www.polikom.ru

Антивирусная защита виртуальной среды на базе Trend Micro Core Protection for Virtual Machines

Антон Рафаэлович Миносьян
Инженер отдела системной интеграции

03.06.2010

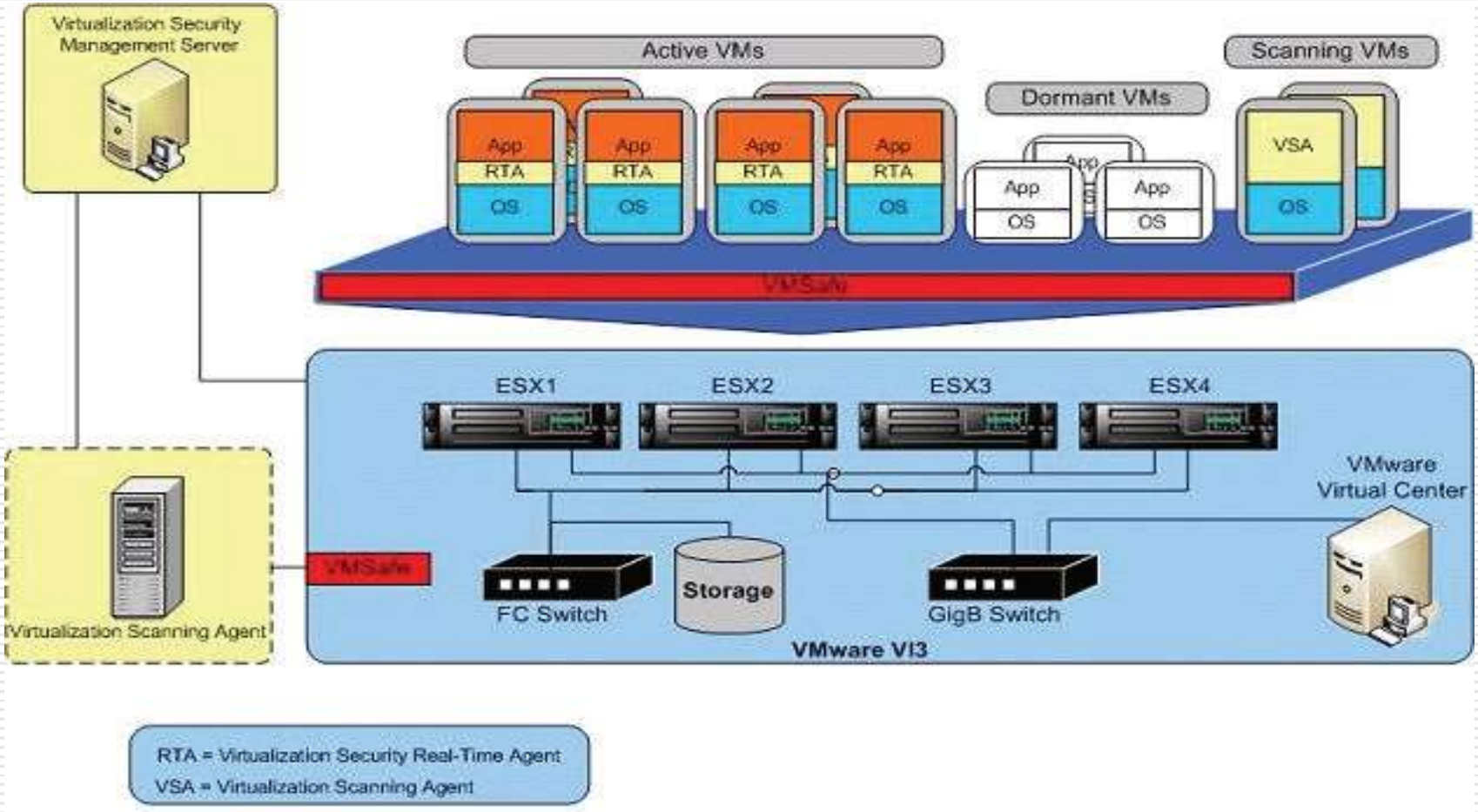
Core Protection for Virtual Machines

- Продукт для защиты гостевых систем под VMWare VI3 (ESX 3.5, ESXi, Vcenter 2.5) и vSphere 4.0 (ESXi 4.0/ESX 4.0 и vCenter 4)
- Использует API VMSafe
- Оптимизирован под виртуальную среду VMWare
- Способен защищать и обновлять выключенные и включенные VM
- Только традиционный метод сканирования
  - SmartScan в текущей версии не используется
  - Антивирусный движок настраивается как “классический” движок OfficeScan

Компоненты

- Модули CPVM
  - CPVM Server: физический хост. Управление и интеграция
  - CPVM Scanning Agent – сканирование по требованию включенных и выключенных (dormant) VM, физический хост или VM
  - CPVM Real-Time Agent – агент защиты в реальном времени, ставится на VM (хотя можно ставить и на физический хост)
- Интеграция
  - Сервер может брать обновления с OSCE и SPNT
  - Для администрирования из OSCE нужен плагин, доступный через интерфейс Plugin Manager

Пример развертывания



Security Management Server

- Физический хост - система управления
- Microsoft™ Windows™ Server 2003 x86 Enterprise SP1/SP2 или R2 SP1/SP2
- IIS 6, .NET Framework 2.0
- 800 МГц PII (2.4 МГц 4 рекомендуется)
- 512 Мб RAM (1 Гб рекомендуется)
- 1 Гб HDD (2 Гб рекомендуется)
- Администрируется через веб-консоль (IE6/7)

Scanning Agent

- Физическая или виртуальная машина
- Сканирование on Demand, в том числе отключенных (dormant) систем
- Windows XP Professional SP3 x86/x64
- Windows 2003 Enterprise SP2 x86/x64
- Windows Server 2008 Standard/Enterprise/Datacenter/Web Edition SP1 x86/x64
- Windows Server 2008 Standard/Enterprise/Datacenter/Web Edition R2 x64

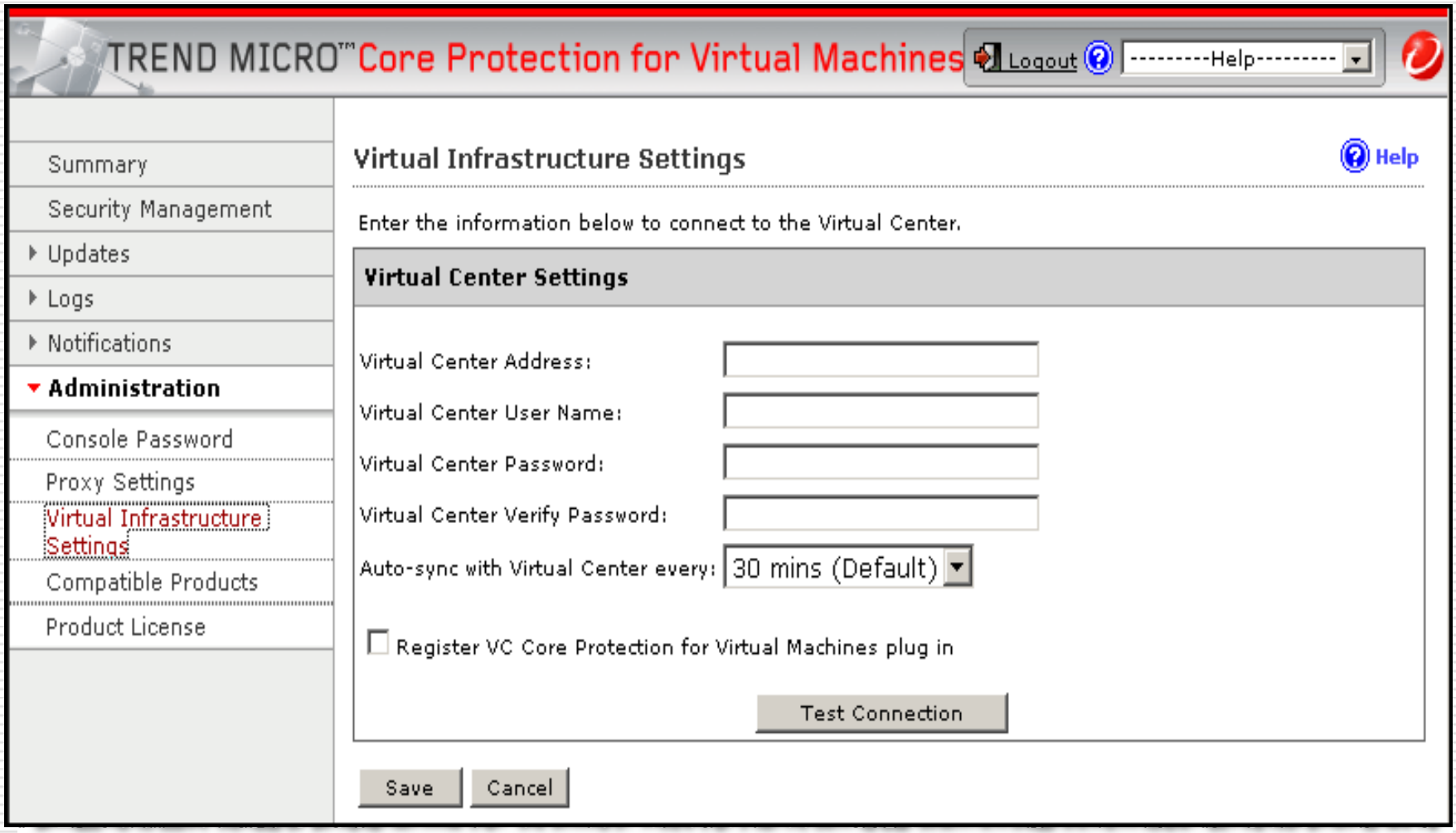
Real-Time Agent

- Виртуальная машина (в силу назначения)
- Сканирование в реальном времени
- Windows XP Professional SP3 x86/x64
- Windows 2000 Server/Advanced Server SP4
- Windows 2003 Enterprise SP2 x86/x64 и выше
- Windows Vista Ultimate SP1 и выше, x86/x64
- Windows Server 2008 Standard/Enterprise/Datacenter/Web Edition SP1 x86/x64 или R2 x64

Функциональность

- Сканирование в реальном времени, по требованию и по графику
- Знакомые технологии сканирования: паттерны, IntelliScan, OLE Layer Scan, обработка архивов, ActiveAction
- QuickScan – быстрое обследование ОС (по типу OSCE Prescan, только Dormant VM)
- Протоколирование событий в логах CPVM и оповещения (Email, SNMP, NT Event Log)
- Без брандмауэра (файрволл есть в Deep Security)

Примеры интерфейса



Применимость продукта

- Hyper-V не поддерживается
- Только Windows VM в текущей версии
- Использовать CPVM вместо OfficeScan для защиты виртуальных сред VMWare
- Связка CPVM + DeepSecurity для виртуальных сред в каком-то смысле эквивалентна связке OSCE + IDF
- В будущих версиях CPVM станет частью ПО DeepSecurity

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