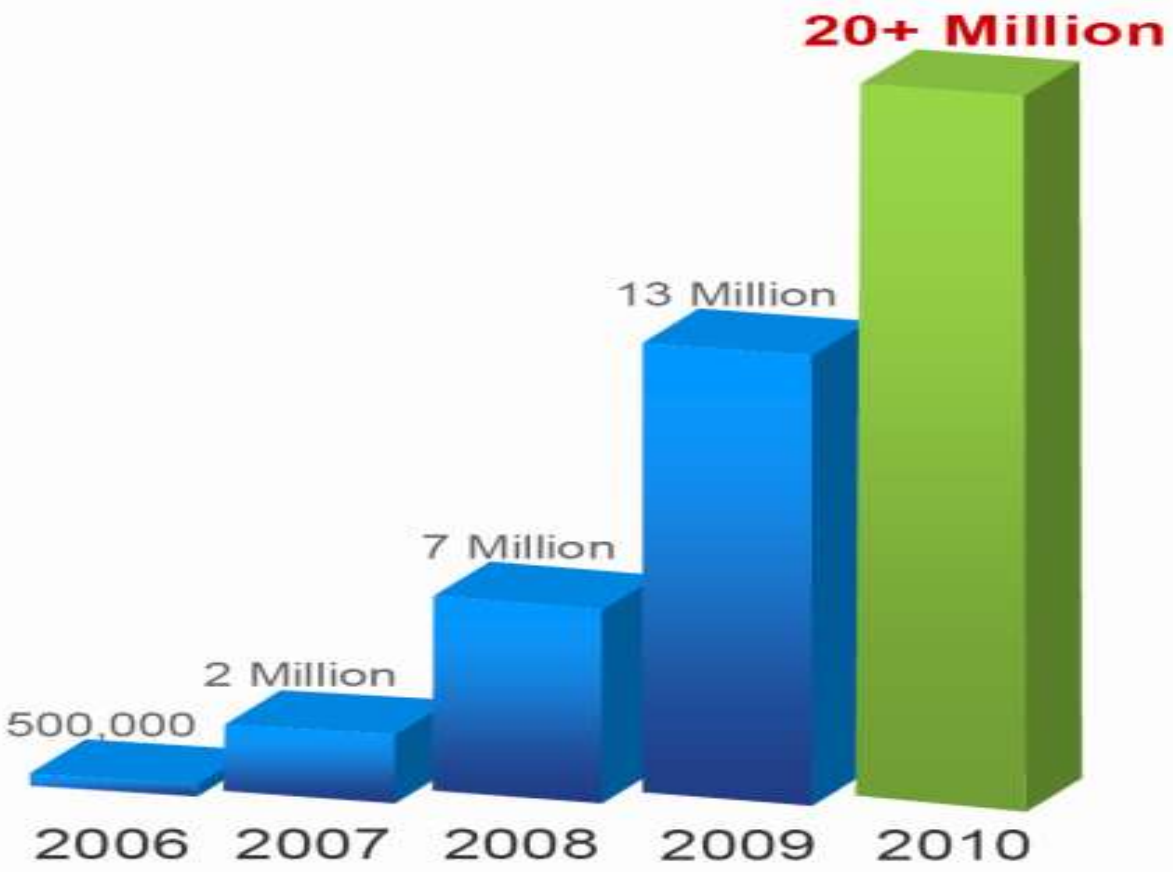
OfficeScan 10 – новая версия основного корпоративного средства защиты конечных точек

Антон Миносьян
Поликом Про

Что на повестке

- OfficeScan 10
  - Основной корпоративный продукт для защиты конечных точек (рабочих станций и серверов)
  - Версия 10 вышла в мае 2009 года
  - 05.10.2009 вышел Service Pack 1 для английской версии, для русской - ожидается

Рост числа угроз



Недостатки стандартного подхода

- Conventional scan
  - Операционная полная копия паттерна хранится на каждом клиенте
- Защита только с помощью паттерна становится неэффективной
  - Паттерны выходят достаточно редко
  - Распространение паттернов порождает сетевой трафик
  - Паттерны размещаются в памяти. Больше паттерн – больше расход памяти и время анализа файла

Технология SmartScan

- “Облачная” архитектура Smart Protection Netw
- Два
  серв
  - Inte
  - Star
    под
- Архи
  - Про
  - Sma
    пол
  - Клиенты используют репутационные запросы и интеллектуальное кэширование результатов

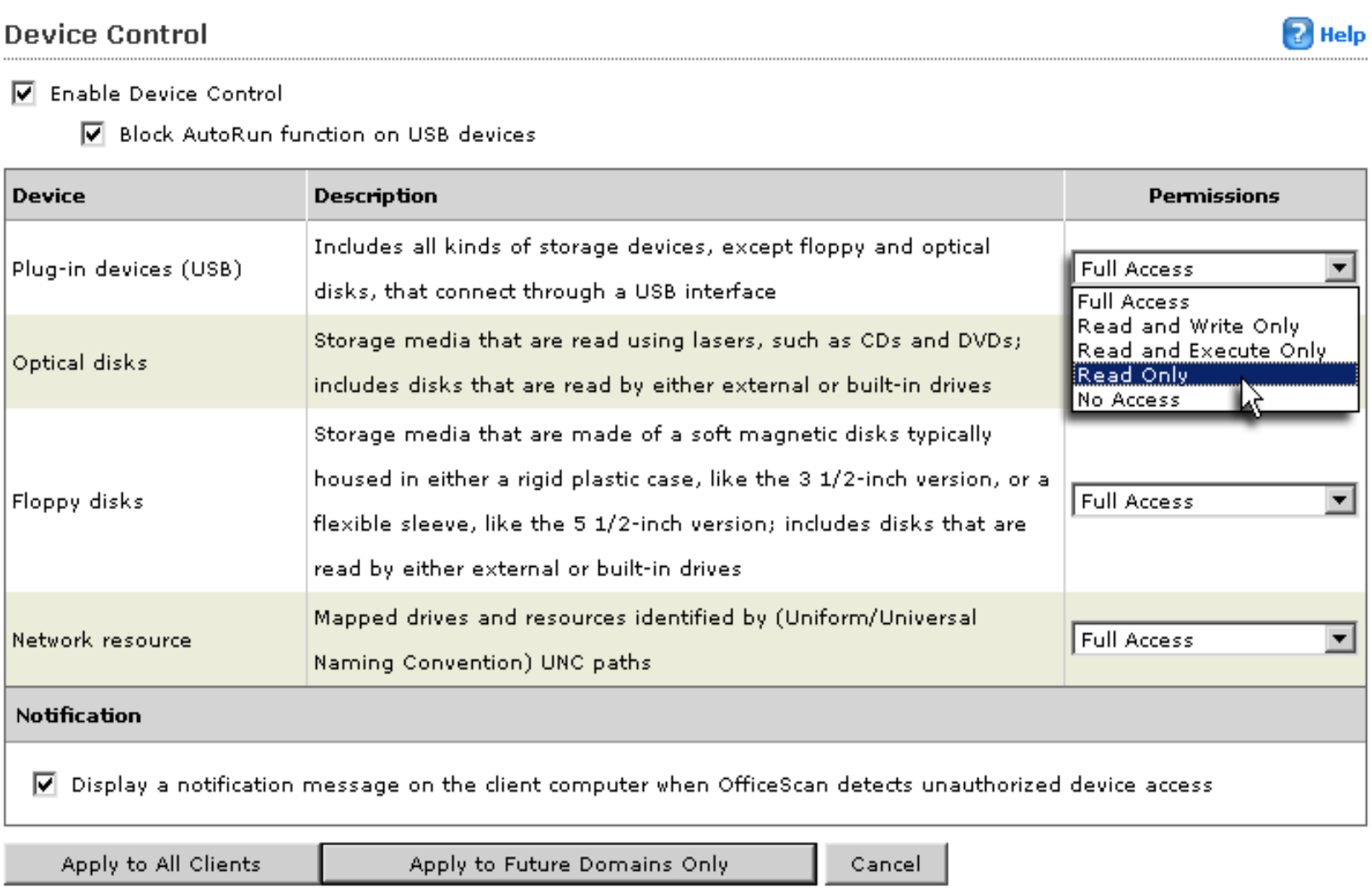
SmartScan vs. Conventional Scan

- Отказоустойчивость Smart Scan
  - Можно указывать больше одного сервера (при недоступности одного будут использоваться остальные
  - Можно указывать разные наборы серверов в зависимости от местоположения клиента
  - Roaming-клиенты могут использовать Smart Scan сервера в облаке Trend Micro (аналогично серверам ActiveUpdate)
  - Для репутационных запросов клиенты используют DNS
- Можно переключать клиентов между режимами в любой момент

Методика внедрения

- Предварительное тестирование
- Группа клиентов в пилотной зоне
- Интегрированный сервер Smart Scan может быть поднят на существующем сервере OSCE 10 без его переинсталляции
- Дополнительные серверы Smart Scan

Другие новшества



Виртуальные платформы

- Поддержка виртуализованных x86 и x64 Windows XP/2003/Vista/2008 на следующих платформах:
  - Microsoft Virtual Server 2005 R2 with Service Pack 1
  - VMware ESX/ESXi Server 3.5
  - VMware Server 1.0.3 or above
  - VMware Workstation and Workstation ACE Edition 6.0
  - Citrix Presentation Server version 4.5 (32-bit and 64-bit versions)
  - Microsoft Hyper-V (гости)
- Hyper-V сервер формально не поддерживается
  - Имеется методика (Solution ID 1054276)

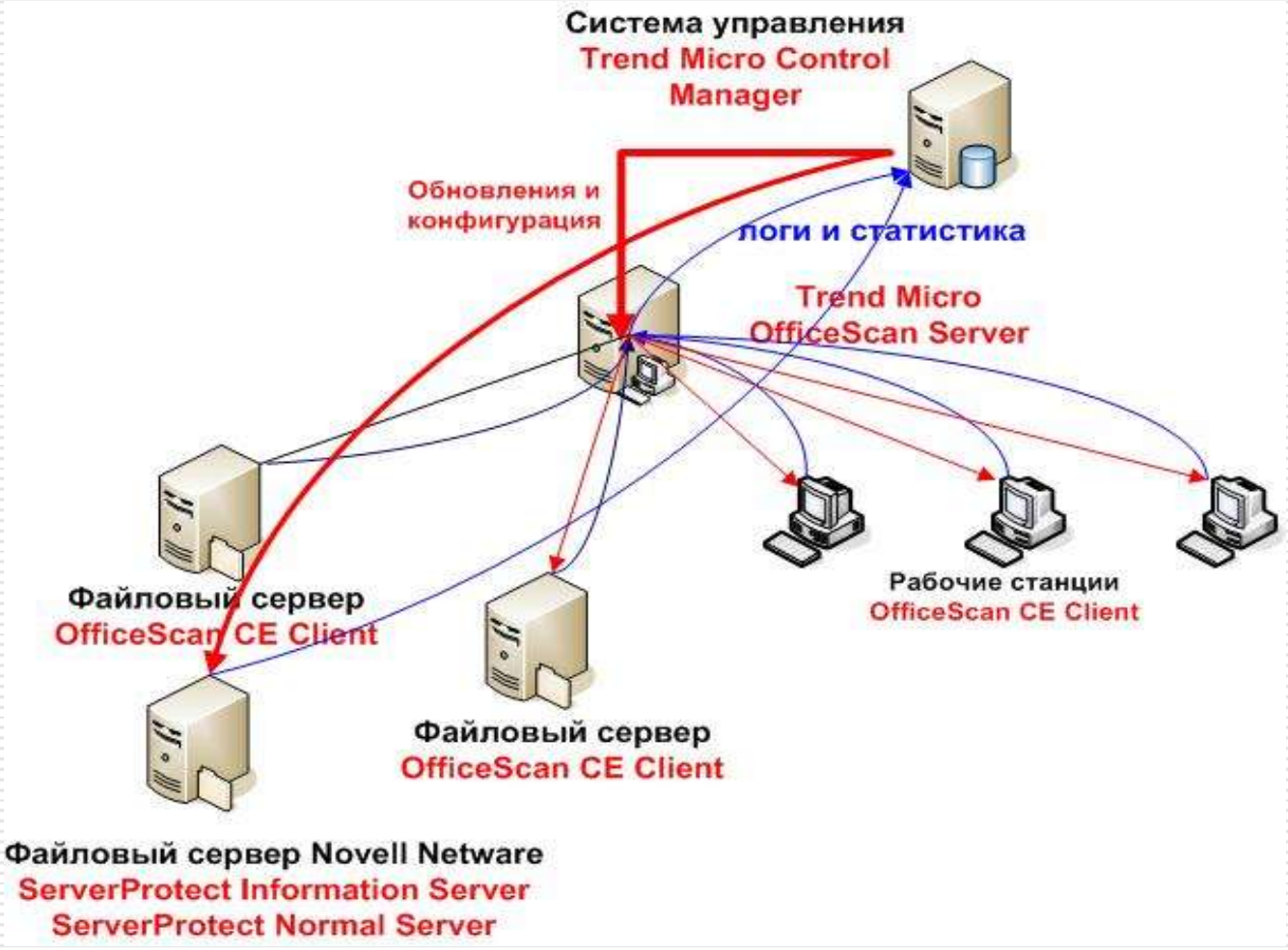
Еще о платформах

- Поддержка Windows 7 в OfficeScan 10 SP1
  - Процессор Intel™ Pentium™ или совместимый, 256 Мб ОЗУ, рекомендуется 512 Мб ОЗУ, 300 Мб свободного дискового пространства
  - ОС: Microsoft Windows 2000 SP4, XP SP2 или старше, 2003 SP1 или старше, Vista или SP1, Home Server, 2008, Microsoft Small Business Server (SBS) 2000, 2003
  - Microsoft Internet Explorer 5.0 или старше для веб-установки
- x86, x64, AMD64
- Поддержка Windows 95, 98, Me, NT4, и платформы IA64 прекращена в версии 8.0
  - В качестве workaround, виртуализовать старую (7.3) версию сервера

OfficeScan

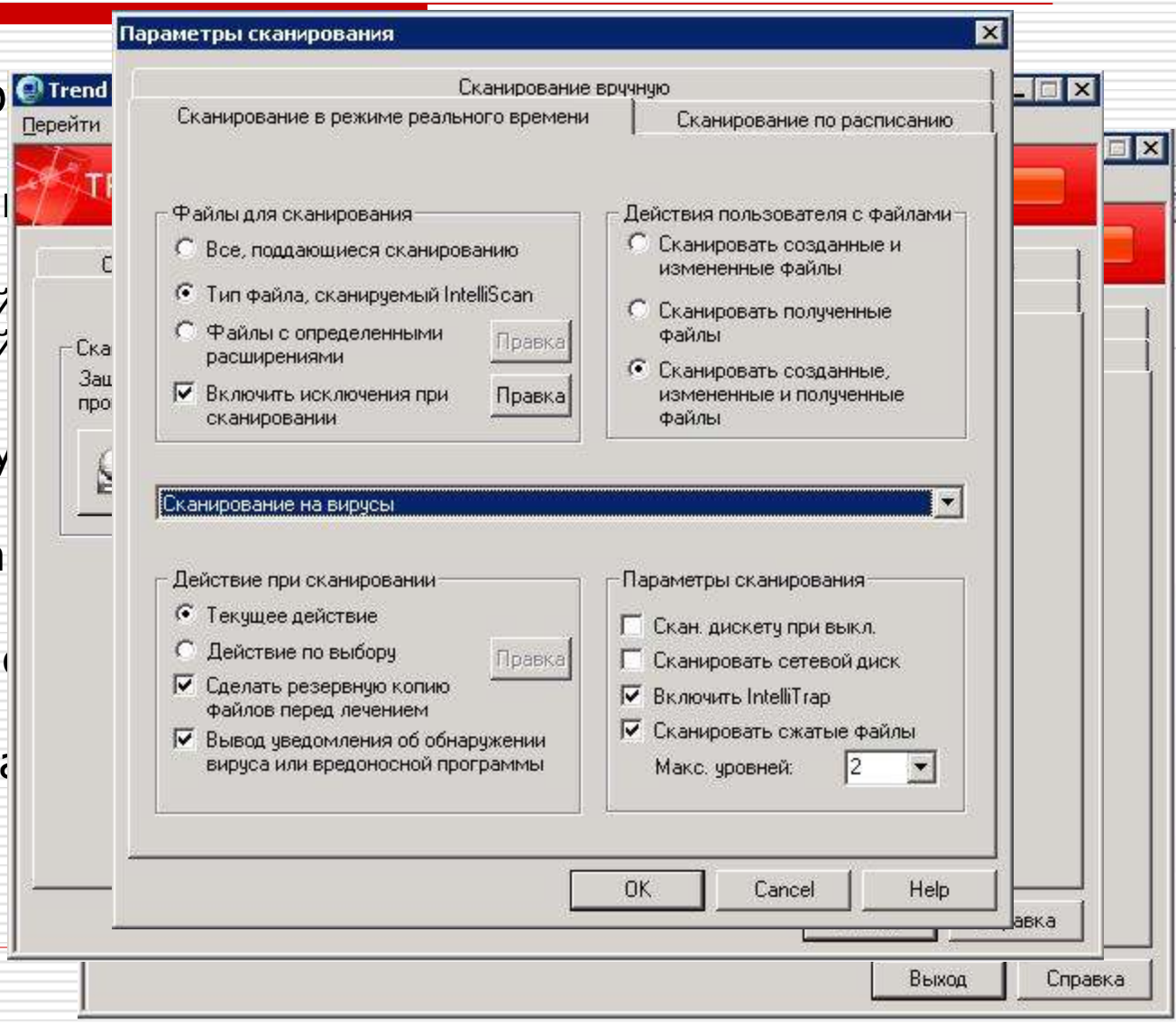
- Medium Business - OfficeScan™ Client/Server Edition
- Предприятия - OfficeScan Corporate Edition
- Клиент/серверная технология
- Сервер занимается только управлением
- Клиентский модуль антивирусной защиты
  - Унифицированный клиент для хоста Windows
  - Антивирус (Antivirus)
  - Антишпион (Anti-Spyware)
  - Защита от руткитов (Anti-Rootkit)
  - Брандмауэр, управляемый политиками

Защита с централизованным управлением

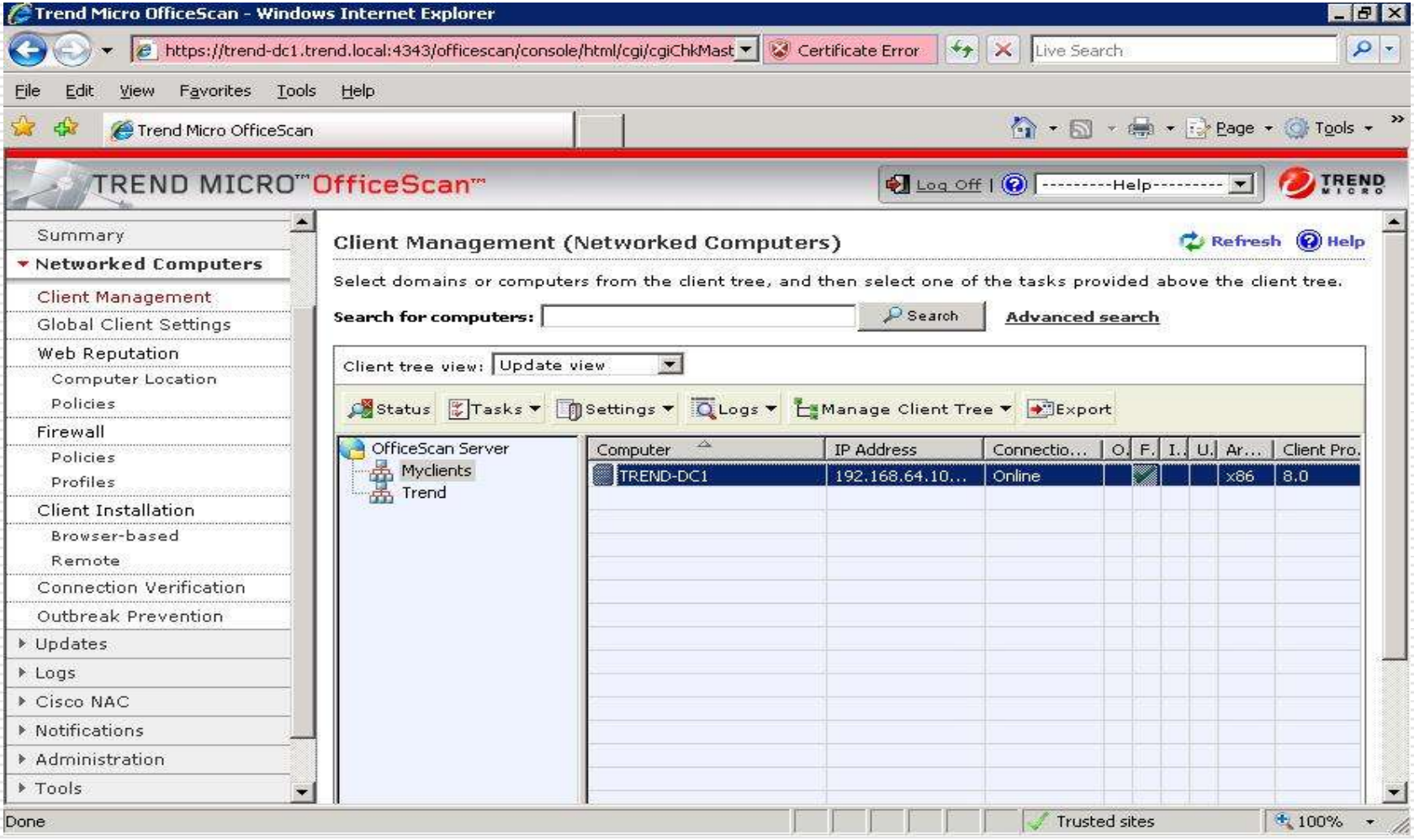


Рабочая станция пользователя

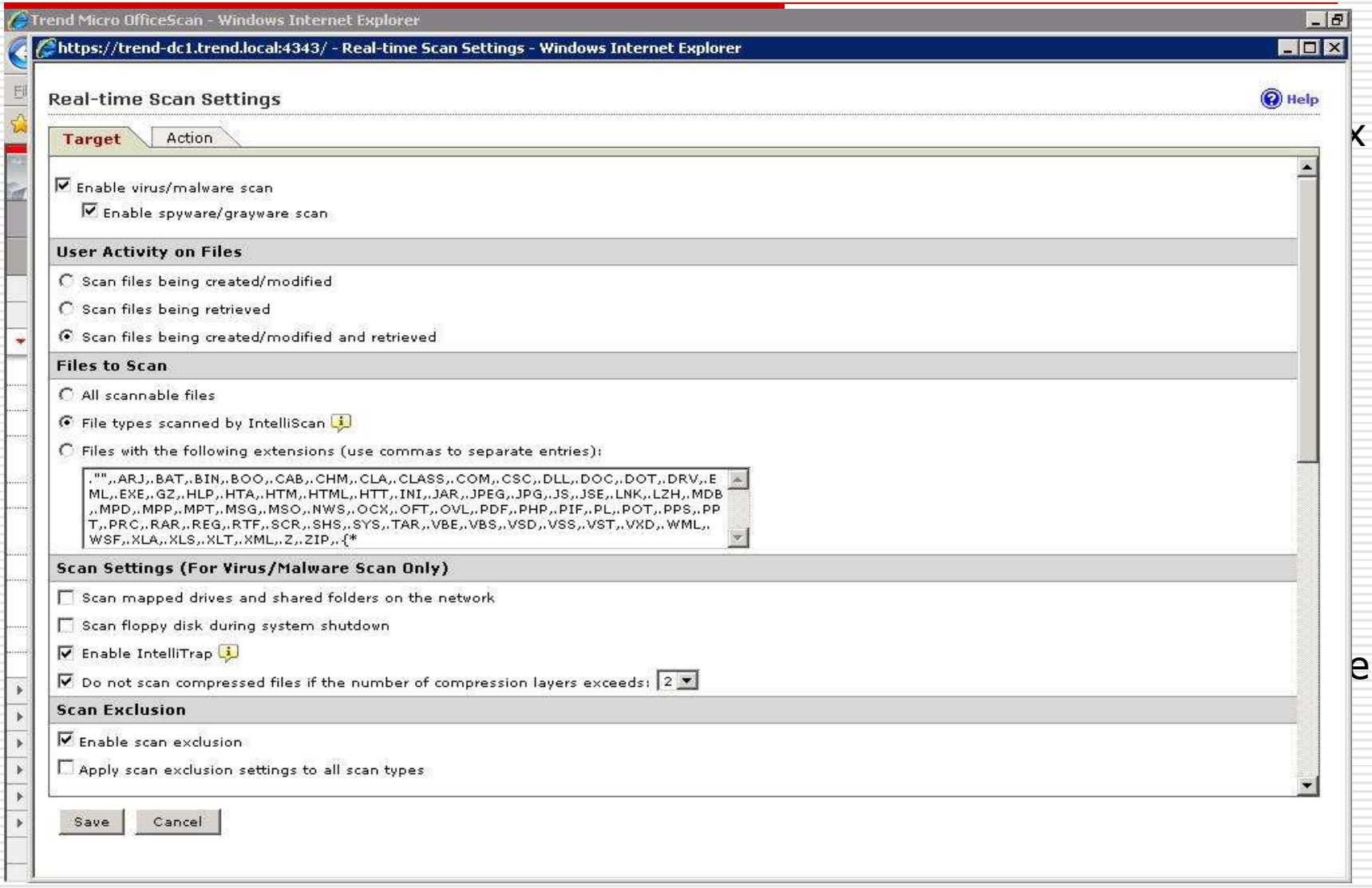
- Office Scan Corp
  - Стандартный
  - Антивирусный персональный
  - Защита от Spy
  - Damage Clean
  - Проверка папо
  - Автоматическа



OfficeScan Server

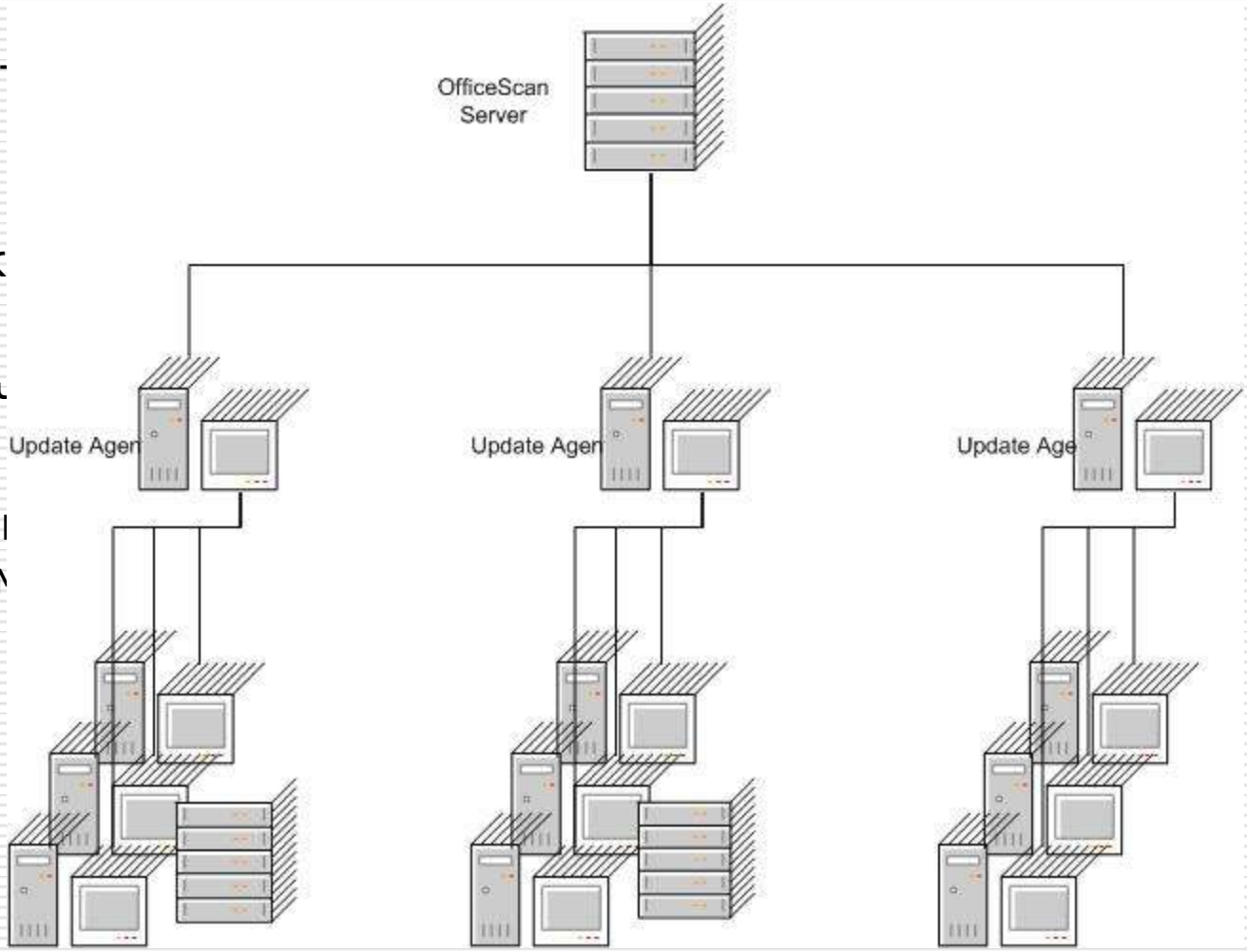


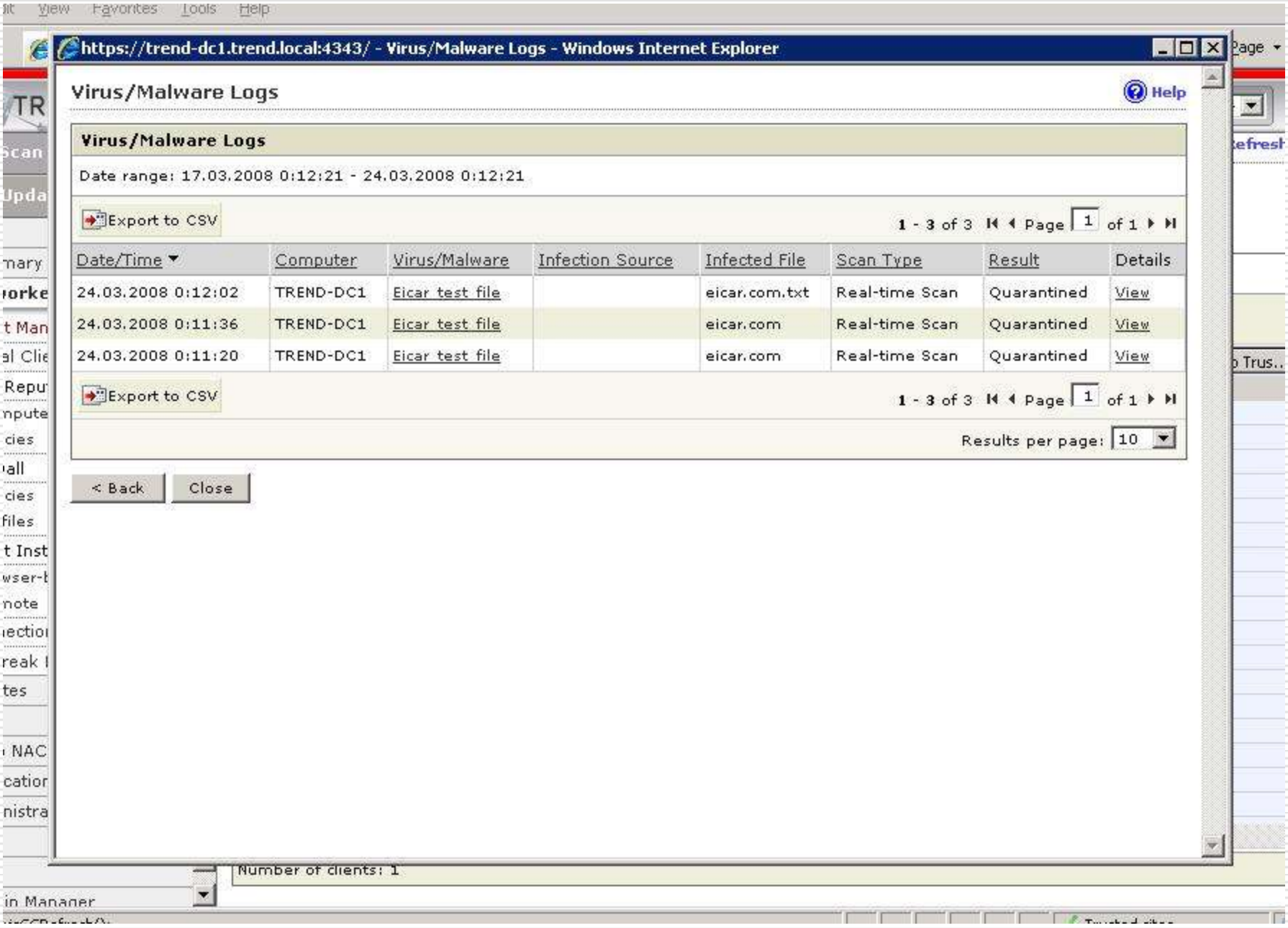
Настройки клиентов



Агенты обновления OfficeScan

- Работают
  требуют
- Разгрузк
- По умолч
- Предназ
  клиентам




https://trend-dc1.trend.local:4343/ - Virus/Malware Logs - Windows Internet Explorer
Virus/Malware Logs
Help
Virus/Malware Logs
Date range: 17.03.2008 0:12:21 - 24.03.2008 0:12:21
Export to CSV
1 - 3 of 3 Page 1 of 1
Date/Time | Computer | Virus/Malware | Infection Source | Infected File | Scan Type | Result | Details
24.03.2008 0:12:02 | TREND-DC1 | Eicar test file | | eicar.com.txt | Real-time Scan | Quarantined | View
24.03.2008 0:11:36 | TREND-DC1 | Eicar test file | | eicar.com | Real-time Scan | Quarantined | View
24.03.2008 0:11:20 | TREND-DC1 | Eicar test file | | eicar.com | Real-time Scan | Quarantined | View
Export to CSV
1 - 3 of 3 Page 1 of 1
Results per page: 10
< Back
Close
Number of clients: 1

OfficeScan Demo

Полезные ресурсы

www.trendmicro.com Trend Micro

www.antivirus.com

www.trendbeta.com

www.apl.ru Прикладная логистика

Support@polikom.ru Техподдержка Поликом Про

Контактная информация

195197, Санкт-Петербург,
Полюстровский пр., дом 59, литер Э
тел. 812 325-8400 факс : 812 320-5686

127018, Москва, Сущевский Вал ул., 16,
строение 3, офис 12
тел. 495 660-3291 факс : 495 660-3293

Антон Миносьян

aminosjan@polikom.ru