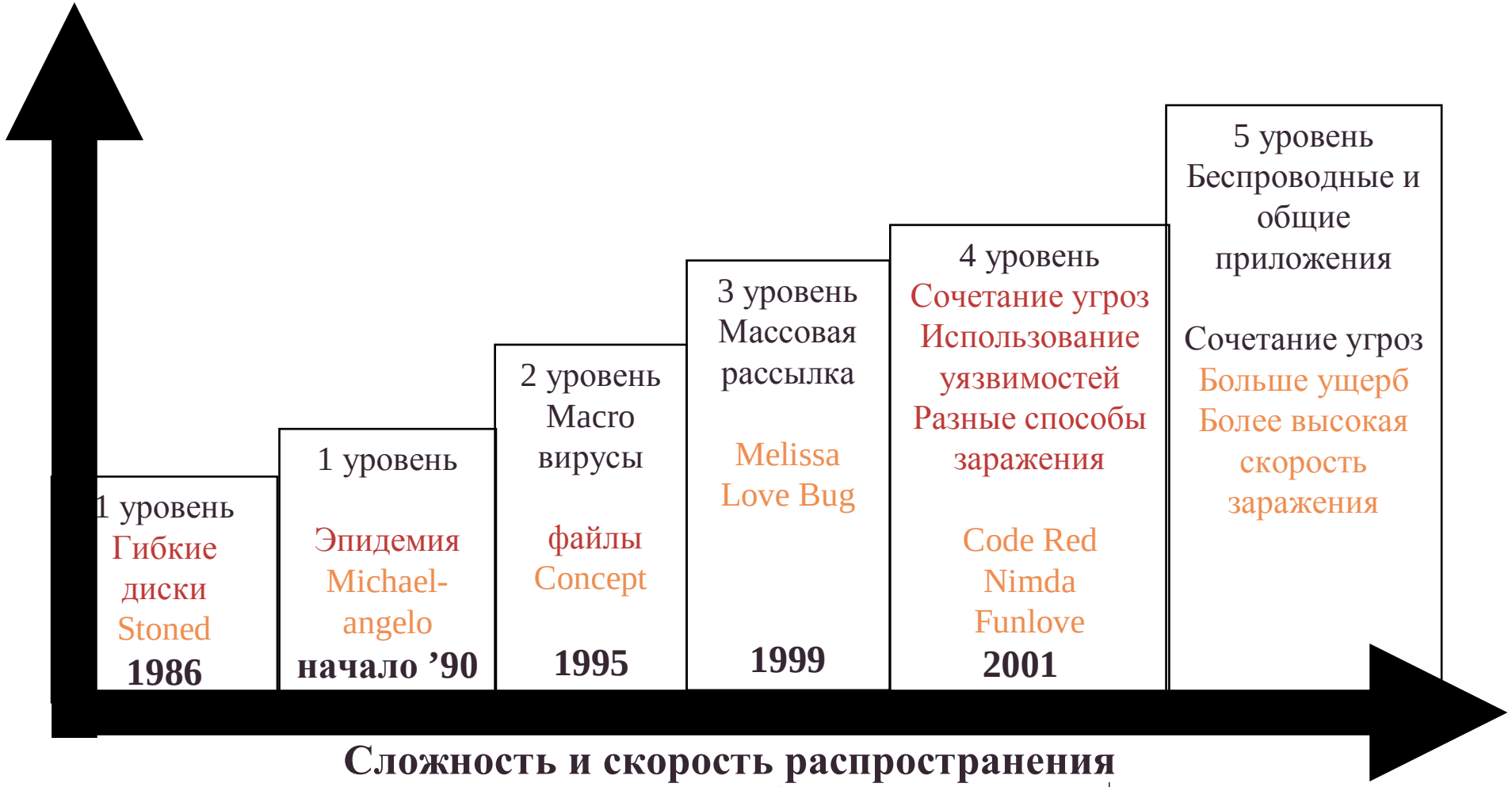
Network ASSOCIATES

YOUR NETWORK. OUR BUSINESS.

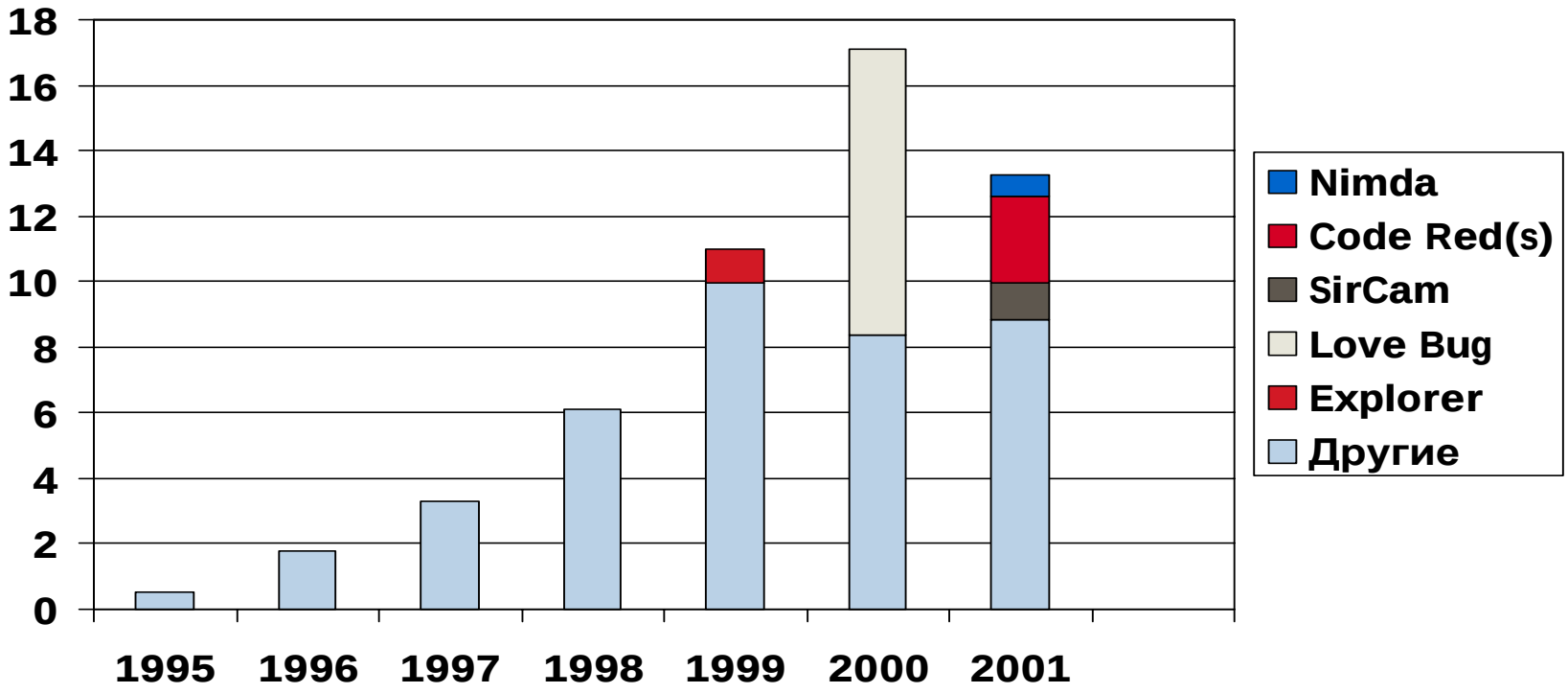
Network Associates – кто это?

-Основана как McAfee Associates в 1989. Network Associates, Inc. Создана в результате слияния McAfee Associates и Network General в 1997.
-8 по размеру разработчик ПО
-Оборот в 2001 - $834 млн, ежеквартальный рост 24%
-Участник рейтинг *Network World's* "Top 10 Most Powerful Companies in Networking"
-McAfee: 70 миллионов пользователей, 60% корпоративных закзачиков
-Sniffer: 70% рынка LAN, 90% рынка WAN

Вирусная угроза – эволюция ущерба



Затраты на ликвидацию вирусных эпидемий (в миллиардах долларов)



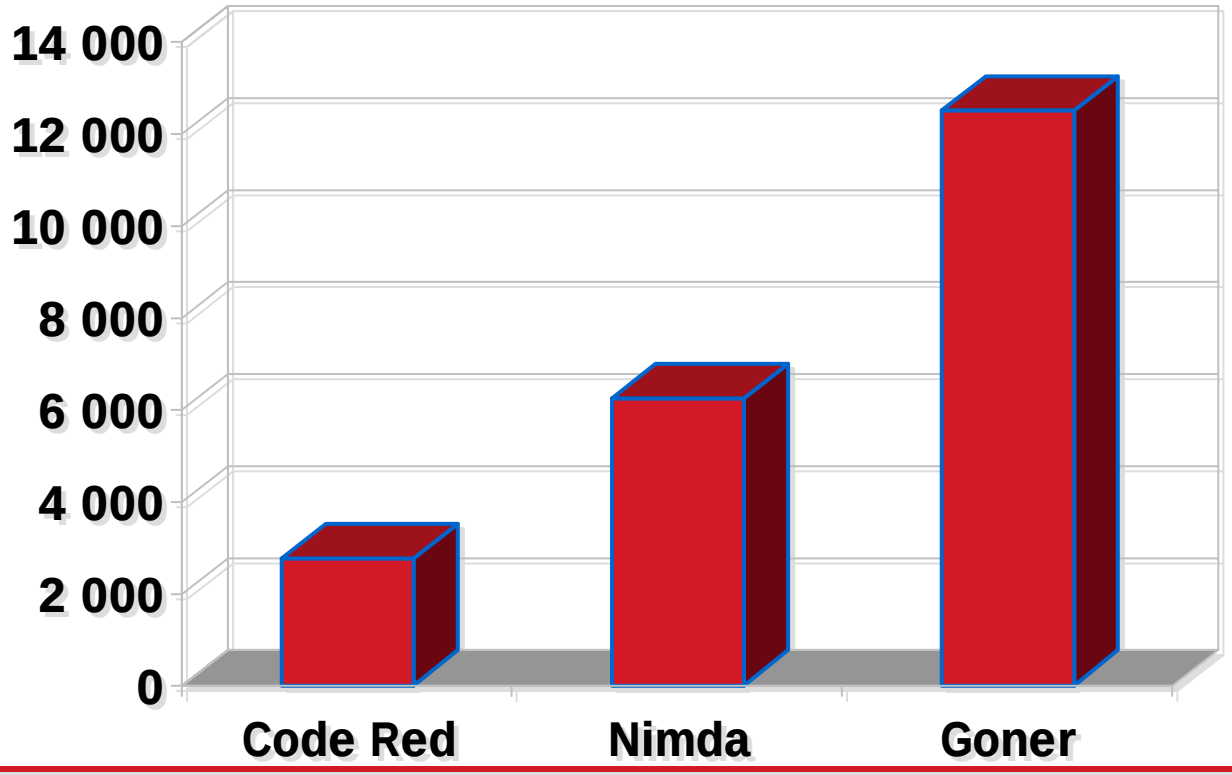
источник: Computer Economics, January, 2002

“1 закон McAfee”

Время, необходимое вирусу для нанесения максимального ущерба, сокращается в 2 раза каждые 18 месяцев

Вирусы распространяются все быстрее

Средняя скорость заражения в час

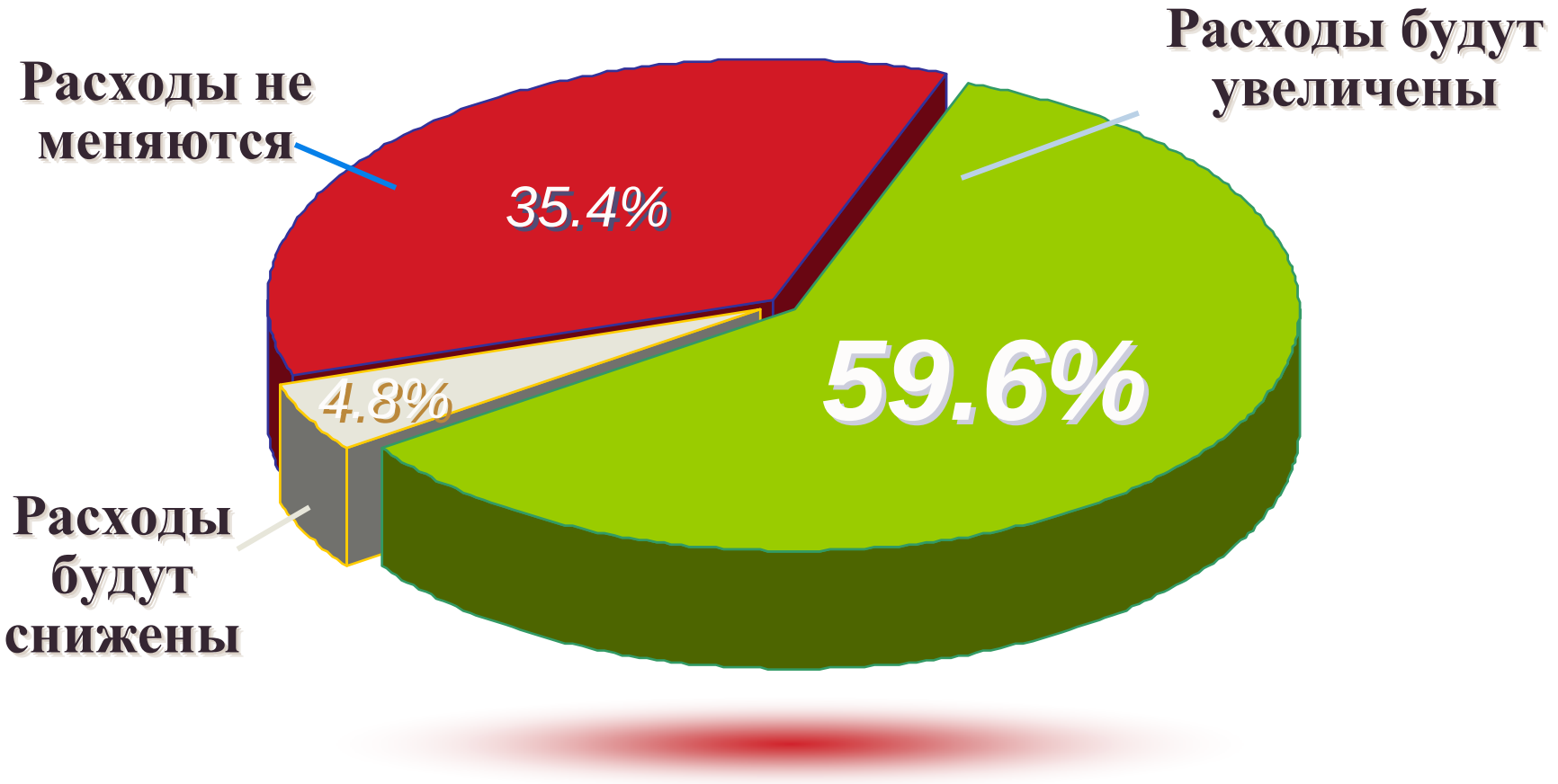


источник: McAfee AVERT 2001-2002

Вероятность заражения увеличивается

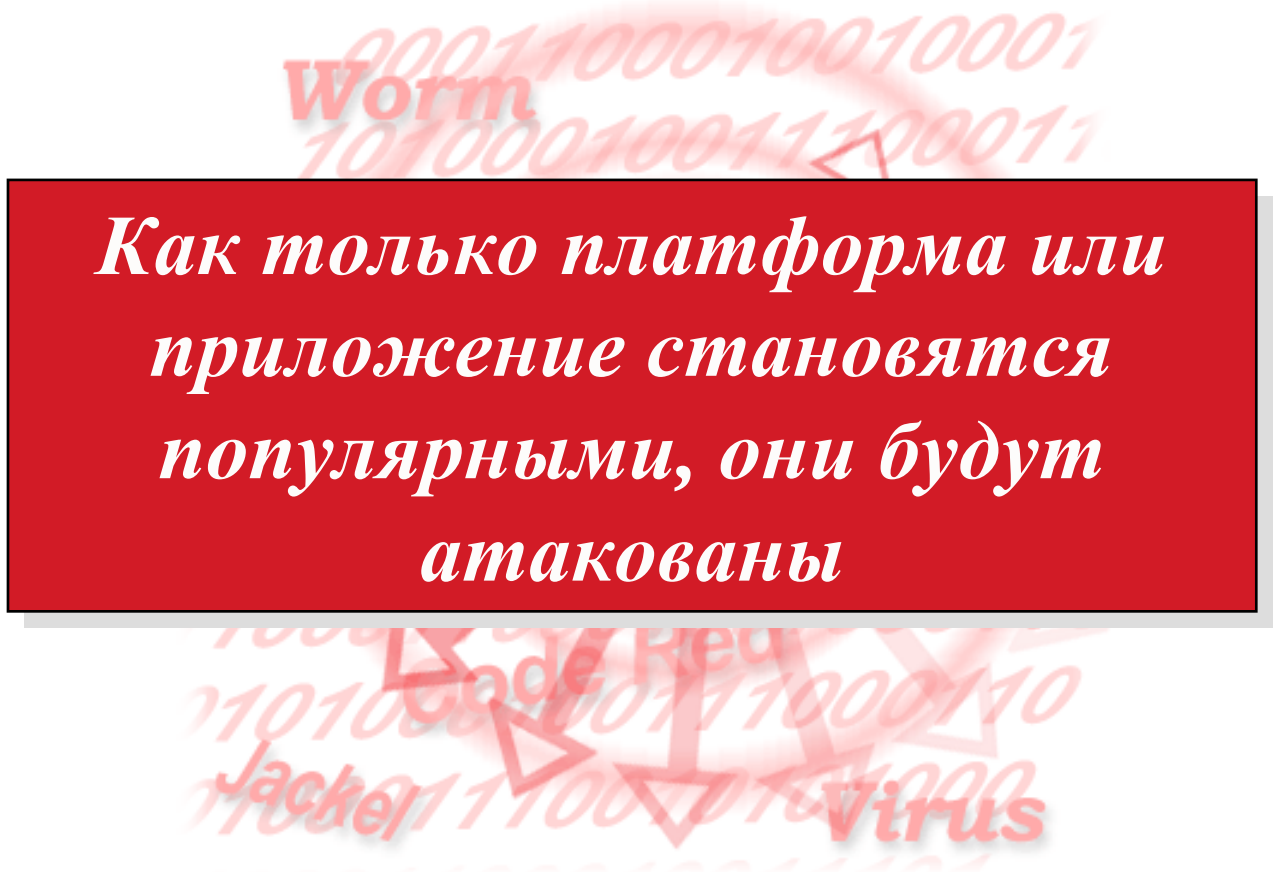
источник: NIPC 2001

Реакция: изменение расходов на безопасность



источник: CIO Magazine 2002

“2 закон McAfee”

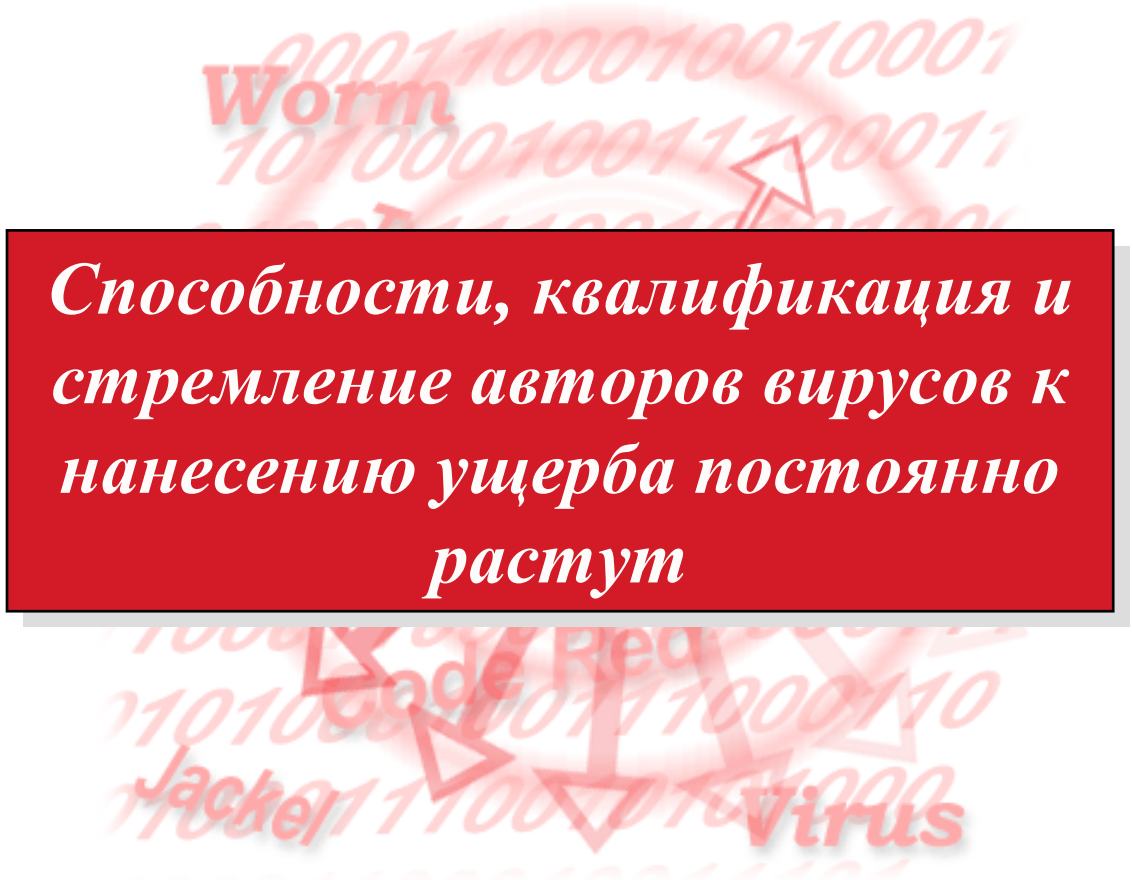


Как только платформа или приложение становятся популярными, они будут атакованы

Вирусы на ладони

- **Personal Digital Assistants [PDA's]**
- **Угроза корпоративным сетям**
- **Первые вирусы для PDA**
  - **Liberty [trojan]**
  - **Vapor [trojan]**
  - **Phage [virus]**

“3 закон McAfee”



Способности, квалификация и стремление авторов вирусов к нанесению ущерба постоянно растут

Комбинированные угрозы

- **Code Red**
  - **Сочетание «трояна», «червя» и уязвимости платформы**
  - **Ущерб $2.65 миллиарда**
- **Nimda**
  - **Сочетание массовой рассылки, «трояна» с удаленным доступом и предыдущих вирусных атак (использовал остатки Code Red для распространения)**
  - **Ущерб $635 миллионов**

источник: Computer Economics 2001

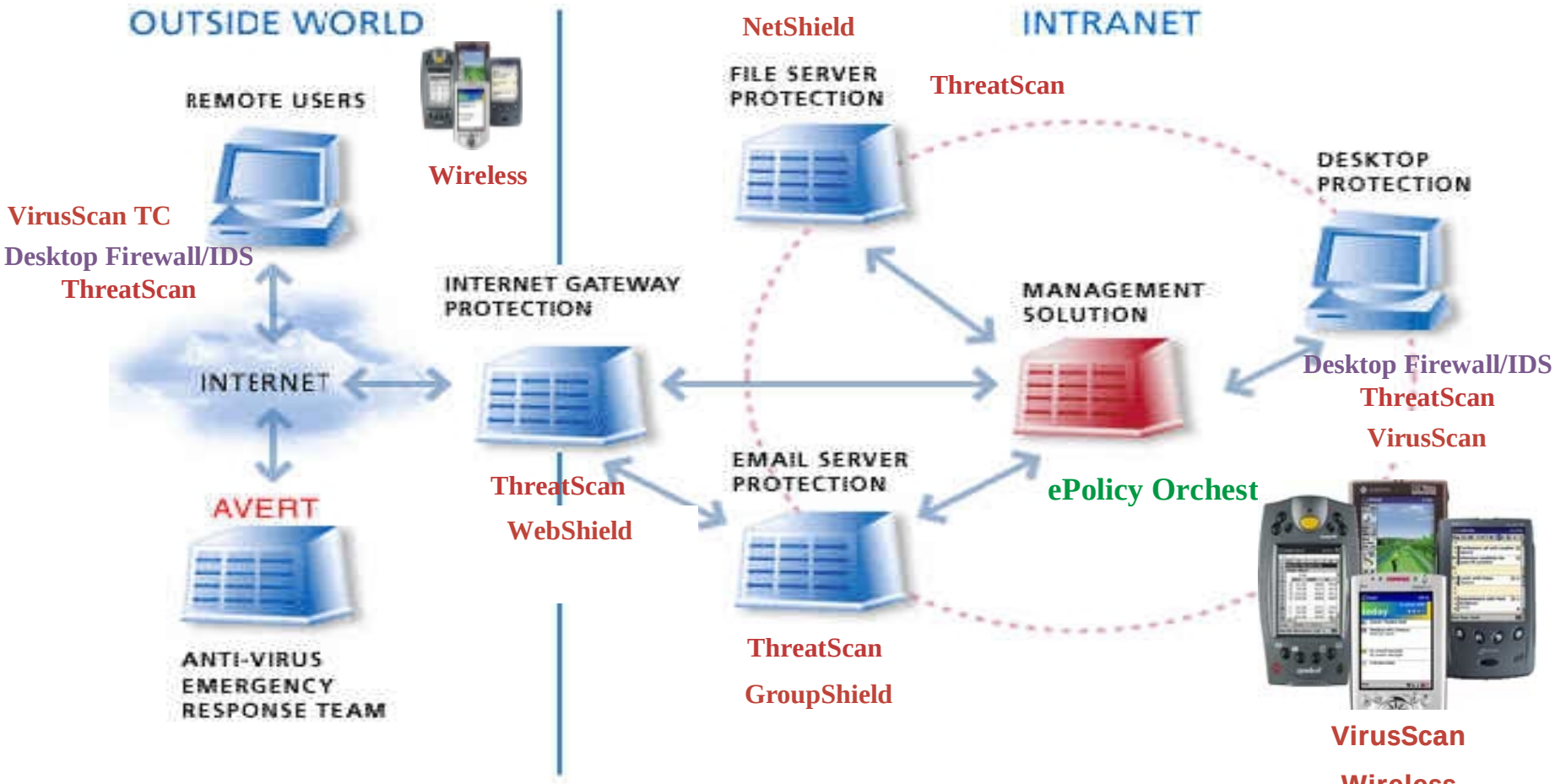
Усложнение угроз ведет к объединению средств защиты

Классических средств определения и отражения атак уже недостаточно

Новые подходы к антивирусной защите

- Эвристический анализ
- Сканирование контента
- Комбинированные решения защиты
  - ePolicy Orchestrator / Desktop Firewall
  - ePolicy Orchestrator / ThreatScan
- Sniffer

Решение McAfee



Active Virus Defense

Защита на каждом уровне

Управление:	**ePolicy Orchestrator**
Десктопы:	**VirusScan, VirusScan TC**
Сервера:	**NetShield**
Почта:	**GroupShield**
Internet шлюз:	**WebShield**
Ноутбуки:	**VirusScan TC**
Wireless:	**VirusScan Wireless**
Поддержка:	**PrimeSupport options**

VirusScan 4.5.1

- Контроль всех типов вирусов, проверка почтовых сообщений и файлов, передаваемых по Internet
- Частичное обновление продукта (только изменения)
- Широкий спектр опций администрирования
- Защита конфигурации паролем
- Не требуется перезагрузки после обновления
- Многоплатформенность
  - Windows 3.x, 9.x, Windows NT, 2000, ME, XP
  - Сканер для DOS, Unix - AIX, HP, Linux, SCO Solaris, BSD
  - Virex для Macintoh

VirusScan Thin Client (TC)

- Тонкий клиент
- Низкая нагрузка на сеть
  - Только 4 MB
  - 1/5 от конкурентных решений
- Невидим для пользователя
- Управление только через ePolicy Orchestrator
- Поддержка Win 9x, NT, 2000
- Для рабочих станций и серверов
- Устанавливается любым инструментом дистрибуции ПО

NetShield 4.5

- Контроль всех типов вирусов, проверка почтовых сообщений и файлов, передаваемых по Internet
- Частичное обновление продукта (только изменения)
- Широкий спектр опций администрирования
- Защита конфигурации паролем
- Windows NT, 2000, Novell
- Удаленное управление сервером
- Не требуется перезагрузки после обновления

GroupShield 4.5 / 5.0

- Сканирование папок (частных и общих) и сообщений
- Использует новые MS-API
  - надежность
  - Повышенная производительность
  - Поддержка Microsoft
- Автоматическое обновление вирусных баз
- Outbreak Manager
- Microsoft Exchange Server 5.x5 , 2000
- Lotus Notes 4.5, 4.6 & 5

GroupShield 5.0

- Поддержка Microsoft Exchange VSAPI 2
  - Извещение отправителя/получателя
  - Сканирование тела сообщения
- Высокая производительность
  - Сканирование в фоновом режиме
  - Меньше загрузка процессора
- Поддержка кластеров «Active-active»
  - Полная поддержка «cluster API»
  - Конфигурирование по виртуальным серверам
- Фильтрация по заголовку сообщения

OutBreak Management

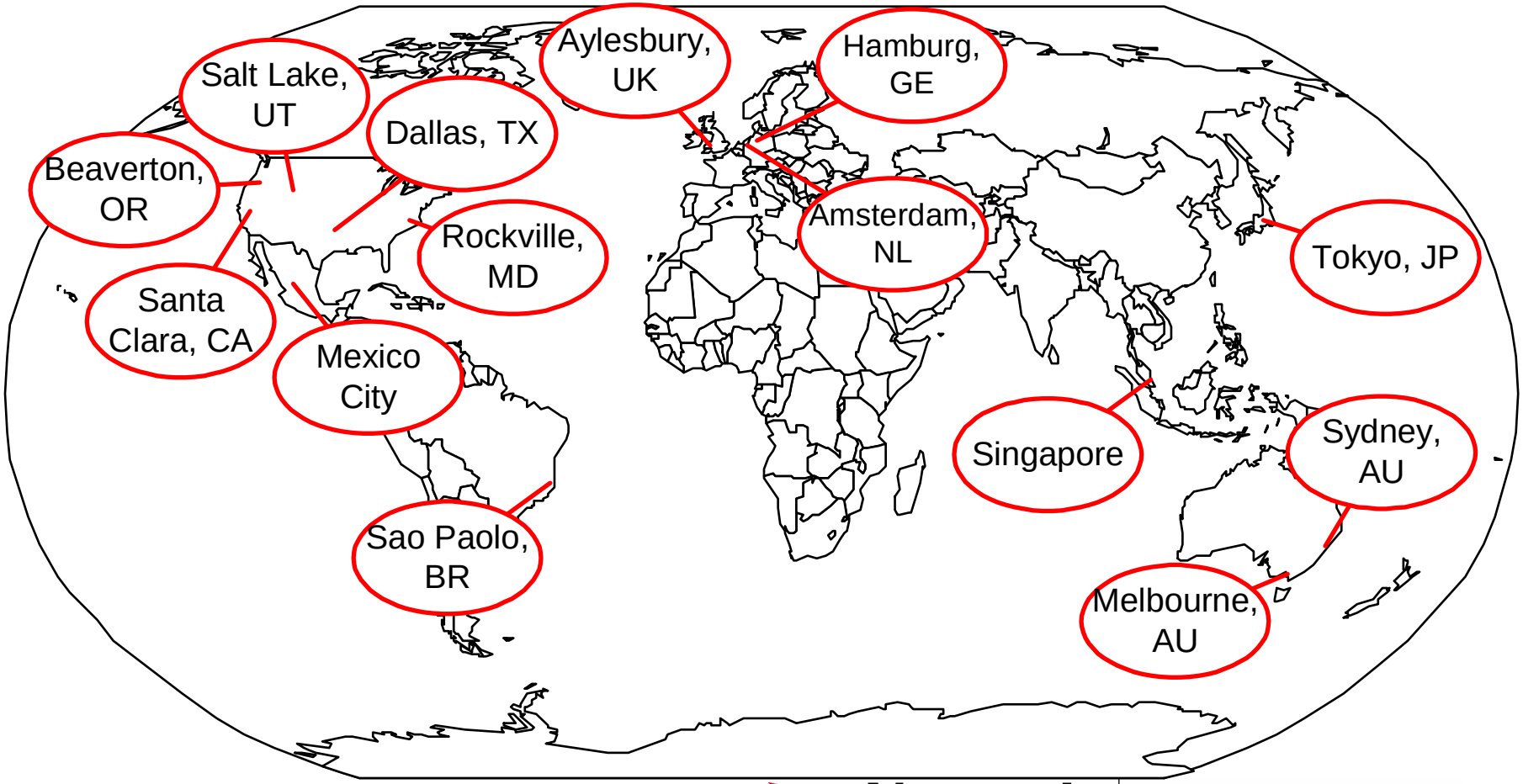
OutBreak Manager & Alerting – больше чем просто извещение об обнаружении/удалении вируса

- Извещения по email, SMS, мобильному телефону, пейджеру
- Администратор определяет извещения и действия
- Проверка наличия новых вирусных баз, скачивание и установка обновлений
- Действия на сервере – остановка сервисов или сервера
- Несколько возможных вариантов действий :
  - Немедленно известить администратора по мобильному телефону
  - Через 5 минут проверить наличие новых вирусных юаз и установить их в случае наличия
  - Через 10 минут остановить сервер

WebShield

- Сканирование всего входящего и исходящего Internet трафика
- Проверка «внешней» почты (из и за пределы сети)
- Сканирование контента (заголовков и тела)
- Блокирование URL
- Автоматическое обновление вирусных баз
- Монитор нагрузки на сеть (статистика)
- Windows NT (Intel) + Sun Solaris

World Wide Technical Support



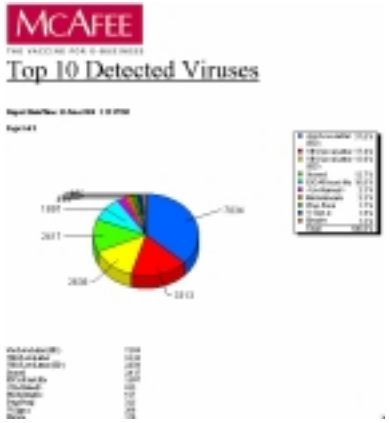
Network ASSOCIATES
YOUR NETWORK. OUR BUSINESS.

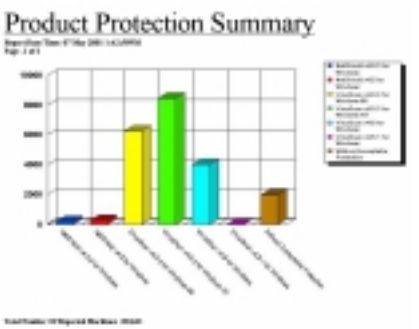
Что такое ePO ?

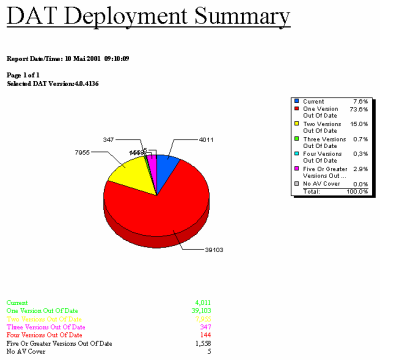
- Централизованный инструмент управления безопасностью сети
- Масштабируемость – до 250000 узлов (станций)
- Скорость – 13000 станций за 2 часа (BP)
- Поддержка гетерогенных продуктов McAfee (антивирусы и системы безопасности)
- Иерархическое управление политикой безопасности для антивирусов McAfee и Symantec
- Подробные графические отчеты:
  - Степень антивирусной защиты
  - Степень заражения сети

ePO - снижение TCO

- Мониторинг антивирусной активности
  - Отслеживание вирусных эпидемий вплоть до источника
  - Обнаружение уязвимостей в антивирусной защите
- Поддержка актуальной антивирусной защиты
  - Установка еженедельных/срочных обновлений и сервис паков
  - Низкая загрузка сети
- Централизованный контроль и выполнение политики
  - Блокирование действий пользователей по отключению защиты
  - Адаптация к новым угрозам
  - Управление по любому протоколу (NetWare, NT, Internet)
  - Клиент для всех Windows платформ
- Управление и отчетность по продуктам Symantec
  - NAV 5.x, 6.x, 7.x - Отчеты об актуальности продуктов
  - NAV 7.5 – Управление политикой защиты для настольных компьютеров и серверов







Проблема: обеспечить постоянную актуальность защиты

Уязвимости в программных продуктах – черный ход для вирусов

- **что это за уязвимости?**
- **на каких компьютерах есть уязвимости?**

Уязвимые приложения выполняются в сети

- **Как узнать об этих приложения? Где они находятся (telnetd, ftpd, IIS)?**
- **Как понять, что компьютер уязвим к новому вирусу и как его защитить от этого вируса (типа вирусов)?**
- **Где можно найти уязвимости и как их исправить?**

Обнаружение уязвимостей и их исправление

- **как можно гарантировать защищенность сети от атаки через черный ход?**
- **Где находятся компьютеры, зараженные через черный ход?**

Информация об уязвимостях – ключ к успешной защите сети

McAfee ThreatScan 2.0

Предпреждение угрозы

- **Обнаружение и ликвидация уязвимостей до проникновения виурсов**

Информация о сети

- **Полные сведения об уровне антивирусной защиты, всех компьютеров, подключенных к сети**

Снижение уровня эпидемии

- **Определение компьютеров с признаками заражения**

Графические отчеты средствами ePo

Снижение TCO:

- **Использование всех возможностей ePO**
- **Более эффективная защита**
- **Снижение расходов на ликвидацию последствий эпидемий**

McAfee Desktop Firewall 7.5

Остановливает враждебный код и атаки хакеров:

- **Пропускает только указанный трафик**
- **Не допускает соединения с неавторизованными приложениями**
- **IDS определяет внешние и внутренние атаки (50-70% атак – внутренние)**
- **Предотвращает распространение враждебных программ (зомби-кода, «троянов» и т.д.)**
- **Основан на PGPfire**
- **Устанавливается и управляется через ePo**

Sniffer Technologies

- **Оптимизация работы корпоративных сетей**
- **Постоянный контроль и предупреждение проблем**
- **Передовое решение для обеспечения безотказной работы критически важных сетей**
- **95% Fortune 100, 75% рынка**
- **«Инструмент №1» (Gartner Group)**

Network Magazine PRODUCT OF THE YEAR 2001
Network Magazine PRODUCT OF THE YEAR 2000
Network Magazine PRODUCTS OF THE YEAR 1999
Network Magazine PRODUCTS OF THE YEAR 1998
Network Computing EDITOR'S CHOICE
PC WEEK LABS ANALYST'S CHOICE

2001 Network Computing WELL-CONNECTED AWARDS

Sniffer Distributed
"Network Analyzer of the Year" Award 2001

Sniffer Portable
"Top 10 Products of the Decade" 2000

Network ASSOCIATES | YOUR NETWORK. OUR BUSINESS.

Sniffer Technologies

- Максимальная производительность сети
- Критерий «стоимость-эффективность»
- Определение рисков в безопасности
- Гарантия надежной работы и выдерживания пиковых нагрузок
- Интеграция с основными системами сетевого управления

Sniffer и безопасность данных

- **Дополнительный сервис для информационной безопасности**
  - **Расширение возможностей систем защиты информации**
  - **Дополнительная информация для анализа уровня безопасности сети**
  - **Необходимый элемент для комплексного решения по обслуживанию корпоративной сети**

Sniffer и безопасность данных

- Детальная информация о сети
  - Трафик и загрузка ресурсов (определение нормы и аномалий)
- При атаке
  - Захват данных для анализа
  - Определение типов атак (DoS, взлом паролей и т.д.)
- После атаки
  - Анализ результатов работы сети по сравнению с эталоном
  - Контроль исправления замеченных аномалий

Sniffer и безопасность данных

- До установки файрвола
  - Контроль протоколов и портов (например, HTTP только на 80 порт)
  - Определение нормальной времени реакции приложений

- После установки файрвола
  - Контроль и исправление проблем с коммуникациями
  - Определение нового уровня времени реакции приложений
  - Проверка установки политик файрвола

Sniffer и безопасность данных

- Дополнение антивирусных продуктов
  - Фильтры безопасности позволяют определить машины, возможно зараженные «червем» (сокращение времени обнаружения и удаления вирусов)
  - Сравнение образцов строк данных для определения пораженных систем (определение вируса типа NIMDA)

Sniffer и безопасность данных

- Дополнение сканеров вторжений
  - Анализ проишествий в реальном времени
  - Определение источника атак
  - Определение атакованных систем
- Дополнительные функции безопасности
  - Контроль и оповещение о неудачных попытках регистрации
  - Контроль и оповещение о попытках обращения к FTP серверу
  - Контроль и оповещение о попытках взлома базы данных и попытках соединения с базой

Итак, почему McAfee?

- **Ведущие позиции в индустрии**
  - **70 миллионов пользователей, 60000 корпоративных клиентов**
- **Ведущая технология**
  - **Outbreak Manager**
  - **Thin Client**
  - **Сертификация ICSA, Checkmark, VB100, Secure Computing Best Buy, #1 в тестах Магдебургского и Гамбургского университетов**
- **Управляемость**
  - **ePO управляет и дает отчеты по всем аспектам антивирусной защиты в сети**
  - **ePO интегрирует дополнительные средства безопасности (Firewall, ThreatScan)**
- **Sniffer**
  - **Оптимизация работы сети и предупреждение проблем**
  - **Дополнение основных систем защиты информации**

+7-095-777-2628

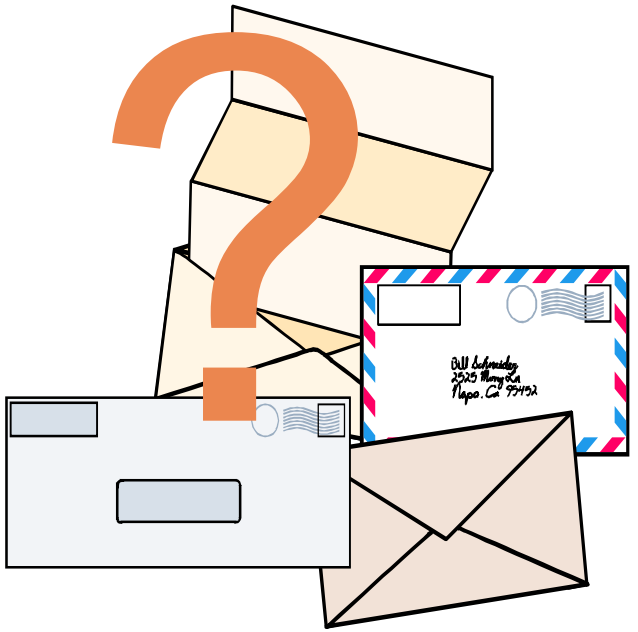
sergey.savinov@obitech.ru

www.obinko.ru

www.nai.com

www.mcafeeb2b.com

www.sniffer.com



MCAFEE